



Збірник матеріалів

Світ телекомунікацій
та інформатизації

V Міжнародна науково-технічна
конференція студентства та молоді

07 грудня 2017 р.



Міжнародний союз електрозв'язку
Державний університет телекомунікацій
Студентська рада Державного
університету телекомунікацій
Наукове товариство студентів та аспірантів
Державного університету телекомунікацій



«СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЙ»

Збірник матеріалів

V Міжнародної науково-технічної конференції студентства та молоді

07 грудня 2017 р.

КИЇВ

«СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЙ»: матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій – Київ: ДУТ, 2017 – 448 с.

Збірник містить матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій «СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЙ». Пропонує статті та тези студентів й аспірантів, що висвітлюють перспективи розвитку інформаційних та телекомунікаційних технологій в Україні та світі.

Упорядники:

Бондаренко Євгеній Олександрович, голова Студентської ради Державного університету телекомунікацій.

Соснова Дана Назарівна, голова Студентської ради факультету телекомунікацій

Щетініна Анастасія Артурівна, голова Студентської ради факультету інформаційних технологій.

Перепелиця Ліна Сергіївна, голова Студентської ради Навчально-наукового інституту захисту інформації.

Лазоренко Анастасія Вячеславівна, голова Студентської ради Навчально-наукового менеджменту та підприємництва.

Відповідальність за грамотність, автентичність цитат, правильність фактів та посилань несуть автори матеріалів

ЗМІСТ

СЕКЦІЯ №1. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

<i>Koltsova A.</i> ORGANIZATION OF COMMUNICATION USING THE FEEDER ANTENNA .	12
<i>Bolotnyi M.</i> 4G IN CHINA.....	13
<i>Lebedynskyi M.</i> ADDITIONAL SERVICES - THE FUTURE OF TELECOMMUNICATIONS. QR CODES STEP TO MOVE ADDITIONAL SERVICES.	15
<i>Кольцова А.</i> РІФА АНТЕННИ И ИХ ПРИВЕЛЕГИИ	16
<i>Соснова Д.</i> РОЗУМНИЙ ІНТЕРНЕТ РЕЧЕЙ — ТЕХНОЛОГІЯ МАЙБУТНЬОГО	17
<i>Мацкевич В.</i> АВТОМАТІЧНА ТЕЛЕФОННА СТАНЦІЯ (АТС).....	21
<i>Мацкевич В.</i> АЛГОРИТМ СОЗДАНИЯ САЙТА. СОЗДАНИЕ ПРИ ПОМОЩИ DRUPAL.....	23
<i>Мацкевич В.</i> АДРЕСАЦИЯ В IP-СЕТЯХ.....	29
<i>Красноліцький В.</i> ГИПЕРТЕКСТ.....	31
<i>Красноліцький В.</i> ТЕХНОЛОГІЯ ІОТ	34
<i>Красноліцький В.</i> АРХІТЕКТУРА ETHERNET.	38
<i>Фурсович І.</i> VPN – ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА.....	40
<i>Гордєєва К.</i> ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ?	42
<i>Нагорна Л.</i> ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ	46
<i>Паламарчук В.</i> НАЙПРОСТІШИЙ СПОСІБ СТВОРЕННЯ САЙТІВ	51
<i>Прокопенко Д.</i> VSAT – СЕТЬ В САМЫХ ОТДАЛЕННЫХ ТОЧКАХ МИРА	53
<i>Соколов В.</i> ИСПОЛЬЗОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ И ПОИСКА АВТОМОБИЛЕЙ	54
<i>Стаднік Д.</i> ЗАСТОСУВАННЯ ІНФОРМАТИКИ В ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ.....	57
<i>Панченко В.</i> ГАЛУЗЬ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ.....	63
<i>Пікуль А.</i> БИОМЕХАНИЧЕСКИЕ ПРОТЕЗЫ.....	65
<i>Калінін Д.</i> ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ.....	67
<i>Бондарьков Є.</i> ЗАЩИТА ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ОТ «КРИПТОМАЙНЕРА»	69
<i>Король-Королевський К.</i> ГОТОВНІСТЬ СВІТУ ДО БЕЗКОНТАКТНОЇ ОПЛАТИ	70
<i>Свірідов Д.</i> РОБОТ – ПЕРВЫЙ ПОМОЩНИК ЧЕЛОВЕКА.....	71
<i>Михайловський А.</i> ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПРОВОДНЫХ СЕТЕЙ РЕГИОНАЛЬНОГО УРОВНЯ	74
<i>Щербина А.</i> СМАРТФОНИ МАЙБУТНЬОГО	77
<i>Лукандій П.</i> ПЕРСПЕКТИВИ ПОЯВИ 5G В УКРЇНІ	79

Жук В. ТЕХНОЛОГИЯ NFC	82
Лозов С. ДОСЛІДЖЕННЯ МЕТОДІВ ОРГАНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ ТЕЛЕВІЗІЙНОГО КАНАЛУ	83
Горохов О. БЕЗДРОТОВІ ЗАСОБИ ЗВ'ЯЗКУ	85
Виговський О. СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ	87
Замша О. КАК «ВИТАЯ ПАРА» ОКУТАЛА МИР?.....	90
Бочко М. ДЕТЕРМИНИРОВАННЫЕ ОДНОФОТОННЫЕ ИСТОЧНИКИ В ДВУМЕРНЫХ ПОЛУПРОВОДНИКАХ	92
Гомзяк Я. MULTIPROTOCOL LABEL SWITCHING	93
Димарчук Д. ЗАХИСТ РОУТЕРА ВІД ЗЛОМУ	95
Андрієнко О. ПЕРСПЕКТИВНІ ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.....	102
Недопако А. АТАКИ С ПРИМЕНЕНИЕМ СНИФФЕРОВ.....	104
Скнар І. ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ	105
Говгаленко М. АНАЛІЗ ТЕХНОЛОГІЇ ДЛЯ M2M МЕРЕЖ З ВЕЛИКОЮ ПЛОЩЕЮ ПОКРИТТЯ.....	107
Карагманова Ю. СИСТЕМА ЗВ'ЯЗКУ END-TO-END.....	109
Поливода Є. АНАЛІЗ ВИМОГ ДО ВИМІРЮВАЛЬНОЇ СИСТЕМИ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ	111
Демченко О. CONTENT MANAGEMENT SYSTEM.....	113
Данилюк В. ЗАГАЛЬНЕ ПРО БЕЗДРОТОВІ МЕРЕЖІ	116
Пономаренко О. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ.....	118
Панченко В. ЗАХИСТ У МЕРЕЖАХ WI-FI	121
Ніколаєнко В. ІННОВАЦІЙНІ МЕТОДИ КРИПТОГРАФІЇ НА ПРИКЛАДІ МЕСЕНДЖЕРА TELEGRAM	123
Димарчук Д. ТЕХНОЛОГІЯ REDTASTON	125
Димарчук Д. ТЕХНОЛОГІЇ ІР ПЕРЕДАЧІ ДАНИХ У СУЧАСНОМУ ТЕЛЕЦЕНТРІ	126
Гомзяк Я. ТЕХНОЛОГІЯ DPI.....	131
Кращенко Д. МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ	133
Гомзяк Я. ТЕХНОЛОГІЯ OLAP	134
Вовков В. 3D ІНТЕРНЕТ. КОРИСТЬ І ПЕРСПЕКТИВИ ЙОГО РОЗВИТКУ	136

СЕКЦІЯ №2.СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Koltsova A. SUGGESTIONS TO IMPROVE THE SET TECHNOLOGY IN UKRAINE	138
Koltsova A. QR-CODE AND ICT APPLICATION	140
Bondarenko Y. ENGINEERING TRUCK PREDICTIVE MAINTENANCE SOLUTION	141
Lavryck N. INFORMATION AND COMMUNICATIONS TECHNOLOGY	142
Semenov V. QR CODES IN CHINA, WHICH WE CAN USED IN UKRAINE	144
Horbacheva H. USING QR- CODES INSTEAD CASH IN OUR LIFE.....	145
Gvozdetska N. HOW TO IMPROVE ICT IN UKRAINE	146
Nikolaychuk D. HOW TO IMPROVE THE ICT TECHNOLOGY IN UKRAINE	148
Rohovyi D. CYCLES, WHICH PLACED ON THE STREETS.....	149
Мищенко В.К. ШУМИ И НЕЛИН АЛГОРИТМІЗАЦІЯ ЯК ОСНОВА ПРОГРАМУВАННЯ	151
Крам О.В. ДОСЛІДЖЕННЯ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЕКТУВАННЯ «РОЗУМНОЇ ТЕПЛИЦІ» НА БАЗІ МІКРОКОНТРОЛЛЕРІВ ARDUINO	156
Логвиненко А.С. ДОСЛІДЖЕННЯ ПОБУДОВИ СЕНСОРНИХ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЙ ZIGBEE	157
Квідкус І.А. РОЗВИТОК WLAN	157
Рубанка Р.С. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ RAKE, ЯК МЕТОДУ БОРОТЬБИ З БАГАТОПРОМЕНЕВИМ РОЗПОВСЮДЖЕННЯМ СИГНАЛУ В СИСТЕМАХ МОБІЛЬНОГО	158
Скаба С. INTERNET OF THINGS. ВАРІАНТИ ПІДКЛЮСЧЕННЯ IOT.....	160
Охременко В. ІННОВАЦІЙНИЙ ВНЕСОК 3G0.....	162
Бердник І.І. АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ БЕЗПРОВОДНИХ МЕРЕЖ ЗВ'ЯЗКУ	162
Бондаренко М.С. ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПОДІЛУ РАДІОРЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ З М2М- ТРАФІКОМ.....	164
Сагайдак В.А. БОТИЗАЦІЯ ІНФОКОММУНІКАЦІОННИХ СЕТЕЙ	165
Скаба С. ЯК ТЕХНОЛОГІЇ IP/MPLS ЗМІНЮЄ СВІТ?.....	167
Зайка М. СУЧАСНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ.....	169
Заріцька О.М. ПРИНЦИПИ ПОБУДОВИ ГЛОБАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	170
Золотухіна О.А.Бученко І.А. ВИКОРИСТАННЯ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ ЗАДАЧ АВТОМАТИЗАЦІЇ ОСВІТНІХ ПРОЦЕСІВ В СЕРЕДНІХ НАВЧАЛЬНИХ ЗАКЛАДАХ	172
Борисенко М.Б. ІВМ В ОБЛАСТІ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ.....	172
Кононенко В.В. ПЕРСПЕКТИВИ ВРОВАЖДЕННЯ IOT-РІШЕНЬ НА БАЗІ СТИЛЬНИКОВИХ МЕРЕЖ.....	175

Кузьменко М.М. КАК ПОСТРОИТЬ КАРЬЕРУ В IT	178
Кузьмич О.В. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ	178
Кравцова М.О. НОВІ СТАНДАРТИ WI-FI МЕРЕЖ	181
Мироненко С.М. МУЛЬТИМЕДІЙНІ ТЕХНОЛОГІЇ	182
Михайлюк В.В. ОЦІНКА ЯКОСТІ ПОСЛУГИ ФІЗІОЛОГІЧНОГО МОНІТОРИНГУ	185
Міщенко В.К. ТЕХНОЛОГІЇ РІВНЯ ДОСТУПУ МЕРЕЖІ NGN	187
Овчаренко М.С. ДОЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ЦЕНТРІВ ОБРОБКИ ДАННИХ, ЩО НАДАЮТЬ ІНФОРМАЦІЙНІ ПОСЛУГИ	189
Остапенко Г.А. КОНЦЕПЦІЯ «ПРИНЕСИ СВІЙ ВЛАСНИЙ ПРИСТРІЙ»	190
Пархоменко Є. ГЛОБАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ	191
Савіцький В. ДОБРО ПОЖАЛОВАТЬ В SWIFT	199
Соколовський Я.В. НЕЙРОННЫЕ СЕТИ	200
Солопова Д.О. НОВЫЕ ВОЗМОЖНОСТИ IBM DB2 EXPRESS 11.1	203
Ставицькая Ю.В. УСПЕХ ВНЕДРЕНИЯ СОВРЕМЕННЫХ ИТ В СТРОИТЕЛЬНЫХ КОМПАНИЯХ	204
Трембовецький М.П., Поливода Є.Г. ДОСЛІДЖЕННЯ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СИСТЕМ МОНІТОРИНГУ МЕРЕЖ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ	206
Черевик В.М. Батіщев С.О. АНАЛІЗ ІСНУЮЧИХ СТРАТЕГІЙ РЕЗЕРВУВАННЯ	207
Бондаренко І.І. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРОГРАМНО КОНФІГУРОВАНІХ МЕРЕЖ ТА ВІРТУАЛІЗАЦІЇ МЕРЕЖЕВИХ ФУНКЦІЙ	208
Курочкіна М.Г. БЛОКЧЕЙНИ – НОВІТНЯ ТЕХНОЛОГІЯ КРИПТОГРАФІЇ В ЦИФРОВОМУ СВІТІ	209
Криворот І.А. ДОСЛІДЖЕННЯ МОДЕЛІ ВЗАЄМОДІЇ ВЗАЄМОДІЇ ІНТЕРНЕТРЕЧЕЙ З ДОПОВНЕНОЮ ТА ВІРТУАЛЬНОЮ РЕАЛЬНОСТЮ	212
Яновський Д.А. ТЕЗИ НАУКОВО-ДОСЛІДНИЦЬКОЇ РОБОТИ «ТРИГОНОМЕТРИЧНА ПІДСТАНОВКА В АЛГЕБРІ»	214
Ковтуненко В.О. ДОСЛІДЖЕННЯ МЕТОДІВ ПЛАНУВАННЯ ТА ОПТИМІЗАЦІЇ СИСТЕМ АБОНЕНТСЬКОГО РАДІОДОСТУПУ НА БАЗІ ТЕХНОЛОГІЙ LTE	215
Живаго К.В. ІОТ	216
Бондаренко М. ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПОДІЛУ РАДІОРЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ З M2M-ТРАФІКОМ	218
Тимошук А.О. ЕРА КОГНІТИВНИХ ТЕХНОЛОГІЙ РАЗОМ ІЗ IBM WATSON	219
Урсол Т. ПОРІВНЯННЯ РІВНОМІРНОСТІ РОЗПОДІЛУ ПОСЛІДОВНОСТЕЙ ВИПАДКОВИХ ЧИСЕЛ ТАБЛИЧНИХ ГПВЧ ТА ЛЮДСЬКИХ РЕСУРСІВ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ R	221
Єкімов В. ЧИМ ВІДРІЗНЯЄТЬСЯ WI-FI ВІД WIMAX	224
Шкаруба М.О. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ	227
Щетініна Д.А. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АВТОМАТИЗАЦІЇ ОФІСУ	228

<i>Щетініна А.А.</i> ДСУЧАСНІ ТЕХНОЛОГІЇ WI-FI ТА LI-FI.....	229
<i>Міщенко В.</i> ЩО ТАКЕ ЦОД?.....	230
<i>Бурліцька А.І.</i> АРХІТЕКТУРА БЕЗДРОВОВОЇ МЕРЕЖІ НА БАЗІ СТАНДАРТУ 802.11	232
<i>Криворот І.А.</i> ДОСЛІДЖЕННЯ МОДЕЛІ ВЗАЄМОДІЇ ІНТЕРНЕТ РЕЧЕЙ З ДОПОВНЕНОЮ ТА ВІРТУАЛЬНОЮ РЕАЛЬНОСТЮ	233

СЕКЦІЯ №3. БЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.

<i>Перепелиця Л.С.</i> ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.....	236
<i>Бойко А.А.</i> ТЕСТ НА ПРОНИКНОВЕНИЕ.....	238
<i>Кононенко І.О.</i> SSL СЕРТИФИКАТ	240
<i>Коваленко Е.В.</i> КРИПТОГРАФИЯ: БАЗОВІ ЗНАННЯ О НАУКЕ ШИФРОВАНИЯ	244
<i>Мисевич К.С.</i> SYN Flood. SPOOFING	247
<i>Седлецький Д.В.</i> СІМ СЕКРЕТІВ НАСТУПАЛЬНОЇ КІБЕРБЕЗПЕКИ	248
<i>Чабан Б.В.</i> ЕТАЛОННА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ МЕРЕЖ ТА СИСТЕМ....	250
<i>Світін О.С.</i> ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ ТА ПРОБЛЕМИ ЇЇ РОЗВИТКУ	252
<i>Світін О.С.</i> КОНЦЕПЦІЯ ТА АРХІТЕКТУРА ЗАХИСТУ ІНФОРМАЦІЇ.....	254
<i>Світін О.С.</i> КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ	257
<i>Веселков Н.Л.</i> ЭЛЕКТРОННАЯ ПОДПИСЬ И СТАНДАРТЫ ЕЕ ПРИМЕНЕНИЯ В УКРАИНЕ	259
<i>Кравцов О.А.</i> ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ PORT-KINOKING ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕКИ СЕРВІСУ	260
<i>Мальгина Е.В.</i> КАК ЗАЩИТИТЬСЯ ОТ КИБЕРАТАКИ	262
<i>Щебланін А.Ю.</i> ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	264
<i>Хапун А.В.</i> ПЕСИМІЗАЦІЯ. ЩО ТАКЕ І ЯК УНИКНУТИ?.....	266
<i>Вовк Н.І.</i> РОЛЬ І МІСЦЕ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ...	268
<i>Добреля В.А.</i> МЕЖСАЙТОВИЙ СКРИТПИНГ	270
<i>Шевчук Я.А., Марченко В.В.</i> ЗАХИСТ БАНКІВСЬКОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ.....	273
<i>Сокол А.В.</i> МОДЕЛЬ OSI.....	275
<i>Дереча Н.А.</i> КІБЕРБЕЗПЕКА-ПРОБЛЕМА СТОЛІТТЯ	281
<i>Хоменко Т.А.</i> ЦЕНТРИ СЕРТИФІКАЦІЇ. ПРОТОКОЛ SSL	283

Марченко В.В., Шевчук Я.А. ЗАХИСТ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ	285
Кукишин Д.В. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ	287
Перепелиця Л.С. КІБЕРБЕЗПЕКА, ЇЇ СТРУКТУРА ТА РОЗВИТОК В УКРАЇНІ ТА СВІТІ.....	291
Вовк Н.І. СИСТЕМА «РОЗУМНИЙ БУДИНОК»: ВИСОКОІНТЕЛЕКТУАЛЬНЕ ЖИТЛО.....	293
Кисіль В.А. ВІРУС ШИФРУВАЛЬНИК ЯК ОДИН З ВИДІВ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	296
Вовк Н.І. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОРГАНІЗАЦІЙНОЇ КУЛЬТУРИ	297
Бердник О.В. ІНТЕРНЕТ РЕЧЕЙ, ЯК ОСНОВНА СУЧАСНА УРАЗЛИВІСТЬ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРИСТУВАЧІВ	300
Дорохін О.О. РОЗВІДКА УРАЗЛИВОСТЕЙ ЯК ПЕРШИЙ ЕТАП КІБЕРАТАКИ	302
Семенова І.Д. ЕТАПИ РЕАЛІЗВЦІЇ АТАКИ.....	306
Пояркін І.С. ОСНОВНІ МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ	310
Протасенко К.К. КАДРОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В УКРАЇНІ	315
Починок М.О. РОЗВИТОК СИТЕМИ BLOCKCHAIN В УКРАЇНІ	320
Загиней А.Ю. ЗВІДКИ ДІЙСНО ПРОХОДИТЬ КІБЕРЗЛОЧИННІСТЬ?	323
Кушнір Д. HOW CYBERSECURITY SOLUTIONS CAN HELP WITH GDPR COMPLIANCE	326
Ліщук І. РОЗБІР УРАЗЛИВОСТЕЙ, МОЖЛИВІСТЬ РЕАЛІЗАЦІЇ АТАК	328
Рыжков Д.О. РОЛЬ СМІ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ КИБЕРВОЙНАХ	330
Шумлянська А. ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ. КЛАСИФІКАЦІЯ, СТАТИСТИКА	333
Шумлянська А. МОДЕЛІ ПОРУШНИКІВ	334
Приходько В.О. КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ І ОБ'ЄТИ КОМП'ЮТЕРНОЇ СИСТЕМИ	336
Чабан Б.В. ПЛАНУВАННЯ ЗАХИСТУ І КЕРУВАННЯ СИСТЕМОЮ ЗАХИСТУ	338
Головін В.Е. ФУНКЦІЇ І МЕХАГІЗМИ ЗАХИСТУ	339
Чабан Б.В. КОНЦЕПЦІЯ ДИСПЕТЧЕРА ДОСТУПУ	340
Хворостяний Р.В. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АС	341
Ахтьоров В.Ю ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕС УПРАВЛІННЯ СУСПІЛЬСТВОМ	342
Калініченко О.Г ДОКАЗОВИЙ ПІДХІД ДЛЧ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПРИКЛАДИ ПОЄДНАННЯ ФУНКЦІЙ ІНФОРМАЦІЙНИХ ЗАГРОЗ	344

СЕКЦІЯ №4. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Мирошниченко Н. ТЕЛЕКОМУНІКАЦІЇ - МЕНЕДЖМЕНТ СОЦІАЛЬНО ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ	347
Мирошниченко Н. АНАЛІЗ МОДЕЛЕЙ УПРАВЛІННЯ РЕСУРСАМИ ТА НАВАНТАЖЕННЯМ КАНАЛІВ ПЕРЕДАЧІ В ТЕЛЕКОМУНІКАЦІЯХ.....	347
Лебедєва І. МЕНЕДЖМЕНТ В ТЕЛЕКОМУНІКАЦІЯХ.....	351
Марчук В. РОЛЬ, ПРОБЛЕМА ТА СТРАТЕГІЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ.....	353
Марчук В. СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ.....	356
Марчук В. СФЕРА ТЕЛЕКОМУНІКАЦІЙ: СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-ПОСЛУГ У СІЛЬСЬКИХ РЕГІОНАХ.....	358
Лазоренко А. ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ	364
Лазоренко А. СОЦІАЛЬНІ ПРОБЛЕМИ МОЛОДІ В ОБЛАСТІ ІНФОРМАТИЗАЦІЇ СИСТЕМИ ОСВІТИ УКРАЇНИ.....	368
Лазоренко А. АКТУАЛЬНІ ПРОБЛЕМИ СТРАТЕГІЇ ЕКОНОМІЧНОГО І СОЦІАЛЬНОГО РОЗВИТКУ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ	370
Смутьська В. ШЛЯХИ ВДОСКОНАЛЕННЯ РЕГУЛЮВАННЯ ТА АКТИВІЗАЦІЇ ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ ...	372
Смутьська В. РОЛЬ ТА ПРОБЛЕМИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ	374
Смутьська В. ДИНАМІКА ТЕЛЕКОМУНІКАЦІЙНОГО РИНКУ УКРАЇНИ.....	376
Токмина Т. ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ	377
Токмина Т. ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОСПРОМОЖНОСТІ.....	379
Шорон П. ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ	381
Мізін О. СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ.....	382
Мізін О. СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ, ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 5G	384
Мізін О. СОЦІАЛЬНО - ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ	386
Трубій І. РОЛЬ І ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ	388
Трубій І. СТРАТЕГІЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ	389

Трубі́й І. ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОЗДАТНОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ ГАЛУЗІ В УКРАЇНІ	391
Козій К. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ	393
Сафін К. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ.....	395
Харакоз М. СОЦІАЛЬНО-ЕКОНОМІЧЕСКИЕ ПРОБЛЕМИ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИЙ.....	398
Пилипей А. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ.....	399
Полєха А. ВПЛИВ ІТ СИСТЕМ НА ЕКОНОМІКУ УКРАЇНИ.....	402
Мирошниченко Н. ПРО СХВАЛЕННЯ КОНЦЕПЦІЇ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ.....	405
Картамишева О. ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ	407
Картамишева О. ВПЛИВ РОЗШИРЕННЯ ЄВРОПЕЙСЬКОГО СОЮЗУ НА РОЗВИТОК УКРАЇНСЬКИХ ТЕЛЕКОМУНІКАЦІЙ.....	409
Картамишева О. РОЗВИТОК МЕРЕЖІ ІНТЕРНЕТ ТА ОНЛАЙН-РЕСУРСІВ В УКРАЇНІ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ.....	410
Гукасян А. СУЧАСНИЙ СТАН СИСТЕМ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ	416
Гукасян А. ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ, ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОЗДАТНОСТІ	417
Гукасян А. РОЗВИТОК ІНФОРМАЦІЙНИХ СИСТЕМ В МЕДИЧНИХ ЗАКЛАДАХ.....	424
Васильєва Ю. ГОСПІТАЛЬНІ ІНФОРМАЦІЙНІ СИСТЕМИ (ГІС).....	426
Васильєва Ю. ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОХОРОНІ ЗДОРОВ'Я УКРАЇНИ	429
Селіна Д. НЕДОСТАТНІЙ РЕГУЛЯРНИЙ ВПЛИВ ДЕРЖАВИ НА РИНОК ТЕЛЕКОМУНІКАЦІЙ.....	430
Григоренко О. ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ.....	432
Григоренко О. ЕЛЕКТРОННИЙ БІЗНЕС	434
Григоренко О. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-ПОСЛУГ У СІЛЬСЬКІЙ МІСЦЕВОСТІ.....	435
Козій К. РЕГУЛЮВАННЯ РИНКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ: МІЖНАРОДНИЙ ДОСВІД	436
Козій К. АКТУАЛІЗАЦІЯ МЕХАНІЗМІВ СПРИЯННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ.....	439

Шарій Т. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ.....	440
Шарій Т. ПЕРСПЕКТИВЫ РАЗВИТИЯ УКРАИНСКИХ ИТ-ПРЕДПРИЯТИЙ.....	443
Шарій Т. РОЗВИТОК СУЧАСНИХ ПОСЛУГ	445

СЕКЦІЯ №1. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Koltsova Anastasiia
National Mining University of Ukraine
Dnipro

ORGANIZATION OF COMMUNICATION USING THE FEEDER ANTENNA

Antenna Feeder System - a set of antenna and feeder path, included as part of an electronic product, a sample, a complex. Antenna Feeder System is used for signal transmission in radio communication systems, broadcasting, television, as well as other radio systems that use radio waves to transmit signals. The antenna function consists in the emission or reception of electromagnetic waves. The electrical connection of the antenna to the source (consumer) can be direct, and can be carried out using a transmission line equipped with radio frequency connectors, i. e. with the help of a feeder. The feeder function is in the transmission of the electromagnetic oscillation from the radio transmitter to the antenna input and the transmission of the electromagnetic oscillation from the antenna to the radio receiver.

The transmitting antenna converts the energy of the waves coming through the feeder from the transmitter to the antenna into the energy of free oscillations propagating in the surrounding space. The transmitting antenna should not simply radiate electromagnetic waves, but provide the most rational energy distribution in space. In connection with this, one of the main characteristics of transmitting antennas is the directional pattern - the dependence of the emitted field on the position of the observation point (the observation point should be in the far zone - at an invariably large distance from the antenna). Requirements for directivity range from very close to directional (broadcasting systems and terrestrial television) to a sharply defined direction in a certain direction (long-range space radio communication, radiolocation, radio astronomy, etc.). The directionality allows without increasing the transmitter power to increase the power of the field emitted in this direction, and also allows to reduce interference to neighboring radio systems, that is, contributes to the solution of the problem of electromagnetic compatibility. Directivity can be obtained only when the dimensions of the antenna significantly exceed the wavelength of the oscillations.

The receiving antenna catches the energy of free oscillations and turns it into energy of waves, which comes through the feeder to the input of the receiver. For receiving antennas, the radiation pattern is the dependence of the current in the antenna load, that is, ultimately at the receiver, or the emf induced at the receiver input, from the direction of arrival of the electromagnetic wave irradiating the antenna. The presence of directional properties at the receiving antennas allows not only to increase the power

released by the current in the load, but also substantially to weaken the reception of various kinds of interference, that is, improve the reception quality.

Any transmitting antenna can be used for reception of electromagnetic waves and generally speaking, on the contrary, however it does not follow from this that they are identical in design.

An important role in the operation of antenna devices is played by the transmission line (feeder), which transfers energy from the generator to the antenna (in the transmitting mode) or from the antenna to the receiver (in the receive mode).

The main requirements for the feeder are reduced to its electrical leakage (no radiation of energy from the feeder) and low thermal losses. In the transmit mode, the feeder impedance of the feeder must be matched to the input impedance of the antenna (which provides the traveling wave mode in the feeder) and with the transmitter output (for maximum power output). In receiving mode, the receiver's input is coordinated with the feeder's wave resistance in the latter mode of traveling wave. Harmonization of the wave resistance of the feeder with the load resistance is the condition for maximum power output to the load of the receiver. Depending on the radio wave band, various types of feeders are used: two or multi-wire air feeders, waveguides of rectangular, round or elliptical cross-sections, lines with a surface wave, and others.

The use of such a system is convenient in that the recoil coefficient is small. Such antennas can be of different sizes depending on the terrain, the conditions for transmitting information and the required range.

Thus, it can be disguised as ordinary items such as air conditioning, street lamps, alarms and so on. In Ukraine, such a system will improve the quality of information transmission, signal level anywhere in the city, reduce the amount of data loss and increase the number of points for Internet access.

In my opinion, the implementation of these technologies in Ukraine will be of great benefit to our society and will allow us to communicate 24 hours a day, regardless of the circumstances. That is: real-time, anywhere, social-to anyone.

Bolotnyi Maksym

Zaporozhye National Technical University

Zaporozhye

4G IN CHINA

I was very excited with the opportunity Huawei provided me recently. The trip to China sounded very exciting to me and I realized that it could become a great source of the creative ideas for me, when I come back to the home. Of course, I meant ICT ideas. Apparently, I was terrifically right.

Shenzhen has inspired me and now I know what I want to improve and implement in Ukraine after I graduate. The idea belongs to the Smart City niche and has a few necessary steps to be possible to happen.

First, the 4G era must start in Ukraine, if I want to proceed with the latest technologies. In Shenzhen, we have learned how to configure the eNodeB base station for the 4G consequences, by the way. Currently, the 4G is not available in Ukraine, which limits the internet speed to the last decade standards.

Secondly, as soon as the 4G implemented, I think it would be great to first make Kiev, which is the capital of Ukraine, the first smart city in Ukraine. "What exactly do you mean by smart city?" - would you ask me. Here is an example. In Shenzhen there are many cameras located all over the city, that are connect between each other and that are monitoring the current traffic situation and helps to avoid the overwhelming of it. I would like to have the same kind of technology in Ukraine, as Kiev is getting bigger and bigger and I fill as if it is something we need. On top of that, the AI can be built into the whole system, to minimize the human interaction to the system and help the AI decide, how to organize the infrastructure in the safest and time-effective way. I think that will significantly affect the way traffic goes nowadays and will secure all the drivers from any accidents that might happen on the road.

In addition, there are some other technologies that are already implement in Shenzhen and are related to those same cameras, which I would like to bring to Ukraine. They have the voice and the face recognition system built in to the Smart Solution. That allows indicating the potential danger within the huge flow of people, recognizing where the voice comes from, who is the person and then interacting accordingly to the situation, to prevent any kind of danger. It is also capable to recognize the face of the potential rubber that is trying to steal something, so that the operator that monitors it can immediately call the police to make sure they are going to catch the bad person. I do strongly believe that this technology can improve the level of the Ukrainian ICT we have now and make our capital a modern, secure and hi-tech city. Of course, I would like to extend it to other cities, once it works fine in Kiev.

To sum up, I have found a very interested technology here in Shenzhen that I think can bring the future to Ukraine and blow the market up. The system is based on smart cameras controlled by AI to organize and relief the traffic, reduce the rubbery over the city and improve the general secure. I hope a lot I will be given a chance to try myself in that specific niche after we come back from the Seeds to the Future program. The training has provided me with a lot of useful material that I am definitely going to use in the nearest future.

ADDITIONAL SERVICES - THE FUTURE OF TELECOMMUNICATIONS. QR CODES STEP TO MOVE ADDITIONAL SERVICES.

Huawei Ukraine offices gave me a mission to find what could be implemented in Ukraine in the IT area. Because there is only one technology to choose, there is a problem with choosing the best. When I flew to China, I saw many technologies that were not in Ukraine. Beijing is a high-tech city in which there are many innovations, for example bicycle rentals, QR code payments, a system to quickly react to incidents using cameras. However, Shenzhen was technological.

Ukraine is now actively developing IT sphere. Especially telecommunications. The Ukrainian operators understood - voice traffic had already reached its peak and it was time to move on to additional functions. Started tariffs directed not to voice, they directed to data transfer. This contributes to the development Internet of things. The Internet of things in turn allows for the emergence of smart things. These are smart devices, smart houses, smart cities, etc.

Fast and high-quality Internet access allows actively use encoded information. Such as QR codes. In QR codes, you can encode a message into a site to get information. You do not have to print a lot of brochures or ads anymore. You need only QR code that will link to the site with the brochure, and so on. In China, QR codes are used everywhere. For payment at the store, for bicycle rentals, and even for umbrellas. They are also use instead of descriptions in museums. You do not need to read the small text, just scan the code and the information will appear on your phone. QR codes will help reduce the how of redundant information. Help reduce how advertising and make the world more informative. You are interested in finding information like: what is the tree or what is the exhibit, you can scan QR code with the information. There is no need to make huge plaques with information, only a small code tag.

You can use QR code not only to get information about the exhibit or sightseeing, but also about paying, renting devices, and much more. If add QR codes to the Ukraine subway with link on a subway map and station information, it will greatly simplify the search for a path and possibly unload the flow of people in subway. QR codes with links to additional information can act as an additional service from the operator. This will increase the amount of information transferred. User's benefit it is obtaining the necessary information and saving time. You can also make statistics visits to other places that will allow tourists to visit the most interesting.

I saw too many technologies in China. Without telecommunications, technology would not have grown. It would not have been possible to obtain information quickly and qualitatively. You had to carry lots of cash, etc. With telecommunications and QR codes, the world becomes easier and more comfortable. If there is a widespread use of

coded information in Ukraine, there can be a significant improvement in human existence, reduction of how queues and reduction of how advertising.

Кольцова Анастасия
Национальный горный университет
Днепр

PIFA АНТЕННЫ И ИХ ПРИВЛЕГИИ **PIFA ANTENNA AND THEIR PRIVILEGES**

The article presents information on the main advantages of PIFA antennas and its possible variations with a description of their differences from the original model. The real values of the working frequency band and efficiency are also give, which are one of the most important parameters of any antennas.

В современном мире, часто используемом широко доступные гаджеты такие как GPS, мобильные телефоны, планшеты и тд – одним словом беспроводная техника, стоит вопрос о способах принятия сигнала. Используемая антенна обязана быть маленьких габаритов, иметь широкую полосу частот, поддержку многодиапазонности и высокую эффективность.

Таким примером является PIFA антенна. Ее полоса рабочих частот достигает до 10 % от резонансной несущей, эффективность достигает 65%, поддерживает многодиапазонность, маленькие габариты, а самым примечательным является то, что усиление достаточно высокое как в вертикальной, так и в горизонтальной плоскостях. Так же PIFA малочувствительна к иным элементам микросхемы, которые так же расположены на ней – это позволяет устранить помехи, которые могут повлиять на качество связи.

Возможность многодиапазонного излучения и приема позволяет произвольно ориентировать антенну в пространстве, что является огромным преимуществом для мобильных средств связи.

В работе Minh-Chau T. Huynh [1] подробно рассмотрено большое количество вариаций изготовления этой антенны и приведены расчеты. Из диаграмм направленности сразу видно, то при разных полосах рабочих частот, диаграмма направленностей не будет терпеть сильных изменений и имеет форму несколько измененной сплюснутой сферы.

В данные момент существует несколько разновидностей PIFA антенн:

- BIFA - пятидиапазонная антенна разработана Челмерским университетом (Швеция);
- PILA – антенна с фрезировкой в горизонтальной пластине L-образной прорези предложенная учеными Бирмингемского университета.
- WC-PIFA – антенна с расширенной полосой пропускания, запатентованная Minh-Chau T. Совместно с профессором колледжа Virginia Tech Antenna Group Вареном Статэманом [2]

В виду перечисленных выше разновидностей PIFA антенн, можно сказать, что каждая из них имеет свои преимущества и недостатки, но решение об их применении в электронике (беспроводных гаджетах) остается за корпорациями производящих эти устройства.

1. Minh-Chau T. Huynh. A Numerical and Experimental Investigation of Planar Inverted-F Antennas for Wireless Communication Applications. – In: Master Thesis of Science in Electrical Engineering. – Virginia Polytechnic Institute and State University. – Blacksburg, Virginia. – Oct. 19, 2000.
2. Слюсар В.И. Антенны PIFA для мобильных средств связи – ЭЛЕКТРОНИКА: НТБ, 2007

Соснова Дана Назарівна
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ

РОЗУМНИЙ ІНТЕРНЕТ РЕЧЕЙ — ТЕХНОЛОГІЯ МАЙБУТНЬОГО

Тренд інтернету речей зараз набирає велику популярність. Найчастіше поняття інтернету речей нерозривно пов'язане з чимось розумним: розумні будинки, розумний транспорт, розумні підприємства. Але коли дивилися на цю інтелектуальність уважніше, то часто розчаровуєшся: видалене управління лампочкою в будинку — це в кращому разі автоматизація, але ніяк не розумний будинок. Здається, що і інтернет виходить не таким вже і розумним. А що ж таке розумний інтернет речей?

Взагалі, історію інтернету можна розділити на 4-5 етапів, зараз ми знаходимося в епоху Інтернету речей (Internet of things, IOT). Коротко його можна описати так: збільшення кількості пристроїв, що взаємодіють не лише з користувачами, але і один з одним. Тобто кожна кавоварка має доступ в мережу — але для чого їй цей доступ потрібний, лише належить вирішити.

Поява інтернету речей — це досить очікуваний крок, адже лінь — двигун прогресу. Навіщо йти до телевізора для перемикання каналів, якщо можна придумати дистанційний пульт управління, навіщо натискувати кнопку на кавоварці, якщо можна зробити це в смартфоні або налаштувати правило, щоб кава наливалася сама. Чи зручно це? Що станеться, якщо людини немає удома або світло в налагоджений час йому не потрібне?

Будинок вийшов не «розумним», адже такий підхід слабо міняє ситуацію: людина як і раніше повинна все контролювати, він — центр управління всього. Виходить, це “всього лише” автоматизація. При цьому я прекрасно оцінюю потужність прогресу, яка до неї привела. Просто хочеться чогось більшого, потрібний “розумний” інтернет.

Що в моєму розумінні означає розумний інтернет речей? Це інтернет речей, який дозволить змінити парадигму досягнення результату: хочеться задавати цілі, а не способи їх досягнення.

Розумний інтернет речей — постійна підтримка людини предметами, які його оточують.

Розумний інтернет речей – це прозорість процесів, це орієнтація на результат.

Розумний інтернет речей – це говорити не як треба робити, а що повинне вийти.

Як цього досягти технічно?

По-перше, мультиагентні технології - вони вже усюди, і інтернет речей без них неможливий. Кожному учаснику з реального світу (тобто кожній людині і кожному пристрою) ставиться у відповідність програмний агент - об'єкт з певним ступенем інтелектуальності, що представляє його інтереси в світі віртуальному. Віртуальний світ можна назвати певною мірою поліпшеною копією нашого життя: там є ті ж учасники, які найчастіше йдуть заздалегідь встановленим і відомими правилами, надаючи достовірні відповіді на поставлені запитання, чесні і відкриті - альтруїсти, в загальному. При цьому взаємозв'язок реального та віртуального світів направлені у 2 напрямки: рішення з віртуального світу віддаються в реальність для виконання, а всі події реального світу (дуже часто непередбачені) відображаються на світі віртуальному.

Як живуть і працюють агенти?

Життєвий цикл агентів досить простий. Спочатку вони сприймають інформацію із зовнішнього світу. Потім її потрібно обробити, тобто запланувати якісь дії. Ну а дії вже потрібно виконати - віддавши відповідні команди в реальний світ.

Виходить, що в нашому "розумному" будинку агент людини постійно спілкується з агентами кавоварки, лампочок та інших холодильників - віддаючи їм команди і обмінюючись інформацією. Щось схоже ми бачимо в офлайн: припустимо, людина хоче запустити прання. Він завантажує речі в пральну машинку, хоче засипати порошок і розуміє, що його не вистачить для прання. Після чого йде в магазин, купує порошок і знову намагається запустити прання. Добре ще, якщо кондиціонер для білизни у нього є і в магазин більше йти не треба.

Тоді агент прального порошку попросить закупитися їм ще до того, як запаси будуть вичерпані. Як він попросить? Швидше за все, він потрапить в чергу до агента покупок і куплений буде саме тоді, коли у людини буде фізична можливість його принести - або навіть буде замовлена доставка, без участі людини. Чи зручно це? Так. Чи складно це? Теж так. Чи це можливо? І знову так.

Все це здається надто вже далеким майбутньому. Але згадаємо про таку чудової речі, як онтології. Це щодо універсальний і машинозчитуваний спосіб представлення знань, причому знання там можуть бути описані найрізноманітніші. В онтології ми можемо описати важливі для нас концепції, описати логічні правила - а наші інтелектуальні агенти використовувати ці знання для досягнення і взаємодії цілей.

Чи можна розробити одну універсальну онтологію, яка буде містити всі потрібні для розумного інтернету речей знання? Напевне так. Але яким повинен бути обсяг цієї онтології, страшно навіть уявити. Набагато більш простим

здається можливість підтримки онтологій предметних областей - і, при необхідності, матчінга між ними.

Виходить, що користувач може створити онтологію будинку, онтологію робочого простору - і дані, описані в них, повинні мати відповідність. При такому підході виходить, що у нас може бути і "розумний" офіс, і "розумний" будинок.

Онтологія для логіки роботи

Найбільш частий спосіб застосування онтологій - це лише спосіб зберігання знань, які жорстко структуровані. При цьому знання ці, як правило, говорять лише про якусь суті фізичного світу. А чому б не піти далі і не зберігати в онтологіях і правила взаємодії, логіку роботи розумного інтернету речей? На практиці це може виглядати так: при створенні агент дивиться на сутність, до якої він належить. Для коректного розуміння властивостей цієї сутності агент повинен звернутися до онтології - звідти він почерпне інформацію, що може робити ця сутність, які у неї потреби. А чи знає він, як досягти ці потреби, як застосувати її здібності? Ця інформація теж лежить в онтології! Розглянемо приклад - придбання кондиціонера. При підключенні кондиціонера в загальну мережу у нього з'являється програмний агент. Агент цей може знати про своє призначення. Тоді йому достатньо лише заявити про себе: «Я агент кондиціонера! Я можу охолоджувати! Я хочу витратити енергію! Я можу ламатися! Я хочу профілактику раз на рік! »

Ці повідомлення повинні отримати всі зацікавлені учасники - наприклад, агент будинку, який відповідає за споживання електрики. Далі ці два агента повинні будуть домовлятися про споживання енергії в будинку - інтернет речей повинен бути економним. При цьому агент кондиціонера може вплинути на інші процеси, які споживають енергію - у випадках, коли підтримка високої температури будинку має високий пріоритет.

Агент кондиціонера і сам може потребувати інформації. Наприклад, непогано було б враховувати поточну температуру за вікном і прогноз на день-два: тоді годі й охолоджувати будинок в спеку перед сильним похолоданням. Як можна отримати необхідні дані? Треба дізнатися з онтології, хто може їх надати.

Розумний інтернет речей - це тільки розумний будинок?

Всі приклади вище - про інтернет речей в побуті, про розумні будинки. Але це не єдина область застосування таких потужних технологій. Підприємства вже зараз виявляють велику зацікавленість до інтернету речей. Так, Airbus в своєму звіті про підприємства майбутнього бачить IoT однією з важливих технологій.

Спробуємо визначити, як інтернет речей може застосовуватися на сучасних підприємствах. На таких підприємствах, як правило, є безліч різних верстатів, безліч різних замовлень на виробництво продукції, безліч різних технологічних процесів. Взагалі, там багато всього різного. І, звичайно, в інтелектуальних системах інтернету речей цих підприємств буде безліч різних агентів. Всі ці агенти зобов'язані входити в єдиний інформаційний простір - тоді застосування інтернету речей дозволить показати більш високу ефективність. Розглянемо приклад - агент замовлення на виробництво продукції хоче, щоб його виконали.

Для цього йому треба знайти вільних робочих - і пошук треба починати саме зі свого цеху! А якщо в цеху вільних робочих немає, у всіх висока зайнятість, то логічно буде спробувати знайти цих людей десь ще. Щоб знайти вільну робочу силу з певними компетенціями, треба зрозуміти, а де взагалі її шукати. Для цього достатньо «лише» звернутися до онтології, яка підкаже, в якому цеху мешкають робочі з потрібними можливостями. А після відповіді вже починати спілкування з цими цехами і намагатися знайти працівників для виконання замовлення.

Інший приклад - це агент верстата, який сам стати проактивним і шукати собі роботу. Цьому агенту треба зрозуміти, які замовлення він може виконувати - для цього йому потрібна інформація про замовлення і технологічних процесах їх виконання. Якщо така інформація у нього вже є, то агент верстата може з онтології визначити, хто приймає рішення про планування цих замовлень - і намагатися переманити їх до себе. Як правило, рішення може приймати або сам замовлення, або менеджер цього замовлення - людина.

Варто відзначити, що в описаному інтелектуальному інтернеті речей людина є повноправним учасником всіх процесів - він постійно бачить актуальну інформацію, може вважати ціну виробленої продукції по-справжньому чесно. При цьому кінцеве слово в прийнятті рішень може залишатися за ним - але йому буде надана якісна підтримка для цього прийняття, а рішення буде повністю прозорим і гнучким.

Сетецентричний принцип

У 80-х роках минулого століття маршал Радянського Союзу Н.В. Огарков сформулював сетецентричний підхід щодо ведення бойових дії (а в США ці ідеї отримали розвиток завдяки віце-адміралу ВМС Артуру Себровскі і професора Джона Гартска). Відповідно до цього підходу всі ресурси, які здатні виконати завдання, повинні входити в одну інформаційну мережу і вміти обмінюватися інформацією для виконання цього завдання. Нічого не нагадує? Інтернет речей - це вкрай логічне застосування сетецентричного підходу, адже він використовує сучасні інформаційні технології для інтеграції розподілених елементів в глобальну систему, здатну до адаптації під мінливі умови зовнішнього світу.

Короткі висновки

Інтернету речей - бути, в цьому вже ніхто не сумнівається. Бути чи розумному інтернету речей - це велике питання, але хотілося б, щоб він був. Вплинути на цю ситуацію можуть компанії, які беруть участь в розробці ПЗ і заліза для інтернету речей. Яким я бачу цей вплив? Хочеться, щоб були єдині і чіткі стандарти, які будуть застосовні по всюди. Хочеться, щоб було єдине і виразне розуміння, яким має бути інтернет речей. Хочеться, щоб цей розумний інтернет речей з'явився якомога швидше.

Література:

1. <https://habrahabr.ru/post/259243/>.
2. <http://mikrotik.kpi.ua/index.php/courses-list/iot/79-what-is-the-internet-of-things-and-why-is-it-important>.
3. <http://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechey-i-navishcho-vin-potriben-1326653.html>

АВТОМАТІЧНА ТЕЛЕФОННА СТАНЦІЯ (АТС)

Автоматична телефонна станція (АТС) — телефонна станція, що забезпечує автоматичне з'єднання абонентів телефонної мережі.

За районом обслуговування АТС поділяють на міські, сільські (внутрішньорайонні), АТС установ, корабельні, шахтні та спеціального призначення.

Залежно від типу комутаційних (з'єднувальних) пристроїв розрізняють АТС машинної, крокової, декадно-крокової, релейної, координатної, квазіелектронної та електронної систем. Основними пристроями машинних, крокових та декадно-крокових АТС є реле та машинні й крокові шукачі, координатних АТС — багаторазові координатні з'єднувачі та релейні керуючі пристрої — маркери й реєстри. В електронних АТС всі пристрої розмовного тракту і керуючі пристрої складаються з електронних елементів; у квазіелектронних АТС — відповідно з герконів (герметичних контактів) та електронних елементів. Ємність АТС збільшують, застосовуючи групові шукачі.

АТС дають змогу абонентам самостійно (користуючись певним кодом) здійснювати також міжміські телефонні з'єднання. Спеціальна апаратура АТС фіксує тривалість таких розмов, провадить необхідні розрахунки.

У СРСР, у тому числі в УРСР, серед міських найпоширенішими були АТС декадно-крокової і координатної систем, повна ємність кожної з яких 10 000 номерів.

Функції управління ресурсами АТС включають в себе призначення і модифікацію станційних параметрів, що характеризують всі логічні та фізичні ресурси в станції (під фізичним ресурсом мається на увазі будь-який станційний пристрій, а логічним ресурсом вважається будь-який об'єкт — такий як пучок з'єднувальних ліній або направлення маршрутизації, — який є значущим з точки зору технічної експлуатації станції); збір даних для нарахування плати; збір та аналіз статистичних даних про навантаження, що обслуговується станцією. Як уже згадувалося, станційне ПО має відомості про фізичних і функціональних реаліях своєї станції через параметри конфігурації, які є змінними величинами, визначеними спеціально для цієї мети.

Функції адміністративного управління АТС включають в себе ведення абонентських даних (номера і категорії абонентських ліній, нарахування плати) та аналогічних за змістом даних, що відносяться до взаємодії з УПАТС і з іншими мережами, а також прийняття рішень, пов'язаних з розвитком мережі зв'язку, і передачу відповідних вказівок функцій управління ресурсами.

Функції технічного обслуговування включають в себе контроль працездатності станції; виявлення несправностей з якомога точнішим визначенням їх місця розташування; блокування наслідків несправностей

(діагностика першого рівня); видалення несправних елементів і їх відновлення (діагностика другого рівня). Це робиться без переривання роботи станції, а для того щоб забезпечувалася можливість глибокої діагностики станційного пристрої, несправність якого може бути причиною серйозних порушень функціонування, пристрої такого типу, як правило, резервуються. Коли діагностика першого рівня визначає, що несправне одне з резервованих пристроїв, процедури техобслуговування забезпечують автоматичну реконфігурацію станції, виводячи з обслуговування пристрій, яке виявилось несправним, і перемикаючи його функції на резервуючий пристрій.

Мережевий комутатор (англ. *network switch*) або **світч** (від англ. *switch* — «перемикач») — пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

На відміну від концентратора, що поширює трафік від одного під'єданого пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Комутатор працює на каналному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Для з'єднання декількох мереж на основі мережного рівня служать маршрутизатори.

Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

Існує три способи комутації. Кожний з них — це комбінація таких параметрів, як час очікування й надійність передачі.

- Із проміжним зберіганням (Store and Forward). Комутатор читає всю інформацію у фреймі, перевіряє його на відсутність помилок, вибирає порт комутації й після цього посилає в нього фрейм
- Наскрізний (cut-through). Комутатор зчитує у фреймі тільки адресу призначення й після виконує комутацію. Цей режим зменшує затримки при передачі, але в ньому немає методу виявлення помилок.
- Безфрагментний (fragment-free) або гібридний. Цей режим є модифікацією наскрізного режиму. Передача здійснюється після фільтрації фрагментів колізій (фрейми розміром 64 байта обробляються за технологією *store-and-forward*, інші за технологією *cut-through*).
- Shortest Path Bridging, QoS, агрегування, віддзеркалення. Складні комутатори можна поєднувати в один логічний пристрій — стек, з метою

збільшення числа портів (наприклад, можна об'єднати 4 комутатори з 24 портами й одержати логічний комутатор з 96 портами).

Мережеві комутатори **застосовуються** в декількох технологіях, але найбільшого поширення знайшли в Ethernet. Головним їхнім завданням в мережі Ethernet є поділ мережі на сегменти. Це особливо актуально в мережах з великим числом робочих станцій, тому чим більше кінцевих пристроїв працюють одночасно з єдиним середовищем передачі даних, тим вища ймовірність виникнення колізії (одночасної передачі даних декількома пристроями) і, отже, нижча ефективність роботи мережі. Комутатор дозволяє розбити єдину мережу на кілька сегментів і збільшити число одночасно працюючих пристроїв.

Джерела:

1. <http://glossary.starbasic.net/index.php?title=%D0%9A%D0%BE%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80>
2. <https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80>

*Мацкевич Владислав Вікторович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев*

АЛГОРИТМ СОЗДАНИЯ САЙТА. СОЗДАНИЕ ПРИ ПОМОЩИ DRUPAL

Drupal (Друпал) — это популярная система управления контентом с открытым исходным кодом. Из-за ее мощного функционала разрабатывать сложные сайты на Друпале значительно проще, чем писать их с нуля. Неудивительно, что благодаря многочисленному сообществу пользователей и огромному количеству модулей, мы слышим о Друпале все чаще и чаще.

Вы готовы? Мы погружаемся в исключительно мощную систему управления контентом!

Достоинства Drupal:

1. Открытый код
2. Гибкость конфигурирования
3. Многочисленное и грамотное сообщество разработчиков
4. Модули
5. Легкость для разработчиков
6. Встроенная система кеширования
7. Достойная встроенная поисковая система

Недостатки:

1. Длительный процесс обучения

2. Сложный интерфейс
3. Сложность для не-разработчиков

Drupal против WordPress

Где бы ни обсуждали Друпал, всегда возникает непреодолимое желание сравнить его с другой ведущей открытой веб-платформой; как правило, это *WordPress*.

И где бы вы ни предположили, что *WordPress* — не полнофункциональная CMS, а платформа для блогов — вас всегда будет ждать жаркая дискуссия, но **иногда возможностей *WordPress* просто не хватает.**

Сайты, работающие на Drupal

1. Mozilla

Мозилла, компания, ответственная за *Firefox*, использует Друпал практически во всех своих веб-проектах. Официальные сайты Мозиллы и Spread Firefox сделаны на Друпале.

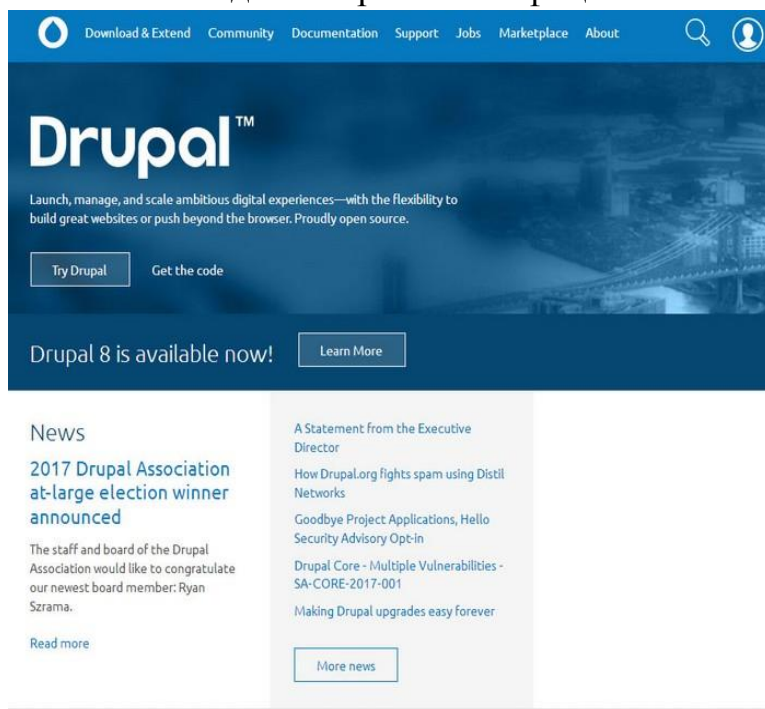
2. Ubuntu

Официальный сайт *Ubuntu*, популярного дистрибутива *Linux*, операционной системы, которая стоит на многих серверах, тоже сделан на Друпале. Обратите внимание на размер этого сайта и количество типов содержимого и функций; вскоре вы поймете, почему для *Ubuntu* выбрали именно Друпал.

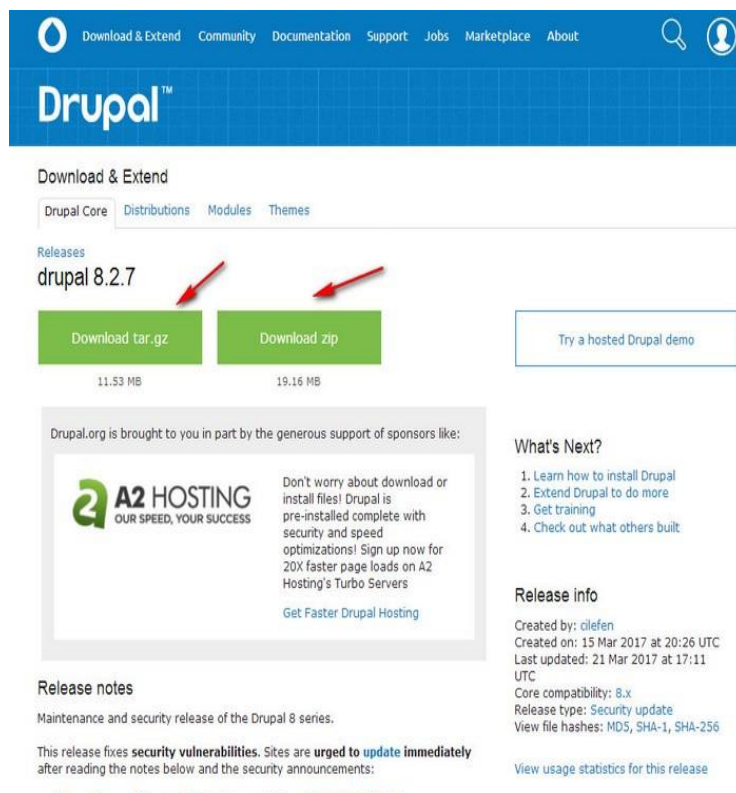
Алгоритм создания и настройки сайта на Drupal

1. Установка

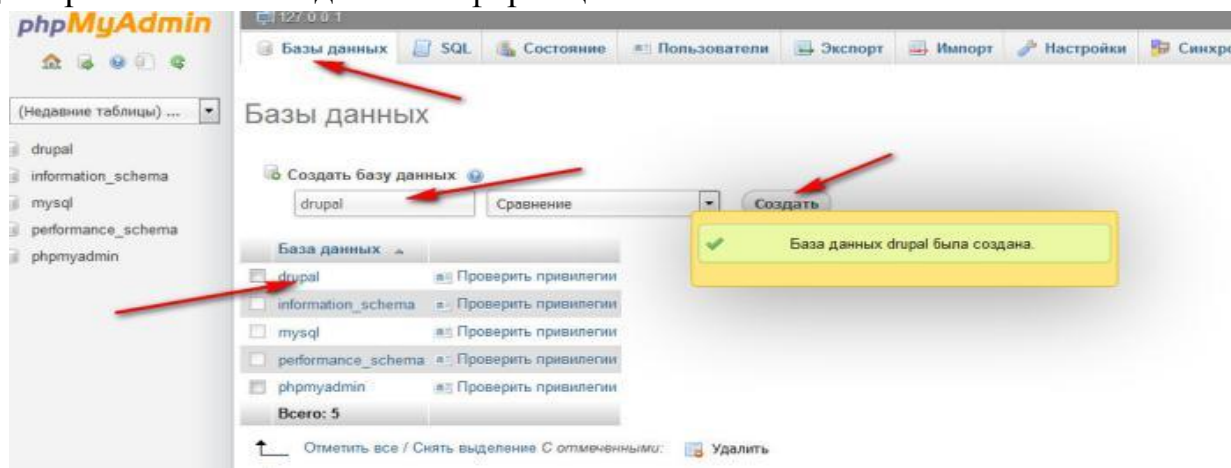
Первый этап создания абсолютно любого сайта с использованием готовой CMS и Drupal не исключение — это, конечно же, установка ее на локальном компьютере, или сразу на реальном сервере в интернете — хостинге, если кому так удобнее. Для этого необходимо перейти на официальный сайт разработчика.



Далее, переходим в раздел загрузок — “Download&Extend”. И кликаем по кнопке “Download Drupal 8.4.2” для перехода на страницу скачивания исходников системы.



Затем выбираем подходящий формат архива (для тех, кто не знает, для операционной системы Windows подойдет формат zip), кликаем по ссылке и сохраняем архив к себе на компьютер. После этого необходимо распаковать полученный архив, в соответствующий каталог локального веб-сервера, создать базу данных, используя инструмент phpmyadmin, которая будет использоваться для хранения необходимой информации.



И обратиться из браузера к вышеуказанному каталогу, для начала процесса установки.

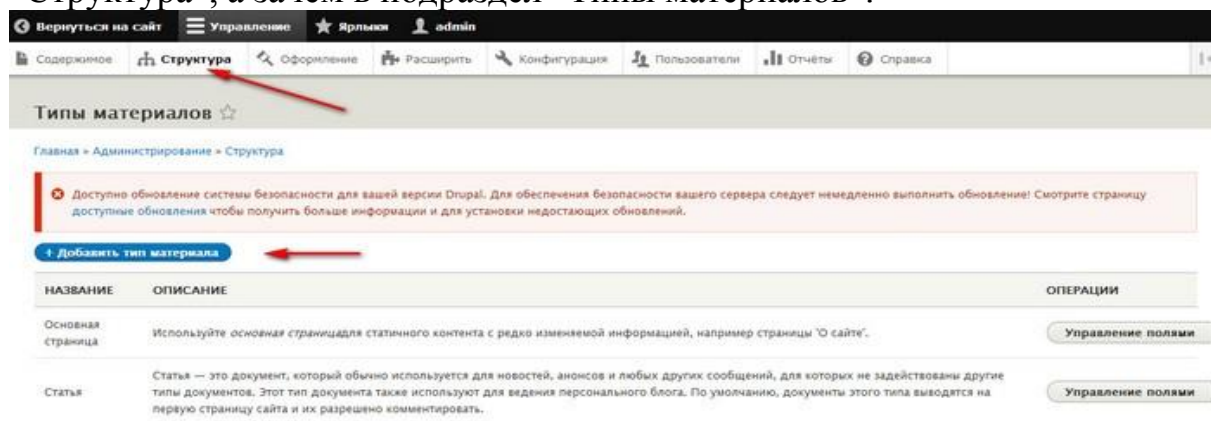
Установка движка относительно проста...

2. Настройка типов контента

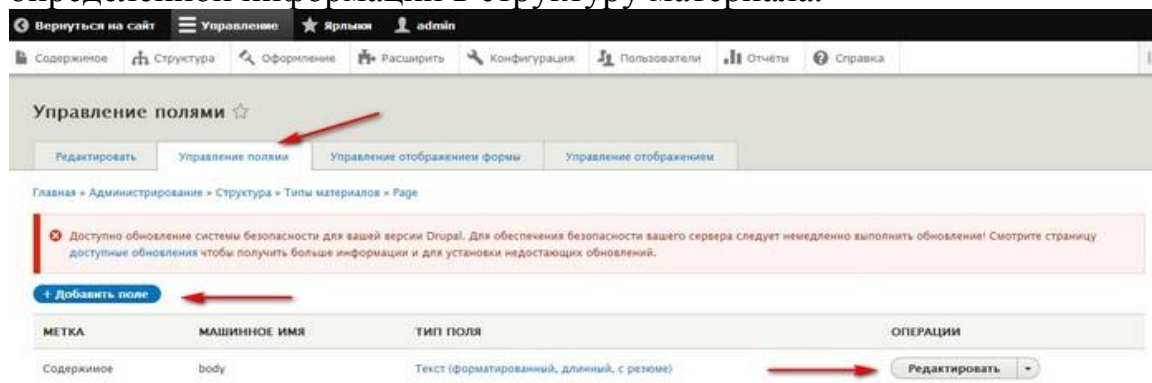
Для начала мы должны продумать какой контент будет публиковаться на сайте и под него создать или настроить типы материалов или нод.

В движке Drupal введено такое понятие как нода, которое представляет собой базовую единицу контента CMS. К примеру простая статья – это нода, отдельная страница – и это так же нода. Таким образом, Вы, скорее всего, догадались, что на данном этапе необходимо подготовить типы нод (материалов), которые будут использоваться на вашем сайте.

Сделать это можно, перейдя в специальный раздел панели администратора – “Структура”, а затем в подраздел “Типы материалов”.

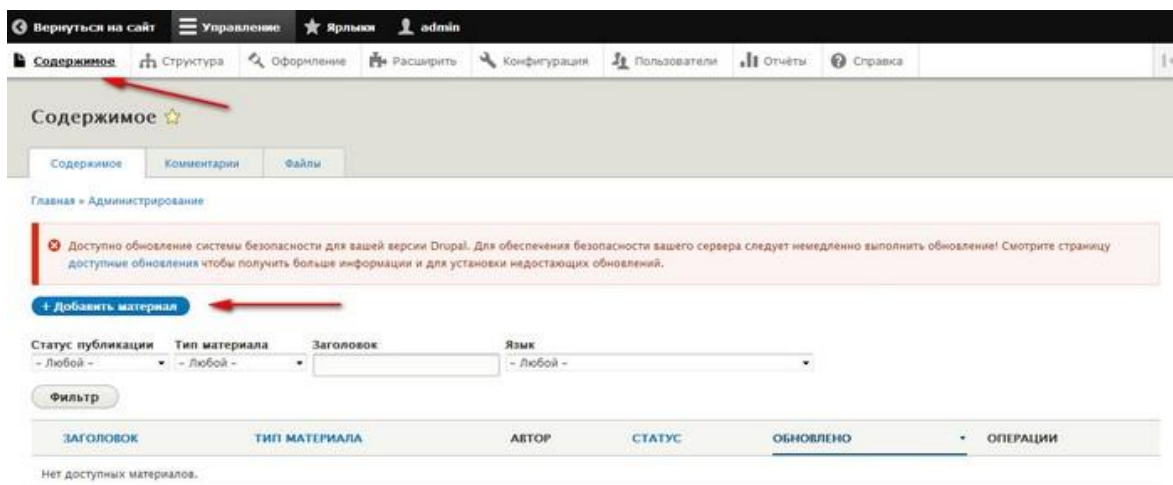


Заметьте, что при настройке или создании типа материала Вы, по сути, работаете с полями формы, которые будут использоваться для добавления определенной информации в структуру материала.



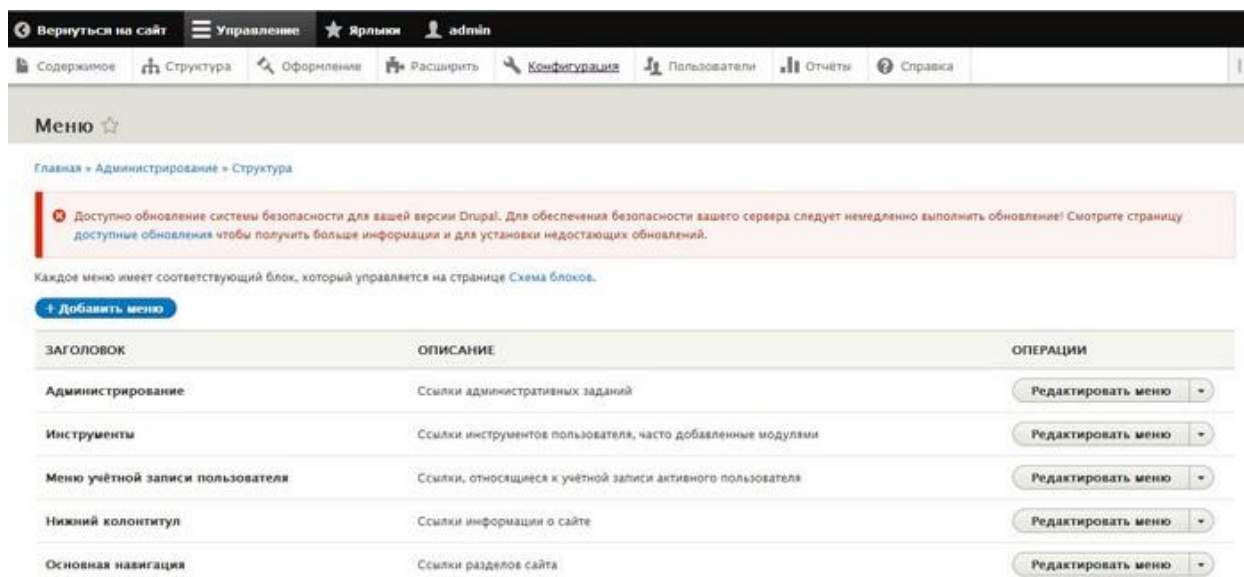
3. Создание меню и наполнение контентом

Для этого переходим в раздел “Содержимое” где и расположена заветная кнопка “Добавить материал”.



При этом, создавая материал, Вы сразу же для него, сможете создать новую ссылку в меню, если конечно это необходимо.

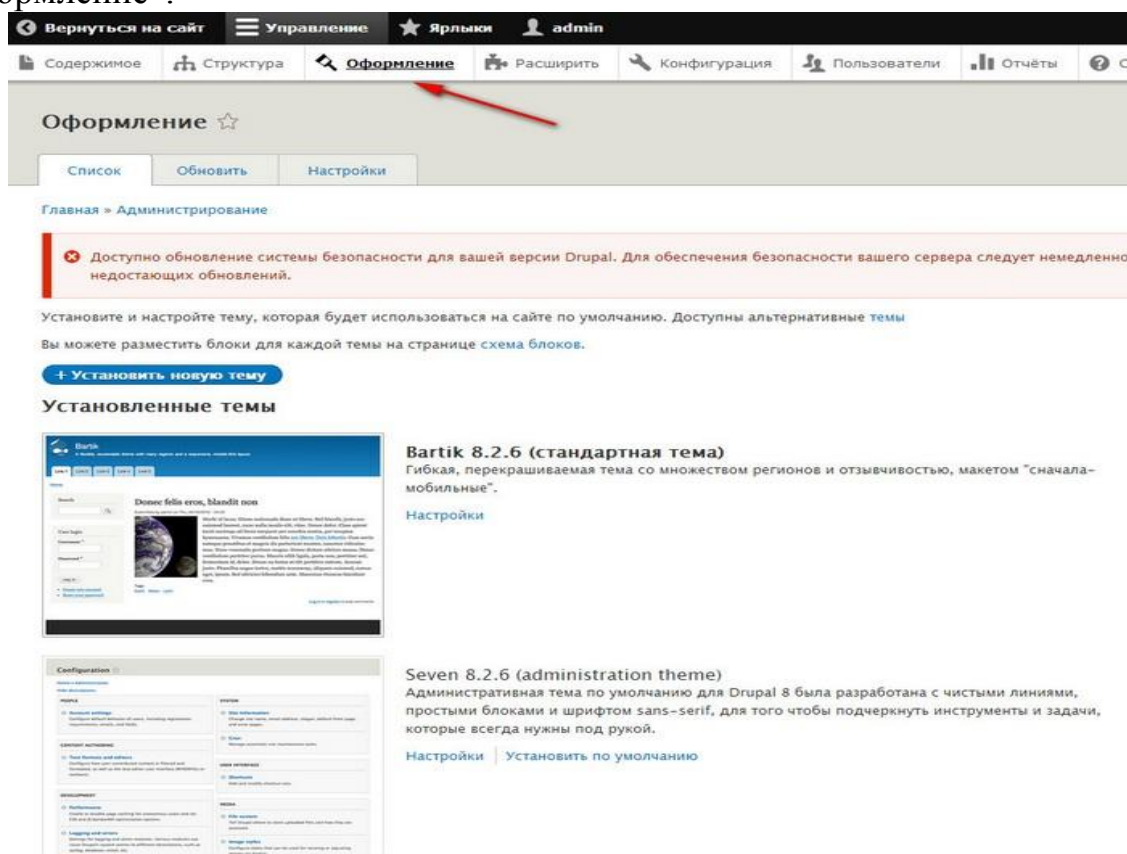
Причем, для работы с меню в движке Drupal предусмотрен специальный раздел, который так и называется “Меню”.



4. Внешний вид

Для тех, кто не знает, весь дизайн сосредоточен в шаблонах CMS, причем как пользовательской части, так и панели администратора.

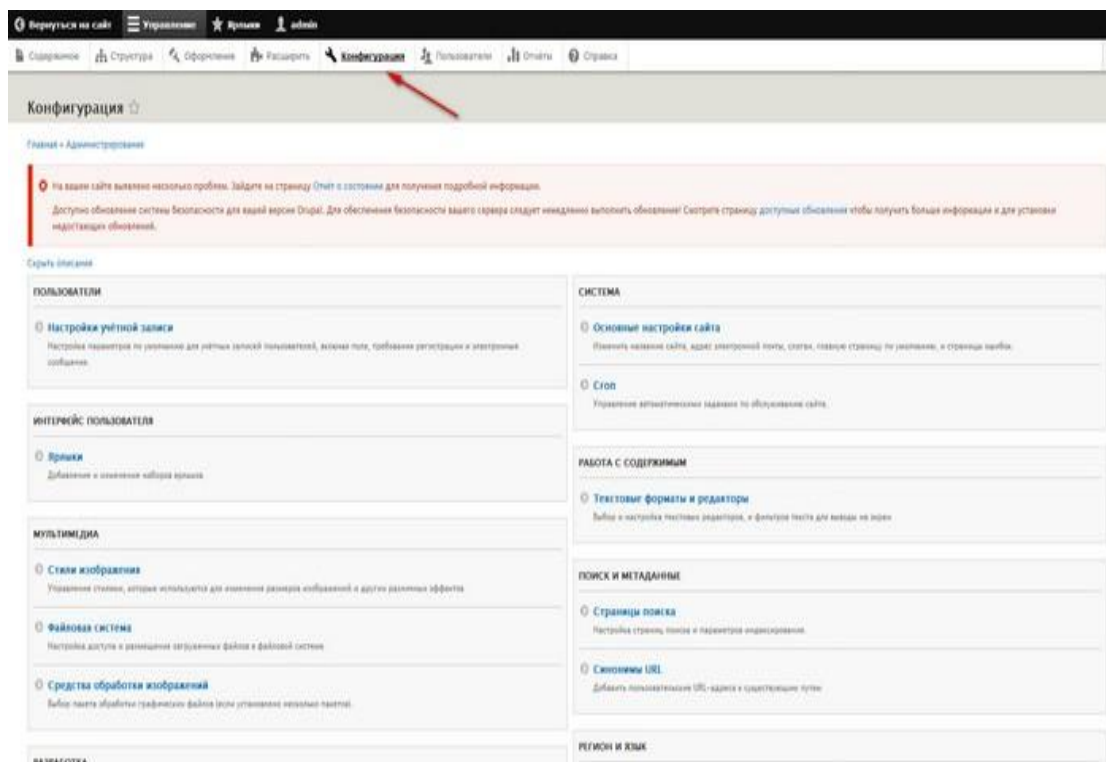
Для выбора интересующего шаблона, необходимо перейти в раздел “Оформление”.



Как Вы видите, есть несколько стандартных тем, которые можно назначить по умолчанию, а так же присутствует кнопка “Установить новую тему”, благодаря которой можно перейти на страницу загрузки нового шаблона.

5. Настройка и внешний вид

Завершающий этап это настройка и поиск ошибок. Для настройки будущего проекта, необходимо перейти в раздел “Конфигурация”.



Доступно огромное количество настроек, поэтому все они поделены на определенные группы, в зависимости от назначения. После настройке, обязательно необходимо тщательно проверить все ошибки и исправить несоответствия, если конечно они есть, а функционале сайта. Вот собственно и все что я хотел сказать в данном докладе. Теперь Вы знаете, как создать сайт при помощи Drupal.

Литература:

1. <https://webformymself.com/sozdanie-sajta-v-drupale-s-nulya/>
2. <https://ru.wikipedia.org/wiki/Drupal>
3. <https://habrahabr.ru/company/arcadia/blog/318808/>

Мацкевич Владислав Викторович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

АДРЕСАЦИЯ В IP-СЕТЯХ

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

1) Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: 3 байта - идентификатор фирмы производителя, а младшие

3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.

2) IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

3) Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

2. Классы IP-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.2.30 - традиционная десятичная форма представления адреса,
10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Существует несколько классов IP-адресов: А, В, С, D и Е.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

1) Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса А количество узлов должно быть больше 216, но не превышать 224.

2) Если первые два бита адреса равны 10, то сеть относится к классу В и является сетью средних размеров с числом узлов 28 - 216. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.

3) Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.

4) Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

5) Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

Соотношение между номером сети и номером узла в IP-адресе определяется с помощью маски подсети (Network mask), которая имеет длину также 4 байта и также записывается в десятичной форме по 4 октета, разделенных точками. Старшие биты маски подсети, состоящие из 1, определяют, какие разряды IP-адреса относятся к номеру сети. Младшие биты маски, состоящие из 0, определяют, какие разряды IP-адреса относятся к номеру узла. IP-адрес и маска подсети — минимальный набор параметров для конфигурирования протокола TCP/IP на сетевом узле.

Список использованной литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (3-е издание) Учебник для ВУЗов 2006 г.
2. В. Столлингс Современные компьютерные сети (2-е издание) 2005 г.

Краснолицкий Владимир Витальевич
Государственный университет телекоммуникаций
Факультет телекоммуникаций
г. Киев

ГИПЕРТЕКСТ

Гипертекст - текст, устроенный таким образом, что он превращается в систему, иерархию текстов, одновременно составляя единство и множество текстов.

Простейший пример гипертекст - это любой словарь или энциклопедия, где каждая статья имеет отсылки к другим статьям этого же словаря. В результате читать такой текст можно по-разному: от одной статьи к другой, по мере надобности, игнорируя гипертекстовые отсылки; читать статьи подряд, справляясь с отсылками; наконец, пуститься в гипертекстовое плавание, то есть от одной отсылки переходить к другой.

Настоящий словарь является подчеркнуто гипертекстовым, то есть построен так, чтобы постоянно провоцировать именно третий путь чтения. Например, сама статья "Гипертекст" безусловно связана со статьями текст и реальность (существует еще понятие гиперреальности), а стало быть, с пространством и временем, с мифом и неомифологизмом, виртуальными реальностями и измененными состояниями сознания, от которых путь недалек к психическим отклонениям, к шизофрении, психозу, неврозу, от чего один шаг до психоанализа, от него к Эдипову комплексу, оттуда к сновидению, от сновидения к проблеме индивидуального языка, от него к аналитической

философии в целом, от нее к теории речевых актов, оттуда к прагматике, к семиотике, мотивному анализу, к интертексту и гипертексту. И тут цепочка (одна из возможных гипертекстовых цепочек - ибо гипертекст нелинеен) замкнется.

Попробуем проследить эту цепочку и заодно понять, что такое гипертекст. Связь с проблемой текста и реальности очевидно, так как гипертекст - это нелинейный лабиринт, своеобразная картина мира, и выйти из него, войдя один раз, труднее, чем может показаться на первый взгляд.

Чтобы пояснить, что мы имеем в виду, приведем два примера. Первый из массового кино. Вероятно, многие помнят фильм "Косильщик лужаек". Герой этого фильма, поначалу нечто вроде Иванушки-дурачка, познакомившись с компьютерными виртуальными реальностями, постепенно интеллектуально и физически окреп, а под конец стал претендовать на мировое господство, но, попав в компьютерный гипертекст, он не мог оттуда выбраться, он был заперт в нем собственной гордыней.

Второй пример - житейский. Когда человек уже выбрал свою профессию, он тем самым выбрал определенный гипертекст своей жизни - определенные языковые игры, определенный круг общения, определенные книги, определенный образ мыслей. И вот вдруг ему все это надоедает. Он хочет вырваться из опостылевшего ему мира. Хочет все бросить, уйти куда-то совершенно в другое пространство, к совершенно другим людям и другим проблемам. Но те кнопки, которые он научился нажимать в своей старой жизни, те речевые акты и языковые игры, в которые он был обучен играть в своей старой жизни, те пружины, которые он привык нажимать, и те психологические установки и мотивации, которыми он привык руководствоваться, - все это остается при нем. И его тянет назад. Если это очень сильный и решительный человек, он сможет победить свой старый гипертекст, но вопрос состоит в том, стоило ли это делать.

Это проблема Льва Толстого - хотел уйти из Ясной Поляны почти на протяжении 30 лет - как будто бы все уже чужое - и не мог - все-таки все родное. Он только описывал эти попытки в своих произведениях (творчество писателя тоже можно представить как своеобразный гипертекст). Так, в рассказе "Отец Сергей" блестящий офицер вдруг уходит в скит замаливать свои светские грехи. К нему в скит приходит женщина, чтобы соблазнить его. Соблазн так велик, что отец Сергей отрубает себе палец, как бы символически себя кастрирует, но он понимает, что проблема, от которой он ушел, осталась при нем.

Гипертекст - это нечто вроде судьбы: человек идет по улице, думает о чем-то хорошем, предвкушает радостную встречу, но вдруг нажимается какая-то кнопка (не будем задавать бесполезного вопроса, кто эту кнопку нажимает и зачем), и жизнь его переворачивается. Он начинает жить совершенно иной жизнью, как бы выходит из дома и не возвращается. Но потом кто-то опять нажимает кнопку, и она вновь возвращает его к тем же проблемам, к той же улице, к тем же хорошим мыслям. Это, по сути, история Иова. Человек чувствует, что совершил какую-то ошибку, и сам не понимает, как это вышло,

его будто бес попутал, новая жизнь, казавшаяся ему такой нужной, такой творческой, теперь кажется просто западной. И тогда он может либо сойти с ума, либо действительно попытаться возвратиться на эту улицу и к этим мыслям. Но ему будет труднее, чем раньше, - новые кнопки, которые он научился нажимать в новой жизни, будут мешать ему в старой.

Я недаром все время говорю о кнопках, потому что понятие гипертекста тесно связано с компьютерными виртуальными реальностями.

Существует даже компьютерная художественная литература и, по меньшей мере, один классик этой литературы. И фамилия у него для классика вполне подходящая - Джойс, правда, зовут его не Джеймс, а Майкл и написал он не "Улисса", а компьютерный роман "Полдень". Особенность этого романа в том, что его можно адекватно читать только на дисплее компьютера. Он построен так, как строится гипертекст. В нем есть "кнопки", нажимая на которые можно переключать движение сюжета в прошлое и в будущее, менять эпизоды местами, углубиться в предысторию героини, изменить плохой конец на хороший и т. п. Серийность (см. серийное мышление, новый роман) - это тоже одна из особенностей гипертекста.

Здесь мы подходим к понятию гиперреальности, которое придумал французский философ, властитель умов современного мира Жан Бодрийар. Для того чтобы понять, что такое гиперреальность, надо отождествить реальность с текстом (что было нами сделано в статье реальность, а текст построить как гипертекст - получится гиперреальность. Бодрийар утверждает, что мы уже живем в гиперреальности. Масс-медиа, бесконечные пересекающиеся потоки информации, создают впечатление, что кто-то нажимает и нажимает различные кнопки, а мы только успеваем рот разевать. Мы перекатываемся, как при шторме на корабле, из одного конца гипертекста в другой.

Например, Бодрийар считал, что войны в Персидском заливе зимой 1991 г. между Ираком и США в обычном "реальностном" смысле не было. Это была гипертекстовая война, вся "посаженная" на дисплеи компьютеров и экраны видеопроекторов. Это не мистика - это особая метафизика гиперреальности, сон наяву, если угодно.

Дальше в нашей цепочке были пространство и время. Конечно, пространство здесь прагматическое (см. пространство, эгоцентрические слова), а время серийное, по нему можно подниматься в будущее и спускаться в прошлое, как по эскалатору. То есть, строго говоря, времени в гипертекст вообще нет.

Возьмем наш словарь. В хронологическом плане он зафиксирован на "отметке" XX век. Но внутри этой отметки времени нет - мы перепрыгиваем из венской культуры начала века в Москву конца века, а оттуда - в Берлин 1943 г. Время здесь становится разновидностью пространства. Это и есть миф, где все повторяется, и это есть неомифологизм, доведенный до последней черты: каждое слово - цитата, каждое предложение - мифологема. И конечно, такое сознание нельзя считать неизменным - мы его сами и изменили. Это своеобразная шизотехника, некоторый культурный психоз, и мы нажимаем кнопки

бессознательно, поэтому это имеет прямое отношение к бессознательному (к парасемантике, - см.), и это имеет отношение к Эдипову комплексу, ибо кого же мы хотим пережитить, как не самого себя и свои чудовищные бессознательные стремления, и это безусловно индивидуальный язык, потому что его, кроме нас, никто не поймет, и это аналитическая философия, потому что мы все время так или иначе анализируем значения употребляемых нами слов, и это теория речевых актов, потому что гипертекстовое путешествие - это очень сложная разновидность речевого акта, а раз так, то он относится к области прагматики и, стало быть, к семиотике, поскольку прагматика - одна третья часть семиотики. И это, конечно, семиотика интертекста.

Надеюсь, что более наглядно и убедительно трудно было объяснить, что такое гипертекст.

Список литературы:

1. Бодрийар Ж. Войны в заливе не было // Художественный журнал. 1993. - М 4.
2. Интервью с Жаном Бодрийаром // Там же. 1995. - М 8.
3. Руднев В. Морфология реальности: Исследование по "философии текста". - М., 1996.
4. Мухин Ю.А., Приборы и устройства полупроводниковой электроники. - М.; МЭИ, 1996. - 234 с.

*Краснолицкий Володимир Віталійович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ*

ТЕХНОЛОГІЯ ІОТ

Інтернет речей (Internet of Things – IoT) перетворює звичні для нас речі у нові пристрої, створюючи як розумні годинники, так і розумні міста. Він під'єднує далекі від Інтернету засоби до мережі та надає їм нові функції. Недарма чекаємо понад 50 мільярдів таких пристроїв уже за кілька років!

Термін “Інтернет речей” (або англійською “Internet of Things”, скорочено – IoT) вперше було сформульовано в кінці ХХ-го століття, у 1999 році. Це концепція комунікації об’єктів (“речей”), які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини. Таким чином, всі пристрої в будинках, в автомобілях, на користувачеві виконують обробку інформації, її аналіз та обмін між собою та, залежно від результатів, приймають рішення і виконують певні дії.

Сфера IoT – один із головних світових трендів. Старі-добрі пристрої стають частиною Інтернет мережі і виконують нові функції. Недарма цю галузь вважають рушієм 4-ї індустріальної революції, яка зараз триває у світі. Експерт IoT – людина, яка творить майбутнє. Стань ним із нашою програмою!

Історія

Автор терміну «Internet of Things» — «піонер технологій» Кевін Ештон. В кінці 1990-х Ештон вивчав RFID — радіочастотну ідентифікацію. Ця технологія

дозволяє кріпити на предмети маленькі мітки, що містять важливу інформацію і дозволяють зчитувати її на відстані.

RFID-мітки можна побачити, приміром, на товарах в магазині. Це маленька наліпка або ж мітка в пластиковому корпусі. В будь-якій формі вона дозволяє, наприклад, запобігти крадіжкам: якщо товар з активною міткою наближується до сенсора, встановленого на виході, звучить сигнал тривоги.

У 1999 році Кевін Ештон, працюючи в компанії Procter & Gamble, запропонував своєму керівництву використовувати радіочастотні мітки, щоб створити покращену систему управління поставками. Пояснюючи ідею, він скористався терміном «інтернет речей».

Використання і перспективи

Концепція інтернету речей дуже широка. Немає чіткого списку приладів, для яких можна застосувати цей підхід. Це можуть бути побутові прилади: пральна машинка, якою можна керувати онлайн, або холодильник, що сам напише список продуктів і замовить доставку. Ще один варіант — гаджети, котрі можна носити: фітнес-трекери, «розумні» годинники. Також до інтернету речей відносять автомобілі та інший транспорт з системою автопілоту — такі, що можуть їздити без водія.

Гаджет може під'єднуватись до глобальної мережі Інтернет або ж «співпрацювати» з іншими приладами, що знаходяться поряд. Так виникають системи «розумного» будинку або ж цілого «розумного» міста.

Технології, що використовуються

Прилади, котрі можна віднести до інтернету речей, зазвичай мають чотири характерні технології: ідентифікатор, датчики, інструменти для зв'язку з іншими приладами та вбудований комп'ютер.

В якості ідентифікатора використовуються RFID-мітки, QR-коди (ті чорно-білі квадратики, що їх може зчитувати майже кожен сучасний телефон) або інші технології. Мітка дозволяє приладу мати своє «ім'я».

Датчики і сенсори потрібні, щоб отримувати інформацію з середовища. Приміром, так фітнес-трекер зчитує інформацію про пульс людини. Також прилади можуть отримувати інформацію від інших приладів та з мережі — за допомогою Bluetooth або WiFi.

І, нарешті, для обробки всіх отриманих даних і виконання програм використовується вбудований комп'ютер. Він може бути доволі складним — як той, що керує автопілотом в сучасному автомобілі — або ж зовсім примітивним.

Небезпеки і ризики

Найбільшим недоліком інтернету речей вважають низький рівень безпеки. Дуже часто такі прилади не мають жодних антивірусів чи навіть перевірки користувача. Під'єднання до інтернету — великий ризик. Хакери можуть отримати доступ до такого пристрою та вкрасти особисту інформацію.

Останнім часом експерти навіть говорять про «ботнети речей» (Botnets of Things). Оригінальне значення терміну «ботнет» — це мережа комп'ютерів, заражених вірусом. Вірус відстежує і передає хакерам всі введені паролі,

фінансові та інші секретні дані. До того ж, комп'ютер в ботнеті інколи порівнюють з зомбі: після зараження він починає «кусати» і заражати інших.

Сучасний стан

Вже зараз інтернету речей приділяється увага на найвищому рівні, зокрема починаючи з 2009 року у Брюсселі при підтримці *Єврокомісії* проходять конференції *Annual Internet of Things*, на якій виступають з доповідями єврокомісари, науковці та керівники провідних ІТ-компаній. За прогнозами аналітиків у найближчі роки очікується справжній бум інтернету речей. Так, за прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн дол. Деякі інші аналітичні агентства висловлюють ще більш оптимістичні прогнози. Найбільші світові ІТ компанії вже почали перегони за лідерство на цьому ринку. Так корпорація Intel у 2014 році після випуску «SoC Edison» оголосила конкурс «*Make it Wearable*» з призовим фондом \$1,3 млн на найкраще застосування своєї системи для концепції IoT та створила власний підрозділ «*Internet of Things Solutions Group*» для розвитку цього напрямку. Компанія «Google» на початку 2014 року за 3,2 млрд доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів. Спеціалісти цієї компанії займалися впровадженням на американському ринку технологій IoT. Виробники побутової техніки також працюють у цьому напрямку. Так на виставці CES 2014 у Лас-Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до інтернет.

Значення на ринку прогнозується на рівні 80 мільярдів доларів.

Лідерами у розробці та впровадженні інтернету речей є країни, в якій розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — це США, Китай, Південна Корея. Також значний прогрес у цій галузі демонструють європейські країни та Японія.

Засоби передачі даних в мережі

Інтеграція з Інтернетом має на увазі, що пристрої будуть використовувати IP-адресу як унікальний ідентифікатор. Проте, через обмежені адресні простори в IPv4 (що дозволяє використовувати 4,3 мільярда унікальних адрес), об'єктам IP доведеться використовувати IPv6, який забезпечує унікальними адресами мережевого рівня не менше 300 млн пристроїв на одного жителя Землі. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, але також пристрої, які виконують дії (наприклад, лампочки або замки, якими керують через Інтернет). Значною мірою, майбутнє інтернету речей не буде можливим без підтримки IPv6, отже, глобальне впровадження IPv6 у найближчі роки буде мати вирішальне значення для успішного розвитку IP в майбутньому.

Для бездротової передачі даних особливо важливу роль в побудові інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт *IEEE 802.15.4*, що управляє

доступом для організації енергоефективних персональних мереж, і є основою для таких протоколів, як *ZigBee*, *WiFi*, *Bluetooth*, *6LoWPAN*.

ZigBee— це комунікаційна технологія, заснована на протоколі *IEEE 802.15.4* для реалізації низькошвидкісних бездротових приватних мереж. *ZigBee* володіє такими характеристиками, як низьке енергоспоживання, низька швидкість передачі даних, низька вартість і висока пропускну здатність. В даний час *ZigBee* використовується в основному при передаванні інформації між різними речами електронного обладнання, які знаходяться в межах короткої відстані і швидкості передачі даних не дуже висока. Це, в основному периферійні пристрої (миша, клавіатура) і побутова електроніка (*TV*, *DVD*), а також пристрої промислового управління (монітори, датчики і засоби автоматизації).

WiFi— це локальна бездротова технологія, яка використовує 2,4 ГГц надвисокої частоти або 5 ГГц супер-високочастотної радіохвилі. Ця технологія дуже добре підходить для передавання великих обсягів даних по бездротовій мережі між пристроями, але це також вимагає багато енергії для роботи і має невеликий рівень пропускну здатності даних. При використанні цієї технології потрібно буде замінювати батареї у всіх пристроях на регулярній основі.

Bluetooth— це бездротова технологія, яка використовується для передачі даних в персональних мережах. Він передає дані по смузі частот від 2,4 до 2,485 ГГц і працює на коротших відстанях, ніж *Wi-Fi*. Ви можете синхронізувати пару пристроїв, таких як телефони, навушники, колонки, комп'ютери і багато іншого. З розвитком *Bluetooth v4.0* з'явилася можливість реалізувати функцію низького енергоспоживання і збільшений радіус дії до декількох десятків метрів.

Серед провідних технологій важливу роль у розповсюдженні інтернету речей відіграють рішення *PLC* — технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення спочатку підключені до мережі електропостачання). *6LoWPAN*, який реалізує шар *IPv6* як над *IEEE 802.15.4*, так і над *PLC*, будучи відкритим протоколом, стандартизованих *IETF*, відзначається як особливо важливий для розвитку інтернету речей.

Джерела:

1. https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9
2. <http://thefuture.news/iot/>
3. <http://iot.lviv.ua/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%80%D0%B5%D1%87%D0%B5%D0%B9/>

АРХИТЕКТУРА ETHERNET

Ethernet - найпопулярніший протокол кабельних комп'ютерних мереж, що працює на фізичному та каналному рівні мережевої моделі OSI Станом на 2016 рік близько 85 % усіх комп'ютерів у світі були підключені до комп'ютерних мереж по протоколу Ethernet.

За строго технічним визначенням Ethernet — сімейство протоколів стандарту IEEE 802.3

Ethernet тісно пов'язаний з моделлю TCP/IP, оскільки у переважній більшості випадків служить для передачі IP-пакетів.

Ethernet є найпоширенішим протоколом у сучасних локальних комп'ютерних мережах, також використовується для побудови MAN мереж з використанням технології Metro Ethernet.

Ethernet було спроектовано згідно з технологією CSMA/CD (*множинний доступ з контролем несучої та виявленням колізій*). Хоча з широким застосуванням мережевих комутаторів та засобу передачі повний дуплекс проблема виникнення колізій в мережах Ethernet майже не зустрічається.

Ethernet-мережі працюють на швидкостях 10Мбіт/с, Fast Ethernet— на швидкостях 100Мбіт/с, Gigabit Ethernet— на швидкостях 1000Мбіт/с, 10 Gigabit Ethernet— на швидкостях 10Гбіт/с. В кінці листопада 2006 року було прийняте рішення про початок розробок наступної версії стандарту з досягненням швидкості 100Гбіт/с (100 Gigabit Ethernet) Легенда створення

Винахідником Ethernet вважається співробітник корпорації Xerox PARC Роберт Меткалф. За його словами Ethernet було винайдено 22 травня 1973 року, коли він завершив написання доповідної записки для керівництва PARC про потенціал технології.

Роберт Меткалф мав наукову ступінь доктора філософії отриману в Гарвардському університеті. Працюючи на Xerox PARC одним з його службових обов'язків було проводити курси навчання для персоналу збройних сил США по першій у світі пакетній мережі ARPANET. Для цього Меткалф був змушений часто відвідувати Вашингтон, зупиняючись у квартирі свого друга. Одного разу перебуваючи в квартирі друга, Меткалф перелистував журнал доповідей з конференції 1970 року Американської федерації товариств обробки інформації¹ та випадково наштотхнувся на доповідь Нормана Абрамсона «*ALOHA System – ще одна альтернатива для комп'ютерних комунікацій*». Доповідь описувала інноваційну бездротову технологію з'єднання комп'ютерів. Хоча Меткалф багато в чому був незгодний з висновками Абрамсона, ця доповідь надихнула його на роботу зі створення нового протоколу комп'ютерних мереж.

Повернувшись до Xerox PARC Меткалф разом з Дейвідом Боггсом почали теоретичні роботи по створенні мережі, результатом яких стала доповідна

записка до керівництва компанії 22 травня 1973 року, що описувала принципи побудови нової системи комунікації між комп'ютерами на основі технології CSMA/CD. Доповідь знайшла підтримку, що послужило початком втілення теорії на практиці. Таким чином 11 лютого 1973 року був створений перший *Ethernet* прототип, який мав фантастичні на той час характеристики: пропускну спроможність 2.94 Мб/с, фізичну довжину 1 кілометр та з'єднував між собою 100 комп'ютерів.

У 1975 році компанія Xerox офіційно анонсувала винахід

Розвиток

У 1979 році Меткалф залишив Xerox PARC, заснував компанію 3Com та переконав DEC, Intel і Xerox спільно просувати Ethernet як стандарт.

З самого початку *Ethernet* базувався на ідеї зв'язку комп'ютерів через єдиний коаксіальний кабель, що виконував роль транзитного середовища. Метод передавання був дещо схожим на методи радіопередавання (хоча й з суттєвими відмінностями, наприклад, те, що в кабелі значно легше виявити колізію, ніж в радіоефірі). Загальний мережний кабель, через який велася передача, був дещо подібним на ефір, і з цієї аналогії походить назва Ethernet (англ. *net* — «мережа»).

З плином часу з відносно простої початкової специфікації Ethernet розвинувся у складну мережну технологію, яка зараз використовується у більшості комп'ютерних систем. Щоб зменшити ціну та полегшити управління та виявлення помилок в мережі, коаксіальний кабель згодом був замінений зв'язками типу «точка — точка», що з'єднувалися між собою концентраторами/комутаторами (хабами/світчами). Своїм комерційним успіхом технологія Ethernet завдячує появі стандарту з використанням кабелю типу «звита пара» як транзитного середовища.

На фізичному рівні станції *Ethernet* спілкуються між собою за допомогою передачі одна одній пакетів — невеликих блоків даних, які відправляються та доставляються індивідуально. Кожна *Ethernet*-станція має свою власну 48-бітну MAC-адресу, яка використовується як кінцевий пункт або джерело для кожного пакету. Мережні картки, як правило, не сприймають пакетів, що адресовані іншим *Ethernet*-станціям. Унікальна MAC-адреса записується в контролер кожної мережної карти.

Незважаючи на серйозні зміни від 10-Мбітного товстого коаксіалу до 1-Гбітного оптоволоконного зв'язку типу «точка-точка», різні варіанти *Ethernet* на найнижчому рівні є майже однаковими з погляду програміста і можуть легко з'єднуватися між собою за допомогою дешевого обладнання. Це є можливим, оскільки формат кадру лишається незмінним, незважаючи на різні процедури доступу до мережі.

Ethernet — архітектура мереж, що ґрунтується на логічній топології шини, з розподіленим середовищем передавання, методом доступу до середовища передавання CSMA/CD, описана стандартом IEEE 802.3. За фізичною реалізацією розрізняють:

- 10BASE5 — Thick («товстий») Ethernet;
- 10Base2 — Thin («тонкий») Ethernet;

- 10BaseT — Twisted-pair Ethernet (Ethernet на витій парі);
- 10Broad36 — мережа на широкосмуговому 75-Омному коаксіальному кабелі;
- 10BaseF — кілька варіантів мережі на оптоволоконному кабелі;
- 100BaseT — стандарти FastEthernet на витій парі

Перший елемент в умовному позначенні архітектури — швидкість передавання в Мбіт/с; другий елемент позначає спосіб передавання: Base — пряме немодульоване передавання, Broad — використання широкосмугового кабелю з частотним ущільненням каналів; третій елемент — середовище передавання (T — вита пара, F — оптоволокно) або довжина сегмента кабелю в сотнях метрів (сучасні мережні адаптери дають змогу збільшувати довжину сегмента, наприклад для 10Base2, до 250—300 метрів).

Джерела:

<https://uk.wikipedia.org/wiki/Ethernet>

Фурсович Іван Юрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

VPN – ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА

Кожного дня 40% людей нашої планети користуються “всесвітньою павутиною” для пошуку різної інформації, для зв’язку з своїми рідними або друзями, тощо. Ми відкриваємо різні сайти і навіть не підозрюємо, що всі наші дані не є захищеними. Уявімо, що з пункту А у пункт Б ми хочемо передати секретну інформацію так, щоб ніхто посторонній про неї не дізнався, звісно якщо це твій сусід можна піти і розповісти, а якщо це на значній відстані, то в пригоді стане інтернет. Але як передати інформацію захищено? Тут знадобиться приватна мережа-VPN, яка підходить не тільки окремим користувачам, а й цілим компаніям.

VPN (скорочено від англ. Virtual Private Network — віртуальна приватна мережа) — загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об’єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв’язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-

клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

Прикладом створення віртуальної мережі використовується інкапсуляція протоколу PPP в будь-який інший протокол — IP (ця реалізація називається також PPTP — Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Деякі інші протоколи так само надають можливість формування захищених каналів (SSH).

Структура VPN:

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступної) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Класифікація VPN:

- По протоколу, що використовується
 - IPX
 - Apple Talk
 - TCP/IP
- По рівню роботи відносно ISO/OSI
 - Канальний(2)
 - Мережевий(3)
 - Транспортний(4)
- По степеню захищеності
 - Довірчі
 - Захищені
- По способу реалізації
 - Програмний комплекс
 - Програмно-апаратний комплекс
 - Інтегроване рішення
- По призначенню
 - Internet VPN
 - Extranet VPN
 - Remote Access VPN

Навіщо потрібна VPN

Крім забезпечення захисту від сторонніх переданих даних, VPN має і ряд інших переваг, у тому числі і економічних. Дослідницька компанія Forrester Research опублікувала дані, що характеризують переваги застосування VPN поверх Інтернет (з розрахунку на 1000 користувачів) в порівнянні зі створенням центру віддаленого доступу (Remote Access Service). Ці та інші дослідження

дозволили Міжнародної асоціації комп'ютерної безпеки (International Computer Security Association, ICSA) включити технологію VPN в десятку найвідоміших технологій, які будуть в першу чергу застосовуватися багатьма компаніями. Це підтверджує і компанія Gartner Group, яка в своєму звіті передбачила, що кошти побудови VPN будуть застосовуватися в 2002 році в 90% компаній. З цим пов'язаний і прогноз ринку засобів VPN, який буде обчислюватися 11,94 млрд. Дол. В 2002 році і 18,77 млрд. Дол. У 2004 році (за даними Frost & Sullivan).

Отже, VPN це чудова технологія для захисту даних в мережі інтернет, яка підходить як для окремих користувачів, так і для цілих компаній.

Література:

<https://hidemy.name/ru/articles/simple-vpn/>

<http://kb.its.psu.edu/article/891>

<http://compress.ru/article.aspx?id=12036%2303>

<http://www.nestor.minsk.by/sr/2005/03/050315.html>

Гордеева Каролина Вирсавия Алексеевна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ?

Содержание статьи: Что может произойти с информацией? Каким видам угроз подвергаются данные телекоммуникационных систем? Как защитить информацию в телекоммуникационных системах? Информация в современном обществе стала одним из основных объектов криминального интереса.

Каждый человек сталкивается с ситуациями, когда похищаются, искажаются, незаконно распространяются те или иные сведения, наносящие вред личности, коммерческой деятельности, государству. Информационная безопасность телекоммуникационных систем (ИБТС) нередко сводится к компьютерной безопасности. Особенно «беззащитны» данные, которые хранятся и передаются с помощью глобальных сетей и систем. Например, взлом электронных почтовых ящиков стал одним из наиболее распространенных видов нежелательного доступа к конфиденциальным данным.

Соблюдение правила «Не болтай!» в информационном обществе означает остановку деятельности. Ведь его субъекты не могут себе позволить погрузиться в молчание: они вынуждены постоянно производить информацию, обмениваться документами. Средства, обеспечивающие безопасность, развиваются в результате печального опыта атак на уязвимые звенья систем хранения данных и информационного обмена.

Такие системы развиваются вместе с технологиями передачи данных на расстояние с помощью технических средств и методов: серверов,

пользовательских компьютеров, телефонных линий, компьютерных сетей, то есть компонентов телекоммуникационных систем.

Что может произойти с информацией?

В процессе хранения и передачи данных субъекты, не соблюдающие безопасность информационного обмена, могут пострадать из-за нарушений конфиденциальности и целостности информации. Наиболее ощутимый ущерб связан с нарушением конфиденциальности, когда сведения, предназначенные лишь для определенного круга лиц, попадают в посторонние руки.

Например, доступ к секретной переписке через интернет или телефон может привести к скандалу в семье, финансовым издержкам, потере репутации.

Информация подвергается искажению, блокированию, стиранию, то есть нарушению целостности. Это может произойти умышленно или вследствие ошибок пользователей и программных систем. Поэтому безопасность телекоммуникационных систем включает использование надежных технических средств, антивирусных программ, квалифицированных кадров.

Каким видам угроз подвергаются данные телекоммуникационных систем?

Информационная безопасность телекоммуникационных систем подвержена угрозам широкого спектра: от вирусного заражения, с которым можно справиться локально, до нормативно-правовых коллизий, требующих работы законодательных и правоохранительных органов власти. Покушения на конфиденциальность и целостность информации могут совершать недоброжелатели, конкуренты. Многообразие угроз для телекоммуникационных систем делится на несколько основных видов:

- Информационные (преднамеренные и случайные);
- Аппаратно-программные (например, «шпионские» средства);
- Радиоэлектронные помехи;
- Физические поломки;
- Организационные и нормативно-правовые.

Информационные угрозы связаны с промахами и нарушениями при сборе информации, ее обработке, сбоями в технологии передачи данных, что приводит к утечке информации, несанкционированному копированию и искажению (подделке). Может происходить блокирование систем и задержка передачи информации. Безопасность нарушается по невнимательности, либо такие угрозы реализуются преднамеренно. К первому варианту часто относится, например, отправление информации по другому адресу, которое в лучшем случае приводит к ситуации «этот неловкий момент», а в худшем — к финансовому и репутационному краху.

Аппаратно-программные и радиоэлектронные угрозы связаны с вирусами и «закладками» — устройствами перехвата информации. Например, информационная безопасность оказывается под угрозой из-за звукозаписывающих закладок, которые используются для снятия информации телефонных переговоров. Видеозаписывающие устройства могут применяться для похищения паролей. Вирусы не только способствуют похищению данных,

но и серьезно ограничивают скорость их передачи, а то и вовсе могут заблокировать возможность работы с информацией. Кроме того, безопасность страдает при сбоях в работе техники и программных систем под воздействием радиоэлектронных сигналов.

Физические угрозы — прямое уничтожение, поломка технических систем коммуникации, похищение информационных носителей. Эта угроза может возникнуть в результате аварий, стихийных бедствий, поэтому система информационной защиты должна включать средства, которые минимизируют последствия аварийных ситуаций.

Источником угроз может быть применение ненадежных, устаревших технологий из-за проблем организации производственного процесса.

Информационная безопасность обеспечена множеством нормативных актов, в частности, указами президента, ведомственными нормативными документами. Каждый руководитель обязан изучить нормативную базу и придерживаться инструкций и руководящих документов Федеральной службы по техническому и экспортному контролю.

Как защитить информацию в телекоммуникационных системах?

Развитие технологий передачи данных требует постоянного изобретения новых методов, позволяющих сохранить конфиденциальность информации, ее целостность, «уйти от придирчивых глаз» в глобальной деревне информационной паутины. Телекоммуникация (связь на расстоянии) не всегда происходит непосредственно через компьютерные сети, однако информация, переданная через телекоммуникационные каналы, зачастую называется компьютерной, так как электронно-вычислительная техника участвует хотя бы на одном из этапов телекоммуникации. Система мер, созданная вокруг обеспечения ИБТС, часто представляет собой разные аспекты компьютерных технологий. Среди них есть традиционные (технические и организационные), а также пока не ставшие традицией, например, криптографические методы.

Безопасность требует резервирования данных, сохранения их на разных носителях. Зачастую до создания резервных копий просто «не доходят руки». В системе, где обеспечивается информационная безопасность, как правило, есть специалист, который постоянно помнит, что не следует «класть все яйца в одну корзину», сохраняя все данные лишь на один компьютер. Необходимо регулярно делать копирование данных на переносные диски, перераспределять ресурсы между работоспособными устройствами. Техническая безопасность также означает, что компьютеры должны быть защищены от перепадов напряжения сетевыми фильтрами, установками бесперебойного питания.

Организационные меры включают защиту носителей информации от кражи, кадровую работу по подбору и обучению надежного и квалифицированного персонала, контроль технического обслуживания и ремонта. Техника и помещение должны тестироваться на наличие «шпионских» средств снятия, перехвата информации.

Для защиты от несанкционированного доступа важно, перед тем как передавать носители информации в посторонние руки, обеспечить правильное удаление

конфиденциальных данных, ведь файлы, отправленные в корзину обычным способом, можно восстановить.

К наиболее известным традиционным методам, которые обеспечивают безопасность при попытках несанкционированного доступа, относится использование систем идентификации для опознавания тех, кто имеет право работать с той или иной информацией. Необходимо защитить систему надежными паролями, которые требуется периодически менять: это снизит вероятность утечки и перехвата данных.

Эффективными методами являются средства идентификации на основе отпечатков пальцев, голосового тембра и других физических особенностей.

Пока не очень массовым способом защиты является криптография, когда сообщения зашифровываются, а лишь затем поступают в телекоммуникационный канал. Пользователь, который получает сообщение, должен иметь идентифицирующий ключ для расшифровки данных.

Защита от подделки официальных документов в настоящее время обеспечивается разновидностью криптографического метода — электронной цифровой подписью. Этот реквизит широко используется при электронном документообороте органов власти.

Распространенные уязвимые места телекоммуникационных систем предприятия. Руководство предприятия должно заботиться о разработке концепции информационной безопасности, закладывать средства на минимальный пакет методов защиты телекоммуникационных систем:

- Антивирусное программное обеспечение;
- Технологии аутентификации;
- Средства шифрования данных;
- Ресурсы для резервного копирования.

Самые частые проблемы при работе с информацией на производстве связаны с вирусами. Сотрудники вносят вирусы при установке программ, посещении зловердных сайтов. Утечка информации может быть связана с работой вирусов, которые перехватывают пароли, причем они могут заблокировать систему или действовать в тихом режиме. В первом случае предприятие быстро начинает заботиться информационная безопасность: устанавливаются антивирусные программы, чтобы разблокировать технику и продолжить работу. Однако этот бессистемный подход не обеспечивает безопасность. Во втором случае сотрудники могут годами не думать про безопасность телекоммуникационных систем, не подозревать, что компьютер атакован вирусом, который снимает конфиденциальную информацию или осуществляет подмену данных.

Другим распространенным случаем является недостаточное внимание аутентификации сотрудников. Также информационная безопасность телекоммуникационных сетей страдает из-за неограниченного доступа. Поскольку компьютерная техника на предприятии зачастую используется не одним, а несколькими сотрудниками, то либо система паролей вовсе не используется, либо пароли просты и открыты для всеобщего обозрения. Обычная

картина, когда пароль указан на бумажке, приклеенной к монитору. В отсутствие должного администрирования локальной сети сотрудники имеют доступ к информации, которая им не предназначена, когда сетевые диски, корпоративные почтовые ящики открыты для любого желающего сотрудника, а то и для посетителя организации.

Даже если у предприятия нет средств на приобретение минимального набора защиты телекоммуникационных систем, это не является оправданием, ведь снижение угрозы в самых типичных случаях достигается организационными и воспитательными мерами формирования культуры информационной безопасности на предприятии.

Литература:

<https://abiturient.tusur.ru/ru/napravleniya-podgotovki/ochnaya-forma-obucheniya/2018-10-05-02-informatsionnaya-bezopasnost-telekommunikatsionnyh-sistem-fulltime>

Нагорная Елизавета Дмитриевна
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В настоящее время современный человек не может представить свою жизнь без телевизора, радио, сотового телефона, а главное без компьютера. В современном мире персональный компьютер играет главную роль во всех сферах деятельности, во всех странах мира. Конечно, можно отметить, что еще несколько десятилетий назад, никто не пользовался ПК и при этом не имели никаких удобств, но мир не стоит на месте и необходимо идти «в ногу со временем».

Информационные технологии — широкий класс дисциплин и областей деятельности, относящихся к технологиям управления и обработки данных, в том числе, с применением вычислительной техники.

Информационная технология - совокупность методов, производственных и программно-технологических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации. Информационные технологии предназначены для снижения трудоемкости процессов использования информационных ресурсов.

Анализируя общее понимание информационных технологий, то можно выделить, что ИТ охватывает все области передачи, хранения, восприятия информации. Но в большинстве случаев ИТ ассоциируются с компьютерными технологиями, так как возникновения компьютеров вывело информационные технологии на новый уровень развития.

Существуют определенные этапы развития информационных технологий:

1. 1 этап (с начала 60 – 70-е гг.) – основным направлением являлась автоматизация рутинных действий человека, обработка данных в вычислительных центрах в режиме коллективного использования, в условиях ограниченных возможностей аппаратных средств, характеризуется проблемой обработки больших объемов информации.
2. 2 этап (70-е года) – появления персональных компьютеров, распространение ЭВМ серии IBM/360, ориентация на индивидуального пользователя, использование централизованных обработок данных, так и децентрализованного, который базируется на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.
3. 3 этап (80-е года) – компьютером начинают пользоваться непрофессионалы, создание информационных технологий, направленных на решение задач, одна из которых максимально удовлетворить потребность пользователя и создания соответствующего интерфейса работы в компьютерной среде.
4. 4 этап (90-е года) – создание современной технологии между организационных связей и информационных систем, организация защиты и безопасности информации, организация доступа к стратегической информации, выработка соглашений и установление стандартов, протоколов для компьютерной связи.

Информационная технология должна обеспечивать разделение всего процесса обработки информации на этапы, действия. При этом этапы, действия должны позволить эффективно осуществлять целенаправленное управление информационными процессами, то есть быть стандартизированы и унифицированы.

Классификация Информационных Технологий

Информационные технологии в различных сферах жизни имеют свою определенную классификацию.

По типу интерактивности информационные технологии делятся:

- с избирательной интерактивностью (технологии, которые обеспечивают хранение информации в структурированном виде, то есть пользователь работает с уже существующими данными. Пример: банки и базы данных, видео -, теле – текст, Интернет и др.)
- с полной интерактивностью (технологии, которые обеспечивают прямой доступ к информации, хранящиеся в информационных сетях или каких –

либо носителях. Дает возможность передавать, изменять и дополнять информацию).

Использовать, применять информационные технологии можно в различных областях: образование, культура, наука, производство, военное дело и др.

Для примера компьютерных и бескомпьютерных технологий рассмотрим область образования. К компьютерным информационным технологиям, которые предоставляют учебную информацию относятся технологии, которые используют компьютерные обучающие программы, мультимедиа технологии, технологии дистанционного обучения.

К числу бескомпьютерных информационных технологий предъявления учебной информации различаются бумажные, оптоэлектронные, электронноэлектронные технологии. Между ними есть отличие: средство предоставления информации и то, что оно делится на бумажные, оптические и электронные. Бумажные средства обучения это учебники, учебные и учебно – методические пособия. Оптические это кинопроекторы, диапроекторы, графопроекторы. К электронным средствам обучения относятся телевизоры и проигрыватели лазерных дисков.

Современные средства компьютерной техники также можно классифицировать:

- персональные компьютеры (развитие современных информационных технологий связано как раз с широким распространением с начала 1980-х гг. персональных компьютеров, в которых сочетается относительная дешевизна и широкие для непрофессионального пользователя функциональные возможности. ПК это наиболее многочисленные классы вычислительной техники).
- Корпоративные компьютеры (вычислительные системы, которые обеспечивают совместную деятельность большого количества интеллектуальных работников в какой либо организации. Сфера использования корпоративных компьютеров – деятельность в крупных финансовых и производственных организациях, организация обслуживания большого количества пользователей: бронирование и продажа билетов, биржевые и банковские системы)).
- Суперкомпьютеры (вычислительные системы, использующиеся в военной и космической отрасли, в фундаментальных научных исследованиях, в глобальном прогнозировании погоды).
- Мультимедиа (технология, которая позволяет использовать текст, графику, видео и мультипликацию в интерактивном режиме).
- Виртуальная реальность (технология неконтактного информационного взаимодействия, которая создается с помощью мультимедийной среды

иллюзию присутствия в реальном времени в стереоскопическом представленном «экранном мире». В виртуальном мире поддерживается иллюзия местна нахождения с помощью определенных предметов: вместо дисплея - очки телемониторы (воспроизводят непрерывно изменяющийся мир), управление – «информационные перчатки» (определяют направление перемещения пользователя относительно виртуальных объектов), устройство создания и передачи звуковых сигналов.

- Технология Интернет (WWW (от англ. World Wide Web - всемирная паутина)), предоставляют пользователям возможность выбора источника информации на серверах сети).

Современные Информационные Технологии

В настоящее время практически все организациям необходимо информационное обслуживание, переработка большого количества информации. Одним из главных техническим средством по передаче, восприятие, обработки информации является компьютер. Роль компьютера усилие интеллектуальных возможностей человека и общества в целом, служит для связи и передачи информации.

Основные характеристики новой информационной технологии

Методология	Основной признак	Результат
Принципиально новые средства обработки информации Целостные технологические системы Целенаправленные создание, передача, хранение и отображение информации	"Встраивание" в технологию управления Интеграция функций специалистов и менеджеров Учет закономерностей социальной среды	Новая технология коммуникаций Новая технология обработки информации Новая технология принятия управленческих решений

Начало 21 века отождествляется с появлением информационного общества. Компьютер в информационном обществе является составляющей частью.

Информационное общество — теоретическая концепция постиндустриального общества; историческая фаза возможного развития цивилизации, в которой главными продуктами производства становятся информация и знания. Отличительные черты: увеличение роли информации, знаний и информационных технологий в жизни общества; возрастание числа людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг в валовом внутреннем продукте; нарастающая информатизация общества с использованием телефонии,

радио, телевидения, сети Интернет, а также традиционных и электронных СМИ; создание глобального информационного пространства, обеспечивающего:

1 - эффективное информационное взаимодействие людей;

2 - их доступ к мировым информационным ресурсам;

3 - удовлетворение их потребностей в информационных продуктах и услугах.⁷

Информационному обществу компьютерные и телекоммуникационные технологии являются потребностью в существенном увеличении производительного труда в информационном секторе общественного производства.

Благодаря широкому распространению компьютеров и созданию Интернета люди могут общаться между собой чрез ПК.

Для большинства, Интернет- это распространенная и привычная глобальная сеть, которая уже используется как обыденный способ в получении, передачи информации. С помощью Интернета, компьютер становится настоящим средством связи. Каждый, кто имеет доступ к WWW, может получить всю необходимую ему информацию, а также передать ее по всему миру. World Wide Web (WWW) на Интернете – это самый демократичный носитель информации: с его помощью любой может сказать и услышать сказанное без промежуточной интерпретации, искажения и цензуры, руководствуясь определенными рамками приличия. Интернет обеспечивает уникальную свободу самовыражения личности и информации. Сейчас именно Интернет делает работу, бизнес более эффективным, чем раньше, так как люди имеют широкий доступ к получению любой информации, о чем раньше нельзя было сказать.

Нельзя не отметить тот факт, что информационные технологии имеют такую особенность устаревать и заменяться новыми: большой ЭВМ в вычислительном центре заменился на персональный компьютер на рабочем месте пользователя, телеграф на телефон, телекс на факс и электронную почту.

Конечно, за всем «не угонишься», но для организаций необходимо не отставать от своих конкурентов, поэтому со временем совершенствовать информационные продукты.

Если в процессе внедрения новой информационной технологии этому фактору не уделять должного внимания, возможно, что к моменту завершения перевода фирмы на новую информационную технологию она уже устареет и придется принимать меры к ее модернизации.

Заключение

Формирование и совершенствование информационных технологий является одним из главных факторов в обществе. Распространение ИТ преобразует жизнь людей, облегчает работу, дает больше свободного времени, приносит развитие в экономической, культурной, образовательной и других сферах.

Развитие информационно-телекоммуникационной инфраструктуры в масштабах страны – это необходимое условие для того, чтобы предприятия могли выйти на зарубежные виртуальные рынки, взять на вооружение самые передовые технологии электронного бизнеса, а создание общенациональных банков данных позволит сделать их привлекательнее для потенциальных клиентов, партнеров и инвесторов.

Информационная насыщенность не только изменила мир, но и создала новые проблемы, которые не были предусмотрены.

Современное общество наполнено и пронизано потоками информации, которые нуждаются в обработке. Поэтому без информационных технологий, равно как без энергетических, транспортных и химических технологий, оно нормально функционировать не может.

Литература:

https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8

***Паламарчук Владислав**
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ*

НАЙПРОСТІШИЙ СПОСІБ СТВОРЕННЯ САЙТІВ

В останні роки ми спостерігаємо стрімкий ріст популярності сервісів для самостійного створення веб-сайтів. Ці сервіси називаються конструкторами сайтів або платформами для створення сайтів.

Конструктор сайтів – це зручний інструмент для простого створення та редагування вашого власного сайту. Використовуючи його, ви отримаєте можливість швидко створити ресурс на базі готового шаблону.

Для того щоб користуватися конструкторів сайтів не треба мати якихось спеціальних знань. Також у вас не буде необхідності встановлювати додаткове програмне забезпечення або обладнання. Основний принцип роботи сайтбілдера – практично моментальне створення сайту, який пізніше можна буде редагувати. Це зручно, просто та ефективно.

Одним з перших конструкторів сайтів був проект Geocities, заснований у 1994 році. Після свого 5- річного існування був проданий компанії Yahoo! За

\$3.6 млн. На той час це була досить велика сума. Але після того як проект технічно застарів, він був закритий у 2009 році. З того часу ринок конструкторів веб-сайтів представлений більш, ніж 70 платформами. Ось деякі з них:

Сервіс BmShop за розумну плату надає своїм клієнтам можливість швидко створювати сайти інтернет-магазинів. Якщо вам потрібний потужний інтернет-магазин, ви не знайдете щось краще ніж BmShop.

Wix - широко відомий у всьому світі конструктор сайтів. Функціонал орієнтований, в першу чергу, на потреби початківців з нульовими знаннями сайтобудування.

uKit – конструктор з чітко позначеною сферою використання: створення сайтів для малого та середнього бізнесу.

Jimdo – довгоживучий міжнародний проект. Основною особливістю цього конструктора від інших є велика степінь захисту даних та безпеки сайту.

BigCommerce – один із найпотужніших платформ для онлайн продаж. Головним плюсом цього конструктора є можливість інтеграції з магазинами в Facebook, Google Shopping та торговими майданчиками Amazon, Ebay та інші.

Створення сайту за допомогою конструкторів має цілий ряд переваг в порівнянні із традиційним замовленням у веб-студії:

- 1) Швидкість розробки. Ви можете за одну годину створити ваш сайт.
- 2) Низька вартість. Вартість використання таких сервісів відносно не велика і на порядки нижча вартості послуг веб-студії.
- 3) Широкі функціональні можливості. Хороші конструктори дозволяють створювати сайти всіх типів.
- 4) Професійний супровід. Ви можете бути впевнені, що ваш сайт буде робити 24 години на добу і 7 днів на тиждень. За це відповідає ваш конструктор.
- 5) Людський фактор. Ви контролюєте усе, що відбувається з вашим сайтом. Але також у конструкторів є свої недоліки:
 - 1) Не завжди функціоналу вистачає для вирішення бізнес-завдань
 - 2) Дизайн, як правило, вибирається з готових шаблонів.
 - 3) Якщо бізнес виросте, то перенести сайт на свій хостинг або додати нові функції буде не просто.

Таким чином, створення сайтів за допомогою конструктора не є раціональним рішенням для використання в комерційних цілях, і тому створення бізнес-сайтів ефективніше здійснювати індивідуально або в професійній студії веб-дизайну.

Але, якщо ви хочете створити свій блог або сайт візитку це буде ідеальним варіантом для вас.

Також створення сайтів за допомогою конструктора буде корисним для тих хто тільки починає освоювати сайтобудування.

Джерела:

bit.ly/2AMcQwc
bit.ly/2Aoaa0
bit.ly/2jduI9s

Прокопенко Дмитрий Олегович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев

VSAT – СЕТЬ В САМЫХ ОТДАЛЕННЫХ ТОЧКАХ МИРА

В наше время интернет имеет очень большое влияние на общество. Ежедневно миллионы людей пользуются интернетом, что бы найти нужную им информацию. Это может быть погода, новости, песня, видео и все остальное. Люди, живущие в городах, не имеют никаких проблем с подключением интернета и нахождением сети. Но стоит перебраться в какую-нибудь отдаленную местность, у вас возможно начнутся проблемы. И к вам на помощь идет VSAT сеть.

VSAT (Very Small Aperture Terminal) – это станция спутниковой связи, предназначенная, главным образом, для надежного обмена данными по спутниковым каналам. Самое главное, что она не требует обслуживания и подключается напрямую к терминальному оборудованию пользователя, выполняя роль беспроводного модема.

История появления VSAT сетей начинается с запуска первых спутников связи. В конце 60-х годов в ходе экспериментов со спутником ETS-1 была создана экспериментальная сеть спутниковой телефонной связи на Аляске.

Сеть состояла из 25 земных станций, установленных в небольших поселках. Эксперимент оказался успешным и было принято решение о создании коммерческой сети телефонной спутниковой связи из 100 терминалов с использованием каналов на спутник « Интелсат ». В то время, самая маленькая спутниковая станция имела антенну диаметром 9 метров и стоила около 500 тыс. долларов. Заказчики же поставили условие, что антенны земных станций сети должны быть не более 4.5 метров, а цена не превышать 50 тыс. долларов. И такие станции были созданы фирмой California Microwaves.

В наше время технология VSAT является очень гибкой и позволяет создавать сети отвечающие самым жестким требованиям, предоставляющие широкий спектр услуг по передаче данных в любой комбинации. Двухсторонняя связь с спутником обеспечивает качественное интернет-соединение для отдаленных и малонаселенных районов мира. Во многих случаях они имеют неоспоримые преимущества перед наземными сетями.

Среди преимуществ VSAT можно отметить: низкую себестоимость, быстрое развертывание, высокое качество связи, простоту конфигурации и высокую надежность.

Но не стоит забывать, что спутниковая связь является разновидностью радиосвязи. Поэтому, теоретически, любая спутниковая станция, находящаяся в зоне обслуживания спутника, если она настроена на нужную частоту, на нужный временной интервал, поддерживает нужные протоколы и работает в нужном стандарте, могла бы перехватывать сигналы. Но, во-первых для этого должно соединиться слишком много факторов одновременно. Во-вторых, в спутниковых

системах связи используются мощные системы кодирования сигнала, что делает перехват практически невозможным. И не следует так же забывать, что такие же проблемы возникают в любом другом канале связи, не только в спутниковом.

Как и любая другая система радиосвязи, спутниковая связь может быть подвержена помехам от других радиосредств. Однако, с одной стороны, для спутниковой связи выделяются полосы частот, не используемые другими радиосистемами. А с другой стороны, в спутниковых системах используются узконаправленные антенны, которые позволяют полностью избавиться от помех.

Таким образом, большинство недостатков устраняются путем грамотного проектирования сети, выбора технологии и места установки антенн. Следует отметить, что любая система связи имеет свои недостатки и преимущества, и выбор той или иной технологии зависит от многих факторов.

Литература:

1. www.eraservice.ru/uslugi_svyazi/vsat/
2. www.altegrosky.ru/istoria-vsa

Соколов Валерий Витальевич
Государственный Университет Телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ИСПОЛЬЗОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ И ПОИСКА АВТОМОБИЛЕЙ

В настоящее время во всем мире намечается значительный рост интереса к системам, обеспечивающим автоматизацию контроля за перемещением автотранспорта.

В последнее время широкое распространение во всем мире получили системы и комплексы технических средств определения местоположения подвижных объектов. Эти системы используются на воде, суше и воздухе для слежения за объектами, определения их местоположения, корректировки маршрута и т.д. Они различаются по методам определения координат объектов, способам передачи информации между подвижными объектами и диспетчерскими пунктами, логикой построения и т.д. Однако во всех этих

системах логично виконується умово-можливість для споживача самостійно визначати її основні параметри:

- зону роботи системи;
- тип транспорту, який потребується контролювати;
- частоту оновлення інформації про рухомий об'єкт;
- перелік завдань, що вирішуються в системі.

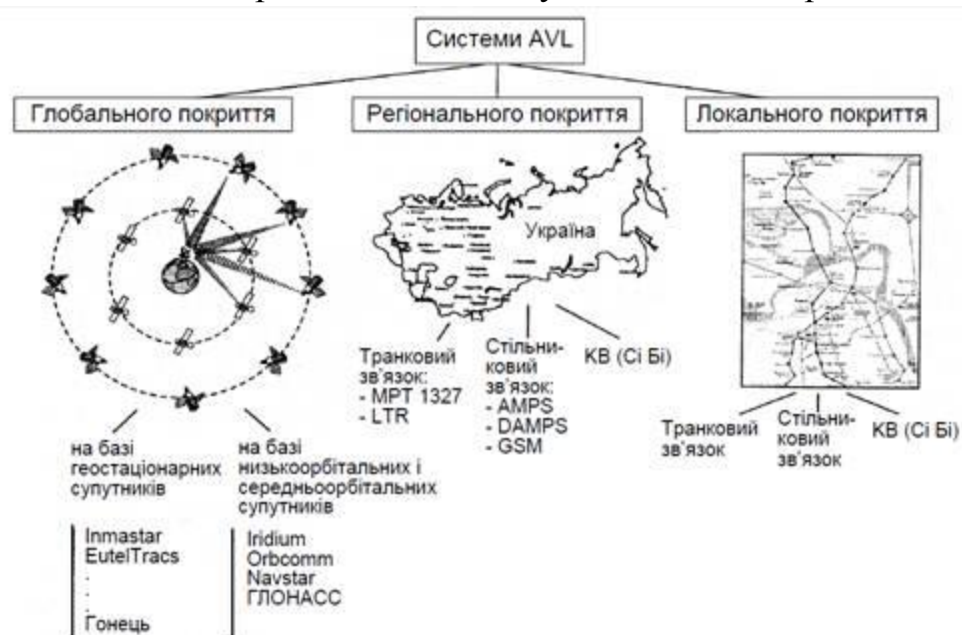
В наші часи найбільш актуальними є завдання автоматизованого визначення місцезнаходження рухомих об'єктів в складі комплексного забезпечення безпеки.

Сучасні системи автоматичного визначення місцезнаходження транспортних засобів-AVL, що виконують ці завдання, автоматично визначають координати транспортного засобу в групі йому подібних за масштабом його переміщення в межах визначеної території.

Система AVL зазвичай складається з підсистеми управління визначенням місцезнаходження, підсистеми передачі даних і підсистеми управління і обробки даних.

Класифікація і характеристика систем автоматичного визначення місцезнаходження

За територією охоплення системи визначення місцезнаходження транспортних засобів умовно логично розділити на наступні зони покриття:



-глобальну, яка охоплює земну кулю, материків або територій декількох держав;

-регіональну, обмежену, як правило, межами населеного пункту, області, регіону;

-локальну, яка розрахована на малий радіус дії, що характерно в основному для систем дистанційного супроводу і пошуку втрачених автомобілів.

Глобальная зона покрытия обычно требуется для контроля подвижных объектов, находящихся от диспетчерских пунктов на несколько тысяч километров. Поэтому наиболее приемлемое решение для реализации систем подобного масштаба - использование спутниковых каналов связи.

Их можно разделить на системы:

- на базе геостационарных спутников;
- на базе низко и среднеорбитальных спутников.

Основная масса систем контроля основана на использовании геостационарных спутников.

В этих системах время доставки информации составляем 5-15 минут в зависимости от организации диспетчерского пункта. Период обновления информации обычно 1 час.

В комплект подвижного объекта обычно входит:

- спутниковая станция;
- GPS антенна;
- бортовой компьютер;
- набор датчиков.

Габариты мобильного передатчика таковы, что он без проблем устанавливается даже на автомобиль. Бортовой компьютер обеспечивает автоматическую передачу навигационной информации на диспетчерский пункт по запрограммированной временной сетке или при возникновении нештатной ситуации. Точность местоположения составляет около 50 метров.

Классификация методов и AVL-систем показаны в данной таблице:

Таблица 5.1. Классификация методов и AVL-систем

Методы					
Методы навигационного счисления	Методы приближения (зонавые методы)		Методы определения местоположения по радиочастоте		
Пути реализации метода					
Системы с применением аппаратуры счисления пути и инерциальной навигации	Системы на базе радиометок	Системы на базе оптического распознавания	Системы на базе стационарной пеленгационной сети	Системы на базе мобильных пеленгаторов	Системы с применением аппаратуры радионавигации
Основные функции систем					
Вычисление координат текущего местоположения или траектории мобильного объекта относительно фиксированных известных реперов	Идентификация мобильных объектов при пересечении ими границ зоны		Определение относительного положения мобильного объекта, возможна идентификация объекта		Вычисление координат текущего местоположения или траектории мобильного объекта
Системообразующие элементы					
Аппаратура счисления пути Бортовой вычислитель Средства связи для передачи данных в центр обработки (УКВ-радиосвязь, сотовые системы связи, спутниковые системы связи) Накопители параметров маршрута Диспетчерские пункты со средствами электронной картографии	Активные, пассивные или полупассивные радиомаяки на мобильных объектах Контрольные пункты (КП) приема сигналов радиомаяков Диспетчерские пункты (ДП) Сети передачи данных: от КП до ДП и между ДП	Аппаратура считывания и распознавания индивидуальных признаков мобильного объекта (автомобильных номеров) на КП Диспетчерские пункты Сети передачи данных от КП до ДП	Активные радиомаяки на мобильных объектах Диспетчерские пункты со средствами электронной картографии Сеть пеленгаторов Сети передачи данных: от пеленгаторов до центров обработки и между ДП	Активные радиомаяки на мобильных объектах Аппаратура мобильной пеленгации Средства связи между пеленгующими автомобилями	Приемники сигналов наземных или спутниковых навигационных систем Бортовой вычислитель Средства связи для передачи данных в центр обработки (УКВ-радиосвязь, сотовые системы связи, спутниковые системы связи) Накопители параметров маршрута Диспетчерские пункты со средствами электронной картографии Средства вычисления дифференц. поправок
Основные области применения					
Системы поиска угнанных автомашин Диспетчерские системы контроля передвижения автомашин на территории города Системы контроля передвижения транспорта или груза на неограниченной территории в реальном времени Системы контроля передвижения транспорта или груза на неограниченной территории с последующей обработкой	Системы поиска угнанных автомашин	Системы поиска угнанных автомашин	Системы поиска угнанных автомашин Диспетчерские системы контроля передвижения автомашин на территории города	Системы поиска угнанных автомашин	Системы поиска угнанных автомашин Диспетчерские системы контроля передвижения автомашин на территории города Системы контроля передвижения транспорта или груза на неограниченной территории в реальном времени Системы контроля передвижения транспорта или груза на неограниченной территории с последующей обработкой

Методы определения местоположения можно разбить на три основных категории:

- методы приближения;
- методы навигационного счисления ;
- методы определения местоположения по радиочастоте.

Литература:

- 1.Автомобильные охранные системы. Справочное пособие. (Андрианов В.И., Соколов А.В.)
2. <http://www.shevchenkove.org.ua>

Стадник Денис Олександрович
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

ЗАСТОСУВАННЯ ІНФОРМАТИКИ В ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Анотація. Проведено аналіз технічного розвитку інформаційних систем та огляд сучасних технологій. Показано переваги вмілого використання новітніх технологій для інтелектуалізації всіх видів людської діяльності.

Мета: Метою цієї роботи є дослідження сучасного використання телекомунікаційних систем, таких як управління базами даних, електронними таблицями, що зменшує матеріальні та адміністративні витрати на виробництві та покращує соціально-побутові умови. Сучасні інформаційні технології суттєво полегшують роботу, підвищують конкурентоспроможність нових систем управління, не обмежувати користувачів у часі та просторі.

Інформатика, як складовий механізм розвитку інформаційних технологій

На сьогоднішній день людство володіє надзвичайно величезними інформаційними ресурсами. Розумне використання яких можливо лише за умови володіння сучасними інформаційними технологіями. Цілеспрямована організація сукупних інформаційних процесів з використання засобів комп'ютерної техніки забезпечить простий та ефективний обмін інформацією, який здійснюється за допомогою різноманітних мереж зв'язку.

Інформація виступає найважливішою складовою інформаційного суспільства і її роль сьогодні важко переоцінити. В зв'язку з виникненням комп'ютерів і інших пристроїв управління ми можемо отримувати, зберігати, перетворювати та передавати інформацію. В широкому розумінні інформацією називають відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх представлення.

Термін «інформатика» з'явився у вжитку в середині шістдесятих років для позначення області автоматичної переробки інформації в усіх сферах людської діяльності. Найдавнішим засобом передавання інформації була мова. Згодом інформацію почали передавати за допомогою матеріальних носіїв (наскальні малюнки, різьблення по кістках тварин, писанки, вишивки та інше. А з середини

19ст. інформація почала поширюватись з використанням радіомагнітних хвиль. Інформацію яку не було передано зникала разом носієм. Тому без засобів передачі інформації неможливе її накопичення, утворення знань, а отже існування суспільства.

Вдосконалення засобів обчислювальної техніки, систем телекомунікацій та інформаційних технологій не лише повною мірою виявляє свою виробничу, технологічну й соціальну корисність, а й поліпшує умови нашої праці і побуту. Незважаючи на вагомі досягнення в певних областях розробки, побудови окремих сучасних ланок зв'язку, фактично лише зараз, усвідомлено нагальну потребу для суспільства мати розвинені, сучасні та захищені системи зв'язку. Зазначу, що захищати інформацію потрібно не лише від зловмисників а й від випадкових втрат, що можуть статись через помилки в технічних системах. Ця проблема не може бути вирішена в повній мірі без підготовки спеціалістів належної кваліфікації.

Насправді фахівців, що впроваджують та використовують інформаційні технології дуже багато це і бізнес-аналітики, які спілкуються з замовниками програмного продукту та визначають вимоги до нього, програмісти які створюють цей програмний продукт, тестувальники або інженери з якості програмних засобів, які перевіряють як він працює.. Адже програмний продукт вирішує прикладні завдання для того, щоб робити кращою роботу в усіх сферах нашого життя.

Огляд мережевих технологій, їх пріоритет в певних галузях

Аналізуючи історію передачі інформації, таку як: голосова (телефонний зв'язок), відео (відео зв'язок, цифрове телебачення), текстова (електронні тексти, книги, послуги мережі Інтернет), можна зробити висновок, що і ці мережі, де використовувались окремі технології передачі даних, пройшли еволюційний процес, тобто об'єднання. Надання послуг засобами єдиної мультисервісної мережі, яка отримала назву NGN (Next Generation Network). Це мережа наступного покоління. Вона існує згідно з міжнародними стандартами та рекомендаціями щодо побудови, тому частково або повністю працює в багатьох країнах. Особливість її, що кількість послуг та типи інформації – не обмежені. Одним із перспективним напрямком розвитку мереж майбутнього є Future Networks (FN). Це ще більш безмежний та багатомірний віртуальний простір та масштабність віртуального часу. Перехід дозволить забезпечення до ще більшої якості обслуговування, враховуючи не тільки технічні особливості мережі, склад обладнання, а й тип інформації, що буде надаватися мережею. Проте й досі достатньо повної методологічної основи побудови та експлуатації мереж майбутнього створити не вдалося. Розробці необхідні міжнародні стандарти, але їм перешкоджають провідні виробники телекомунікаційного обладнання, які фактично впроваджують свої власні стандарти щодо протоколів, портів і т. ін.

Без швидкісного мобільного інтернету доступного зараз – неможливо. Відеохостінги, потокові сервіси, спілкування в месенджерах з функцією відеодвінків – все це потребує якісного швидкісного з'єднання. Саме тому, основна ціль створення стандарту 4G (LTE) є:

- збільшення швидкості мобільного зв'язку (до 100 Mb/s);
- зменшення вартості передачі даних;
- можливість надання спектру недорогих послуг.

Також, зв'язок 4 покоління передбачає використання цілого спектру технологій які раніше розвивалися паралельно. В мережі 4G весь трафік проходить через єдину архітектуру по протоколу IP, саме тому, базові станції в 4G стали більш інтелектуальними та самостійними, що дозволило організувати з'єднання між абонентами напряму.

5G- стандарт зв'язку наступного покоління, що буде підтримувати інтернет-речей (розумні автомобілі, будинки) та іншу техніку. У порівнянні з 4G швидкість стандарту 5G зросте у 50 разів, тобто до 5 GB/s.

Можливі приклади застосування:

1) Автомобілі будуть обмінюватися між собою інформацією (У разі аварії автомобіль, що знаходиться найблище до місця події повідомлять про нього всім машинам, що їдуть вслід. Це дозволить ним знизити швидкість чи у разі пробки, розрахувати маршрут).

2) В епоху 5G вся домашня електроніка буде взаємопов'язана (якщо раніше при переході з однієї кімнати в іншу доводилося переносити з собою портативні пристрій, щоб продовжувати, наприклад, слухати улюблену радіостанцію, то тепер, динаміки в різних кімнатах зв'яжуться між собою і прослуховування продовжиться з перерваного місця).

3) Також, можна буде стежити за споживанням енергії кожним пристроєм (чайник, праска, телевізор та інше.)

4) Використання 5G у службах порятунку (мережа 5G змінить екстрені служби, забезпечивши надійний зв'язок в екстрених ситуаціях і першочерговість повідомлень поліції та інших служби).

Стандарт 5G вимагає більш досконалого обладнання, антен, а також розширеного спектру частот. У США процес розподілу даного ресурсу вже почався. Очікується що за наступні 10 років швидкість мобільних мереж зросте ще в 1000 разів.

Комплекс технічних і програмних засобів сучасних телекомунікаційних і мережних технологій забезпечує роботу фахівця у єдиному інформаційному просторі. Дуже важливо вміти самостійно оцінювати засоби телекомунікаційної інфраструктури та аналізувати визначні зміни у менеджменті різних бізнесових сфер, що сталися внаслідок поширення інформаційних технологій, які призвели до появи:

1) електронного офісу - це технологія обробки інформації в установі електронними засобами (даних, документів, таблиць, текстів, зображень, графіків). Електронний офіс дозволяє ефективно вирішувати широкий спектр завдань, що стоять перед кожним підприємством, що прагне до оптимальних трудовитрат: скорочує операційні витрати на управління і прискорює прийняття рішень; знижує непередбачені/надмірні витрати; підвищує якість роботи з клієнтами, іншими підприємствами, включаючи звітні документи; підвищує

ефективність командної роботи (характерним прикладом такого є машинописні роботи. Наприклад: шаблон для підготовки документів).

2) електронної комерції - це термін, що відноситься до використання Інтернету для проведення комерційних операцій між підприємствами або між підприємством та споживачами. Одне з найважливіших завдань сучасної електронної комерції - заміна традиційного механізму торгівлі. При цьому передбачається, що клієнт попередньо вибирає товар, а з допомогою Інтернету проводиться операція продажу (добре розвиненими прикладами електронної комерції є: rozetka.ua, olx.ua).

3) корпоративних інформаційних системи — це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві (в корпорації) і поставляє інформацію для прийняття управлінських рішень. Тобто це управлінська ідеологія, що об'єднує бізнес-стратегію підприємства і новітні інформаційні технології (найпоширеніші корпоративні інформаційні системи: 1-C підприємство, Scala, Baan IV, "Галактика", R/3, Oracle Applications.).

4) багатовимірні інформаційні сховища з аналітичним обробленням даних - це особлива форма організації бази даних, що призначена для зберігання в погодженому вигляді інформації, що отримується на основі баз даних різних систем та зовнішніх джерел (Сховище даних (Data Warehouses, OLAP-системи).

Широко відомі такі основні сфери ефективного застосування телекомунікацій:

розрахунки за угодами (наприклад з цінними паперами на фондовій біржі) У розрахунках за угодами дані можуть негайно (або після накопичення і збереження) прийматися терміналами і передаватися з віддалених місць в центральний комп'ютер для обробки. Ці можливості телекомунікацій можуть використовуватися в офісах, торговельних складах, центрах постачання.

системи типу «запит/відповідь» (пошук інформації в Інтернеті — це слова, фрази або набір символів, що відображають основну думку, які користувач Інтернету вводить у спеціальне поле (рядок) пошуку з метою одержання інформації, що його цікавить. Запит обробляється пошуковою машиною, що знаходить у своїх базах дані адреси Web-ресурсів, у яких присутні ключові слова і клієнтові видаються результати пошуку.

автоматизації офісу із застосуванням телекомунікацій здійснюється шляхом підключення до корпоративної мережі офісних ПК та інших офісних пристроїв. Автоматизований офіс привабливий для менеджерів усіх рівнів керування у фірмі не тільки тому, що підтримує внутріфірмовий зв'язок персоналу, але також тому, що надає їм нові засоби комунікації з зовнішнім оточенням.

персональні послуги (база персональних даних клієнтів. Широко застосовується в усіх сферах життя: банківська інформація, медично-лікувальна, кредитна, користувач-послуги тощо.)

навчання (для доступу до електронного навчання, організації процесу навчання, успішності, методичних видань тощо).

Сучасні ІТ ноу-хау

Сьогодні світ перейшов на новий етап життя де головну роль диктують новітні технології, а мобільні додатки реалізуються у формі одержання найважливішої інформації прямо з екрану смартфона.

Інформаційний простір сьогодні багатий подіями, пов'язаними з:

Блокчейн – це база даних всіх операцій, які проводяться в системі. Організована вона у вигляді ланцюжка блоків інформації, в кожному з яких записана певна кількість операцій. При цьому кожний наступний блок містить в собі частину інформації попереднього блоку. В Україні пілотний проект застосування блокчейн в системі державного управління відбувається на ринку оренди та продажу державного майна. Онлайн-аукціон eAuction 3.0. – неспівмірна спроба позбавити процедуру аукціонів від брудних ігор. Система побудована так, що кожен користувач може в режимі реального часу бачити, хто бере участь в аукціоні і які умови пропонує. Можна також зібрати будь-яку інформацію про аукціони та їх учасників, проаналізувати їх поведінку їх цінові пропозиції. Найбільше блокчейн підходить для обліку активів і прав власності. У платіжних системах технологія дає можливість значно підвищити швидкість, прозорість і безпеку взаєморозрахунків, а, отже, знизити вартість транзакцій.

Біткоїн це, власне, перша і найвідоміша з безлічі інших віртуальна валюта. Походить від двох англійських слів – “bit” (мінімальна одиниця інформації) та “coin” (монета). Використовується для здійснення віртуальних платіжних операцій. Його ще називають криптовалютою. Головна її перевага — неможливість підробки. З точки зору економіки це – цифровий товар с обмеженою пропозицією. Його алгоритм побудований таким чином, що у системі може існувати не більше 21 мільйону одиниць. Незважаючи на таку порівняно невелику кількість монет, їх вистачає для здійснення щоденних розрахунків, оскільки 1 біткоїн ділиться на 100 мільйонів частин, що називаються «сатоші» на честь людини, що створила саму систему.

Фінтек хочеться зазначити - це революція в сфері мобільного банкінга. Спектр таких проектів безмежний – від онлайн і мобільних додатків до сфер трейдинга, обміна валют, керування особистими фінансами. Застосовуються в таких галузях, як онлайн-кредитування, грошові перекази та кредитні рейтинги. FinTech компанії порушують домінування великий гравців на ринку фінансових послуг.

Стартап - це тільки що створена компанія (можливо навіть не є юридичною особою), яка знаходиться на стадії розвитку і будує свій бізнес на основі нових інноваційних ідей, або на основі технологій, які нещодавно з'явилися. Найчастіше, характерними особливостями стартапу є брак фінансів. Основним ресурсом для створення нового стартапу служить якісна новаторська ідея.

Перспективи розвитку інформаційних технологій

Міжнародний союз електрозв'язку (МСЕ) – спеціалізована установа ООН у сфері глобального електрозв'язку, покликана здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв'язку та формулювати

рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг.

Поява нових послуг, а також зростаючі вимоги користувачів змушує власників телекомунікаційних мереж модернізувати своє обладнання. Аспект побудови мереж наступних поколінь передбачає визначення базових характеристик та можливостей регламентованих певними технологіями. Основною ціллю міжнародного союзу електрозв'язку є забезпечення і розширення міжнародного товариства на регіональному рівні використовуючи всі види зв'язку, покращення технічних засобів та ефективної експлуатації.

Технологічний процес – це процес виготовлення напівпровідних виробів та матеріалів, який складається з послідовних технологічних операцій, є частиною виробничого процесу. Сучасні технології в сфері технологічного процесу сприяють поліпшеним характеристикам (розміри, енергоефективність, робочі частоти та вартість). Особливе значення це має для процесорних ядер. На сьогоднішній день остання технологія яка доступна для користувачів – 10 нанометрів (Samsung Exynos 8895, Intel Xeon X26v4). Такі компанії як Samsung и Intel вже досягли технології 7 нанометрів, але звичайні користувачі зможуть оцінити її не раніше 2019 року. Щодо компанії Samsung, то віце-президент Хокью Кам відмітив те, що: «Багато виробників зіткнулися з труднощами при переході на процес 10 нанометрів, але компанія Samsung впоралася з цим завданням і буде надалі зменшувати елементи до 5 нанометрів.» Основною ціллю найменшого технічного процесу є більш швидка обробка інформації за рахунок зменшення енерговитрат.

Інтернет-речей - це глобальна мережа підключених до інтернету фізичних пристроїв оснащених сенсорами, датчиками передачі інформації. В найблищому майбутньому концепція об'єднання телефонів, пральних машин, чайників, навушників, світильників і всього іншого – нікого не здивує. В світі вже підключених до інтернету пристроїв більше ніж людей на землі. Але, нажаль, інтернет-речей реалізувати за 100 % зараз не можливо, оскільки він вимагає існування мереж нового покоління. (5G) У сучасній мережі (4G) час прийому передачі перевищує 10 м/с. що вкрай багато. Мережа 5G матиме час прийому передачі 1 м/с. Також, інтернет-речей вимагає пристроїв з низьким енергоспоживанням, високою надійністю та низькою ціною. Для того щоб реалізувати потенціал інтернету-речей потрібна тісна співпраця бізнесу, телекомунікаційних операторів та простих користувачів. Розвиток ринку буде залежати від безлічі факторів, але абсолютно точно, всім учасникам цього процесу доведеться змінюватися набагато швидше, ніж це відбувається сьогодні.

Висновки

Застосування відкритих інформаційних систем, розрахованих на використання всього масиву інформації, доступної в даний момент суспільству в певній його сфері, дозволяє удосконалити механізми управління суспільним устроєм, сприяє освіченості, підвищує рівень добробуту населення. Процеси, що відбуваються у зв'язку з інформатизацією суспільства, сприяють не тільки прискоренню науково-технічного прогресу, інтелектуалізації всіх видів

людської діяльності, а й створенню якісно нового інформаційного середовища соціуму, що забезпечує розвиток творчого потенціалу людини. Розвиток інформаційних технологій - шлях до майбутнього. ІТ і зв'язок стануть основою глобального суспільства, що повинно підняти його на новий ступінь розвитку.

Електронні ресурси:

1. journals.dut.edu.ua/index.php/communication/article/.../131..
2. <http://poradu.pp.ua/internet/32672-merezha-5g-oglyad-opis-ta-shvidkst-merezha-novogo-pokolnnya-5g.html>
3. [/pidruchniki.com/.../tehnologiyi_organizatsiyi_informatsiyi](http://pidruchniki.com/.../tehnologiyi_organizatsiyi_informatsiyi)
4. www.economy.nayka.com.ua/?op=1&z=2264
5. superstudent.com.ua/.../korporativn-nformaczjn-sistemi-kont
6. polka-knig.com.ua/article.php?book=419&article=21939
7. <http://axon.partners/uk/blog/what-is-a-blockchain-and-how-cryptocurrency-will-help-to-defeat-corruption-in-ukraine/>
8. <https://mozok.net/shcho-take-bitcoin>
9. <http://startuplife.by/fintech-startups.html>
10. https://3222.ua/article/scho_take_startap.html
11. [https://uk.wikipedia.org/wiki/Міжнародний союз електрозов'язку](https://uk.wikipedia.org/wiki/Міжнародний_союз_електрозов'язку)
12. <https://uk.wikipedia.org/wiki/techtprogress>

Панченко Владислав Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ГАЛУЗЬ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

Україна має потужну галузь зв'язку та інформатизації, доходи якої щороку зростають.

Так, лише за січень—квітень 2004 р. вони збільшилися на 53,3% у порівнянні з аналогічним періодом 2003 р. і склали 5,952 млрд гривень. 30% загальної суми доходів припадає на послуги міжміського, в тому числі й міжнародного, зв'язку. Обсяг цих послуг зріс до 1,787 млрд гривень. У 2,4 раза зросли доходи операторів мобільного зв'язку, які за наведений період склали 2,457 млрд гривень, а доходи операторів супутникового зв'язку зросли на 39,7% — до 9,5 млн гривень. Організації, які передають і приймають теле- та радіопрограми, отримали дохід у розмірі 164,2 млн гривень, що на 59,7% більше у порівнянні з чотирма місяцями 2003 р. У комп'ютерному зв'язку (передача даних та Інтернет) обсяги наданих послуг збільшилися на 42,5% — до 271,8 млн гривень.

Флагманом галузі зв'язку в Україні є ВАТ "Укртелеком", створене наприкінці 1993 р. Підприємство є лідером за обсягом і діапазоном послуг електрозв'язку. ВАТ "Укртелеком" володіє первинною мережею, магістральними та зоновими лініями зв'язку, надає всі види телекомунікаційних послуг — міжнародний, міжміський та місцевий телефонний зв'язок, проводове радіомовлення,

радіозв'язок, трансляцію теле- та радіопрограм, документальний електрозв'язок, відеоконференцзв'язок, супутниковий зв'язок, цифрові канали (в оренду), ATM/Frame Relay, ISDN, доступ до Інтернет.

Сьогодні це підприємство налічує у своєму складі 30 філій, у тому числі 27 регіональних.

У складі підприємства діють вертикальні структури з експлуатації первинної мережі зв'язку, місцевих мереж зв'язку та радіофікації, з обслуговування споживачів і продажу послуг.

БАТ "Укртелеком" є співзасновником ряду спільних підприємств, які функціонують на телекомунікаційному ринку України. До них належать: "Інфоком", "Утел", "Український мобільний зв'язок", "Елсаком Україна", "Телесистеми України" та "Телекомінвест".

БАТ "Укртелеком" забезпечує телефонним зв'язком 9 млн абонентів, на його телефонній мережі загального користування працюють 44 автоматичні міжміські телефонні станції, у тому числі 18 аналогових та 26 цифрових, а також 4 міжнародні центри комутації[1].

Засоби інформатизації освіти – це засоби нових інформаційних технологій із навчально-методичним, нормативно-технічним й організаційно-інструктивним матеріалом, що забезпечує їх педагогічно доцільне використання.

Нові інформаційні технології навчання – це методологія і технологія навчально-виховного процесу з використанням новітніх електронних і засобів навчання й, насамперед, ЕОМ. В умовах професійного ліцею для інтелектуального розвитку учнів важливо, щоб педагог не просто використовував ці засоби в процесі власної діяльності.

Нові інформаційні технології відкривають учням доступ до нетрадиційних джерел інформації, підвищують ефективність самостійної роботи, створюють цілком нові можливості для творчості, знаходження і закріплення професійних навиків, дають змогу реалізувати принципово нові форми і методи навчання.

Поява і широке впровадження у практику освіти такого поняття як «нова інформаційна технологія (НІТ)» пов'язано з появою і значним розповсюдженням комп'ютерів в освіті. Комп'ютер використовують як допоміжний засіб для ефективнішого вирішення вже існуючої системи дидактичних завдань. Змістом об'єкта засвоєння в комп'ютерній навчальній програмі цього типу є довідкова інформація, інструкції, обчислювальні операції, демонстрації тощо.

Література:

http://pidruchniki.com/12991010/politologiya/telekomunikatsiyi_merezhi_sistemi

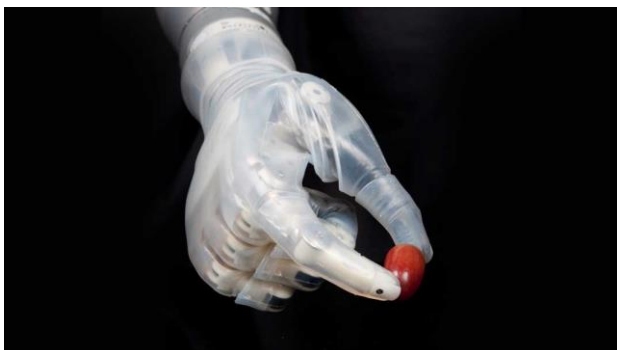
<http://www.startpedahohika.com/sotems-517-4.html>

БИОМЕХАНИЧЕСКИЕ ПРОТЕЗЫ

Сегодня тела людей сливаются с технологиями так, как мы и представить не могли несколько десятилетий назад. Сверхчеловеческая сила, ловкость и чувства перестали быть уделом научной фантастики — все это уже доступно обычному человеку. Несмотря на то, что новейшие технологии дают нам возможность увидеть возможности людей в будущем, в наши дни они наиболее полезны для людей, страдающих от инвалидности в том или ином виде. Технологии в буквальном смысле способны делать из людей киборгов, заменяя недостающие конечности, внутренние органы и органы чувств. Иногда они даже могут улучшить обычную функцию тела.

Протезирование — замена утраченных или необратимо повреждённых частей тела искусственными заменителями — протезами. Протезирование представляет собой важный этап процесса социально-трудовой реабилитации человека, утратившего конечности, или страдающего заболеваниями опорно-двигательного аппарата.

«Рука Люка»



LUKE Arm, она же «Рука Люка» (названная в честь Люка Скайуокера), — это высокотехнологичный протез, который позволяет владельцу осязать. Специальный мотор обеспечивает обратную связь, имитируя сопротивление, которое оказывают различные физические объекты — пользователь может почувствовать, что подушка обладает меньшим сопротивлением, чем кирпич. Электронные датчики получают сигналы от мышц пользователя, которые затем переводят в физическое движение. Носитель может одновременно манипулировать несколькими суставами при помощи переключателей, которыми можно управлять с помощью своих ног. Первая коммерчески доступная «рука Люка» станет доступна небольшой группе военных ампутантов в 2016 году.

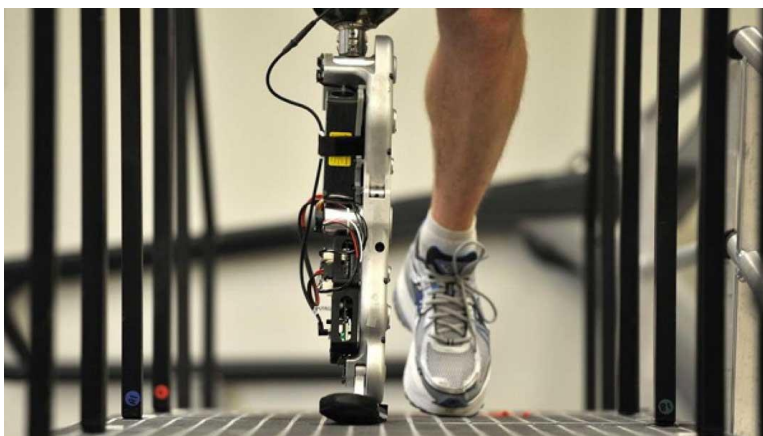
Рука bebionic



Компания по производству протезов bebionic создает самые современные протезы рук. Индивидуальные моторчики в каждом суставе движут каждой частью руки независимо. Для помощи в повседневном использовании у bebionic есть 14 заранее определенных схем захвата. Высокочувствительные двигатели меняют скорость и силу

захвата в режиме реального времени — они достаточно деликатны, чтобы пользователь мог удерживать яйцо между указательным и большим пальцем, и достаточно надежны, чтобы выдержать до 45 килограммов. Рука bebionic стала коммерчески доступна уже в 2010 году. За следующие семь лет модели лишь улучшались в отношении времени автономной работы, гибкости и программного обеспечения.

Бионическая нога, управляемая силой мысли



Управляемую силой мысли ногу впервые начал использовать Зак Ваутер в 2012 году, программный инженер из Сиэтла, которому ампутировали ногу выше колена в 2009 году. Технология, преобразующая сигналы мозга в физическое движение, называется TMR (Targeted Muscle Reinnervation)

и была создана в 2003 году для протезов верхних конечностей. Но протез Ваутера был в некотором роде революционным, потому что впервые заменил ногу. В 2012 году Зак Ваутер преодолел 2100 ступенек Уиллис-тауэр в Чикаго при помощи своего протеза ноги. Ему потребовалось 53 минуты и 9 секунд.

Итог: У 15% людей на планете есть нарушения функций и структур организма, которые препятствуют физической активности и мешают социальной жизни, и больше 50 миллионов человек в год становятся инвалидами. Благодаря современным материалам, сбалансированному размещению двигателей, датчикам силы прикосновения и вместительным аккумуляторам разработчики

протезов смогли создать бионические руки, ноги которые способны на большую часть повседневных действий.

Литература:

<https://geektimes.ru/post/276638/>

*Калинин Денис Павлович
Государственный университет телекоммуникаций
Факультет Телекоммуникаций
г. Киев*

ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ

Интерес к технологиям бесконтактной оплаты при помощи смартфона постепенно растет. Ведь многим нравится, что телефон решает разнообразные задачи. Теперь это не только звонки, мессенджеры, интернет и прочее, но и платежи. Сегодня люди больше боятся потерять телефон, чем кошелек, а насыщение устройства новым функционалом усиливает привязанность человека к этому предмету.

В плане безопасности бесконтактные платежи не менее надежны, чем контактные.

Как работает технология токенизации? В телефон заносится информация не оригинальной карты, которая находится у человека в кошельке (или выпущена виртуально) и зарегистрирована в соответствующей системе банка. Заносятся данные ее образа или, если использовать соответствующую терминологию, – токена (некой копии, которая не идентична оригиналу), вследствие чего компрометация данных в телефоне не является компрометацией данных реальной карты.

Технология токенизации, суть которой в подмене данных одной карты другими, где хранилищем выступает либо процессинговая система банка-эмитента, либо сама платежная система, являющаяся надежным хранилищем соответствий оригинальных карт их токенам, значительно повышает уровень безопасности транзакций.

Кроме того, бесконтактные платежи удобны, а потому их популярность будет со временем расти. Комфорт заключается не только в том, чтобы платить телефоном в торговой точке (как раз это многим потребителям не по душе). Гораздо важнее, что у этой технологии есть скрытый потенциал, о котором многие не знают, поскольку использование этого способа платежей в интернете еще не получило широкого распространения. Но именно здесь преимущества новой технологии становятся наиболее наглядными и очевидными.

Платя обычной картой, мы вбиваем ее данные (имя и фамилию владельца, срок действия, код), после чего начинается процедура вторичной идентификации владельца, как правило подразумевающая получение одноразового пароля и так

далее, что делает покупку длинной и не очень удобной. Безусловно, безопасность данного способа платежа не вызывает сомнений (эмитенты и эквайеры застрахованы от разнообразных мошеннических действий). Но поскольку предполагается, что для перевода денежных средств необходимо преодолеть несколько ступенек аутентификации, нередко происходят отказы от проведения платежа. Особенно часто это случается в европейских странах. Поэтому активно ищутся способы ухода от этой технологии для создания более простых и удобных форматов платежей в интернете.

Напротив, технология Apple Pay позволяет человеку, зарегистрировавшись в данном платежном сервисе или электронном кошельке, покупать товар в онлайн-магазине, который поддерживает такой способ оплаты, в один клик. Это необыкновенно быстро и удобно, и тот, кто хоть один раз попробовал воспользоваться этим сервисом, вряд ли захочет вернуться к прежним схемам.

Что значит «в один клик»? Покупатель выбирает товар, нажимает на кнопку «Apple Pay», тем самым идентифицируя себя и верифицируя оплату. Он не вводит никаких данных, никаких имен, никаких паролей, не зависит от надежности интернет-соединения, которое подчас рвется в случае длительного ожидания ответа от торговой точки или банка и пр. Особенно ярко эти преимущества раскрываются при проведении всей операции на смартфоне: в приложении или в интернете клиент и выбирает, и оплачивает покупки.

Конечно, карточные данные при этом «гуляют» по Сети, поскольку банк-эквайер обязательно должен получить ответ на свой запрос у банка-эмитента, но это данные не оригинальной карты, а токена (защищенной копии).

Таким образом, оплата покупок в интернет-магазинах с использованием технологий «... Pay» удобнее и проще, чем, скажем, 3D Secure с переводом вас на страницу банка-эмитента, где вы должны вбить руками код верификации, полученный по СМС или еще каким-то образом.

Эксперты ожидают многократного роста пользователей таких сервисов в ближайшие месяцы. Это не просто погоня за новизной – это упрощение, ускорение процедуры оплаты. Кроме того, передаваемые данные находятся под защитой, что особенно важно в современном мире. Платить при помощи бесконтактных технологий проще и безопаснее, чем посредством пластика. А ведь задача всех интернет-магазинов, задача самого общества потребления состоит в том, чтобы побудить людей платить, платить часто, много и чтобы им ничто не мешало это делать.

Наверняка новые технологии оплаты не заменят полностью «устаревающие», на это потребуется не один год. И о полном отказе от пластика речь, конечно, не идет. Да этого и не нужно, ведь жить на рынке должно то, что удобно пользователям.

Литература:

1. <https://www.vedomosti.ru>
2. <https://www.mastercard.ru>
3. <https://ru.wikipedia.org>

ЗАЩИТА ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ОТ «КРИПТОМАЙНЕРА»

Киберпреступники стали чаще использовать специальные вирусы и трояны для добычи криптовалют через чужие компьютеры. Под угрозой — не только серверы крупных компаний, но и домашние ПК, особенно с более мощной конфигурацией. Как же обезопасить себя в такое время? Как защитить свой персональный компьютер, и какие профилактические меры стоит проводить, чтобы защитить себя?

Как работают вирусы-майнеры и каким компьютерам угрожает опасность

За последний месяц "Лаборатория Касперского" обнаружила две крупные сети компьютеров, зараженных вирусами для майнинга криптовалют, — об этом говорится в сообщении компании. Одна из них насчитывает 5000 машин, вторая — около 4000, их большая часть находится в СНГ регионе.

В отличие от классических вирусов, которые просто крадут и пересылают информацию с компьютера, вирусы-майнеры используют его технические мощности. "По самым скромным оценкам, майнинговая сеть приносит своим владельцам до 30 000 долларов в месяц", — подсчитали аналитики. Самыми популярными криптовалютами у мошенников, по данным "Лаборатории", являются Monero (XMR) и Zcash.

Популярнее всего для атаки — игровые компьютеры: они больше подходят для добычи криптовалют, благодаря своим мощным процессорам и графическим видеокартам.

Как обезопасить свой компьютер от вируса

По данным "Лаборатории Касперского", у злоумышленников есть два способа заразить компьютер вирусом. Во-первых, они могут сделать это через установочные файлы рекламного ПО. Такие файлы пользователь сам скачивает с файлообменников — они маскируются под безопасные программы или ключи для активации лицензионной продукции. Во-вторых, вирусы могут атаковать сервер, используя уязвимости в программном обеспечении.

Для того чтобы избежать этой угрозы, следует соблюдать основные правила компьютерной безопасности. Установка антивируса — условие необходимое, но не достаточное. Кроме этого, необходимо соблюдать еще хотя бы три правила: вовремя обновлять свою операционную систему и используемые программы, не ставить никакое подозрительное ПО с файлами-распаковщиками и работать с правами пользователя, а не администратора.

Как понять, что компьютер все-таки заражен, и что делать

По словам директора по продуктовому и технологическому позиционированию компании Acronis, первый признак того, что вирус-майнер

проник в компьютер, — это снижение скорости его работы и увеличение потребления энергии. По его мнению, если компьютер защищен хорошим антивирусным ПО, оно должно заметить угрозу.

Также в этом случае нужно проверить диспетчер задач и просканировать систему антивирусами на трояны. Отчасти это верный подход, но если подумать – то это крайне поверхностные меры. Что бы удалить майнер наверняка, и окончательно, специалисты из компании «Лаборатория Касперского» также советуют отформатировать жесткий диск, и заново установить ОС.

Литература:

<https://ria.ru/economy/20170907/1502026690.html>

<https://bitnovosti.com/2017/08/16/skritiy-mayning-nayti-unichtojit/>

*Король-Королевський Кірілл Андрійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ*

ГОТОВНІСТЬ СВІТУ ДО БЕЗКОНТАКТНОЇ ОПЛАТИ

Навіть зараз, спостерігаючи за процесом оплати в гіпермаркеті або на терміналах оплати зв'язку, можна бачити, що перехід до безконтактного грошового обороту в Україні йде нешвидко - більшість, навіть молоді люди вважають за краще носити в кишені купюри і монети, а магазини періодично вивішують таблички з вже трохи дратівливим оголошенням «Карти не приймаємо». Так чи готові ми зустріти майбутнє, яке вже тут?

Судячи за даними одного цікавого дослідження - так, готові.

Компанія PRIME Research провела третє щорічне дослідження Mobile Payments Study, щоб виявити мінливе ставлення споживачів до цифрових платежів і мобільних рішень. Було проаналізовано понад 19 100 000 коментарів соціальних медіа за 2014 рік у таких джерелах, як Twitter, Facebook, Instagram, Weibo (Китай), Google+, YouTube і на форумах. Дослідження охопили споживачів на 56 ринках в Північній і Південній Америці, Європі (в тому числі в Україні), Африці, Азії і Тихоокеанському регіоні і виявило понад 8 мільйонів обговорень на ці теми, включаючи коментарі споживачів і обговорення новин.

Результати дослідження були оприлюднені навесні 2015 року. Вони показують не тільки значне зростання кількості дискусій, а й зміну їх тону і спрямованості - стало більше позитивних коментарів. Ось деякі висновки дослідження:

Ставлення до цифрових платежів продовжує поліпшуватися. У 2014 році позитивними були 94% обговорень цієї теми по всьому світу, у порівнянні з 77% в 2013 році і 70% в 2012 році.

Найбільше позитивних обговорень присвячені інноваціям, привілегіям і бонусам, а також зручність мобільних платежів (91% повідомлень за цими темами позитивні).

Безпека платежів - одна з лідируючих тем за кількістю позитивних повідомлень. Споживачі сприятливо відгукувалися про безпеку платежів в 91% випадків. У 2012 році ця тема викликали найбільше негативу.

Нерозуміння і сумніви в безпеці платежів, зафіксовані в дослідженнях 2012 і 2013 років, змінилися позитивними відкликання.

Істотну роль у зміні настроїв споживачів зіграли токенизація і біометричні технології, ключові теми обговорень в 2014 році.

Фокус уваги змістився на переваги, які надають інновації в мобільних платежах.

Незважаючи на те, що безпека платежів обговорювалася найбільш позитивно, таких дискусій було небагато. Розмови про цифрові інновації та нові можливості для користувачів, які використовують мобільні та інші підключення до інтернету, в 2014 році стали найпопулярнішими серед зацікавлених учасників дискусій (їм присвячені 71% обговорень).

Зручність мобільних платежів стало найпопулярнішою темою позитивних повідомлень (94% відгуків - позитивні). З найбільшим ентузіазмом користувачі розповідали в соцмережах про конкретні придбання, скоєних за допомогою мобільних пристроїв, і особливо в тому, як вони робили повсякденні покупки.

Крім зручності, Обговорюючи нововведення в мобільних платежах, користувачі також часто згадували бонуси, наприклад купони, програми лояльності та бали (24% коментарів від усіх зацікавлених сторін). Мобільна оплата стає більш привабливою, якщо надаються додаткові привілеї (58% розмов на цю тему почали споживачі).

Зрозуміло, що користувачі по всьому світу дозріли для того, щоб зустріти нові платіжні можливості. У свою чергу, в платіжних систем і технологій, є майбутнє, в яке можна дивитися зі сміливим оптимізмом і впевненістю в затребуваності.

Література:

<https://newsroom.mastercard.com/press-releases/new-global-retail-study-reveals-consumer-demand-for-new-ways-to-pay/>

Свиридов Дмитрий

Государственный университет телекоммуникаций

Факультет телекоммуникаций

г. Киев

РОБОТ – ПЕРВЫЙ ПОМОЩНИК ЧЕЛОВЕКА

Робототехника— прикладная наука, занимающаяся разработкой автоматизированных технических систем и являющаяся важнейшей технической основой интенсификации производства.

Робототехника опирается на такие дисциплины, как электроника, механика, телемеханика, мехатроника, информатика, а также радиотехника и электротехника. Выделяют строительную, промышленную, бытовую, медицинскую, авиационную и экстремальную (военную, космическую, подводную) робототехнику.

Робот – это автоматическое устройство, созданное по принципу живого организма, запрограммированное на то или иное действие.

- Манипуляционный робот — автоматическая машина (стационарная или передвижная), состоящая из исполнительного устройства в виде манипулятора, имеющего несколько степеней подвижности, и устройства программного управления, которая служит для выполнения в производственном процессе двигательных и управляющих функций. Такие роботы производятся в напольном, подвесном и порталном исполнениях. Получили наибольшее распространение в машиностроительных и приборостроительных отраслях.

- Мобильный робот — автоматическая машина, в которой имеется движущееся шасси с автоматически управляемыми приводами. Такие роботы могут быть колёсными, шагающими и гусеничными (существуют также ползающие, плавающие и летающие мобильные робототехнические системы).

Системы управления:

Под управлением роботом понимается решение комплекса задач, связанных с адаптацией робота к кругу решаемых им задач, программированием движений, синтезом системы управления и её программного обеспечения.

По типу управления робототехнические системы подразделяются на:

Биотехнические:

- командные (кнопочное и рычажное управление отдельными звеньями робота);
- копирующие (повтор движения человека, возможна реализация обратной связи, передающей прилагаемое усилие, экзоскелеты);
- полуавтоматические (управление одним командным органом, например, рукояткой всей кинематической схемой робота);

Автоматические:

- программные (функционируют по заранее заданной программе, в основном предназначены для решения однообразных задач в неизменных условиях окружения);
- адаптивные (решают типовые задачи, но адаптируются под условия функционирования);
- интеллектуальные (наиболее развитые автоматические системы);

Интерактивные:

- автоматизированные (возможно чередование автоматических и биотехнических режимов);
- супервизорные (автоматические системы, в которых человек выполняет только целеуказательные функции);
- диалоговые (робот участвует в диалоге с человеком по выбору стратегии поведения, при этом как правило робот оснащается экспертной системой, способной прогнозировать результаты манипуляций и дающей советы по выбору цели).

Среди основных задач управления роботами выделяют такие:

- планирование положений;
- планирование движений;
- планирование сил и моментов;
- анализ динамической точности;
- идентификация кинематических и динамических характеристик робота.

Области применения:

- Образование;
- Промышленность;
- Медицина;
- Сельское хозяйство;
- Космонавтика;
- Спорт.

Преимущества и недостатки роботов

Роботы часто совершают тяжёлые или вовсе невыполнимые для человека задачи. Их просто нужно запрограммировать на решение задачи, задать им все переменные, и они вычислят ответ. Если представить всё это упрощённо, то это сродни калькулятору – ты вводишь данные, и за тебя всё делают.

Роботы не знают усталости и могут работать хоть круглые сутки, главное, чтобы хватило заряда батареек. А про эффективность роботов не следует и говорить – то, что у людей может занять год работы, робот выполнит за месяц.

Роботы гораздо выносливее и сильнее человека, поэтому часто, там, где человек не может справиться используют роботов.

Роботы обладают возможностями гораздо выше человеческих способностей, поэтому так часто нами применяются.

Однако, уповая на возможности и безотказность роботов, неправильно думать, что всё за нас они будут делать, это чревато многими неприятными и даже фатальными последствиями.

Во-первых, мы тогда потеряем свой интерес к жизни, зачем он нам, если мы просто будем потребителями и пожинать плоды трудов роботов. Можно спокойно сидеть, есть, спать, ничего не делать, не ходить на работу, не найти вторую половинку, не создать семью.

Во-вторых, мы рискуем деградировать. Если труд сделал из обезьяны человека, то отсутствие его может повернуть процесс вспять.

Ну и в-третьих, мы рискуем полностью исчезнуть как вид. Зачем слабые люди на планете Земля, если есть сильные роботы?

Это лишь те немногие последствия, которые мы можем ощутить, если полностью делегируем свои полномочия роботами. Мы должны быть их «хозяевами», а не завесить от них. Роботы лишь помощники в нашей жизни, но никак не больше, и нам надо это понимать.

Литература:

1. <https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B1%D0%BE%D1%82%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B0>
2. <http://your-happy-life.com/robotyi-v-nashey-zhizni/>

Михайловский Александр Ильич
Государственный университет телекоммуникаций
Факультет телекоммуникаций
г. Киев

ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПРОВОДНЫХ СЕТЕЙ РЕГИОНАЛЬНОГО УРОВНЯ

IEEE 802.22 WRAN — стандарт беспроводных региональных сетей, описывающий двухуровневую архитектуру (уровень RNY и уровень MAC) с многоточечным (Point-to-Multipoint) соединением. Сеть предназначена как для работы с профессиональными фиксированными базовыми станциями, так и с портативными (либо фиксированными) пользовательскими терминалами (модемами). Обмен данными по стандарту производится на «свободных» частотах ОВЧ/УВЧ (VHF/UHF) телевизионного вещания. По утверждению разработчиков, сеть в основном предназначена для использования в малонаселённых пунктах, а также сельской местности, где вероятнее всего будет достаточное количество свободных каналов в рабочей полосе частот стандарта.

Уникальные особенности данного стандарта:

- относительно низкий уровень производственных и ионосферных шумов;
- разумные габариты антенн для эффективного приема и передачи сигнала;
- хорошие характеристики распространения сигнала в условиях прямой видимости;

- идеальная возможность для обеспечения больших зон покрытия, особенно в пригороде и сельской местности.

Основные характеристики стандарта:

- ***Назначение:*** широкополосный беспроводной доступ к Интернету для сельской местности.
- ***Ядро:*** технология когнитивной радиопередачи, предназначенная для безлицензионного использования частот телевизионного диапазона.
- ***Целевая аудитория:*** промышленность, правительство и управляющие органы, академические организации, провайдеры.
- ***Проекты:*** IEEE 802.22.1, IEEE 802.22.2
- ***Портативность:*** можно использовать в движении до 114 км/ч
- ***Топология сети:*** многоточечная (Point-to-Multipoint)
- ***Радиус зоны покрытия:*** 10-100 км (для фиксированной базовой станции и модема)
- ***Максимальная скорость:*** до 22 Мбит/с
- ***Мощность излучения:*** 4 Вт (под мощностью излучения понимается эффективная изотропно излучаемая мощность, EIRP)
- ***Антенны:*** на базовой станции используется ненаправленная (либо секторная) приемопередающая антенна, а на стороне абонента направленная антенна с 14 дБ подавлением заднего лепестка; помимо этого, есть ненаправленная антенна для сканирования частотного диапазона (когнитивная радиосвязь).
- ***Геопозиционирование:*** GPS или наземное (необходимо для функционирования системы).

Использование когнитивных технологий в IEEE 802.22.

Концепция когнитивного радио впервые была представлена в 1999 и с тех пор получила значительное развитие. Одним из направлением развития когнитивных технологий является область динамического доступа к спектру, в котором сеть когнитивного радио динамически определяет и использует часть спектра, которая не используется другими системами. Эти неиспользуемые участки спектра получили название «белые пятна». «Белые пятна» могут состоять из неиспользованных частот или временных интервалов в данном месте. В IEEE 802.22 под «белыми пятнами» обычно понимаются неиспользуемые каналы телевидения на данной территории, то есть частотные промежутки между зонами покрытия.

Когнитивная радиосистема — самоорганизующаяся радиосистема с динамическим доступом к радиочастотному спектру, которая способна познавать свою эксплуатационную и географическую среду, адаптировать к ней свои функциональные параметры и протоколы и/или изменять свою эксплуатационную среду за счет накопленных в процессе функционирования знаний и приобретенных навыков, с учетом установленных регуляторных политик и своего функционального состояния.

Существует несколько методов, которые могут быть использованы когнитивной радиосетью для анализа спектра окружающей среды. В стандарте IEEE 802.22 применяется метод геолокации/базы данных и сканирования частотного спектра. В первом методе используется информация о расположении когнитивных устройств в сочетании с базой данных лицензированных передатчиков, что позволяет определить, какие каналы локально доступны для их повторного использования. В рамках спецификации предполагается применять спутниковое или наземное позиционирование. Расположение базовой станции должно быть известно с точностью до 15 м, а оборудования пользователя с точностью до 100 м.

Сканирование частотного спектра в анализе используемого спектра и определении, какие каналы заняты лицензированными передатчиками. Эта процедура проходит в обязательном порядке при включении нового оборудования в сеть. Кроме того, сканирование частот происходит периодически при работе системы. Управление сканированием осуществляется базовой станцией, которая не только посылает управляющие команды пользовательскому оборудованию, но и сама осуществляет сканирование частот. Такая система позволяет актуально поддерживать информацию о состоянии радиоканала во всей зоне покрытия базовой станции и при необходимости своевременно менять рабочие частотные каналы.

Таким образом, управление спектром в стандарте IEEE 802.22 – это когнитивная функция на базовой станции, которая использует входные данные от функции сканирования спектра (SSF), геолокации, и действующей базы данных, чтобы принять решение о частотном канале который будет использоваться, а также ограничения на излучаемую мощность, которые накладываются для конкретного пользовательского устройства.

Требования к антеннам

Все узлы в сети IEEE 802.22 используют два типа антенн – направленные антенны для передачи данных и антенны сканирования.

На базовых станциях, для передачи данных, используются обычные для систем мобильной связи антенны – секторные или всенаправленные. У пользователей применяются направленные антенны с коэффициентом усиления до 14 дБ. Антенны сканирования это всенаправленные антенны, обеспечивающие чувствительность к вертикальной и горизонтальной поляризации, что позволяет воспринимать сигнал от телевизионных станций и беспроводных микрофонов. У пользователя такая антенна должна быть установлена вне помещения на высоте 10 м над уровнем земли.

Существенным недостатком стандарта IEEE 802.22 является невозможность поддержки технологий множественных антенн (MIMO) и формирования диаграммы направленности. Это связано с тем, что в диапазоне частот 54-862 МГц физически сложно обеспечить достаточное разнесение нескольких антенн, которое должно составлять не менее трех длин волн (то есть более 3 метров на средней частоте).

Перспективи розвитку в Україні

В нашій країні дуже багато вільних ТВ каналів, особливо в сільській місцевості, а з 2015 року їх стало ще більше, так як були відключені аналогові телеканали, залишилися тільки цифрові. Але, за думкою фахівців, використовувати цю технологію краще в місцях, де немає прямої видимості до базових станцій, що працюють в діапазонах 2.4 і 5 ГГц, тобто використовувати разом з 2.4 і 5 ГГц. Така конфігурація є найпродуктивнішою. Але поки що це тільки припущення. Цей питання потрібно піднімати на вищому рівні, потрібен спеціальний закон, що дозволить виділяти відповідні частоти для подібного використання, а цим поки ніхто не займається.

Список літератури:

1. https://en.wikipedia.org/wiki/IEEE_802.22
2. <http://asp24.com.ua/blog/standart-ieee-802-22-tehnologii-primenenie-perspektivy/>
3. <http://netobzor.org/stati/4131-chto-takoe-super-wi-fi-ili-ieee-802-22>

Щербина Анастасія Олегівна
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

СМАРТФОНИ МАЙБУТНЬОГО

Інтелект смартфона майбутнього зросте багаторазово, апарат, аналізуючи досвід використання, буде передбачати бажання господаря і пропонувати запуснути саме той набір додатків, який в даний момент необхідний.

Смартфон майбутнього стане головним джерелом довідкової інформації, в нього буде інтегрована світова база грамоти. Розумний комунікатор буде виправляти орфографічні, синтаксичні і навіть стилістичні помилки. У цьому хмарному сервісі буде зосереджена інформація про всі мови планети, так що завдяки апарату у власника смартфона майбутнього більше не буде мовних проблем при перетині кордону.

Уже зараз багато людей використовують перекладач Google для живого спілкування. Проте еволюція програм розпізнавання та обробки мови і потужний вбудований процесор зроблять смартфон комунікатором-перекладачем. За допомогою SPF люди різних мов зможуть спілкуватися один з одним не вдаючись до послуг перекладачів - людей, просто розмовляючи через чудо-комунікатор.

Дизайн

Смартфони майбутнього однозначно не матимуть звичну сьогодні форму плитки шоколаду. По закінченню декількох років екрани смартфонів і зовсім стануть гнучкими, кажуть фахівці цієї сфери. При цьому вони зможуть не тільки згинатися і стискатися, але і скручуватися в різні боки, причому не просто так, а для виконання певних дій. Наприклад, щоб отримати електронну пошту потрібно

буде зігнути правий кут, а щоб подивитися смс-повідомлення - лівий. Смартфон можна буде просто обернути навколо зап'ястя і носити як годинник. В цілому, пристрої, які придуть на зміну нинішнім смартфонам, і будуть більше нагадувати «розумні» годинник, але тільки з розширеними в рази телефонними і розважальними функціями.



Відмова від SIM-карт

Швидше за все, через якісь кілька років ми все забудемо про SIM-картах. Уже сьогодні корпорації Apple і Samsung почали впровадження нового стандарту e-SIM, при якому сімки вже вбудовані в смартфон, тобто віртуальні. Вибір оператора та тарифу проводиться за рахунок налаштувань в меню телефону, як і будь-яка інша функція.

Управління

У найближчому майбутньому віртуальні кнопки на сенсорних екранах стануть відчутними. Тобто, користувач буде відчувати, ніби вони реальні, відчувати їх межі, тактильну віддачу при натисканні і т.д. вважається, що так буде простіше управляти смартфоном, а екран стане більш інформативний. Експерти провідних корпорацій припускають, що смартфони майбутнього будуть оснащені технологією безконтактного управління. Тобто, ними можна буде керувати силою думки і поглядом. Вже зараз ведеться розробка операційної системи, що дозволяє розблокувати екран рухом сітківки ока або посмішкою господаря.

Функціонал

В Intel заявили, що через десять років у них з'явиться 48-ядерний процесор, який відкриє абсолютно нові можливості перед користувачами в частині споживання мобільних ресурсів. А в Samsung повідомили, що вже через сім років в Кореї буде розгорнута 5G-мережу, що дозволяє завантажувати фільм високої якості за кілька секунд. Словом, близький той день, коли різниця між комп'ютером і смартфоном в продуктивності стане практично непомітною. Щоб забезпечити стабільну роботу смартфона з 48-ядерним процесором і 5G-

модулем, доведеться розробити літій-іонні акумуляторні батареї з ємністю більшою, ніж сьогоднішня, в дві тисячі разів. А значить, на зарядку смартфонів знадобиться кілька секунд.



Але це далеко не всі можливості смартфонів майбутнього. Вкрасти такий апарат буде просто неможливо, адже в руках чужої людини він просто відмовиться працювати, а свого господаря буде легко розпізнавати за манерою мови або тембром голосу.

Література:

1. <https://inshe.tv/tehnologii-2/2017-07-16/247606/>
2. <http://it-tehnolog.com/zalizo/smartfoni-maybutnogo>

Лукандій Петро Іванович

Держаний університет телекомунікацій

Факультет телекомунікацій

м.Київ

ПЕРСПЕКТИВИ ПОЯВИ 5G В УКРЇНІ

Тема зв'язку п'ятого покоління була однією з основних на Всесвітньому мобільному конгресі, що минув нещодавно в Барселоні – головній події в області телекомунікацій.

Давайте з'ясуємо, що ж таке 5G. Як стандартизованої технології, 5G ще не існує. Є рекомендації Міжнародного союзу електрозв'язку (ITU), в яких описано, яким критеріям має відповідати зв'язок п'ятого покоління (IMT-2020). Згідно із початковим планом ITU, розробка стандарту повинна завершитися до 2020 року. Після цього можна очікувати перші приклади комерційного впровадження мереж п'ятого покоління. Деякі експерти прогнозують, що цей процес пройде швидше і стандарт буде готовий вже в 2018 році.

У якомусь сенсі 5G – це еволюційний стрибок у розвитку мобільних технологій. Якщо попередній розвиток йшов в основному по шляху збільшення швидкості передачі даних в мобільних мережах, то 5G ставить перед собою інші завдання.

Шведський телеком-гігант Ericsson морально готує європейських операторів і абонентів до того, що в 2020 році комерційне використання 5G стане

неминучою потребою сучасного високотехнологічного суспільства. Як повідомив на прес-брифінгу Афіф Оссейран, представник Ericsson, експоненціальне зростання трафіку в мережах, розвиток нових технологій та бізнес-моделей в найближчому майбутньому призведе до того, що можливостей 3G і 4G виявиться недостатньо. Вихід один – уже зараз необхідно розробляти і затверджувати концепцію будівництва мереж п'ятого покоління.

З цією метою офіційні особи Європейського союзу ухвалили рішення створити робочу групу під назвою METIS («Mobile and wireless communications Enablers for the Twenty – twenty Information Society» – «Способи реалізації мобільного і бездротового зв'язку в інформаційному суспільстві 2020»). До неї увійшли п'ять виробників на чолі зі шведською Ericsson, 5 операторів зв'язку, 13 науково-дослідних організацій та один автомобільний гігант. Координатором проекту став Афіф Оссейран.

В 2018-2020 очікується розгортання перших некомерційних мереж 5G для дослідної експлуатації. Комерційний запуск мереж п'ятого покоління відбудеться не раніше 2020 року.

Варто відзначити, що METIS далеко не перший проект у світі, який займається розробкою концепції мережі 5G, тому в рамках спільних конференцій і форумів він активно переймає досвід більш ранніх проектів, запущених в декількох країнах Південно-Східної Азії. Зокрема, у Південній Кореї питаннями впровадження 5G займається асоціація 5G Forum, в Китаї – група IMT-2020 Promotion Group, в Японії – ARIB 2020 Beyond AdHoc.

Примітно, що на відміну від технологій 3G і 4G, основною перевагою стандарту 5G, зі слів Афіф Оссейрана, є не швидкість передачі даних (хоча і передбачається, що вона буде значно вища, ніж в 4G), а сукупність технічних рішень, які виведуть мобільний ШПД на принципово новий якісний рівень.

Так, зі слів координатора METIS, мережа 5G повинна задовольнити потребу в більш високій швидкості передачі даних, яка буде обумовлена зростанням споживання потокового відео, використання файлообмінних мереж і хмарних сервісів. В офісних приміщеннях і міському середовищі, де щільність звернень до мережі найбільш висока, мережа повинна забезпечувати швидкість передачі даних в кілька гігабіт на сек.

Мережа п'ятого покоління також має забезпечити доступність всім підключеним пристроям. Вже сьогодні в мережах у всьому світі працюють більше 5 млрд мобільних пристроїв. Очікується, що в майбутньому ця кількість зросте в 10-100 разів. І разом із зростанням кількості пристроїв, що підключаються, будуть значно зростати і вимоги до мережі з точки зору її доступності.

Ступінь мобільності підключених до мережі пристроїв, на думку Афіф Оссейрана, є одним з найбільш серйозних викликів: «Технологія 5G повинна забезпечувати безперебійну роботу пристроїв, що знаходяться як на борту автомобілів, так і поїздів».

В цілому експерти Ericsson відзначають збільшення кількості підключених пристроїв і загальна тенденція така, що «в кінцевому підсумку буде підключено

все, що може виграти від підключення до мережі, починаючи від світлофорів, побутової техніки до автомобілів, медичного устаткування і систем електропостачання». Технологія 5G покликана забезпечити такі підключення, а це в свою чергу відкриє практично необмежені можливості для людей, бізнесу та суспільства.

Очевидно, мобільний зв'язок п'ятого покоління створить в Європі нову систему координат для появи нових сегментів ринку, які в мережах 3G і 4G неможливі в принципі. Європейські чиновники прекрасно розуміють, що крім багатомільярдних інвестицій в 5G економіка Євросоюзу стане майданчиком для створення нових типів бізнесу, що означатиме появу нових робочих місць і мільярдні податкові надходження.

Існують і інші очікування: більш ефективне використання радіочастотного ресурсу, підвищення ефективності енергоспоживання та ін. Як ми бачимо, для різних сценаріїв використання мобільного зв'язку потрібна різна комбінація параметрів. Наприклад, для перегляду відео високої чіткості на мобільному телефоні важлива швидкість передачі даних. Для самокерованих автомобілів критичним є час затримки сигналу. А для датчиків і сенсорів головне – це низьке енергоспоживання, автономність і можливість підключення великої кількості пристроїв в одному місці. Щоб задовольняти такі різні запити, мережі операторів повинні бути здатними оперативно і гнучко виділяти ресурси залежно від потреб користувача і сценаріїв використання зв'язку. При цьому зберігає чинність базовий принцип – чим вище швидкість передачі даних, тим менше дистанція, на яку дані можуть бути передані з такою високою швидкістю. Тобто щоб повсюдно забезпечити швидкість 5G, кількість майданчиків з мобільним обладнанням повинна бути в десятки разів більше, ніж в існуючих мережах. 5G-мережі все ще дуже далекі від готовності до комерційного використання. Нові мережеві технології ще належить стандартизувати. Необхідно також визначення бездротового діапазону, в якому вони будуть працювати. Потрібно також визначити, яке апаратне забезпечення доведеться для них розробити. Але якщо все буде реалізовуватися відповідно до графіка, 5G-мережу стане працювати в Південній Кореї під час Зимових Олімпійських ігор 2018 року.

Запуск 5G, в першу чергу, буде виправданий в районах з високою щільністю користувачів мобільного інтернету – людей і машин. Якщо говорити про перспективи появи 5G в Україні, то, на мій погляд, мова може йти про 2020-2022 роки, тобто приблизно через два роки після запуску перших комерційних мереж 5G в світі. Зазвичай саме стільки часу потрібно, щоб оцінити «зрілість» нової технології і запустити її на своїй мережі. Також необхідно, щоб з'явилася достатня кількість смартфонів і інших пристроїв, що вимагають/підтримують роботу 5G і виник «платоспроможний» попит.

На першому етапі варто очікувати точкового впровадження 5G, але з часом покриття буде розширюватися. Крім того, стандарт 5G буде розвиватися, що приведе до виникнення нових сценаріїв використання мобільного зв'язку. Як показує попередній досвід, нове покоління мобільного зв'язку з'являється

приблизно кожні 10 років, тому до 2030 року ми цілком можемо очікувати появи мобільного зв'язку шостого покоління – 6G.

Література:

1. <https://news.finance.ua/ua/news/-/316934/5g-nam-lyshe-snytsya> Кіберзагрози [Електронний ресурс] / Офіційна веб-сторінка ФБР. - Режим доступу: <https://www.fbi.gov/investigate/cyber>.
2. <http://biz.nv.ua/ukr/experts/serbin1/chogo-ochikuvati-vid-mobilnogo-zv-jazku-5g-845912.html>
3. <http://i-ua.tv/index.php?newsid=657>

Жук Виктор Юрьевич
Государственный Университет Телекоммуникаций
Факультет Телекоммуникаций
г. Киев

ТЕХНОЛОГИЯ NFC

Near field communication, NFC («коммуникация ближнего поля», «ближня бесконтактная связь») — технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров; анонсирована в 2004 г. NFC нацелена прежде всего на использование в цифровых мобильных устройствах NFC — это беспроводная короткодистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель; инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены. Технология NFC делает не нужными многие другие устройства, и элементы. Только смартфон, с чипом NFC используемый в качестве основного объекта повседневной жизни, будет достаточен для реализации всех ежедневных действий. Смартфоны могут быть использованы для блокировки / разблокировки дверей дома, автомобиля и офиса, оплаты за покупки, обмена визитными карточками, оплаты общественного транспорта.

Существуют три основных области применения NFC:

- 1) эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
- 2) режим считывания: устройство NFC является активным и считывает пассивную RFID-метку;
- 3) режим P2P: два устройства NFC вместе связываются и обмениваются информацией.

Рабочее расстояние с компактными стандартными антеннами: до 10 см; Поддерживаемая скорость передачи данных: 106, 212, или 424 Кбит. Существуют два режима:

Пассивный режим связи: устройство инициатор обеспечивает несущее поле, а целевое устройство отвечает посредством модулирования имеющегося поля. В этом режиме целевое устройство может вытягивать свою рабочую мощность из предоставленной инициатором электромагнитной области, таким образом делая целевое устройство ретранслятором.

Активный режим связи: и инициатор, и целевое устройство взаимодействуют путём поочередного создания своих собственных полей. Устройство деактивирует своё радиочастотное поле в то время, как оно ожидает данных. В этом режиме у обоих устройств должно быть электропитание.

Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передает данные со скоростью 106 кбит, тогда используется модифицированный код Миллера с 100 % модуляцией. Во всех других случаях используется манчестерское кодирование с коэффициентом модуляции 10 %.

Устройства NFC в состоянии одновременно и получать, и передавать данные. Таким образом, они могут контролировать радиочастотное поле и обнаруживать противоречия, если полученный сигнал не соответствует переданному.

И всё же, основная область применения технологии NFC в наши дни - безконтактные платежи. Таким образом, в Украине услуга NFC-платежей уже давно появилась в некоторых украинских банках. В начале 2017 года «ПриватБанк» запустил обновленный мобильный кошелек в приложении «Приват24». Расплачиваться в магазинах с помощью смартфона также могут клиенты «Сбербанка» (Сбер PAY), «Кредобанка» (KredoPay) и «Укрэксимбанка».

Технология Android Pay от Google стала доступной с ноября этого года.

Литература:

- 1) <http://www.mdpi.com/1424-8220/15/6/13348/htm>
- 2) <http://nfc-ukraine.com>
- 3) https://ru.wikipedia.org/wiki/Near_Field_Communication

Лозов Сергій
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ ОРГАНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ ТЕЛЕВІЗІЙНОГО КАНАЛУ

В роботі розглянуті принципи побудови сучасних систем телевізійного мовлення. Досліджено супутникові системи зв'язку та телевізійного мовлення. Проведено обґрунтування вибору та засоби побудови телерадіомовної

інфраструктури телевізійної студії. При проектуванні перевага надавалася цифровим засобам обробки та передачі телевізійного сигналу. Оскільки цифрові технології дозволяють надавати високоякісне зображення на телевізійних приймачах кінцевого користувача. Для спроектованої телекомунікаційної інфраструктури телеканалу проведено розрахунок супутникового каналу зв'язку.

Телекомунікації як частина інфраструктури суспільства служать одним із джерел забезпечення функціонування та підйому економіки держави.

На рубежі ХХІ століття телекомунікації виявилися однією з частин суспільства, що найбільш швидко розвиваються. При цьому темпи розвитку світової телекомунікаційної галузі в 2 рази перевищують темпи росту всієї світової економіки. У цей час обсяг доходів галузі перевищує трильйон доларів, причому 70 % цієї суми приїде на послуги, а 30 % - на продаж устаткування зв'язку.

В ХХІ століття, на думку більшості аналітиків багатьох країн, стане століттям переходу від індустріального суспільства до інформаційного, в основі якого буде лежати інформаційна інфраструктура, багато в чому обумовлена створюваними системами багатопрограмного ТВ мовлення (БПТМ).

Практична реалізація БПТМ можлива тільки у випадку переходу до цифрових способів обробки, передачі та консервації ТВ сигналів. При цьому стає очевидною конвергенція телебачення, комп'ютерної та телекомунікаційної техніки. Наприклад, уже зараз вивчаються можливості використання ТВ мереж для високошвидкісної передачі даних [1, с. 58].

Використання цифрових технологій у ТВ мовленні - це новий етап у розвитку технічних засобів масової інформації. Природно, що впровадження нових технологій, що докорінно змінюють основний склад і багатомільйонний парк телевізорів такої величезної мережі, як мережа ТВ мовленні, може відбуватися тільки шляхом поступової модернізації. Причому телекомунікаційні мережі практично вже готові до широкого впровадження цифрового телебачення.

Досвід, накопичений у ТВ мовленні, показав, що телебачення, переходячи в цифрову еру, здатне надати ряд нових можливостей при збереженні економічної ефективності. Для впровадження цифрового телебачення, у принципі, необхідне створення єдиного світового стандарту. У цей час технологічними лідерами в цій області є США, Європейський Союз та Японія. Відповідно існує і кілька проектів цифрового ТВ мовлення, розроблених у США, Європі і Японії.

Важливою ланкою в ланцюзі джерело інформації - споживач є засоби доставки. Відомо, що сьогодні традиційним ефірним засобам доставки ТВ і радіомовних програм доводиться конкурувати з такими засобами масмедіа, як провідне мовлення (аналогове та цифрове), системи безпроводового кабельного телебачення (мікрохвильова багатоканальна розподільна система - MMDS).

Проте ефірна система в діапазонах дуже високих і надвисоких частот залишається та буде залишатися найбільш доступною, розгалуженою та привабливою, оскільки створення такої системи не вимагає більших (у

порівнянні з іншими) витрат, і, саме головне, населення вже має десятки мільйонів ефірних теле- і радіоприймачів, а можливості підвищення якості прийому ще не вичерпані.

Традиційно сигнал усередині ТВ компанії поширюється у вигляді аналогового композитного (суміш декількох сигналів). Це найбільш дешевий і майже самий поганий спосіб. При послідовній обробці сигналу кожен вузол обробки - будь то АЦП, фільтр, мікшер - погіршує сигнал, і ці погіршення накопичуються. Зрозуміло, можна спробувати включити в ланцюг пристрій, що відновлює параметри. Однак є можливість уникнути цього, оскільки цифровий формат передачі дає недосяжну раніше можливість - зберегти високу якість зображення на всіх етапах обробки. І найперше, що необхідно зробити - це перейти від поширення сигналу в аналоговій формі до поширення в цифровому виді. Любий репортаж про будь-які реальні події тільки виграє, якщо буде знятий і змонтований у цифровому форматі, тому що глядач побачить всі дрібні деталі, відчує себе присутнім, значить причетним, а рекламодавець відзначить, що зображення в компанії високоякісне навіть у гірших умовах. А якщо зображення нечітке, скільки не намагайся - вийде "побутове відео" [2, с. 18].

В роботі розглянуті принципи побудови сучасних систем телевізійного мовлення. Досліджено супутникові системи зв'язку та телевізійного мовлення.

Проведено обґрунтування вибору та засоби побудови телерадіомовної інфраструктури телевізійної студії. При проектуванні перевага надавалася цифровим засобам обробки та передачі телевізійного сигналу. Оскільки цифрові технології дозволяють надавати високоякісне зображення на телевізійних приймачах кінцевого користувача.

Для спроектованої телекомунікаційної інфраструктури телеканалу проведено розрахунок супутникового каналу зв'язку.

Література:

1. Никитин Н. П. Телевизионные цифровые системы: учебное пособие / Н. П. Никитин, В. И. Лузин, В. И. Гадзиковский, Ю. В. Марков. - Е: Изд-во Урал. ун-та, 2016. - 108 с.
2. Мамчев Г.В., Носов В.И. Спутниковое телевизионное вещание: Учеб. пособие Новосибирск: изд. Новосиб. электротехнического ин-та связи, 2015. - 82 с.

Горохов Олександр Сергійович
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

БЕЗДРОТОВІ ЗАСОБИ ЗВ'ЯЗКУ

Для збору та передачі інформації використовуються різні засоби зв'язку. До ранніх засобів зв'язку на відстані належать візуальні сигнали, такі як маяки, димові сигнали, оптичний телеграф, сигнальні прапорці, звукові повідомлення, такі як бій в барабан, гра на горні або трембіті. У 20-му та 21-му століттях для телекомунікацій на відстані зазвичай використовують електричні та електромагнітні технології, такі як телеграф, телефон, телетайп, телекомунікаційні мережі, радіозв'язок, оптоволоконний, супутниковий зв'язок.

Сьогодні навколоземний простір заповнено зондами і супутниками глобальних систем навігації. Мінімум 25 апаратів було відправлено для вивчення близьких до Землі небесних тіл і самої планети Земля.

Весь радіозв'язок між наземними і космічними технічними системами, в тому числі GPS-приймачі та мобільний зв'язок та побутові радіоприймачі базуються на радіохвилях.

Найбільше значення для дистанційного дослідження має радіовипромінювання НВЧ - діапазону, що володіє великою проникаючою здатністю і тому безперешкодно досягає земної поверхні незалежно від метеорологічних умов.

Основними приладами, в яких застосовується радіовипромінювання є локатори (радари). Після пристосування радіолокаторів до формування зображень земної поверхні їх почали застосовувати для "льодової розвідки" з літаків, а вже згодом і до ДЗЗ з космосу.

Для обробки радіолокаційних досліджень важливим є знання формування "радіовідлуння" від об'єктів земної поверхні. На характер відбиття штучного радіосигналу впливає структура поверхні, речовинний склад природних об'єктів (в т.ч. рослин, ґрунтів, гірничих порід та води).

Радіовипромінювання також є основою зв'язку між Землею та її штучними супутниками, що виконують різні програми ДЗЗ, для наддалекого планетарного радіо- і телезв'язку, міжматерикового мобільного зв'язку, у радіогеографії, геофізиці, у військовій справі (зокрема, для забезпечення польотів крилатих ракет), а також для дослідження космосу (радіоастрономія).

Із технічної точки зору, найпростіша галузь застосування ДЗЗ — прогноз погоди.

На цьому прикладі й розповімо, як працює система. Зазвичай телевізійні прогнози погоди супроводжуються знімками з космосу. Проте яскраві картини на телеекрані — це, звісно, не все, що потрібно для прогнозу погоди!

Супутник не може сфотографувати всю поверхню Землі відразу. Він, облітаючи навколо Землі, «бачить» тільки певну смугу. Ширина цієї смуги може коливатися від 7 до 1500 км і залежить від необхідної точності обстеження: чим більш детальна інформація одержується, тим вужча смуга. Під час наступного оберту супутник «оглядає» суміжну смугу і так далі. Якщо об'єднати отримані дані від кількох таких смуг, можна одержати «картинку» для великої території, наприклад для всієї нашої країни.

Супутник передає отриману інформацію на приймальні антени; інформацію обробляють і перетворюють на звичні фотографії. Потім інформація передається метеорологам, які об'єднують дані з космосу з результатами наземних спостережень і на основі складних математичних моделей

прогнозують температуру та стан атмосфери на день, тиждень, місяць... Для аналізу стану поверхні Землі використовують багато супутників.

Більшість із них одержують дані в діапазоні видимих оком електромагнітних хвиль, але є й такі, які зондують поверхню електромагнітними пучками в діапазоні сантиметрових довжин (НВЧ-випромінювання), а також хвиль із більшою довжиною (понад 1 м).

Одержанням і обробкою даних від супутників займаються різні організації; в нашій країні - це Державне космічне агентство України.

Література

1. Муха Б.П., Байрак Г.Р. Дистанційні дослідження Землі: Навч. підручник. – Видавничий центр ЛНУ імені Івана Франка, 2008.

2. Фізика : підруч. для 9 кл. загальноосвіт. навч. закл. / [В. Г. Бар'яхтар, С. О. Довгий, Ф. Я. Божинова, О. О. Кірюхіна] ; за ред. В. Г. Бар'яхтара, С. О. Довгого. — Харків : Вид-во «Ранок», 2017.

Виговський Олександр Сергійович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
М. Київ

СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ

У сучасній реальності кожен день ми оперуємо великими обсягом інформації, що становить приватну, комерційну або державну важливість. Будь-яка компанія в процесі своєї роботи оперує інформацією, яка є найважливішою складовою повсякденної роботи, в 90% випадків це інформація критично важлива для функціонування компанії. Безумовно відмовостійкість і успішність будь-якої компанії залежить наскільки надійно зберігаються її дані, їх захищеність від несанкціонованого доступу або втрати інформації. Компанія якого розміру, стикається з необхідністю зберігання своїх власних інформаційних баз, і від того наскільки серйозно поставилися до зберігання даних і вибору системи зберігання, зазвичай залежить успішність.

Сам факт існування персональних комп'ютерів і зростання їх можливостей впливає на моделі обчислень і архітектуру інформаційно обчислювальних систем. Мабуть найбільш сильно проявляється цей вплив в стрімкому розвитку мережових технологій і широкому застосуванні архітектури обчислень клієнт-сервер. Ця модель стала причиною поширення серверно базованої моделі зберігання корпоративних, і загальних даних.

Зростання числа додатків інтенсивно використовують великі обсяги даних, вимагає все більше нових і нових гігабайт пам'яті. Зберігання, високошвидкісне читання, оперативна обробка транзакцій і мультимедіа програми змушують

майже щорічно збільшувати дискову ємність забезпечивши надійність зберігання.

Система зберігання даних (NAS)

це програмно-апаратна система що відповідає за надійне зберігання і управління даними. Це окрема підсистема, основною метою роботи якої є зберігання даних з належним рівнем надійності. Уже з назви, ясно що основна мета подібних систем забезпечувати безкомпромісне зберігання виключаючи при цьому втрату даних і зберігаючи при цьому максимальну доступність і високу швидкість доступу.

Відмовостійкість мережевого сховища, як і будь-яких інших систем забезпечується в результаті резервування компонентів системи. Резервування, це єдина техніка збереження як даних так і працездатності системи в цілому і забезпечує потенціал для зростання обсягу збережених даних.

Надійні системи, характеризуються кількома рівнями резервування, серед основних з них можна виділити апаратне і програмне резервування основних підсистем.

Більш детально відмовостійкість систем зберігання даних, можна розглядати розібравшись у компонентах сучасної системи зберігання в цілому.

Компоненти системи мережевого сховища

Дискова підсистема – масив з декількох високопродуктивних дисків класичного виконання (HDD) або флеш накопичувачі (SSD), об'єднані в групи.

Контролери дискової підсистеми – це мозок системи зберігання, зі своєю індивідуальною операційною системою, обчислювальним процесором (ами), підсистемою вводу-виводу і управління дисками, тобто дисковою підсистемою. Саме контролер надає інтерфейс управління всім процесом запису / читання, розподілу простору, розбиття і контролю дискового простору.

Підсистема живлення – забезпечує харчуванням систему і відповідає за резервування.

Повноцінне резервування мережевого сховища

на апаратному рівні виглядає як система з двома і більше контролерами жорстких дисків, кожен з яких готовий взяти на себе функції основного, у разі виходу з ладу одного з контролерів. Два і більше блоку живлення, що гарантують відмовостійкість і надійність підсистеми живлення шасі. Дискова підсистема, розбиті на групи диски формують дисковий масив, з дублюванням даних і резервуванням дисків, в тому числі на апаратному рівні, так звані spare диски які призначені, взяти на себе навантаження того диску що вийшов з ладу.

Концепція збереження даних

Способами реалізації концепції зберігання даних є мережі пристроїв масової пам'яті SAN (Storage Area Networks) які будуються на базі технології FiberChannel з блоковим доступом і NAS (Network Area Storage) IP рішення в яких може бути використані цілий ряд протоколів найбільш широко

застосовуються зараз для доступу (iSCSI , NFS, CIFS, FTP), так звані конвергентні системи, що дозволяють одночасно забезпечувати кілька протоколів доступу до даних.

Системи зберігання початкового рівня

це відмовостійка система з одним або двома контролерами жорстких дисків, резервування даних забезпечується на рівні груп дисків дискової підсистеми, резервування мережевої інфраструктури забезпечує відмовостійкий доступ до даних. Резервні блоки живлення системи запобігають вихід з ладу з причин живлення.

Системи зберігання корпоративного класу та рішення для центрів обробки даних (ЦОД)

являють собою набір відмовостійких і зарезервованих систем, с розподіленої інфраструктурою, і механізмами синхронної реплікації, для забезпечення максимальної надійності та доступності даних компанії.

Системи зберігання даних є модульними системами здатними до легкого масштабування, і набуваючи спочатку невелику систему в якій закладений потенціал для зростання і розширення продуктивності, замовник з легкістю може наростити потужність системи зберігання, і обсяг дискового простору, підключивши додаткові дискові шасі зберігання або замінивши класичні HDD на більш продуктивні SSD диски, які дозволяють істотно наростити продуктивність системи.

Сучасні мережеві сховища даних, і схеми резервування є невід'ємною частиною інфраструктури при побудові центрів обробки даних і дозволяють реалізовувати рішення територіально розподілені системи зберігання із забезпеченням синхронної реплікації (синхронізації збережених даних) на далеких відстанях, аж до 260 кілометрів. У портфелі компанії є рішення що дозволяють повноцінно реалізувати розподілені системи зберігання.

Дані системи максимально оптимізовані для роботи з віртуалізованими серверними системами під управлінням VMware, Microsoft Hyper-V рішеннями. Ми маємо багатий досвід щодо інтеграції рішень зберігання даних і готові забезпечити інтеграцію системи зберігання в вашу інфраструктуру, або призвести міграцію існуючої серверної системи зберігання на мережеву систему зберігання даних з прив'язкою до систем віртуалізації апаратної платформи.

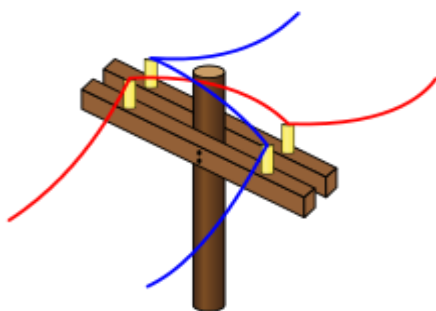
Як і в будь-якій сфері діяльності є свої лідери та інноваційні компанії, у сфері надійного зберігання інформації ми спираємося рішення компанії NetApp і готові запропонувати оптимальні рішення для вашого бізнесу.

Література:

https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_%D0%B7%D0%B1%D0%B5%D1%80%D1%96%D0%B3%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

КАК «ВИТАЯ ПАРА» ОКУТАЛА МИР?

Первые средства связи использовали однопроводную линию с цепью заземления и этого было бы достаточно если бы не всемирный технологический прогресс. С началом электрификации в сети появились помехи «шумы» что негативно сказалось на передаче сигнала.

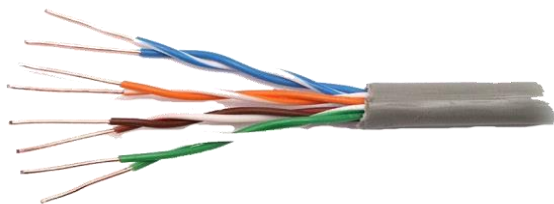


Для устранения этой проблемы инженерами был разработан метод транспозиции проводов, что бы свести помехи на нет. Суть заключалась в изменении положения проводов через определенное количество опор. Это представляло собой раннюю реализацию скручивания с шагом транспозиции проводов.

Витая пара была изобретена в 1881 году и уже тогда нашла свое применение когда вся американская сеть телефонных линий была на витой паре или на открытых проводах с транспозицией для защиты от помех.

Витая пара в наши дни

Витая пара (англ. twisted pair) — вид кабеля связи. Представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитные помехи одинаково влияют на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара — один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet, Token ring, USB. В настоящее время, благодаря своей дешевизне и лёгкости монтажа, является самым распространённым решением для построения проводных (кабельных) локальных сетей.



Витая пара «фундамент» всемирной сети

Витая пара нашла применение в кабелях Ethernet которые в союзе с оптоволоком и создают всемирную сеть Internet. Существуют различные версии этих кабелей но все они используют технологию «витой пары». Самый распространенный стандарт построения локальной сети это Fast Ethernet это 4-парный кабель, который используется при построении локальных сетей 10BASE-T, 100BASE-TX и 1000BASE-T и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар.

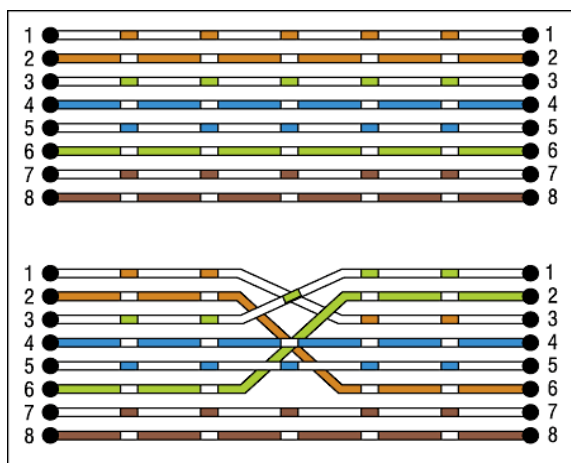
Сам витопарный кабель состоит из нескольких витых пар. Проводники изготовлены из монолитной медной проволоки. Материал изоляции – обычно поливинилхлорид или полиэтилен. Также внутри кабеля встречается «разрывная нить», которая используется для облегчения разделки внешней оболочки. Внешняя изоляция изготовлена также из поливинилхлорида который имеет хрупкость для удобства монтажа.

Концы кабеля обжимаются с помощью различных коннекторов.



Для выполнения различных задач существуют следующие примеры варианты обжима:

1. «Прямой» кабель для подключения компьютер на хаб/свитч
2. Кросс-кабель Ethernet -предназначен для соединения однотипного оборудования (например, компьютер-компьютер).



Литература:

Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.: ил. — (Серия «Учебник для вузов»). ISBN 978-5-496-01967-5

Бочко Марк Андреевич

Государственный университет телекоммуникаций

Факультет Телекоммуникаций

г. Киев

ДЕТЕРМИНИРОВАННЫЕ ОДНОФОТОННЫЕ ИСТОЧНИКИ В ДВУМЕРНЫХ ПОЛУПРОВОДНИКАХ

Двумерные полупроводники представляют новый потенциальный твердотельный носитель для однофотонных источников. Примечательной характеристикой этих систем по сравнению с традиционными однофотонными источниками, такими как квантовые точки InGaAs (тройное соединение мышьяка с трехвалентными индием и галлием, соединение переменного состава, состав выражается химической формулой $\text{Ga}_x\text{In}_{1-x}\text{As}$) или цветовые центры в алмазе, является способность улавливать одиночные экситоны (квазичастица, представляющая собой электронное возбуждение в диэлектрике, полупроводнике или металле) на поверхности. Этот актив мог бы разблокировать потенциал для разработки высокоэффективных механизмов извлечения фотонов и для связывания ограниченных экситонов с фотонными структурами и другими квантовыми системами.

Сообщалось, что с 2015 года однофотонные испускающие участки неизвестного происхождения появляются в случайных местах в монослоевых пластах WSe_2 , WS_2 и MoSe_2 . В этом году учёные смогли детерминистически спроектировать такие источники в точном месте с 96 процентами доходности, в неограниченном количестве, масштабируемым образом и с лучшими оптическими свойствами, чем их случайно встречающиеся аналоги.

Учёные достигли этого детерминированного источника, деформируя материал локально в наноуровне, используя узорчатые подложки. Учёные сначала отслаивали однослойные пласты WSe_2 и WS_2 из объемных кристаллов. Затем учёные перенесли пласты на подложки из диоксида кремния, узорчатые квадратными матрицами нанопилларов, расположенные на расстоянии 4 мкм и в диапазоне от 100 до 200 нм в высоту и с диаметром вершины 90 нм. Сканирование атомно-силовой микроскопии показывает, что покрытые пластом над каждым нанопилларом и прикрепляется Ван-дер-Ваальсом к плоским участкам субстрата между ними.

Измерения низкотемпературной фотолюминесценции показали освещение низкотемпературной фотолюминесценции и узких спектральных линий из местоположений столбцов. Фотонно-корреляционные измерения на этих узких линиях подтвердили однофотонный характер излучения, а спектральные измерения с высоким разрешением выявили тонкую структуру в большинстве точек. Измеренные параметры очень близки к измеренным для случайного появления однофотонных излучающих участков в тех же материалах, что предполагает общее происхождение. Характеристика квантовой эмиссии с ростом высоты столба также дала интересные результаты: количество узких линий на участок уменьшается, а спектральное блуждание улучшается на порядок по сравнению с местами случайной эмиссии.

Учёные считают, что эта работа открывает путь для истинного однофотонного излучателя, который можно легко масштабировать и интегрировать с другими фотонными компонентами. Кроме того, в качестве новой платформы для детерминированного квантового взаимодействия свет-вещество между одиночными экситонами и фотонами, она позволяет исследователям исследовать потенциал оптического односпинового управления к квантовым информационным приложениям.

Литература:

1. Научный журнал “Optics & Photonics News”. Сайт <https://www.osa-opn.org>

*Гомзяк Ярослав Олегович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ*

MULTIPROTOCOL LABEL SWITCHING

MPLS - багатопротокольна комутація по мітках - механізм в високопродуктивній телекомунікаційній мережі, який здійснює передачу даних від одного вузла мережі до іншого за допомогою міток. MPLS є масштабованим і незалежним від будь-яких протоколів механізмом

передачі даних. У мережі, заснованій на MPLS, пакетам даних присвоюються мітки. Рішення про подальшу передачі пакета даних іншого вузла мережі здійснюється тільки на підставі значення присвоєної мітки без необхідності вивчення самого пакета даних. За рахунок цього можливе створення наскрізного віртуального каналу, незалежного від середовища передачі і використовує будь-який протокол передачі даних.

MPLS дозволяє досить легко створювати віртуальні канали між вузлами мережі. Технологія дозволяє інкапсулювати різні протоколи передачі даних. Основною перевагою MPLS є незалежність від особливостей технологій каналного рівня, таких як ATM, Frame Relay, SONET / SDH або Ethernet; відсутність необхідності підтримки декількох мереж другого рівня, необхідних для передачі різного роду трафіку.

По виду комутації MPLS відноситься до мереж з комутацією пакетів. Технологія MPLS була розроблена для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів (маються на увазі програми з датаграмною передачею пакетів).

MPLS може бути використаний для передачі різного виду трафіку, включаючи IP-пакети, осередки ATM, фрейми SONET / SDH і кадри Ethernet. Для вирішення ідентичних завдань раніше були розроблені такі технології, як Frame Relay і ATM. Багато інженерів вважали, що технологія ATM буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому забезпечують передачу пакетів даних змінної довжини з встановленням з'єднання між вузлами мережі.

Принцип роботи

Технологія MPLS заснована на обробці заголовка MPLS, який додається до кожного пакету даних. Тема MPLS може складатися з однієї або декількох «міток». Кілька записів (міток) в заголовку MPLS називаються стеком міток .

Формат запису в стек міток

32біта

20 біт	3 біта	1 біт	8 біт
Label	TC	S	TTL

Кожен запис в стек міток складається з наступних чотирьох полів:

- значення мітки(Label) займає **20 біт**;
- поле «клас трафіку» (Traffic class) використовується для реалізації механізмів якості обслуговування (QoS) і явного повідомлення (до RFC 5462 це поле називалося Exp займає **3 біти**;

- прапор «дно стека» (Bottom of stack) якщо прапор встановлений в 1, то це означає, що поточна мітка остання в стеці; займає **1 біт**;
- поле TTL (Time to live) використовується для запобігання петель MPLS комутації; займає **8 біт**.

У MPLS-маршрутизаторі пакет з MPLS-міткою комутується на наступний порт після пошуку мітки в таблиці комутації замість пошуку по таблиці маршрутизації. При розробці MPLS пошук міток і комутація по мітках виконувалися швидше, ніж пошук по таблиці маршрутизації або RIB (Routing information base - інформаційна база маршрутизації), так як комутація може бути виконана безпосередньо на комутаційній фабриці замість центрального процесора. Маршрутизатор, розташований на вході або виході MPLS-мережі, називаються LER (Label edge router - граничний маршрутизатор міток). LER на вході в MPLS-мережа додають мітку MPLS до пакету даних, а LER на виході з MPLS-мережі видаляє мітку MPLS з пакета даних.

Порівняння MPLS і IP

MPLS як протокол некоректно порівнювати з протоколом IP, оскільки MPLS працює спільно з IP і протоколами маршрутизації (IGP).

Основні переваги технології IP / MPLS: більш висока швидкість просування IP-пакетів по мережі за рахунок скорочення часу обробки маршрутної інформації; можливість організації інформаційних потоків в каналах зв'язку. За допомогою міток кожному інформаційному потоку (наприклад, несе телефонний трафік) може призначатися необхідний клас обслуговування (CoS).

Література:

<https://ru.wikipedia.org/wiki/MPLS>

Димарчук Дмитрій Сергійович
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

ЗАХИСТ РОУТЕРА ВІД ЗЛОМУ

Розглянемо основні рекомендації, які дозволять знизити ймовірність злому практично до нуля.

Дуже важливо використовувати захищені пристрої маршрутизації або роутери. За допомогою цих пристроїв відбувається обмін пакетами між пристроями мережі і провайдера на основі правил і таблиць маршрутизації. Отримуючи доступ до роутера можна отримати різну інформацію, яка може бути

використана в різних цілях. Наприклад, це може бути інформація про пристрої, відвідуваних сайтах, настройках і т.д.

Для опису всі дій, буде використовуватись роутер фірми TP-LINK.

Як можна отримати доступ до роутера?

Зловмисники використовують автоматичні сканери за певними мереж. Сканери пристроїв маршрутизації проводять сканування по портах, які традиційно займають роутери. Відбувається сканування на знаходження стандартних портів з певними даними для входу. Якщо ваш роутер має стандартні настройки, то дуже велика ймовірність, що зловмисник зможе отримати доступ до ваших даних. На прикладі однієї з програм для сканування було отримано 73 успішних роутера за 40 хвилин роботи. Якщо враховувати, що в середньому роутер використовують 3-4 пристрої, то це досить велика кількість користувачів.

IP	Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type	Radio Off	Hidden	BSSID	ESSID	Security	Key	WPS PIN	LAN IP Address
12.153	8080	0	Done	admin:admin	D-Link DSR-150, hardware: A1, firmware: 1.05B46_RU	-	-	-	no wireless	-	-	-	192.168.10.1
12.168	1080	15	Done	admin:admin	TP-LINK TL-WR1043ND	-	-	64:7D:52:17:3E:FC	Alex	WPA/WPA2	0903304381	-	192.168.1.1
12.170	8080	0	Done	admin:admin	ASUS RT-AC66U, firmware: 2.0	-	-	08:50:E6:CB:3C:00	tmson	WPA/WPA2	67042029	192.168.1.1	192.168.1.1
13.136	8080	31	Done	admin:1234	ASUS RT-N12LX	-	-	-	Hawaii Five-0	WPA/WPA2	kanasaki	-	192.168.1.1
13.219	80	16	Done	admin:1234	ZyXEL Keenetic Giga III	-	-	-	-	-	-	-	192.168.1.1
81.13	80	78	Done	admin:admin	TP-LINK TL-WR740N	[X]	[X]	84:36:F9:9C:E2:D0	TP-LINK_E3D0	WPA/WPA2	87367300	87367300	10.10.10.254
81.152	8080	31	Done	admin:admin	Netis WF2411UR Router	-	-	E4:8E:ED:3A:71:D6	KuFuJ	WPA/WPA2	plushyprink	38303205	192.168.10.1
134.253	8080	15	Done	admin:admin	TRENDnet TEV61-65.5BR	-	-	00:14:01:D5:E8:A7	TRENDnet65.1	WPA2	ScotAgben612	36423666	192.168.10.1
146.107	8080	0	Done	admin:admin	ASUS RT-N10U	-	-	-	-	-	-	-	192.168.1.10
146.122	8080	188	Done	admin:admin	ASUS RT-N10U	-	-	-	-	-	-	-	192.168.1.1
146.234	80	78	Done	admin:admin	ASUS RT-N12E	-	-	0C:EE:7B:65:29:2C	ASUS	WPA/WPA2	4fona3ton	72810032	192.168.1.1
147.6	80	15	Done	admin:admin	TP-LINK TL-WR741ND	-	-	F8:5A:67:C3:8E:14	Lanc	WPA2	0673466409	94992343	192.168.0.1
147.43	8080	31	Done	admin:admin	Netis WF2411UR Router	-	-	94:8D:36:2C:3C:89	netis	WPA/WPA2	password	61871389	192.168.1.1
147.99	8080	31	Done	admin:admin	TP-LINK TL-WR740N	-	-	18:A6:F7:A2:E5:E4	TP-LINK_E5E4	WPA2	12345678	70630013	192.168.0.1
190.67	80	0	Done	admin:admin	TP-LINK TL-WR1043ND	-	-	P4:F2:6D:3E:65:D2	Dovzhanka Magadr	None	<empty>	30057893	192.168.0.1
190.116	80	0	Done	admin:admin	TP-LINK TL-WR1043ND	-	-	C4:6E:5F:4D:E8:6C	Mala Hata	WPA/WPA2	22851192	22851192	192.168.0.1
190.120	80	0	Done	admin:admin	D-Link DVG-F45402GP VoIP, firmware: R2_1.00, hardware: A1	-	-	84:C9:82:CE:9C:C7	dnk	None	<empty>	24125871	192.168.8.254
228.44	8080	15	Done	admin:admin	TP-LINK TL-WR741ND	-	-	F8:5A:67:C3:8E:14	P8H	WPA2	negative_1983	50431700	192.168.0.1
228.85	80	31	Done	admin:12345678	ASUS RT-N12LX	-	-	54:04:A6:5E:A4:4C	ASUS_2	WPA/WPA2	genetep3	96988778	192.168.1.1
228.90	8080	16	Done	admin:admin	ASUS RT-N10LX	-	-	54:04:A6:5E:A4:4C	KP_V	WPA2	new-vist.com	38472299	192.168.7.1
9.168	80	63	Done	admin:admin	TP-LINK TL-WR841N	-	-	18:A6:F7:42:32:12	TP-LINK_423212	WPA2	0683802602	80972280	192.168.0.1
9.175	80	31	Done	admin:admin	TP-LINK TL-WR841N	-	-	18:A6:F7:42:32:12	TP-LINK_423212	WPA2	71510309	71510309	192.168.0.1
9.188	80	63	Done	admin:admin	TP-LINK TL-WR841N	-	-	A4:2B:5D:03:AA:EE	PowerNet Ofc	WPA/WPA2	ofcpassword	54614601	192.168.0.1
9.197	8080	63	Done	admin:admin	TP-LINK TL-WR1043ND	-	-	P4:F2:6D:3E:65:D2	TP-LINK_33D4	WPA2	70736946	70736946	192.168.0.1
9.250	80	32	Done	admin:admin	TP-LINK TL-WR841N	-	-	C0:4A:00:5F:72:F2	Daouda	WPA/WPA2	Daouda2107	53391285	192.168.0.1
112.107	8080	0	Getting info...	Adminpower77	D-Link DSR-825, hardware: B1, firmware: 2.10VW	-	-	-	dnk24	WPA	lauruhn77	27194515	192.168.1.1

Сканування засобів маршрутизації за діапазоном

Як звести шанси злому до нуля?

Для того, щоб знизити шанси і мінімізувати ризик злому необхідно виконати невеликий список дій.

Зміна стандартного IP-адреси для локального управління

Для початку, необхідно перевірити адресу, на якому знаходиться адмін. панель. Для цього потрібно ввести в браузері два адреси:

<http://192.168.0.1/> та <http://192.168.1.1/>

Як правило, для входу використовується логін і пароль admin / admin. Таким чином, перше, що потрібно зробити - це змінити адресу розміщення адмін. Панелі, логін та пароль. Це дозволить захистити нас від засобів масового сканування, наприклад, Router Scan. Для роутерів TP-LINK:

Функция QSS

Сеть

- WAN

- Локальная сеть

- IPTV

- Клонирование MAC-адреса

Беспроводной режим

DHCP

MAC-адрес:

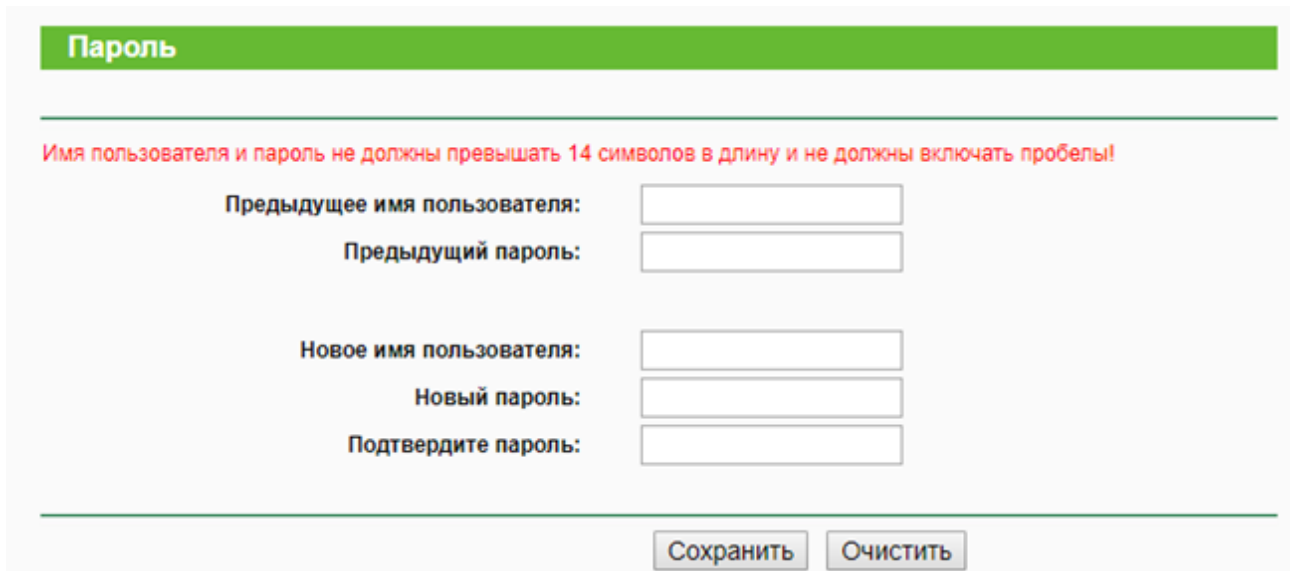
IP-адрес:

Маска подсети:

Сохранить

Зміни авторизаційних даних для входу

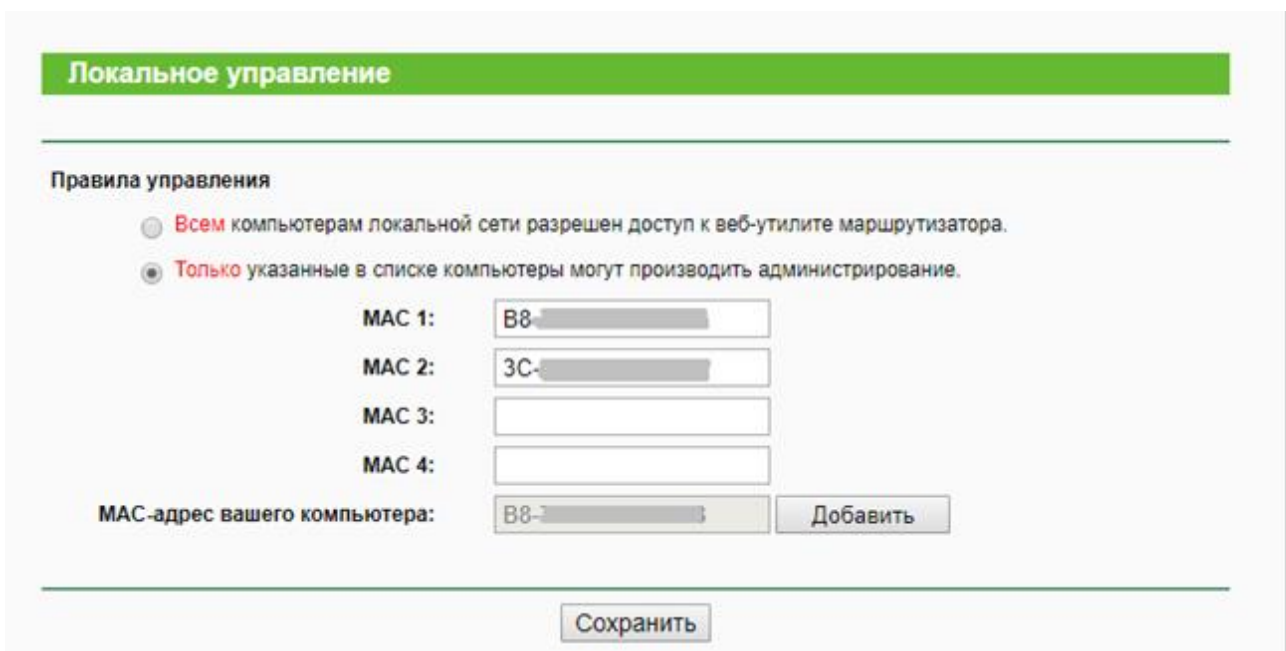
Ім'я користувача і пароль можна змінити в розділі «Системні інструменти» -> «Пароль»:



Обмеження списку комп'ютерів для локального управління

Далі необхідно заборонити доступ до засобів адміністрування із зовні. Для нашого роутера необхідно зайти в розділ «Безпека» - «Локальне управління». У нашому випадку можна вказати MAC адреси комп'ютерів, які матимуть доступ до адмін. панелі. Цей спосіб можна застосовувати для відкритих мереж з великою кількістю учасників.

Фільтрація MAC-адрес



Створення фільтрації дозволяє додати в список пристроїв тих користувачів, які не мають небезпеки. Це можна обійти, але це додатковий бар'єр, який може зупинити школярів-хакерів.

Роутери TP-Link дозволяють створити список бажаних і небажаних пристроїв для мережі. Цей спосіб має переваги з великими мережами.

Фильтрация MAC-адресов

Фильтрация MAC-адресов в беспроводной сети: **Включена**

Правила фильтрации

☒ **Запретить** доступ станциям, указанным в списке.
☐ **Разрешить** доступ станциям, указанным в списке.

ID	MAC-адрес	Состояние	Описание	Редактировать
----	-----------	-----------	----------	---------------

Правила фільтрації

Зміни порту для віддаленого управління

Додатково необхідно змінити порт, який може використовуватися для віддаленого управління. Ця дія дозволить захиститися від автоматичний сканерів, які сканують адреси на порти 80 і 8080. Це стандартні значення роутерів. Програми автоматичного сканування не перевірятимуть усі значення від в межах від 1 до 65534. Тому краще змінити стандартні порти на інші значення, якщо ви використовуєте віддалене управління. В ідеалі краще цю функції зовсім відключити. Для цього у роутерів сімейства TP-LINK краще відключити цю функцію. Досить вказати IP адреса 0.0.0.0. Тоді за замовчуванням ця функція буде відключена.

Удаленное управление

Порт веб-управления:

985

IP-адрес удаленного управления:

0.0.0.0

(Укажите 255.255.255.255 для всех)

Відключення DHCP сервера

Настройки DHCP

DHCP-сервер:

☒ Отключить ☐ Включить

Начальный IP-адрес:

192.168.25.100

Конечный IP-адрес:

192.168.25.199

Срок действия адреса:

120

минуты (1~2880 минут, значение по умолчанию 120)

Основной шлюз:

192.168.25.25

(необяз.)

Домен по умолчанию:

(необяз.)

Первичный DNS:

0.0.0.0

(необяз.)

Вторичный DNS:

0.0.0.0

(необяз.)

Відключення DHCP сервера

Протокол DHCP застосовується для автоматичного призначення IP-адреси, шлюзу, DNS-сервера і т.д. В якості транспорту даний протокол використовує UDP, а це значить, що ми можемо без особливих проблем підміняти все цікавлять нас поля в мережевому пакеті, починаючи з канального рівня: MAC-адресу джерела, IP-адреса джерела, порти джерела - тобто все, що нам хочеться. Тому, щоб позбавити себе від різного роду атак, краще відключити DHCP на роутері.

Прив'язка MAC адреси і IP

Прив'язати можна в меню IP & MAC Binding (Прив'язка IP і MAC). Зв'язування з протоколу ARP є зручною функцією для контролю доступу комп'ютерів, що знаходяться в локальній мережі. Список пристроїв можна подивитися в ARP таблиці.

Параметры привязки

Связывание ARP: ☐ Отключить ☒ Включить

ID	MAC-адрес	IP-адрес	Связать	Изменить
1	B8-76-3F-A4-47-6B	192.168. []	☒	Редактировать Удалить
2	68-3E-34-20-51-03	192.168. []	☒	Редактировать Удалить
3	30-76-6F-FC-FF-D4	192.168. []	☒	Редактировать Удалить

1 ▾ Стр.

Параметри прив'язки

Прихований SSID

Як правило, майже всі WiFi мережі мають свою назву. Ця назва і є SSID (Service Set Identifier). Це ім'я можна побачити, скануючи мережі навколо. За замовчуванням роутери показують ім'я всім бажаючим. Це дозволить знизити кількість різних атак, які будуть здійснюватися на вашу мережу. Так як для реалізації уразливості потрібно знати SSID.

У роутерах TP-Link це можна зробити в основному меню (Налаштування бездротового режиму).

Приховування SSID

Настройки беспроводного режима

Имя сети: (Также называется SSID)

Регион: ▾

Предупреждение: Убедитесь, что вы правильно выбрали страну, чтобы соответствовать местным законам. Некорректные настройки могут вызвать помехи.

Канал: ▾

Режим: ▾

Ширина канала: ▾

☒ Включить беспроводное вещание роутера

☐ Включить широковещание SSID

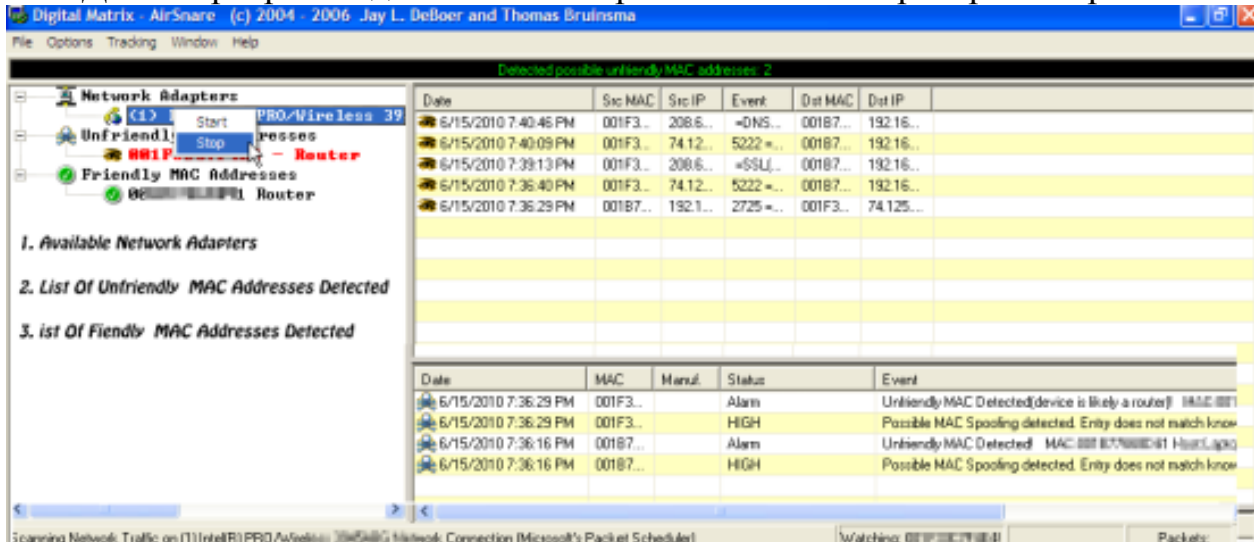
☐ Включить WDS

Відключити WPS підключення

WiFi Protected Setup (WPS) - це технологія апаратного підключення до мережі, яка працює за спрощеним принципом підключення до мережі WiFi. Вона має досить багато вразливостей, тому краще відмовитися від її використання.

Моніторинг мереж за допомогою програми AirSnare

Дана програма дозволяє контролювати всі пристрої мережі. Якщо



з'являється новий пристрій, то засіб може відправляти повідомлення на пошту, записувати лог в журнал або відображати цю інформацію в інтерфейсі програми. Додатково програма вміє відправляти повідомлення підключеному пристрою з міткою, що за ним ведеться детальне спостереження.

Висновок

Таким чином, ми змогли максимально убезпечити свій роутер. Звичайно, не варто забувати, про дві речі. По-перше, практично всі модеми мають кнопку скидання налаштувань. Тому, краще розміщувати роутер в місці, де немає фізичного доступу інших користувачів. По-друге, якщо ви скачуєте файл і запусіть файл з експлоїтів у себе на комп'ютері, тоді користі від захисту немає. Так, як зловмисник отримає доступ до всіх ваших даних. Тому, варто уважно перевіряти дані, які ви завантажуєте і відкриваєте.

Література:

<http://prowomantoday.ru/rizne/10554-jak-nalashtuvati-router-tp-link-bez-storonnoi.html>

http://www.internet-technologies.ru/articles/article_1804.html

<https://ok-wifi.com/tp-link/nastrojka-routera-tp-link-v-rezhime-mosta-wds-soedinyayem-dva-routera-po-wi-fi.html>

ПЕРСПЕКТИВНІ ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

І. Постановка проблеми

І.І Перспективи розвитку нашої цивілізації багато в чому залежать від того, наскільки швидко і адекватно людство проникне в сокровенні таємниці інформації, усвідомлює переваги і небезпеки, пов'язані зі становленням суспільства, заснованого на виробництві, розповсюдженні та споживанні інформації і званого інформаційним.

Суть змін, що відбуваються, що охопили сферу діяльності людини, в самому загальному вигляді полягає в тому, що матеріальна складова в структурі життєвих благ поступається місцем інформаційної. І хоча ми за інерцією все ще продовжуємо підраховувати складові основу традиційного багатства тонни, метри, декалітри виробленої продукції, стає очевидним, що економічна міць держави визначається вже далеко не цими показниками.

І.ІІ Актуальність теми. Багато ділових людей і організації виявили, що вони повинні використовувати у своїй діяльності комп'ютерні комунікації (електронну пошту, інтерактивні інформаційні служби і т.д.) не тільки для своїх співробітників, але і для широкого кола споживачів своєї продукції через електронні дошки оголошень (BBS - Bulletin Board System), телеконференції інтерактивних інформаційних служб або через вузли Всесвітньої Павутини Internet. Обсяг і способи інформування споживачів за допомогою засобів комп'ютерних комунікацій докорінно змінилися за останні рік - два. Якщо раніше ця інформація в основному призначалася для фахівців, то тепер вона розрахована на саму широку аудиторію.

ІІ. Мета

Кілька років тому передача даних за допомогою комп'ютерів цікавила тільки фахівців і досвідчених користувачів. В даний час використання локальних і глобальних комп'ютерних мереж стає настільки ж рутинною і поширеним, як і ПК. Якщо вам необхідна електронна пошта, використання інформаційних ресурсів Internet та інших інтерактивних комерційних інформаційних служб, наприклад, CompuServe, віддалене з'єднання домашнього ПК з локальною мережею на роботі, пересилання файлів в інше місто, то ласкаво просимо в світ комп'ютерної передачі даних. Саме тому метою написання даної статті є подальший розгляд та дослідження перспективних телекомунікаційних та інформаційних технологій.

ІІІ. Виклад основного матеріалу

У числі технологій, які найближчим часом будуть чинити вирішальний вплив на розвиток телекомунікацій, слід назвати:

- Оптичні технології (SDH / SONET), що забезпечують збільшення швидкості, здешевлення доступу до мережі, а отже, збільшення числа користувачів;

- Широкосмугові канали (B-ISDN), що дозволяють передавати різноманітну інформацію з одного і того ж каналу і, як наслідок, підвищують швидкодію та інтелектуальність мережі;

- Єдину технологію мультиплексування і комутації (ATM), що підвищує інтелектуальності мережі;

- Методи кодування і стиснення інформації, яким належить зіграти ключову роль в еволюції широкосмугових мереж, різко (на кілька порядків) збільшивши передані інформаційні потоки і тим самим забезпечивши можливість передачі з високою якістю мультимедійної, телевізійної та іншої інформації (найбільш значущі стандарти стиснення: рекомендації МККТТ серії H, стандарти JPEG і група стандартів MPEG-1, 2, 3, 4);

- Комутовані ЛВС (Fast Ethernet, FDDI FDDI II, ATM), збільшують продуктивність та інтелектуальність мережі;

- Цифрову бездротовий зв'язок, що сприяє зростанню числа і мобільності користувачів;

- Інтероперабельність мереж (Java)

- Універсальний доступ до послуг Internet (WWW).

Висновок

Телекомунікаційні технології розвиваються настільки стрімко, що неминуче вторгаються в усі галузі електроніки. Знання, які ще вчора були долею вузьких фахівців, стають необхідними практично будь-якій людині. У результаті глобальних змін у структурі і масштабах виробництва, прискорення науково-технічного прогресу, підвищення ділової активності суспільства, зростання освітнього і культурного рівня населення, розширення зв'язків у національному та міжнародному масштабі значно зростає роль інформації. Сучасні засоби телекомунікації надають нам великі можливості для здійснення обміну інформацією. І ми просто зобов'язані скористатися цим безцінним даром для спілкування та комунікацій із суспільством, людством, Всесвіту.

Література:

1. Нижегородцев Р. Про інформаційну економіку // РЕЖ, 1994, № 4;
2. Сидоров А., Байн В. Інформація як економічна категорія // ЕКО, 2000, № 8 ;
3. Методичні рекомендації з дисципліни "ОТТМП" для 2 курсу, Державний університет телекомунікацій ;

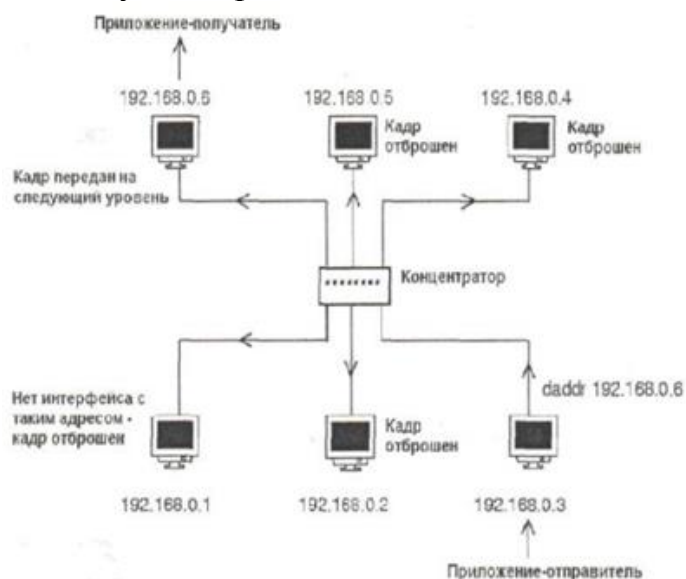
АТАКИ С ПРИМЕНЕНИЕМ СНИФФЕРОВ

Сниффинг (Sniffing) - это перехват пакетов, передающихся между двумя компьютерами. Перехват может произойти в любой точке маршрута данных. В локальной сети перехватчиком может быть любой узел сети, в интернет - провайдер.

В сетях, построенных на основе TCP/IP, вся информация передается, в основном, в открытом виде (в том числе и всякие секретные данные - пароли и логины). Поэтому очень выгодно бывает настроить на одной машине софт, который будет просматривать все пакеты, проходящие по сети, и проверять, не содержится ли в них каких-нибудь паролей. Это и есть сниффинг. А такой софт называется сниффером. Сниффинг - излюбленный метод многих хакеров.

Проблема сниффинга в Интернете решаемая. Самое главное, нужно передавать приватные данные в зашифрованном виде (протоколы SSH и SSL). Для понимания процесса посмотрим на сниффинг в локальной сети.

Перехватить пакет в Ethernet-сети очень просто. В Ethernet-сети любой отправленный пакет предназначается каждому компьютеру. Компьютер смотрит поле адреса получателя и сравнивает его со своим адресом. Если адреса совпадают, пакет будет принят, иначе - отброшен. Это в сети с концентраторами. Концентратор сети - это устройство, которое просто повторяет принятый от машины пакет на все свои порты. Если компьютер определит, что пакет предназначен для него, он его примет. Если пакет не предназначен для него, он будет отброшен. Но если перевести сетевую плату в специальный режим (promiscuous mode), то она будет принимать все полученные пакеты, независимо от того, кому они предназначались.



Самая большая угроза sniffingа состоит в перехвате паролей часто используемых протоколов - Telnet, FTP, POP3, HTTP, которые передают информацию о пароле в сети в открытом виде. С помощью sniffingа можно перехватывать даже передаваемые по сети файлы, прикрепленные к какому-нибудь письму.

Популярный sniffer пакетов для Linux - программа Ethereal. Программа обладает удобным графическим интерфейсом, позволяет просматривать как список всех перехваченных пакетов, так и отдельно содержимое каждого пакета. Имеется версия Ethereal и для Windows. Sniffer можно не устанавливать на каждой машине сети. Достаточно установить его на одной взломанной машине или на своей машине - если машина находится в локальной сети. Если нужна текстовая версия программы, то удобнее использовать текстовый sniffer - например, Ettercap или tcpdump.

Как предотвратить угрозу перехвата пакетов? На самом деле защититься от sniffера очень трудно, но есть некоторые средства которые помогут уменьшить риск перехвата ваших конфиденциальных данных.

- использование разных сложных паролей для аутентификации
- установка и настройка программных или аппаратных средств, распознающих sniffеры
- использование крипто-шифрования каналов связи
- использование программ для защиты беспроводных сетей

Литература :

1. <https://it-sektor.ru/chto-takoe-sniffing/-sniffing.html>
2. <http://www.spy-soft.net/chto-takoe-sniffer-analizator-trafika/>

*Скнарь Ірина Миколаївна
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ*

ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ

І. Постановка проблеми

В умовах динамічного розвитку ринкової економіки зростають вимоги до соціально-економічної адаптованості та відповідного рівня функціонування усіх галузей та сфер економіки України. Прогресивний розвиток науки, техніки і технологій, інноваційність та висока наукомісткість сучасного виробництва висувають особливі вимоги до шляхів розвитку інформаційно-телекомунікаційної сфери.

Сфера телекомунікацій як складова сфери зв'язку та інформатизації має стратегічне значення для сталого розвитку й стабільного функціонування виробничої і соціальної інфраструктури України, що призначена для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах.

Це можливо зробити лише за умов стабільної роботи підприємств телекомунікаційної сфери, що спрямована на подальший успішний розвиток. Так підприємства телекомунікацій повинні бути динамічними, адаптивними, швидко реагувати на стрімкий, схильний до кардинальних змін телекомунікаційний ринок. Унаслідок цього інформаційно-телекомунікаційні послуги не можуть ефективно поширюватись без налагодженого механізму управління даними послугами.

II. Мета

Формування моделі структури проблем та суперечностей, необхідної для подальшого вдосконалення системи управління телекомунікаційних підприємств України в сучасних економічних умовах.

III. Виклад основного матеріалу

У сучасних умовах недостатній аналіз кола актуальних суперечностей та проблем не дає змогу підприємствам реалізувати весь потенціал виробничих, економічно-соціальних і науково-технологічних можливостей з точки зору ефективного виробництва й реалізації кінцевих продуктів телекомунікацій. Ця проблема безпосередньо пов'язана з відсутністю структурного підходу до формування ефективної моделі структури проблем та протиріч, що визначає необхідність вивчення останніх.

Сфера послуги телекомунікаційного ринку в Україні як складова сфери послуг країни на даному етапі відноситься до однієї з найдинамічніших за розвитком сфер економіки. Доходи від надання телекомунікаційних послуг за 9 місяців (січень-вересень) 2016 року порівняно з аналогічним періодом минулого року збільшилися на 2,9 % і склали 36289,0 млн. грн., що становить 92,3 % від загальної кількості доходів від надання послуг зв'язку.

Але, не дивлячись на вищезазначене, сьогодні в Україні існує, так званий, феномен цифрової нерівності, цифрової прірви (digital divide) – поділ окремих верств населення на основі нерівного доступу до сучасних технологій. Це особливо актуально для споживачів важкодоступних сільських, гірських районів та соціально вразливих груп споживачів: малозабезпечені сім'ї, пенсіонери та інваліди.

Для розв'язання окресленої проблеми Законом України «Про телекомунікації» (далі – Закон) було введено поняття «загальнодоступні телекомунікаційні послуги» (набір обов'язкових послуг загального користування встановленого рівня якості), які надаються споживачам на всій території України за тарифами, що регулюються державою і встановлені не тільки нижче їх реальної вартості, але інколи й нижче собівартості.

Висновки

Підхід до вирішення суперечностей і проблем повинен бути цілеспрямований та структурований. У процесі глобалізації національної економіки і в період трансформації ринкових відносин в Україні сфера телекомунікацій як складова сфери зв'язку та інформатизації є головною

«артерією», що постачає, обробляє, допомагає споживати інформацію і потребує швидкого реагування на соціально-економічні протиріччя, що виникають, та їх загострення у вигляді проблем. Це можливо зробити, якщо комплексно підійти до системи управління об'єктом телекомунікацій та питання структури проблем на прикладі запропонованої моделі структури проблем.

Дотримання певних дій з боку системи управління підприємствами телекомунікацій в Україні для мотиваційного впливу за допомогою вирішення проблем системи управління на усіх соціально-економічних рівнях об'єкта та приведення останнього на бажаний фінансово- економічний та соціальний рівень. Але це вимагатиме певних, конкретних обмежень на виробництві й використання трудових і матеріальних ресурсів. Слід також зазначити, що в умовах стрімкого розвитку українського телекомунікаційного ринку зростає konieczність постійного моніторингу та аналізу отриманих даних на предмет реального стану справ і необхідність своєчасного реагування й усунення протиріч, що зароджуються.

Література:

1. Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009. – № 1. – С. 83-89.
2. Кузьмінов А.В. Узгодження мотиваційних впливів на ефективність механізму управління телекомунікаціями регіону: дис. ... канд. екон. наук: 08.07.04 / А.В. Кузьмінов, Одеська національна академія зв'язку ім. О.С. Попова. – Одеса, 2005. – 224 с.
3. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.
4. Економіка та соціальна політика [http://zt.knteu.kiev.ua/files/2014/5-6\(76-77\)/uazt_2014_5-6_25.pdf](http://zt.knteu.kiev.ua/files/2014/5-6(76-77)/uazt_2014_5-6_25.pdf)

Говгаленко Максим

Державний університет телекомунікацій

Факультет Телекомунікацій

м. Київ

АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ M2M МЕРЕЖ З ВЕЛИКОЮ ПЛОЩЕЮ ПОКРИТТЯ

У зв'язку зі значною кількістю різних технологій радіозв'язку, що застосовуються для підключення пристроїв IoT, і великого різноманіття смуг радіочастот, в звіті наведено детальний опис класів таких технологій разом з конкретними прикладами технологій. Особливу увагу слід приділити новому класу радіотехнологій, оптимізованих для обслуговування різних датчиків і сенсорів, що працюють довгий час від батарейок і мають велику дальність, отримав назву LPWAN

Додатки M2M, яким необхідна велика дальність зв'язку або велика зона покриття, широко використовують стільникові мережі. Найкращою стільниковою технологією в даний час є UMTS, частково через її низьку вартість, а також тому, що це єдина технологія передачі даних, яка в даний час забезпечує покриття на національному рівні. Однак останнім часом

розробляється багато технологій для роботи в безліцензійних смугах частот, які націлені на даний сегмент застосувань M2M. Зокрема, інтерес проявляється до конкретних технологій M2M, які оптимізовані для виконання великого числа з'єднань, але при відносно невеликих обсягах, переданих даних.

В першу чергу дані технології передбачається використовувати в різних системах інтелектуального обліку. Інтелектуальні лічильники все частіше застосовуються в системах по оптимізації використання електроенергії. Як доповнення до стільникового UMTS-мережі для передачі даних від інтелектуальних лічильників до мережевого вузла будуть використовуватися вузькосмугові системи в окремих смугах частот. Існує ряд комерційних компаній, які пропонують розгортання виділеної бездротової вимірювальної інфраструктури в це дозвіл частот 410-430 МГц, і які планують використовувати існуючі мережі для забезпечення великого охоплення території в поєднанні з низьким енергоспоживанням комплектуючих системи.

Бездротові технології M2M, що не відносяться до стандартів стільникового зв'язку або мобільного широкосмугового доступу, але забезпечують широке охоплення.

У 2015 році Semtech Corporation і дослідницький центр IBM Research був представлений новий відкритий енергоефективний мережевий протокол LoRaWAN (Long Range Wide Area Networks) для бездротової передачі даних з і на пристрої IoT, а також був створений альянс LoRa Alliance для просування даного стандарту[1]. Стандарт є відкритим за винятком реалізації на чіпі, яка контролюється Semtech Corporation.

В основу сигналу LoRa покладено канал 125 кГц з сигналом на основі розширення спектра шляхом лінійної частотної модуляції (CSS - chirp spread spectrum) з інтегрованою прямою корекцією помилок FEC. Однак основною особливістю LoRa стало створене навколо стандарту співтовариство, яке почало активно впроваджувати даний стандарт як в якості операторської технології (країни Європи), так і в якості локальних рішень для окремих будівель або невеликих підприємств (країни Азії). Зокрема, даний стандарт був підтриманий деякими великими стільниковими компаніями, що ще більше підштовхнуло розвиток екосистеми для даного стандарту. Відкритість бізнес-моделі стандарту (за винятком чіпа) дозволила операторам інтегрувати рішення LoRa в свою діючу інфраструктуру. Загальна схема організації сервісу на основі LoRa показана на рис.1. Відмінністю цієї схеми від таких технологій як «Стриж» та Sigfox є можливість організації власних серверів на базі одного з доступних програмних рішень від спільноти розробників LoRa.

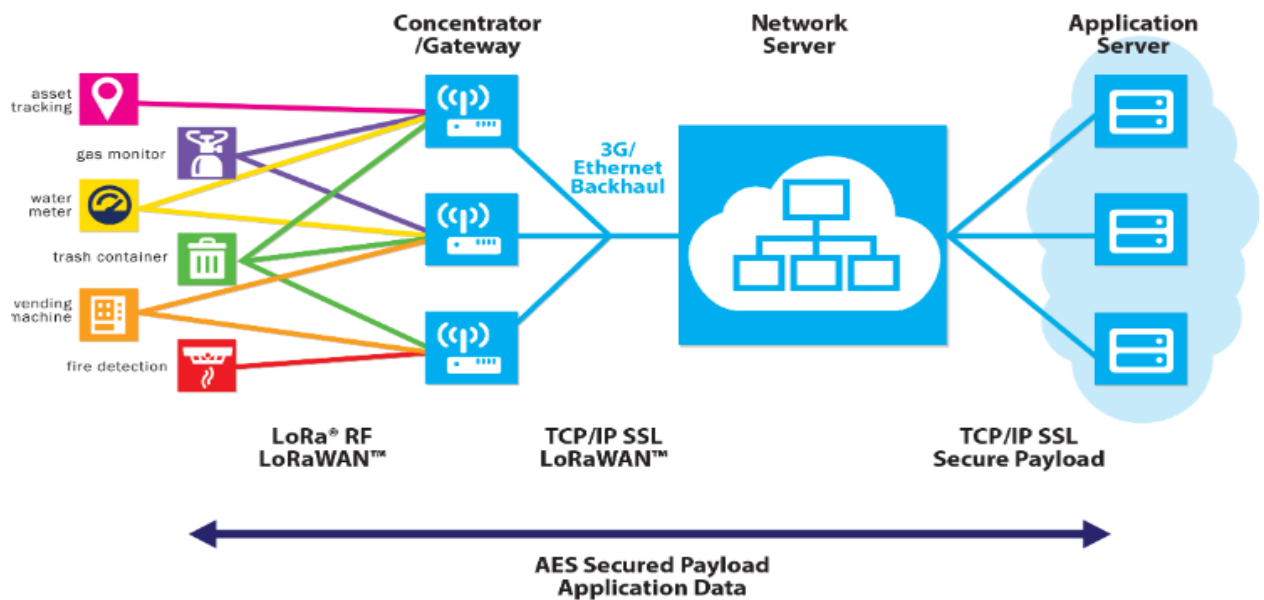


Рисунок 1 - Схема організації мережі LoRa

Ключові канали оповіщення і зв'язку з пристроями для Європейського ринку зосереджені в смугах радіочастот 868.0-868.6 МГц і 869.4-869.65 МГц. З урахуванням перевантаженості даних каналів в Європі LoRa Alliance зміг пролобіювати з іншими організаціями виділення у 2017 році чотирьох додаткових каналів в діапазоні 865-868 МГц для пристроїв малого радіусу дії.

Література:

1. Augustin A.; Yi J.; Clausen T.; Townsley W.M. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors* 2016, 16, 1466.
2. Koucheryavy, A. E. Internet of Things // *Electrosvyaz*. 2013. No. 1. pp. 21–24.

Каграманова Юлія
Державний університет телекомунікацій
Факультет Телекомунікацій
м. Київ

СИСТЕМА ЗВ'ЯЗКУ END-TO-END

Мене часто питають, навіщо ховати електронне листування, мені нема чого приховувати. Що ж можливо вам і насправді немає чого ховати, проте безпека персональних даних це щось значно більше.

Уявіть, що вийде, якщо ваше листування буде доступне кому завгодно, і кожен зможе знати, що ви робите, куди йдете, у що вірите, кого любите, або навпаки, кого не любляете. Такий світ стане всього на крок від тоталітарної системи описаній в книзі Ореула - 1984. Також існує і фактор технічної безпеки - усе наше життя сьогодні в мережі. Ми користуємось послугами банків, ми укладаємо угоди, висилаємо персональну інформацію, і усе це в електронному

вигляді. Уся світова економіка стала електронною і без шифрування сьогодні просто не обійтись.

Сама ідея end-to-end не нова. У 1991-му році Філом Зіммерманом було розроблено програмне забезпечення для шифрування повідомлень і інших даних PGP (Pretty Good Privacy). У наступні роки алгоритм і відповідне ПО вдосконалили і додали додаткові механізми.

У 1997-му році компанія PGP Inc. запропонувала ініціативу OpenPGP, а в 1999-му учасниками руху вільного програмного забезпечення на основі відкритого стандарту була створена вільна реалізація PGP - GnuPG.

Це все до того, що, так як злом PGP ще не був зафіксований, на основі відкритого PGP (адже вихідні коди є) можна створювати механізми шифрування, ніж, швидше за все, і займаються розробники месенджерів. Чи не писати адже з нуля.

Особливості

>>Технологія шифрування end-to-end робить повідомлення доступними тільки для співрозмовників.

>>Переважна більшість фахівців з інформаційної безпеки визнають наскрізне (end-to-end) шифрування найбільш стійким методом захисту інформації.

>>При end-to-end шифруванні ключі, які використовуються для шифрування та розшифрування інформації, генеруються і зберігаються тільки на кінцевих вузлах листування, тобто, у її учасників.

>>Серверна сторона не бере ніякої участі в створенні ключів, а, отже, не має до них доступу, в результаті чого, бачить тільки закодовані дані, що передаються між учасниками. Тільки останні можуть розкодувати і прочитати інформацію.

Як працює?

Технологія шифрування end-to-end це доволі складна технологія шифрування, яку можливо пояснити буквально на пальцях. Спілкуючись зі своїм другом я відсилаю йому відкритий замок і невелику дорожню скриню. Мій друг кладеш свій лист, закриває його на замок своїм відкритим ключем і відсилає його мені. І ніхто, крім нас двох не може прочитати записку, яка лежить у цій скринці тому, що у них не буде закритого ключа, яким володію тільки я, і ніхто більше. Тим самим я зможу майже на 100% захистити своє листування.

Під час початку сеансу зв'язку, на стороні кожного співрозмовника генеруються по 2 ключа: відкритий і закритий. Останній використовується для розшифровки даних, цей ключ не залишає межі локального пристрою.

Відкритий ключ з відкритого каналу зв'язку передається співрозмовнику (одному або всім, в разі, якщо їх декілька). За допомогою відкритого ключа співрозмовник може тільки зашифрувати дані, а розшифрувати їх може тільки власник відповідного закритого ключа. Тому, не важливо, хто перехопить відкритий ключ. В результаті цього, він зможе тільки передавати свої зашифровані дані.

Згенерувавши по парі ключів, співрозмовники обмінюються відкритими ключами, після чого починається захищене спілкування.

Текст, відео, аудіо, файли після шифрування у відправника потрапляють на сервер, де зберігаються, поки одержувач не буде в змозі отримати дані. Після цього, в залежності від стратегії компанії - власника сервера, дані або знищуються, або зберігаються ще на якийсь термін.

Література:

iphones.ru/iNotes/595634

geektimes.ru/post/273884

spark.ru/startup/actor/blog/7905/end-to-end-shifrovanie-ono-togo-stoit

swissinfo.ch/rus/видео_что-такое-end-to-end-шифрование--i-/42288308

en.wikipedia.org/wiki/End-to-end_encryption

Поливода Євгеній Григорович
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

АНАЛІЗ ВИМОГ ДО ВИМІРЮВАЛЬНОЇ СИСТЕМИ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ

У галузі зв'язку відбуваються радикальні зміни: загострюється конкуренція на ринку, зростають вимоги до якості обслуговування з боку користувачів, відбувається технічне переозброєння мереж зв'язку, змінюється характер розподілу трафіку. Проходячи через призму експлуатації, ці зміни призводять до необхідності здійснення контролю та управління трафіком і якістю мереж різних технологій.

Тут на допомогу оператору приходять системи моніторингу мереж зв'язку. Вони не тільки змінюють уявлення про систему експлуатації, переходячи від експлуатації окремих станцій до експлуатації всієї мережі.

В даний час мобільні оператори використовують вимірювальні комплекси, розроблені закордонними виробниками. Зарубіжні вимірювальні комплекси володіють високою точністю і вартістю. Постійна присутність інженера необхідно при пошуку і усунення несправностей, а також збоїв в роботі окремих базових станцій або мережі в цілому. Для постійного моніторингу мережі такий підхід є витратним і не завжди ефективним, оскільки необхідно залучати велику кількість висококваліфікованих операторів для постійних об'їздів зони покриття.

У кожного оператора управління мережею влаштовано по-різному. Оператори зв'язку переходять на нові моделі управління своїми мережами. І якщо раніше централізованим був виключно моніторинг, то зараз до цього додається можливість повноцінного управління як на магістральних лініях зв'язку, так і на окремих сегментах підмереж в самих різних регіонах України.

Центр контролю є пункт віддаленого управління рис.1. Обладнання встановлене по всій мережі, а центр отримує до нього віддалений доступ. Під контролем знаходиться більше 30 тис. базових станцій, понад 350 ключових елементів мережі, понад 500 MSC і MGW і, приблизно 22 млн. абонентів.



Рисунок 1- Пункт віддаленого управління

Центр управління мережею включає в себе чотири основні компоненти.

Network resource inventory - система обліку даних мережі.

Fault management - система аналітики і реагування на проблеми і збої в роботі.

Trouble Ticketing - єдина система роботи з інцидентами і координації планових робіт.

Performance management - технічна статистика. Для зниження витрат на періодичний моніторинг мережі стільникового зв'язку, а також для безперервного моніторингу якості надаваних послуг пропонується використання розподіленої інформаційно вимірювальної системи.

Дана система повинна забезпечувати вимірювання наступних параметрів:

1). В системі WCDMA (3G):

- Відношення сигнал/шум обслуговуючої стільниці (CPICH EC/NO);
- Рівень сигналу обслуговуючої стільниці (CPICH RSCP);
- Рівень пілот сигналу до 6-ти сусідніх сот;
- Передає частота (Tx Rate);
- Приймальня частота (Rx Rate);
- Скремблювальний код;
- Каналоутворюючий код.

2). В системі GSM (2G):

- Рівень несучого обслуговуючого стільника (Rx Lev);
- Якість сигналу обслуговуючого стільника (Rx Qual);
- Рівні несучих до 6-ти сусідніх сот;
- Абсолютне значення частоти каналу (ARFCH (BCCH/TCH)).

3). В системах WCDMA- GSM:

- Ідентифікатор стільника;
- Код локальної зони (LAC);
- Координати точки вимірювання;
- Тест бітової швидкості Інтернет-з'єднання.

При довготривалому моніторингу параметрів зони покриття неважлива висока точність виміряних значень, набагато важливіше здатність інформаційно-вимірювальної системи проводити вимірювання автономно і автоматизовано.

Мобільні комплекси повинні проводити вимірювання без активної участі оператора.

Література:

1. Инфокоммуникационные системы и технологии: проблемы и перспективы. – СПб.: Изд-во Политехн. ун-та, 2007. – 592 с.
2. Попов В.И. Основы сотовой связи стандарта GSM/ Попов В.И., В.В. Андреев// М.: ЭкоТрендз. - 2005. - 296с.
3. Ипатов В.П. Системы мобильной связи/ В.П. Ипатов, В.К. Орлов, И.М.Самойлов, В.Н. Смирнов. - М.: Горячая линия-Телеком. - 2003.- 272с.
4. Шишкин В.В. Интеллектуальные технологии при проектировании сетей сотовой связи/ Шишкин В.В., Серов Д.В.// Ульяновский государственный технический университет

Демченко Александр Викторович
Государственный университет телекоммуникаций
Факультет телекоммуникаций
Г.Киев

CONTENT MANAGEMENT SYSTEM

Термин CMS в последнее время достаточно часто встречается на просторах интернета. Что же это? Одни говорят, что это «движок» и «сердце» сайта, другие - инструмент для эффективного решения рутинных задач по размещению информации и редактированию или созданию разделов. В данном случае правы обе стороны.

Основной задачей такой системы является сбор и объединение в единое целое, на основе ролей и задач, различных источников информации. Эти источники могут быть доступны как внутри самой организации, так и вне её пределов. К тому же данная система обеспечивает возможность взаимодействия различных сотрудников, проектов и рабочих групп, с теми базами знаний и данных, которые были ранее созданы, в таком виде и таким способом, чтобы сделать процесс поиска и повторного использования максимально комфортным и привычным.

В такой системе управления контентом определяется всё многообразие существующих данных: стандартные документы, музыка и звуки, видео, каталоги всевозможной информации и многое-многое другое. И именно для управления, хранения, обработки, просмотра и публикации таких данных различными группами пользователей и служат CMS. Отсюда кстати возникает и новый род профессиональной деятельности - контент менеджер, или проще говоря - редактор сайта.

Для чего нужна CMS?

Если смотреть с точки зрения обычного заказчика, то разработка сайта на основе какой-либо CMS должна приносить следующие преимущества:

- в работе используется наиболее эффективный инструмент для решения конкретной задачи;
- использование CMS позволяет владельцу сайта самостоятельно создавать и удалять разделы сайта, редактировать различную информацию без привлечения стороннего специалиста - это одно из преимуществ статическими сайтами;
- работа сайта постоянно тестируется множеством пользователей, а найденные ошибки и уязвимости достаточно оперативно устраняются, при этом сайт работает на самых передовых и проверенных технических решениях;
- временные затраты на разработку сайта существенно снижаются, так как разработчику не надо фиксировать своё внимание на чисто технических задачах: «как сделать ленту с новостями» или «как научить CMS искать товары в каталоге», а можно сосредоточиться на информационной и визуальной составляющих будущего сайта;

КАКИЕ БЫВАЮТ CMS?

Совершенно разные! Некоторые системы ориентированы только на решение конкретных задач (ведение блогов, интернет магазины, форумы), другие являются универсальными и предоставляют разработчиком удобную среду проектирования и программирования для разработки чего угодно. Часть CMS состоять из множества функциональных блоков и модулей, другие монолитны, неделимы, да ещё и зашифрованы. Одни системы поставляются бесплатно и с возможностью внесения своих доработок, а некоторые предоставляются за деньги и не допускают возможность редактирования ядра «движка».

До сих пор нет единой и чёткой классификации, принятой рынком, существующих CMS, однако это не мешает выделить лидеров в данной области. Тут приведём лишь краткий их перечень, без выделения сильных и слабых сторон:

- Joomla - (самая противоречивая система) - яркая, современная, постоянно обновляющаяся, достаточно простая в разработке и использовании, предоставляется совершенно бесплатно;
- Drupal - (для любителей разработки сайтов с нуля) - это не просто полноценная функциональная среда для разработки и создания всевозможных сайтов, которая предоставляется так же бесплатно и имеет гибкие возможности, но и в каком-то смысле - стиль программирования и даже жизни;
- MODx - достаточно современная разработка, которая в последнее время уверенно набирает обороты и увеличивает свою аудиторию поклонников. К тому же она является чрезвычайно гибкой и эффективной, при этом поставляется безвозмездно, но и порог вхождения в число разработчиков на этой CMS несколько выше, чем у других систем;

- 1С Битрикс - монстроподобная разработка от небезызвестной 1С, в которой можно найти различные редакции от простой, до порталной, при этом стоимость её значительно отличается от версии к версии;

Важное замечание: бесплатность CMS отнюдь не означает низкое качество кода или наличие ограничений в использовании. Наоборот, чаще всего, открытые и бесплатные CMS во многом выигрывают у своих коммерческих собратьев именно из-за своей общедоступности. Над этими системами трудятся не только коллективы профессиональных разработчиков, но и сотни и даже тысячи добровольцев, которые стремятся сделать любимую CMS ещё лучше и безопасней.

Сложно сделать правильный выбор среди такого разнообразия, поэтому необходимо чётко осознавать назначение и функционал будущего сайта. К примеру, если заказчику нужен всего лишь небольшой личный блог, то нет смысла ему приобретать «1С-Битрикс - корпоративное решение» за 100 с лишним тысяч рублей. Поэтому задача разработчика сайта - не только в том, чтобы сделать сайт точно в срок и с учётом пожеланий заказчика, но и выбрать правильную и достаточную CMS для этих целей.

НЕДОСТАТКИ САМОПИСНЫХ CMS

Многие web-студии и разработчики предлагают системы собственной разработки именно как лучший из возможных вариантов. Для небольших сайтов типа: сайт-визитка или каталог, или сайтов, которые в будущем не планируется модернизировать, такой вариант может быть ещё как-то приемлемым. А вот в случае разработки чего-то более-менее серьёзного или масштабного, а так же того, что в скором времени потребует доделок, или изменений, такая CMS будет сильно проигрывать любой из популярных систем. Заказчик будет просто привязан непосредственно к первоначальному разработчику, ведь для того чтобы изучить новую систему - требуется определённое время и силы, а найти того, кто захочет разобраться в чужой разработке не так уж и просто.

Ещё одним минусом самописных CMS является её уязвимость, особенно это касается интернет-магазинов, в которых вопрос безопасности стоит очень высоко. Ведь на подобных сайтах могут храниться номера кредитных карточек, различные платёжные документы и прочая конфиденциальная информация - это очень лакомый кусочек для различного рода злоумышленников и просто любителей что-нибудь испортить. А без массового тестирования уязвимостей и своевременного обновления «сердца» системы - безопасное функционирование сайта становится под угрозой.

И ещё один момент: очень часто разработчики сайтов, уверяют будущих владельцев сайтов, что с помощью их всемогущей, удобной и простой CMS - заказчик самостоятельно сможет создавать или редактировать структуру сайта, добавлять новый функционал одним кликом и т.п. На самом деле - это полуправда. Да, выполнять элементарные вещи по созданию новых материалов, публикации или редактированию статей с новостями или загрузке картинок в галерею - почти не требует никаких особых навыков, но для использования расширенных возможностей CMS несомненно нужно разбираться в базовых

web-технологиях, знать основы программирования и самое главное- иметь желание и возможность разбираться в чём-то новом.

Любая CSM - это не волшебство и не панацея, а всего лишь инструмент, который в умелых руках действительно способен творить чудеса.

Литература:

1. <http://moolkin.ru/joomla/cms/chto-takoe-cms-dlya-chego-ona-nuzhna-kakie-byvayut-cms>
2. https://ru.wikipedia.org/wiki/Система_управления_содержимым

***Данилюк Віталій Олександрович**
Державний університет телекомунікацій
Факультет телекомунікацій
м. Київ*

ЗАГАЛЬНЕ ПРО БЕЗДРОТОВІ МЕРЕЖІ

Термін Бездротовий використовується на позначення класу технологій зв'язку та технологій передачі даних без використання електричних провідників, або «дротів». Ця відстань може бути як малою (декілька метрів, як у телевізійному дистанційному керуванні), так і дуже великою (тисячі або навіть мільйони кілометрів для телекомунікацій). Ідея бездротового середовища вельми приваблива, оскільки її компоненти:

- забезпечують тимчасове підключення до кабельної мережі;
- допомагають організувати резервне копіювання у кабельну мережу;
- гарантують певний рівень мобільності;
- дозволяють зняти обмеження на максимальну протяжність мережі, що накладаються мідними або навіть оптоволоконними кабелями.

МЕРЕЖ НА СТІЛЬНИКОВИХ МОДЕМАХ

Мережі на стільникових модемах використовують наявну інфраструктуру стільникової телефонії. Вони працюють в особливо важких умовах великих завод, періодичного зникнення сигналу. Стільникові технології пройшли декілька етапів розвитку:

- 1G-технології. Початок 80-х, Перше покоління стільникових мереж використовувало аналогові технології. В таких мережах передавали тільки телефонні розмови;
- 2G-технології. Середина 90-х. Цифрове кодування та передавання мовлення і коротких текстових повідомлень;
- 2,5G- технології. 2001 рік (США). Цифрові мережі з передаванням мовлення, тексту, приєднання до Internet;
- 3G-технології. Технологія наступного покоління. Швидкість передавання до 2 Мбіт/с. Передавання мультимедійних даних. Окремі технології доступні у Японії, планується впровадити в Україні.
- Серед методів доступу виділяють аналогові, які використовують для передавання аналогового сигналу. Це класичні методи у стільникових

мережах **FDMA** (Frequency Division Multiple Access), **TACS** (Total Access Communication System).

- Серед методів доступу, які використовують цифрове передавання, популярні різні модифікації **TDMA** (Time Division Multiple Access). Вони застосовують відомий принцип розподілу часу передавання на окремі часові слоти. До цієї групи методів належать **AMPS** (Advanced Mobile Phone Service) (частотні канали завширшки 30 КГц поділяють на три часові слоти), **NAMPS** (Narrowband AMPS), **PDC** (канали по 25 КГц, три слоти), **GSM** (діапазон 200 КГц, вісім слотів).

- Найпередовішою сьогодні є технологія **CDMA** (Code Division Multiple Access), що використовує цифрове передавання.

Цей механізм кодування забезпечує такі властивості:

- сигнал захищений від підслуховування. Треба знати псевдовипадкову послідовність-ключ. Цим пояснюють широке використання цього підходу військовими;

- сигнал захищений від завад. Широкопasmовість сигналу дає змогу просто поновлювати сигнал, особливо якщо завади вузькопasmові. Так само сигнал захищений і від тимчасового зникнення на окремих частотах (фейдінг (fading));

- широкопasmове передавання та ліпший захист від завад дають змогу зменшити потужність передавачів, збільшити час дії акумуляторів та дещо зменшити безперечно шкідливий вплив цієї технології на здоров'я людини;

- дві абонентські станції, які працюють у межах однієї стільникової комірки на однаковій частоті з використанням різних кодувальних послідовностей, практично не створюють завад одна одній.

- Ще однією перевагою CDMA є змога використання у сусідніх комірках одного й того ж частотного діапазону, що полегшує планування мережі та збільшує кількість каналів.

- Особливістю, яка поліпшує якість передавання у CDMA-мережах, є механізм відпрацювання переходу абонента з однієї комірки до другої. В інших технологіях під час такого переходу спочатку розривається зв'язок з одією базовою станцією, а потім налагоджується з іншою (hard handoff, break before make). Це знижує якість передавання. У технології CDMA завдяки збереженню однієї частоти-носія у сусідніх комірках можна спочатку налагодити сполучення з новою станцією, а вже потім розірвати з попередньою. Це поліпшує якість переходу і дає змогу коректно опрацювати передавання у "прикордонній зоні", коли передавач може багато разів переходити зі сфери діяльності однієї базової станції у сферу діяльності іншої та навпаки.

- Технологія **CDPD** (Cellular Digital Packet Data) реалізує як пакетне передавання (протокол TCP/IP), так і модемний інтерфейс (АТ-команди). На відміну від радіомодемів, стільникові модеми використовують не спеціальні антени та приймачі-передавачі, а відповідні пристрої стільникового телефону.

- Розвиток технологій на вищих рівнях протоколу виражений в організації доступу до Internet. Цей доступ можливий завдяки використанню WAP-технологій. Дякую за увагу.

Список літератури:

1. <https://goo.gl/LdUKbf>
https://studopedia.su/9_51323_merezhi-na-stilnikovih-modemah.html

Пономаренко Олег Олександрович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

Головним напрямком перебудови менеджменту і його радикального удосконалення, пристосування до сучасних умов стало масове використання новітньої комп'ютерної і телекомунікаційної техніки, формування на її основі високоефективних інформаційно-управлінських технологій.

Засоби і методи прикладної інформатики використовуються в менеджменті і маркетинзі. Нові технології, засновані на комп'ютерній техніці, вимагають радикальних змін організаційних структур менеджменту, його регламенту, кадрового потенціалу, системи документації, фіксування і передачі інформації.

Особливе значення має впровадження інформаційного менеджменту, значно розширювальної можливості використання компаніями інформаційних ресурсів. Розвиток інформаційного менеджменту зв'язано з організацією системи обробки даних і знань, послідовного їх розвитку до рівня інтегрованих автоматизованих систем управління, що охоплюють по вертикалі і горизонталі всі рівні і ланки виробництва і збуту.

Технологія — це комплекс наукових і інженерних знань, реалізованих у прийомах праці, наборах матеріальних, технічних, енергетичних, трудових факторів виробництва, способах їх з'єднання для створення продукту чи послуги, що відповідають визначеним вимогам.

Технологія нерозривно зв'язана з машинізацією виробничого чи невиробничого, насамперед управлінського процесу. Управлінські технології ґрунтуються на застосуванні комп'ютерів і телекомунікаційної техніки.

Відповідно до визначення, прийнятому ЮНЕСКО, **інформаційна технологія** — це комплекс взаємозалежних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і збереженням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим устаткуванням, їхні практичні додатки, а також зв'язані з усім цим соціальні, економічні і культурні проблеми. Самі інформаційні технології вимагають складної підготовки, великих первісних витрат і наукомісткої техніки. Їхнє введення повинне починатися зі створення

математичного забезпечення, формування інформаційних потоків у системах підготовки фахівців.

Які сучасні технічні засоби використовуються для автоматизації інформаційно-управлінської діяльності?

В останні десятиліття менеджменти в найбільш розвинутих країнах, зокрема, у США і Японії, на творчі інформаційні технології так званого третього (вищого) рівня. Вони охоплюють повний інформаційний цикл — вироблення інформації (нових знань), їх передачу, переробку, використання для перетворення об'єкта, досягнення нових більш вищих цілей.

Інформаційні технології третього рівня означають вищий етап комп'ютеризації менеджменту, дозволяють задіяти ЕОМ у творчому процесі, з'єднати силу людського розуму і міць електронної техніки.

Повна інтегрована автоматизація менеджменту припускає охоплення наступних інформаційно-управлінських процесів: зв'язок, збір, збереження і доступ до необхідної інформації, аналіз інформації, підготовка тексту, підтримка індивідуальної діяльності, програмування і рішення спеціальних задач. Основні напрямки автоматизації інформаційно-управлінської діяльності компаній наступні: автоматизація процесу обміну інформацією, включаючи управлінську АТС, "електронну пошту". До сучасних технічних засобів автоматизації інформаційно-управлінської діяльності відносяться:

- персональні комп'ютери, об'єднані в мережі;
- електронні друкарські машинки;
- текстооброблюючі системи (проблемноорієнтовані комп'ютерні системи, які мають великі функціональні можливості);
- копіювальні машини;
- комунікаційні засоби, телефонну техніку;
- засоби для автоматизації введення архівних документів і пошуку інформації (до них відносяться нетрадиційні носії інформації: магнітні диски і стрічки, мікрофільми, диски з оптичними записами);
- засоби для обміну інформацією — "електронна пошта";
- відеоінформаційні системи;
- локальні комп'ютерні мережі;
- інтегровані мережі установ.

Сучасні телекомунікаційні технології у корпоративному управлінні

Корпоративне управління - це комплекс управлінських дій, що компанія повинна здійснити, щоб досягти свою ціль, завоювати гарну репутацію і довіру кредиторів і інвесторів.

Інвестори, перш ніж прийняти рішення про співробітництво й інвестиції в яке-небудь підприємство, аналізують його положення, у першу чергу з погляду існуючої системи менеджменту. Підвищення управлінської культури тісно зв'язано з використанням сучасних телекомунікаційних і інформаційних технологій.

У сучасному світі перед компаніями, які займаються тим чи іншим бізнесом, постійно виникають ті самі питання:

- як краще й ефективніше організувати обмін інформацією усередині компанії, а також з партнерами і клієнтами,
- як зробити інформаційний простір компанії єдиним, незважаючи на географічну далекість ряду офісів,
- як дотриматись безпеки передачі даних і забезпечити високої надійності зв'язку,
- як при цьому не упускати переваг нових технологій і мінімізувати свої витрати.

Такі питання виникають у будь-якій країні світу і перед компаніями різних сфер діяльності, незалежно від розміру чи кваліфікації. Усі перераховані проблеми мають "телекомунікаційну складову". Адже будь-який бізнес не може існувати без обміну інформацією. Від того, наскільки ефективно й оптимально побудована корпоративна мережа зв'язку і буде деякою мірою залежати успіх чи неуспіх компанії у веденні бізнесу в цілому.

Можливі наступні варіанти. Як правило, компанія, перед якою встали подібні проблеми, може вирішити їх двома способами. Перший полягає у використанні власних ресурсів для рішення виникаючих задач. При такому підході компанії прийдеться створити департамент зв'язку, який виконує в тій чи іншій степені функції професійного оператора, скористатися послугами одного чи декількох незалежних операторів зв'язку для одержання "базових телекомунікаційних сервісів".

Також необхідно самостійно проаналізувати сучасне устаткування, підготувати приміщення, у яких установити і настроїти апаратне і програмне забезпечення. Рішення цих проблем займає тривалий період часу, є витратним, не гнучким, не технологічним, тому що реалізується, у кінцевому рахунку, не професійним телекомунікаційним оператором.

Інший варіант - це вдатися до послуг оператора зв'язку, що може запропонувати такій компанії-клієнту готове рішення. Подібний підхід виявляється оптимальним і відповідає вищевикладеним вимогам. Саме тому компанії всі частіше для рішення комплексної задачі створення універсальної корпоративної мережі зв'язку прибігають до послуг телекомунікаційних провайдерів.

Для оператора зв'язку такий аутсорсинг також дуже цікавий і вигідний, оскільки розширює сферу його діяльності і дозволяє йому одержувати додаткові доходи.

Послуги по створенню і управлінню віртуальними приватними корпоративними мережами зв'язку відносяться до числа сучасних "аутсорсингових" технологій. Більшість операторів як за рубежом, так і в Росії вже пропонують чи активно розробляють подібні сервіси. Для прикладу, нова послуга Компанії Транстелеком, ТТК IP VPN належить до їхнього числа. ТТК IP VPN - широкосмугова приватна віртуальна мережа зв'язку (ВЧС) на основі магістральної IP-мережі Компанії Транстелеком і IP-технологій.

У рамках послуги Транстелеком організує інтегральну мережу зв'язку Клієнта, забезпечує управління мережею й експлуатацію. Тим самим компанія-клієнт може зосередитися на своєму основному профільному бізнесі, доручаючи професійному оператору рішення всіх телекомунікаційних питань, що виникають у процесі своєї бізнес-діяльності.

Особливістю послуги ТТК IP VPN є те, що вона може бути надана в комплексі з доступом у мережу Інтернет.

Технологія Інтернет також має безпосереднє відношення до систем корпоративного управління. Ось декілька областей, у яких Інтернет використовується в даний час найбільш продуктивно: маркетинг, прямі продажі, зв'язки з громадськістю, взаємодія з партнерами.

Використовуючи високошвидкісну магістральну мережу зв'язку компанія може мати виділений доступ в Інтернет, який володіє наступними перевагами:

- високошвидкісне з'єднання з міжнародною частиною Інтернет;
- доступність послуг не тільки у великих містах, але й у будь-яких інших населених пунктах, через які проходить залізниця;
- висока надійність наданих послуг за рахунок резервування магістралей IP мережі.

Історія автоматизації управління підприємствами обчислюється десятиліттями. Але останнім часом при стрімкому розвитку телекомунікаційних технологій у компаній з'являються нові можливості по оптимізації корпоративних систем керування. Дякую за увагу.

Список літератури:

1. <https://uk.wikipedia.org>
2. <http://hi-news.pp.ua/tehnika-tehnologiyi/7039-telekomunikacyn-tehnologiyi-tehnchn-zasobi-funkcyi-vikoristannya-rozvitok.html>

Панченко Владислав Ігорович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м.Київ

ЗАХИСТ У МЕРЕЖАХ WI-FI

WEP-шифрування:

Аналог шифрування трафіку в провідних мережах. Використовується симетричний потоковий шифр RC4, який досить швидко функціонує. На сьогоднішній день WEP і RC4 не вважаються криптостійкими.

Є два основних протоколи WEP: 40-бітний WEP (довжина ключа 64 біта, 24 з яких — це вектор ініціалізації, який передається відкритим текстом); 104-бітний WEP (довжина ключа 128 біт, 24 з яких — це теж вектор ініціалізації); Вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності алгоритму.

TKIP-шифрування(Temporal Key Integrity Protocol):

Використовується той же симетричний потоковий шифр RC4, але є більш криптостійким. Вектор ініціалізації становить 48 біт. Враховані основні атаки на WEP. Використовується протокол Message Integrity Check для перевірки цілісності повідомлень, який блокує станцію на 60 секунд, якщо послані протягом 60 секунд два повідомлення не пройшли перевірку цілісності. З урахуванням всіх доопрацювань і удосконалень TKIP все одно не вважається криптостійким.

СКІР-шифрування(Cisco Key Integrity Protocol):

Має подібності з протоколом TKIP. Створений компанією Cisco. Використовується протокол CMIC (*Cisco Message Integrity Check*) для перевірки цілісності повідомлень.

WPA-шифрування:

Замість уразливого RC4, використовується криптостійкий алгоритм шифрування AES (*Advanced Encryption Standard*). Можливе використання EAP.

Є два режими:

Pre-Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі; Enterprise - перевірка здійснюється серверами RADIUS;

WPA2-шифрування:

Прийнятий у 2004 році, з 2006 року WPA2 повинна підтримувати все вироблене Wi-Fi обладнання. В даному протоколі застосовується RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Спочатку в WPA2 використовувався протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника). Основою є алгоритм AES. Для сумісності зі старим обладнанням є підтримка TKIP і EAP (*Extensible Authentication Protocol*) з деякими його доповненнями. Як і в WPA є два режими роботи: Pre-Shared Key і Enterprise.

Для виходу в інтернет переважна більшість користувачів домашньої мережі використовує Wi-Fi роутери. Коли мережа незахищена, її можуть використати зловмисники, вважають у Департаменті кіберполіції України. Саме тому, для захисту домашньої мережі від шахрайських дій кіберполіція склала рекомендації. Що варто знати і зробити – у рекомендаціях нижче:

1) Зміна налаштувань DNS серверу. Будь-яке доменне ім'я, наприклад, google.com.ua відповідає індивідуальній IP-адресі, тобто сайт google.com.ua відповідає IP-адресі 74.125.232.255. Якщо ввести у браузері замість сайту google.com.ua IP-адресу 74.125.232.255, завдяки DNS-серверу буде здійснено перехід на веб-сайт google.com.ua. Так, зловмисник може змінити DNS-сервер на свій власний і налаштувати, наприклад, щоб браузер при введенні сайту google.com.ua переходив на його особисту IP-адресу. Внаслідок цього буде здійснено перехоплення веб-трафіку або зараження вашого особистого ПК, чи будь-якого пристрою, який отримує доступ до мережі з вашого роутера.

2) Наступне, що може здійснити зловмисник – це перехоплення вашої особистої інформації шляхом атаки man-in-the-middle. В такому випадку ваш веб-трафік, який за замовчуванням відправляється до Wi-Fi роутера, буде

відправлений спочатку зловмиснику, а потім від нього до роутера. При цьому роутер не помітить змін. Така атака дозволяє хакеру викрасти ваші особисті дані (логіни, паролі), продивитись ваш веб-трафік – сайти, на які ви заходили.

3) Зловмисник, перебуваючи у вашій особистій Wi-Fi мережі, може здійснювати хакерські атаки (взломи сайтів, DDOS-атаки, додати ваші пристрої до бот-мережі, скачувати дитячу порнографію), тобто будь-які незаконні дії від вашого імені, оскільки Wi-Fi роутер має IP-адресу, яку вам надає ваш провайдер при сплаті інтернет-послуг: всі пристрої, підключені до вашого роутера або точки доступу в інтернет, будуть ідентифікуватись за вашою IP-адресою.

Література:

1. <https://uk.wikipedia.org/wiki>
2. <http://watcher.com.ua/2016/09/20/yak-zahystyty-domashnyu-wi-fi-merezhу-vid-hakeriv/>

Ніколаєнко Валерія Ігорівна
Державний університет телекомунікацій
Факультет Телекомунікацій
м.Київ

ІННОВАЦІЙНІ МЕТОДИ КРИПТОГРАФІЇ НА ПРИКЛАДІ МЕСЕНДЖЕРА TELEGRAM

У сучасному світі основна частина інтернет спілкування зосереджена на системах обміну миттєвими повідомленнями. І тут для будь-якого користувача з'являється основне питання: «Наскільки конфіденційне моє спілкування?». Очевидно, що всі криптографічні способи захисту повинні мати принаймні дві основні властивості: приватність та цілісність повідомлень. Приватність передбачає відсутність доступу третьої сторони до особистих даних та повідомлень, а цілісність, у свою чергу, захист від зловмисних атак заміни та випадкових спотворень. Звідси робимо висновок: основна задача розробників месенджерів – ефективна функція шифрування.

Досить цікавим та яскравим прикладом є мультиплатформенна служба миттєвих повідомлень – Telegram. Даний месенджер окрім звичного чату передбачає, так звані, «секретні» онлайн діалоги.

Для початку розглянемо хмарний, тобто звичайний чат. Його шифрування відбувається наступним чином: співрозмовник А відправляє повідомлення → воно шифрується спеціальними протоколами до вигляду незрозумілого поєднання символів → у такому вигляді зберігається в історії на пристрої користувача А → зашифрований текст переходить на сервер, де зберігається у тому ж вигляді → повідомлення приходить на пристрій отримувача Б і зберігається так само (в історії у зашифрованому вигляді) → за допомогою протоколів відбувається дешифрація даних → користувач Б отримує початкове

повідомлення ідентичне відправленому. Даний приклад криптографії є потенційно більш доступним для третіх осіб, так як ключі шифрування зберігаються на серверах компанії, тому що навіть найбільш захищений сервер має певні можливості для доступу хакерів до приватної інформації користувачів.

Тепер перейдемо до секретного чату, тут вже маємо реалізовані додаткові механізми захисту. Схема передачі повідомлення подібна до попередньої але містить деякі зміни: повідомлення не йдуть на сервер, а оминаючи його, потрапляють безпосередньо на пристрій учасника діалогу; переписка автоматично самознищується на пристроях через певний час; при видаленні в одного зі співрозмовників секретні повідомлення видаляються і в іншого; ключ шифрування прив'язується до конкретного пристрою, при його зміні не вдасться відновити повідомлення секретних чатів. Саме ця особливість передачі даних практично зводить нанівець вірогідні можливості втручання у особисті голосові або текстові повідомлення.

Для реалізації секретного чату використовується End-to-End шифрування, для месенджера був створений спеціальний протокол MTProto, який передбачає використання кількох протоколів шифрування – сервер-сервер та клієнт-сервер. А як відомо, застосування комбінованих методів захисту ускладнює можливість доступу третіх осіб у геометричній прогресії. Його робота базується на основі наступних алгоритмів:

- AES – симетричний 256-бітний алгоритм блочного шифрування, що є прийнятим в якості стандарту шифрування урядом США
- RSA – криптографічний алгоритм, основою якого є обчислювальна складність задачі факторизації великих цілих чисел
- Протокол Діффі-Геллмана – метод обміну криптографічними ключами, який дозволяє отримати захищений від підмін, але незахищений від прослуховування секретний ключ кільком співрозмовникам
- SHA-1 та MD5 – хеш-функція, що використовується для безпечного хешування.

Маючи можливість використовувати сучасний месенджер, користувач має практично 100% гарантію, що його особиста інформація потрапить саме туди, куди має, а можливість перехоплення чи зміни голосових або текстових повідомлень практично відсутня.

Таким чином, можна зробити висновок, що технології шифрування не стоять на місці, заходячи все більше сфер застосування, і саме обмін повідомленнями дозволяє відчути їх переваги кожному, хто має доступ до мережі інтернет.

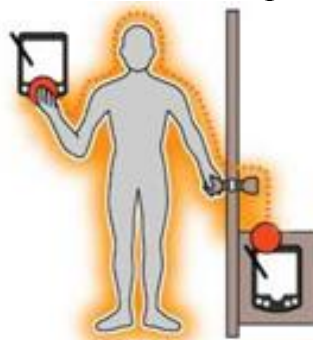
Джерела:

1. telegram.org/faq
2. Jakob Jakobsen. A practical cryptanalysis of the Telegram messaging protocol. Master Thesis, Aarhus University (Available on request)., 2015
3. core.telegram.org/mtproto
4. Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. CRC Press, 2014

ТЕХНОЛОГІЯ REDTACTON

Куди рухатиметься науковий прогрес, що буде зі світовим телекомунікаційним ринком надалі, які технології стануть доступними пересічним Інтернет-користувачам, наскільки можуть збільшитися швидкості інтернет-доступу в найближчі 5-10 років? На сьогоднішній день це експериментальна розробка, але через кілька років вона може щільно увійти в наше повсякденне життя.

Технологія RedTacton використовує найбільший біологічний канал передачі даних - шкіру людини. Чи бувало з вами таке, що ви дивилися фільм про шпигунів з їх високотехнологічними штучками і теж хотіли одним дотиком руки отримувати інформацію на свій телефон, обмінюватися електронними візитками і будь-якими іншими даними за допомогою рукостискання або роздруковувати документи, просто провівши рукою по принтеру? Все це і ще багато іншого може стати реальністю, якщо технологія RedTacton отримає розвиток.



Суть технології: технологія побудована на тому, що кожна людина має електромагнітним полем, а його шкіра може виступати каналом передачі сигналу між декількома електронними пристроями. В основі технології лежить використання електрооптичних кристалів, властивості яких змінюються під дією електромагнітного поля людини. А вже з кристалів за допомогою лазера зчитуються зміни і переводяться в більш-менш прийнятний формат. Причому система RedTacton може працювати не тільки в звичайних умовах, але і під водою, у вакуумі, в космосі.

Застосування: сьогодні нам доводиться часто користуватися різними кабелями, перехідниками та ін. для того, щоб, наприклад, підключити телефон до ноутбука або принтер до ПК. Якщо технологія RedTacton буде розвиватися, то незабаром всі ці дроти стануть непотрібними. Досить буде взяти в одну руку один гаджет, а іншою рукою торкатися другого пристрою. І з'єднання між ними відбудеться через наш шкірний покрив. Уже сьогодні більшість смартфонів оснащені екранами, які працюють від електромагнітних імпульсів на кінчиках наших пальців.

І це тільки перші кроки в популяризації даної технології. Вона може застосовуватися в медицині (всі ваші медичні дані можна записати на спеціальний чіп, який попередить лікаря про алергіях і непереносимості того чи іншого препарату після дотику до вас), збройних силах (можна зробити зброю, яке зреагує тільки на руки власника, і ваші діти ніколи не зможуть зашкодити собі, якщо знайдуть вдома ваш пістолет або мисливську рушницю), в побуті (ключі до входних дверей більше не потрібні, можна просто доторкнутися до замку і він спрацює від електромагнітного імпульсу), на виробництві (на заводах будуть встановлені датчики, які попередять вас про небезпечні зони і поломки, ви зможете швидко залагодити несправність, просто доторкнувшись до приладу) та інше.

Недоліки: технологія поки не вивчена достатньо, щоб точно сказати, що вона є абсолютно нешкідливою для організму людини. Впроваджувати RedTacton в маси можна буде тільки після того, як буде проведено безліч дослідів і досліджень. Небезпеки, перш за все, можуть піддаватися люди з підвищеною чутливістю і деякими медичними проблемами (особливо з серцевими захворюваннями). Крім того, хакери через якийсь час знайдуть спосіб красти дані людей або запускати комп'ютерні віруси, торкаючись до них в транспорті або на вулиці. Але основною проблемою цієї технології може стати психологія людей - багато сьогодні бояться комп'ютерів, Wi-Fi мереж і мікрохвильових печей, а можете собі уявити, що з ними буде, якщо їх власне тіло стане передавачем інформації?

Наука і технології рухаються вперед. А Інтернет-технології розвиваються чи не швидше за всіх інших. Щороку вчені винаходять все нові способи обмінюватися інформацією, спілкуватися на відстані, збирати, зберігати і передавати різні дані. Пройде ще десяток років, і ми будемо користуватися кожен день тими пристроями і можливостями, про які сьогодні можемо тільки мріяти.

Література:

1. <http://www.broadband.org.ua/tekhnologii-bystrogo-interneta/2381-internet-tekhnologii-budushchego-top-3-samykh-neobychnykh-sposobov-peredachi-informatsii>
2. https://studwood.ru/1610039/informatika/internet_tehnologiyi_maybutnogo

Димарчук Дмитрій Сергійович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

ТЕХНОЛОГІЇ ІР ПЕРЕДАЧІ ДАНИХ У СУЧАСНОМУ ТЕЛЕЦЕНТРІ

Головним трендом у розвитку телевізійних технологій є впровадження у виробництво технологій ультра високої роздільної здатності UHD TV 4к або 8к та мережевих технологій. І якщо сегмент «file based», для SD/HD/3G/UHD TV, демонструє сталий прогрес, то у сегменті «stream based» спостерігається певна невизначеність. Невизначеність не віддзеркалює розгубленість виробників щодо

шляху майбутнього розвитку - яку технологію обрати у якості базової? Вдосконалювати SDI, намагаючись підняти пропускну спроможність до рівня 4к і більше. Або, остаточно перейти на IP платформу. Ця невизначеність впливає з відсутності нових підмурків для розвитку того чи іншого напрямку. Хоча вже давно зрозуміло, що майбутнє за IP рішеннями.



Окрім бажання працювати у мережі, вибір між класичним SDI та IP спричинений і деякими додатковими чинниками: власне зараз не існує спеціалізованого SDI сигналу для передачі повного 4к та вище відео сигналу. Використовується просте збільшення кількості ліній зв'язку. Це дуже схоже на RGB або YUV інтерфейси за аналогової доби. Але передача одного сигналу одночасно по 4х окремих SDI кабелях не така вже і зручна. Інше обмеження виходить з бурхливого розвитку надшвидкісних відео камер. HD SSM камери доступні зі швидкостями x2, x3, x6. Відповідно збільшується кількість вихідних відео інтерфейсів.

Для вирішення проблеми передачі великої кількості сигналів одночасно, є більш ефективні засоби ніж звичайний SDI.

Аналізуючи події, що відбулися останнім часом, можна зробити майже 100% висновок - телевізійне виробництво переходить на IP платформу також і для передачі сигналів від/до камер, мікшерів, роутерів, модулів і тд. Обравши IP у якості наступного кроку виробники відкривають нові обрії виробництва. Це не лише production та post-production у форматі UHD TV, але й студійне виробництво та ефір. До того ж з'являються нові можливості пов'язані з використанням «хмарних» технологій у будівництві об'єктів телевізійної інфраструктури.

Стандартизація

Підмурком для будь-якої технологічної революції є стандартизація. Якщо у минулому та сьогодні інженери у визначенні типів сигналів користуються SMPTE-259 для SD SDI (270Mbps), SMPTE-292 для HD SDI (1.485Gbps), SMPTE-424 для 3G SDI (3Gbps), то зараз слід запам'ятати новий стандарт SMPTE 2022. Сам по собі цей стандарт має де кілька окремих підгруп:

SMPTE-2022 1/2/3/4 (IEEE802.3ab) – стандарт «real time» передачі відео, аудіо сигналів, постійного або змінного bitrate у вигляді скомпресованого MPEG-2, JPEG200 транспортного потоку у IP мережах.

SMPTE-2022 5/6 (IEEE802.3ae) – стандарт «real time» передачі відео, аудіо сигналів у вигляді не скомпресованого потоку даних у IP мережах.

Зазвичай, швидкість передачі відео за стандартом SMPTE-2022 1/2 достатня для роботи у мережах зі швидкістю до 1Gbps, в той час як стандарт SMPTE-2022 5/6 потребує мережі від 10Gbps. Такі відмінності визначають і галузь застосування стандартів:

SMPTE-2022 1/2/3/4 – прийнятий вже понад 20 років тому і є загальновідомим стандартом, використовується для одиночної або пакетної (video contribution, video distribution) доставки сигналів у стиснутому вигляді між віддаленими об'єктами інфраструктури, обміну сигналами між кількома виробниками, або доставки сигналів до кінцевих споживачів.

SMPTE-2022 5/6 – прийнятий лише у 2014 році і одразу кілька провідних виробників професійного обладнання анонсували його повну підтримку. Стандарт використовується для одиночної або пакетної доставки сигналів у професійній якості (камера – мікшер, мікшер – сервер, сервер – програмний кодер). Наслідуючи попередні версії 1/2/3/4 нова версія 5/6 також підтримує ущільнення кількох відео потоків у професійній якості в одному 10G мережевому інтерфейсі.

Відео у форматі SMPTE-2022 5/6 ідеально підходить для використання у складі студійних, ефірних апаратних, серверних. А також для обміну між кількома виробниками які працюють над спільним проектом.

Слід зазначити, що існування та розвиток «serial digital interface» не припиняється. У 2014 році анонсовані роботи з розробки стандартів для SDI відео сигналів UHD TV. Це SMPTE ST-2081 для 6G SDI (6Gbps), SMPTE ST-2082 для 12G SDI (12Gbps), SMPTE ST-2083 для 24G SDI (24Gbps). Однак з прийняттям SMPTE 2022 склалась ситуація за якої розвиток IP інфраструктури для передачі відео сигналів почав випереджати розвиток класичної інфраструктури з використанням SDI.

В частині передачі аудіо сигналів спостерігається більше різноманіття стандартів та технологій. Не будемо перелічувати технології які розроблені окремими виробниками для власних потреб, їх надзвичайно велика кількість. Зазначимо лише стандарти які мають шанси стати загально вживаними, серед багатьох представників галузі:

AES-67 – стандарт «real time» передачі аудіо сигналів у вигляді не скомпресованого потоку даних у IP мережах, Layer

AVB (IEEE-802.1xx) audio, video bridging – група стандартів IEEE-802 що описує передачу аудіо, відео сигналів у IP мережах, Layer Станом на 2014 рік, використовується для роботи з аудіо сигналами.

Галузь застосування.

Вирішивши побудувати телецентр, або його частину з використанням IP рішень, слід уявляти можливості технології. Усвідомлювати позитивні та

негативні сторони використання суцільного IP. У подальшому ми не розглядатимемо варіанти побудови комплексів що складаються із standalone модулів не пов'язаних цілісною ідеологією використання.

Узагальнюючи багаторічний досвід роботи з цифровими інтерфейсами, то: якщо є SDI, то в ньому є 16 звукових доріжок. Але адреса SDI сигналу прив'язана до номера порту у комутаторі, проте як у «хмарному» середовищі вона прив'язана до джерела чи споживача. При проектуванні будь-якої ланки, вирішується завдання опрацьовувати SDI+Embedded audio, де кількість звукових доріжок мінімально достатня для формування потрібної, вихідної програми. Далі, сформований сигнал передавався по транспортній мережі, до кінцевого споживача. Якщо передбачалась незалежна маршрутизація звукових доріжок, то використовувалась окремий звуковий комутатор, а найбільш просунуті, використовували матрицю з вбудованими de-embedder, embedder.

Але за такої архітектури, наявні суттєві вади: суттєва обмеженість використовувати одиничні відео, аудіо сигнали для формування вихідного сигналу із заданим переліком супутніх доріжок. Практично неможливо довільно переформатувати відео сигнал від будь-якого джерела. Вихідний сигнал формується ланцюгом вихідних модулів с заздалегідь заданими властивостями. Практично неможливо додати звукові доріжки від власного аудіо мікшеру, додати звукові доріжки додаткової мови від віддаленої апаратної, додати службовий канал інтеркому, додати сигнал LTC або сигнал керування. До того ж неможливо гнучко міняти місцями звукові доріжки відповідно до потреб користувача. Ланцюг модулів з найширшими сервісними функціями та їх загальна кількість робить реалізацію мало ефективною.

Потреба виділяти значні комутаційні ресурси на потреби системи моніторингу. Тут основна складність у потребі додавати додаткову точку комутації у матриці, після додавання вхідного сигналу. Матричні комутатори, які мають у своєму вбудовані багато екранні процесори відразу втрачають майже половину своїх комутаційних потужностей для вирішення цієї задачі. Ті ж комутатори що мають зовнішні процесори потребують додаткової, окрім main, backup, плати комутації.

Потреба будувати окрему, транспортну систему доставки сигналів до «віддалених» споживачів. Така транспортна система також накладає ряд суттєвих обмежень. Для кожного сигналу потрібно формувати транспортній канал що відповідатиме загальній режисурі події. Зазвичай, з метою загальної економії, для передачі використовуються вихідні, програмні відео сигнали і дуже обмежено «чорнові» відео, аудіо сигнали безпосередньо від джерела.

Використання технологій IP передачі даних, майже позбавлене цих вад. Через однозначну ідентифікацію кожного сигналу у мережі, не має значення місце його виникнення. Користувач збиратиме сигнали незалежно від того де вони сформовані! Такі собі віртуальні сигнали, які в оригінальному вигляді не існують в системі. Наприклад: узявши програму апаратної додаємо звукові доріжки з відео від камерних каналів, хоча вони, напрямку, не є складовими головної аудіо програми або додаємо у той самий програмний сигнал, сигнал від

головної станції службового зв'язку. Багато переваг отримує моніторна система. Кількість сигналів на вході багатого екранного процесора, принципово, не впливає на комутаційні можливості «хмарного» середовища. Через 99% використання ВОЛЗ (волоконно-оптичних ліній з'єднання) та можливість ущільнення сигналів у одному мережевому кабелі відпадає потреба розробки окремої транспортної системи. Справа лишень за підбором SFP модулів з адекватним оптичним бюджетом.

Найвищим рівнем використання, для технологій передачі відео, аудіо даних по IP мережах, є побудова універсального медіа середовища з функціями пакетування, перепакування та ущільнення сигналів. Передача сигналів відбувається за єдиними стандартами, які, у свою чергу дозволяють створювати віртуальні сигнали.

У якості нижнього рівня, можливо розглядати ситуацію за якої побудовано медіа середовище, але сигнали транспортуються від джерела до споживача без можливості використання їх для інших технологічних операцій. Якщо користувачеві не потрібно маніпулювати сигналами, то й немає потреби притримуватися одного стандарту. Різні типи сигналів можуть передаватися окремими потоками, але без можливості віртуалізації.

За будь яких умов проектування телевізійного комплексу зводиться до підбору максимальної кількості обладнання що підтримую мережеву передачу даних з обраним стандартом. Чим більше цього обладнання: камери, мікшери, сервери, багато екранні процесори, модульна інфраструктура тим більш ефективним та економічно доцільним стане телевізійний комплекс. Основну долю у витратах становитимуть «gate», що виконують функцію перетворення звичайних відео, аудіо сигналів у IP потоки необхідних стандартів. Слід пам'ятати, якщо користувач планує передавати файли програм у такій мережі, для них так само повинні використовуватись IP gate. Важливим є вибір головного, допоміжних IP маршрутизаторів. На деяких ділянках доцільне використання не спеціалізованих IP маршрутизаторів («офісного» типу – HP, Cisco, Arista), які підтримують стандарт SMPTE2022 5/6. Під час проектування слід визначитися, чи є потреба використовувати комутаційні панелі, як за класичної технології та здійснювати ручну комутацію IP потоків. У неспеціалізованому IP маршрутизаторі ця функція не використовується. Але робота у телецентрах вимагає широкого застосування ручної комутації. Наприклад: швидкий вибір сигналу (IP потоку) між кількома наявними для подачі у програму, вибір сигналу для перегляду та вимірювання, формування та подача сигналів для передачі по лініях ВОЛЗ. У такому випадку звичайні маршрутизатори не підходять. Слід обирати спеціалізовані пристрої, що передбачають ручну комутацію. У цьому випадку, маршрутизатор працюватиме під управлінням спеціалізованого програмного забезпечення, що реалізовуватиме цю функцію.

Головним чинником вдалої: технологічно ефективною та економічно доцільної реалізації проекту є попередня розробка загальної концепції розвитку та неухильне її дотримання.

Література:

1. <http://comtel.ua/solutions/communication/tehnologiyi-ir-peredachi-danih-u-suchasnomu-teletsentri/>
2. <http://www.eutelsat.com/en/satellites/the-fleet/EUTELSAT-KA-SAT.html>

Гомзяк Ярослав Олегович
Державний університет телекомунікацій
Факультет телекомунікацій
м.Київ

ТЕХНОЛОГІЯ DPI

Deep Packet Inspection - технологія накопичення статистичних даних, перевірки і фільтрації мережевих пакетів по їх вмісту. На відміну від брандмауерів, Deep Packet Inspection аналізує не тільки заголовки пакетів, а й повне вміст трафіку на рівнях моделі OSI з другого і вище. DPI здатний виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям. DPI може приймати рішення не тільки по вмісту пакетів, але і за непрямими ознаками, властивим якимось певним мережевим програмами і протоколам. Для цього може використовуватися статистичний аналіз (наприклад статистичний аналіз частоти зустрічі певних символів, довжини пакета). Часто використовуються провайдерами для контролю трафіку, а іноді і для блокування деяких протоколів, таких як BitTorrent. За допомогою Deep Packet Inspection можна визначити, яка програма згенерувало або отримує дані, і на підставі цього зробити будь-яку дію. Крім блокування, DPI може збирати детальну статистику з'єднання кожного користувача окремо. Також, за допомогою quality of service Deep Packet Inspection може управляти швидкістю передачі окремих пакетів, піднявши її або, навпаки, зменшивши.

Приклад роботи Deep Packet Inspection

Ідентифікація протоколу транспортного рівня мережевої моделі OSI у структурі пакета протоколу IPv4 виділений спеціальний байт для вказівки номера протоколу транспортного рівня. Їм є десятий байт від початку заголовка IPv4 пакета. Наприклад: номер дорівнює шести - для TCP протоколу, номер дорівнює сімнадцяти - для UDP протоколу. У структурі пакета IPv6 також існує спеціальна область, в якій знаходиться аналогічний ідентифікатор протоколу транспортного рівня. Ця область називається Next Header.

Ідентифікація HTTP

Для ідентифікації HTTP протоколу досить перевірити, що пакет є TCP, і вміст цього TCP пакету починається з однієї з наступних команд: «GET», «POST», «HEAD». Крім того, після команди повинен стояти пробіл, а також

через деякий проміжок повинен зустрітися текст «HTTP /». Якщо все це виконується, то цей пакет несе в собі HTTP запит.

Для чого застосовується DPI

З точки зору експлуатації, оператор може контролювати утилізацію підключених через DPI каналів на рівні додатків. Раніше він вирішував завдання реалізації QoS (Quality of Service) виключно засобами побудови черг на підставі маркування трафіку службовими бітами в заголовках IP, 802.1q і MPLS, виділяючи найбільш пріоритетний трафік (різного роду VPN'и, IPTV, SIP та т. Д.) і гарантуючи йому певну пропускну здатність в будь-який момент часу. Трафік типу Best Effort, до якого належить весь інтернет трафік домашніх абонентів (HSI - High Speed Internet), залишався фактично без контролю, що давало можливість того ж Bittorrent забрати собі всю вільну смугу, що, в свою чергу, вело до деградації будь-яких інших веб -додатків. З використанням DPI у оператора з'являється можливість розподілити канал між різними додатками. Наприклад, в нічні години дозволити трафіку Bittorrent забирати собі більше смуги, ніж вдень, в години-пік, коли в мережі ходить велика кількість іншого веб-трафіку. Інша популярна міра у багатьох мобільних операторів - блокування Skype-трафика, а також будь-яких видів SIP-телефонії. Замість повного блокування оператор може вирішувати роботи даних протоколів, але на дуже низькій швидкості з відповідною деградацією якості надання сервісу у конкретного додатка, щоб змусити користувача платити за послуги традиційної телефонії, або за спеціальний пакет послуг, що дозволяє доступ до VoIP-сервісів.

Програми

Hipfire (Hi-Performance Protocol Identification Engine) - реалізація Deep Packet Inspection для Linux з відкритим вихідним кодом .

L7-filter - ще одна реалізація Deep Packet Inspection для Linux з відкритим вихідним кодом, орієнтована на класифікацію даних сьомого рівня моделі OSI.

SPID (Statistical Protocol IDentification) - реалізація Deep Packet Inspection для Windows з відкритим вихідним кодом на C #. Ідентифікує протокол сьомого рівня моделі OSI за допомогою статистичного аналізу трафіку.

Література:

https://ru.wikipedia.org/wiki/Deep_packet_inspection

МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ

Для захисту від шкідливих програм і комп'ютерного шахрайства існують і застосовуються різні методи боротьби з ними. Це методи юридичні, освітні та технічні.

У всіх комп'ютеризованих країнах прийняті закони, що забороняють створення і поширення вірусів і інших типів шкідливих програм. До того ж часто дії інтернет-злочинців потрапляють під абсолютно некомп'ютерні статті кримінальних кодексів - наприклад, шахрайство, вимагання, неправомірний доступ до конфіденційної інформації і т.д. Дані закони регулярно застосовуються на практиці. Однак слід визнати, що часто подібні злочини скоюються технічно грамотними фахівцями, і це досить серйозно ускладнює розслідування злочину. Плюс до того більшість кримінальних атак залишаються поза увагою поліції. З цих причин виключно юридичними методами можна знизити загальний рівень комп'ютерної злочинності, але повністю перемогти не можна.

Другим важливим методом захисту від комп'ютерних зловмисників є навчання користувачів і суворе дотримання основних правил поведінки в мережі. Всього є три основних правила, які правильні як для домашніх, так і для корпоративних користувачів:

1. Обов'язкове використання антивірусного захисту.

Якщо ви не є експертом з комп'ютерної безпеки, то краще за все вас захистить надійний антивірусний захист і захист від мережових атак (брандмауер) - довірте свою безпеку професіоналам. Більшість сучасних антивірусних програм захищають від найрізноманітніших комп'ютерних загроз - від вірусів, хробаків, троянських програм і рекламних систем. Інтегровані рішення з безпеки також ставлять фільтр проти спаму, мережових атак, відвідування небажаних і небезпечних інтернет-ресурсів і т.д.

2. Не слід довіряти всій інформації, що надходить на комп'ютер - електронним листам, посиланням на веб-сайти тощо.

Ніколи не слід відкривати файли і посилання, що приходять з невідомого джерела. Навіть якщо повідомлення отримано з джерела відомого (від знайомого або колеги по роботі), але присланий файл або посилання приходить для вас несподівано, - краще перепитати про справжність повідомлення, оскільки зворотня адреса в електронній пошті легко підробляється. Інтернет - досить небезпечне місце, де слід поводитися обережно.

На жаль, жорсткі обмежувальні заходи можуть конфліктувати з побажаннями кожного конкретного користувача або з бізнес-процесами підприємства, - в таких випадках треба шукати баланс, причому в кожному окремо взятому випадку цей баланс може бути різним.

3. Слід звертати велику увагу на інформацію від антивірусних компаній і від експертів з комп'ютерної безпеки.

Зазвичай вони своєчасно повідомляють про нові види інтернет-шахрайства, нові віруси, епідемії і т.д. - приділяйте більше уваги подібній інформації.

Використання антиспамових фільтрів допомагає захиститися і від деяких поштових черв'яків. Найочевидніше застосування - це при отриманні першого зараженого листа (за відсутності антивіруса це можна визначити за непрямими ознаками) відзначити його як небажане і надалі всі інші заражені листи будуть заблоковані фільтром.

Поштові черв'яки відомі тим, що мають велику кількість модифікацій незначно відрізняються один від одного. Тому антиспамовий фільтр може допомогти і в боротьбі з новими модифікаціями відомих вірусів. У цьому сенсі антиспамовий фільтр навіть ефективніше антивіруса, так щоб антивірус виявив нову модифікацію необхідно дочекатися оновлення антивірусних баз.

У будь-якому випадку, антивіруси є найефективнішими засобами захисту від вірусів, і їх використання на робочих станціях обов'язково.

Література:

[http://ua-](http://ua-referat.com/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D1%96%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B8%D0%BA%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83)

[referat.com/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D1%96%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B8%D0%BA%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83](http://ua-referat.com/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D1%96%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B8%D0%BA%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83)

Гомзяк Ярослав Олегович

Державний університет телекомунікацій

Факультет телекомунікацій

м.Київ

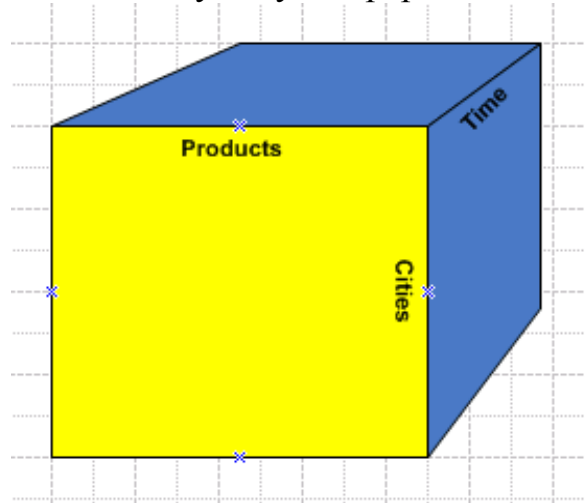
ТЕХНОЛОГІЯ OLAP

OLAP (Online analytical processing, інтерактивна аналітична обробка) - технологія обробки даних, яка полягає в підготовці сумарною (агрегированной) інформації на основі великих масивів даних, структурованих по багатовимірному принципу. Реалізації технології OLAP є компонентами програмних рішень класу Business Intelligence.

Причина використання OLAP для обробки запитів - швидкість. Реляційні БД зберігають дані в окремих таблицях, які зазвичай добре нормалізовані. Ця структура зручна для операційних БД (системи OLTP), але складні багато табличні запити в ній виконуються відносно повільно.

OLAP-структура, створена з робочих даних, називається OLAP-куб. Куб створюється з з'єднання таблиць із застосуванням схеми зірки або схеми сніжинки. У центрі схеми зірки знаходиться таблиця фактів, яка містить ключові факти, за якими робляться запити. Множинні таблиці з вимірами приєднані до

таблиці фактів. Ці таблиці показують, як можуть аналізуватися агреговані реляційні дані. Кількість можливих агрегування визначається кількістю способів, якими початкові дані можуть бути ієрархічно відображені.



Існують три типи OLAP:

Багатовимірна OLAP (Multidimensional OLAP - **MOLAP**);

Реляційна OLAP (Relational OLAP - **ROLAP**)

Гібридна OLAP (Hybrid OLAP - **HOLAP**).

MOLAP - класична форма OLAP, так що її часто називають просто OLAP. Вона використовує підсумовує БД, спеціальний варіант процесора просторових БД і створює необхідну просторову схему даних зі збереженням як базових даних, так і агрегатів.

ROLAP працює безпосередньо з реляційним сховищем, факти і таблиці з вимірами зберігаються в реляційних таблицях, і для зберігання агрегатів створюються додаткові реляційні таблиці.

HOLAP використовує реляційні таблиці для зберігання базових даних і багатовимірні таблиці для агрегатів.

Реалізація

З точки зору реалізації, діляться на «фізичну OLAP» і «віртуальну» (реляційну Relational OLAP, ROLAP). «Фізична», в свою чергу, в залежності від реалізації підрозділяється на багатовимірну (Multidimensional OLAP, MOLAP) і гібридну - (Hybrid OLAP, HOLAP). У першому випадку наявна програма, яка виконує на етапі попереднього завантаження даних в OLAP попередній розрахунок агрегатів (обчислень по декількох початкових значень, наприклад «підсумок за місяць»), які потім зберігаються в спеціальну багатовимірну базу даних, що забезпечує швидке вилучення та економічне зберігання. Гібридна реалізація є комбінацією: самі дані зберігаються в реляційній базі даних, а агрегати - в багатовимірній. У ROLAP-реалізаціях всі дані зберігаються і обробляються в реляційних системах управління базами даних, а агрегати можуть не існувати взагалі або створюватися за першим запитом в СУБД або кеші аналітичного програмного забезпечення.

З точки зору користувача, всі варіанти виглядають схожими за можливостями. Найбільше застосування OLAP знаходить в продуктах для

фінансового планування, сховищах даних, рішеннях класу Business Intelligence.

Література:

<https://ru.wikipedia.org/wiki/OLAP>

Волков Вадим Олегович
Державний Університет Телекомунікацій
Факультет Телекомунікацій
м. Київ

3D ІНТЕРНЕТ. КОРИСТЬ І ПЕРСПЕКТИВИ ЙОГО РОЗВИТКУ

Об'ємне бачення світу на зображенні. Про це люди мріяли ще до появи фотографії. Перший стереоскоп в 1838 році представив світу Чарльз Уїтсон. У його пристрій поміщалися дві намальовані тушшю картинки, що відрізняються для правого і лівого ока. Саме завдяки невеликій відмінності таких картинок, людський мозок був здатний «намалювати» об'ємне зображення, поєднуючи два плоских зображення в одне. Той же принцип формування тривимірної картини використовується в сучасних технологіях 3D-бачення: нам здається, що замість двох плоских зображень очі бачать об'ємні предмети під різними кутами, як в реальному житті. Тривимірна графіка - розділ комп'ютерної графіки, сукупність прийомів і інструментів (як програмних, так і апаратних), призначених для зображення об'ємних об'єктів.

Інтернет переживає кризу середнього віку: коли йому виповнилося 40, він почав переходити в 3D вимір. Розвиток все ще перебуває на ранній стадії, але ідеологи даного явища вважають його природним і неминучим, вважаючи, що в найближчі роки очікується масове поширення 3D Інтернету. 3D зробить глобальну мережу більш соціальною і відкриє людям неймовірні можливості в освіті, бізнесі та медицині. Яні Піркола, першопроходець в цій сфері, передбачає, що пік використання 3D Інтернету буде в 2018 році, коли молодші користувачі очолять цей процес. І, за словами фахівця, він увійде в тренд набагато швидше, ніж 2D Інтернет. Що таке 3D Інтернет? Уявіть собі його як набір взаємозв'язаних віртуальних світів. Користувачі можуть відвідувати їх, споживаючи послуги, і «переміщуватися» з одного в інший. Віртуальні світи використовують багато технологічних компонентів 2D Інтернету - браузер, пошукові машини і сервери. Але особливістю, яка відрізняє даний вид Інтернету від традиційної всесвітньої павутини є 3D комп'ютерна графіка і, в багатьох випадках, аватари. Останні, як вважає Піркола, зроблять його набагато соціальнішим за свого попередника. «Читаючи будь-який документ, ви зможете побачити інших користувачів, які читають цей документ. Ви будете природно пов'язані з людьми, які мають спільні з вами інтереси і споживають ті ж самі послуги, »- прогнозує він. Одне застереження: якщо ви очікуєте того, що пошук в 3D Інтернеті буде виглядати як нескінченна комп'ютерна гра з приголомшливою графікою, то будете розчаровані. Піркола звертає увагу на те, що віртуальні світи в високоякісних комп'ютерних іграх є результатом роботи багатьох художників і

мають бюджети зрівняні з бюджетами кінофільмів. У порівнянні з ними, 3D Інтернет може виглядати тьмяно. «3D службам буде потрібно частково пожертвувати зовнішнім виглядом і швидкістю,» - говорить Піркола.

Зараз існують міради віртуальних світів по всьому світу з різними 3D платформами, як-то: Open Wonderland, MeshMoon, OpenSim і Sirikata. Однак, на сьогоднішній день каменем спотикання є відсутність загальноприйнятих стандартів для забезпечення їх сумісності.

2D графічний інтерфейс досяг межі своїх можливостей і настав час рухатися вперед і освоювати світ 3D.

Список використаних ресурсів:

1. <https://nvworld.ru>
2. <https://knowledge.allbest.ru>
3. <http://venture-biz.ru>

СЕКЦІЯ №2. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Koltsova Anastasiia
National Mining University of Ukraine
Dnipro

SUGGESTIONS TO IMPROVE THE SET TECHNOLOGY IN UKRAINE

During my stay in China, I turned my attention to the QR code. QR code (Quick Response Code) - a trademark for the type of matrix barcodes. Either a sensor or a camera as a two-dimensional image scans it. It contains information or an object reference to which it refers. Use 4 coding mode standards: numeric, alphanumeric, binary, kardzi - this allows you to expand the number of possible character combinations.

QR code consists of black squares arranged in a square grid on a white background, which can be read using image processing devices (camera) and processed using the Reed-Solomon code. Further, the necessary data is extract from the templates that are present in the horizontal and vertical components of the image.

In China, the use of QR code is widespread. With simple actions and the presence of a smartphone that supports the recognition program, you can easily pay for goods, transportation, go to the site and get the necessary information about the object of interest, even rent a bicycle and so on.

On the example of a bicycle, I can judge that this is a very useful way of reading information - at anytime, anywhere, and for carrying out usual daily activities, it is enough to carry only a telephone.

As a result of my observations, I can say that QR code facilitates access to information about the product, speeds up the method of payment for a product or service, allows you to quickly reach the necessary site, a way of exchanging information (for example WeChat), one of the types of identification.

In Ukraine, this technology is already present (scanning code in a railway ticket), but very little is used. I believe that this technology will be adopted by society and will be applied in all spheres of people's livelihood both in Ukraine and in any country.

I was also interested in the way to organize communication using a feeder antenna.

Antenna Feeder System - a set of antenna and feeder path, included as part of an electronic product, a sample, a complex. Antenna Feeder System is used for signal transmission in radio communication systems, broadcasting, television, as well as other radio systems that use radio waves to transmit signals. The antenna function consists in the emission or reception of electromagnetic waves. The electrical connection of the

antenna to the source (consumer) can be direct, and can be carried out using a transmission line equipped with radio frequency connectors, i. E. with the help of a feeder. The feeder function is in the transmission of the electromagnetic oscillation from the radio transmitter to the antenna input and the transmission of the electromagnetic oscillation from the antenna to the radio receiver.

The transmitting antenna converts the energy of the waves coming through the feeder from the transmitter to the antenna into the energy of free oscillations propagating in the surrounding space. The transmitting antenna should not simply radiate electromagnetic waves, but provide the most rational energy distribution in space. In connection with this, one of the main characteristics of transmitting antennas is the directional pattern - the dependence of the emitted field on the position of the observation point (the observation point should be in the far zone - at an invariably large distance from the antenna). Requirements for directivity range from very close to directional (broadcasting systems and terrestrial television) to a sharply defined direction in a certain direction (long-range space radio communication, radiolocation, radio astronomy, etc.). The directionality allows without increasing the transmitter power to increase the power of the field emitted in this direction, and also allows to reduce interference to neighboring radio systems, that is, contributes to the solution of the problem of electromagnetic compatibility. Directivity can be obtained only when the dimensions of the antenna significantly exceed the wavelength of the oscillations.

The receiving antenna catches the energy of free oscillations and turns it into energy of waves, which comes through the feeder to the input of the receiver. For receiving antennas, the radiation pattern is the dependence of the current in the antenna load, that is, ultimately at the receiver, or the emf induced at the receiver input, from the direction of arrival of the electromagnetic wave irradiating the antenna. The presence of directional properties at the receiving antennas allows not only to increase the power released by the current in the load, but also substantially to weaken the reception of various kinds of interference, that is, improve the reception quality.

Any transmitting antenna can be used for reception of electromagnetic waves and generally speaking, on the contrary, however it does not follow from this that they are identical in design.

An important role in the operation of antenna devices is played by the transmission line (feeder), which transfers energy from the generator to the antenna (in the transmitting mode) or from the antenna to the receiver (in the receive mode). The main requirements for the feeder are reduced to its electrical leakage (no radiation of energy from the feeder) and low thermal losses. In the transmit mode, the feeder impedance of the feeder must be matched to the input impedance of the antenna (which provides the traveling wave mode in the feeder) and with the transmitter output (for maximum power output). In receiving mode, the receiver's input is coordinated with the feeder's wave resistance in the latter mode of traveling wave. Harmonization of the wave resistance of the feeder with the load resistance is the condition for maximum

power output to the load of the receiver. Depending on the radio wave band, various types of feeders are used: two or multi-wire air feeders, waveguides of rectangular, round or elliptical cross-sections, lines with a surface wave, and others.

The use of such a system is convenient in that the recoil coefficient is small. Such antennas can be of different sizes depending on the terrain, the conditions for transmitting information and the required range.

Thus, it can be disguised as ordinary items such as air conditioning, street lamps, alarms and so on. In Ukraine, such a system will improve the quality of information transmission, signal level anywhere in the city, reduce the amount of data loss and increase the number of points for Internet access.

In my opinion, the implementation of these technologies in Ukraine will be of great benefit to our society and will allow us to communicate 24 hours a day, regardless of the circumstances. That is: real-time, anywhere, social-to anyone.

Koltsova Anastasiia
National Mining University of Ukraine
Dnipro

QR-CODE AND ICT APPLICATION

QR code (Quick Response Code) - a trademark for the type of matrix barcodes. It is scanned either by a sensor or a camera as a two-dimensional image. It contains information or an object reference to which it refers. Use 4 coding mode standards: numeric, alphanumeric, binary, kerdla - this allows you to expand the number of possible character combinations.

QR code consists of black squares arranged in a square grid on a white background, which can be read using image processing devices (camera) and processed using the Reed-Solomon code. Further, the necessary data is extracted from the templates that are present in the horizontal and vertical components of the image.

In China, the use of QR code is widespread. With simple actions and the presence of a smartphone that supports the recognition program, you can easily pay for goods, transportation, go to the site and get the necessary information about the object of interest, even rent a bicycle and so on.

On the example of a bicycle, I can judge that this is a very useful way of reading information - at any time, anywhere, and for carrying out usual daily activities it is enough to carry only a telephone.

As a result of my observations, I can say that QR code facilitates access to information about the product, speeds up the method of payment for a product or service, allows you to quickly reach the necessary site, a way of exchanging information (for example WeChat), one of the types of identification.

In Ukraine, this technology is already present (scanning code in a railway ticket), but very little is used. I believe that this technology will be adopted by society and will be applied in all spheres of people's livelihood both in Ukraine and in any country.

Bondarenko Yevhenii
State University of Telecommunications
Kyiv

ENGINEERING TRUCK PREDICTIVE MAINTENANCE SOLUTION

My name is Yevhenii Bondarenko. I am a 5th year student at the State University of Telecommunications (Ukraine, Kyiv). A participant in the Seeds for the Future 2017 program from Huawei.

During my stay in China, I was acquainted with many ICT smart solutions and it is no secret that thanks to ICT, the Chinese "economic miracle" has appeared.

In Beijing, our team organized a meeting with the Ambassador Extraordinary and Plenipotentiary of Ukraine to the People's Republic of China. At the meeting, we discussed the economic situation in the country, of course, it came about the agrarian sector and it became clear that the country with a population of 1.2 billion is only 30% of the territory suitable for growing food.

For the first time I thought about the effective cooperation of the agrarian sphere and the sphere of information technologies at the forum "Idea for Future 2015" in Kiev.

Ukraine has great potential in this direction.

Now, the implementation of agrarian ICT solutions is very important, unlike other smart solutions, the agrarian can not only reduce losses but also bring income, to both business and the state.

In Ukraine, not for the first year experts raise such issues and are engaged in the selection of the best solutions, because of which we already have: precise steering systems, pointing systems, hardware upgrades and a variety of mobile applications.

In general, the agrarian sphere in Ukraine is developing and is actively moving to new technical and software solutions.

However, what is important, the exploitation of technical means, leads to breakdowns that require repair, as a rule, this occurs at the most inappropriate time and violates the work plan subsequently causing losses.

To solve this problem, I propose to refer to the world-famous solution from Huawei - Engineering Truck Predictive Maintenance Solution. What offers centralized collection of information on the status of technical parameters of the equipment used; the main indicators can noted geolocation, speed and direction of movement, temperature of machinery, material consumption and so on.

Centralized collection of information and analytical software component will prevent losses and allow managers to competent manage their enterprise.

Experts Huawei argue that the full implementation of this solution will reduce the fault rate by 70%, fault time by 40%, and maintenance costs by 30%. Conclusion I want to note that only using the potential will lead to an effective result. Therefore, I will deal with this issue in detail with a large-scale goal - the development of the ubiquitous digital future of Ukraine.

Lavryck Nazar
Lviv Polytechnic National University
Lviv

INFORMATION AND COMMUNICATIONS TECHNOLOGY

ICT, or information and communications technology (or technologies), is the infrastructure and components that enable modern computing. ICT is sometimes use synonymously with IT (for information technology); however, ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

The list of ICT components is exhaustive, and it continues to grow. Some components, such as computers and telephones, have existed for decades. Others, such as smartphones, digital TVs and robots, are entries that are more recent. ICT commonly means more than its list of components, though. It also encompasses the application of all those various components. It is here that the real potential, power and danger of ICT can found.

ICT is advantage for economic, societal and interpersonal transactions and interactions. ICT has drastically changed how people work, communicate, learn and live. Moreover, ICT continues to revolutionize all parts of the human experience as first computers and it means that this direction is important to develop and improve in Ukraine.

In my opinion, one of the most promising ICT technologies is Smart Parking. Most of us are acquainted with how frustrating it can be trying to find a parking spot in a crowded big city. As technologies are ever changing people's lives, there is no exception when it comes to parking. In the near future, parking will be unprecedentedly convenient with the help of an app on your phone. You can find and reserve a parking spot before you head out the door, follow the app's built in GPS navigation, and pay for the parking spot inside the app. NB-IoT-based Smart Parking is the technology behind this miraculous experience.

Very common problem in Ukraine is a problem of parking in large-sized cities. Therefore, technology Smart Parking is extremely relevant for Ukraine and can help solve this problem.

This technology based on the NB-IoT solution and has many advantages, for example:

- NB-IoT solution uses operators' network coverage. No additional network devices are required. This contributes to leading competitiveness in network deployment costs. NB-IoT features wide and intensive coverage. It saves additional costs caused by infrastructure construction in sparsely populated areas and areas where cable layout is complicated and erection of poles for installing antennas is inconvenient. NB-IoT uses licensed spectra. This prevents unlicensed spectra causing network interference.

- The NB-IoT network is maintain by operators, saving network operation costs for parking lots. Huawei IoT platform provides open APIs for parking lots. Third-party software vendors can develop specified operation software based on actual requirements, better meeting operation different requirements.

- The IoT platform can be connect to existing systems such as the GIS deployed for users. Open APIs provided by the IoT enable software vendors to develop customized software for users, meeting different experience requirements.

- Compared with LoRa, ZigBee, and Telensa, the NB-IoT solution requires almost the same costs in parking space modules and higher costs in communication, but lower costs in network gateways, local network deployment, and local network maintenance. Therefore, the NB-IoT solution takes the lead in comprehensive commercial costs.

- In terminal deployment, NB-IoT integrates NB-IoT modules through the vehicle detector. The reliability is high.

After implementation, the Smart Parking technology in Ukraine country can continue to develop in this direction. For example, private companies can start using technology such as IoV. The IoV solution integrates data, device, and operation management. Through the implementation of unified and secure network access, flexible device adaptation, and massive data collection and analysis, it contributes significantly to generate a new potential revenue source. The IoV solution uses the Agent solution to streamline and simplify the development of many vehicle vendor terminals and shield complex interfaces to provide rapid access to terminals. This creates numerous application capabilities for IoV services to ensure that industry partners can rapidly develop new services, and reduce the inherent service rollout cycle and subsequent development costs.

In the conclusion, solving the problem of parking in large-sized cities of Ukraine will improve the infrastructure of cities, as well as increase their tourist and investment attractiveness. An effective parking system can potentially provide a significant contribution to budget revenues of cities and become an attractive business for private companies. In addition, it will increase the quality of life of cities dwellers and will provide comfortable traffic within the city.

QR CODES IN CHINA, WHICH WE CAN USED IN UKRAINE

When we were preparing to the visit to China we had a task-to know about the technologies, that can be applicable in Ukraine to make people`s lives easier.

Smart tech that I saw at first time in China were in Beijing. When our team was in the main office of Huawei in Kyiv, I saw a bike there. When we had asked, that he is doing here, we became an answer, that there are many bikes in China that can be unlock and then used by phone.

I saw huge bike parking, while we were going from airport to hotel in Beijing. Next day we asked our guide Lusi, if we can use these bikes. She helped us with bike app and how to unlocked that. In few minutes everybody, who wanted, scanned QR-codes a than were driving bikes. I took only 1 minute to understand the app and use it. There are a lot of companies, that are managing with bikes, so, the user get few free rides to understand, if this company meets his needs and it is enough for him.

When I used bike at first time, I mat IoT tech at first time. Because after the end of trial period bike is changed into very cheap taxi. I think, that Ukrainians could like this form, when”high-teck” bikes will appear there.

Two place, where I met with this tech was small common shop. Every person, who had bought something there just brought their phones to the scanner and played by their smartphones. This tech saves your time.

There are less people in Ukraine, so such “time management” could save more time, then in China. Due to that, people will be late in their jobs not so often, or vice versa, hay will come home earlier, because they do not have to spend so much time near the cashier.

This payment method also extremely saves state budget, because it becomes easier to control and produce paper money.

In order to know more about this payment method, I talked with one of the locals. He was not speaking in any language, that I do, but when I had shown him WeChat icon on my phone, he understood, what it is. WeChat is a messenger that use QR-codes to create a chat in order to help two foreigners to understand each other and to have a discussion.

This local told me, that it is very easy to connect a smartphone with your bank account. Special knowledge or skills are not need. My next question was about Security. He made me sure enough to believe, that it is secure. Paper money or coins are not always felt in our pockets, so they can be easily stolen or get lost. In addition, our smartphones are always with us, so our money loss is lower.

Moreover, what will be, if our smartphone had stolen? The answer is very easy-before the transaction person have to enter his PIN-code, as we do with ATM in Ukraine.

Next day after this dialog, I asked other local. His answers were the same. Therefore, I understood that this technology spread everywhere and many people use it. In Schengen realized, that IoT tech is use in whole China.

Implementing of this payment method can easily change the standard of living in Ukraine and we have to do everything to bring this technology in life as soon as possible.

Horbacheva Hanna
Odessa national academy of telecommunications
named after O.S.Popov
Odessa

USING QR- CODES INSTEAD CASH IN OUR LIFE

In the modern Ukraine, the level of the ICT is on the path of development, but if you compare it with the level in China, you could found a big amount of differences. Having visited one of the most developed countries in the world - China, I discovered many new technologies that are not available in Ukraine and that could improve the level of the ICT in the country.

First, it surprised me that the majority of the population moved around the city with the help of bicycles. They are located throughout the city; each person can take them everywhere and then leave wherever he want. You can use this bike with a special mobile application, which will help you to find a bike, then to pay for it and unlock it. The QR-code is located on the bicycle. It is a two-dimensional barcode with a random pattern formed by small squares on a white background, which can contain in 300 times information more than a regular barcode. The application reads the QR code, money is withdrawn for renting a bicycle from a bank account and then you can unlock your it. I think it is very convenient. You can move from one-city points to another on a bicycle with mobile application only.

Secondly, I was surprised that people do not use the cash they use smartphones and the application WeChat for payment of any other services and purchases. You only need to put your phone to the seller so that he can scan your code for payment.

Google, Facebook and other popular services do not available in China but here you can also live without them. This is another advantage of QR codes. Therefore, the messenger and social network WeChat with its system of interaction became the most important in everyday life. Nowadays, we are giving not business cards, we giving a QR-code to the new acquaintances. Even street musicians put up tables with a QR codes, in order to getting money from passers-by by this way.

Every modern Chinese resident can go out without a purse, a bankcard and cash, his make payments only by scanning the code. In addition, you can find a bicycle and get by it from one point of the city to another by scanning the code too. I believe that the introduction of such methods of paying, communication and movement, using QR codes, is raise the level of ICT in Ukraine. This will simplify the daily life of the population of the country.

Gvozdet'ska Nataliia
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”
Kyiv

HOW TO IMPROVE ICT IN UKRAINE

Ukraine is still a developing country and ICT can become a real driver for changes there. Many spheres of human activity could be improve by new ICT technologies that could in its turn substantially influence economic development. Nowadays, only 3rd generation of mobile networks (3G) is launch in Ukraine. Fixed optical fiber networks are being implement, but their penetration is low as for the whole country. Recently some cities have started to implement some Smart City & IoT technologies (e.g. “Zaporizhiya Safe City” project, “Kyiv Smart City” concept, etc.). However, these solutions are implement locally and brought changes only to small part of citizens. Moreover, there is no unified platform for Smart City, that could gather all solutions, allow adding new services easily and providing services’ scalability.

I think, that the first highly required steps to ICT improving in Ukraine are 4G launch and developing optical fiber channels. It would become a base for widening the range of available

Services by developing video-services and IoT services (using NB-IoT technology with LTE, for example) in particular. As for my city, nowadays it is a main site in Ukraine where new technologies are implemented and tested, as I live in Kyiv (the capital of Ukraine). But, I consider such strategy to be incorrect. The ICT should be spread all over the country. I do really appreciate an idea of pilot Smart City projects implementing in some particular towns or regions (or even villages), like it was made in Shenzhen and Longgang in China. ICT became a bridge from the village environment to magnificent megapolis environment for these cities. At the same time, these cities gave the chance to others to test the entire ecosystem of Smart and ICT-developed city.

From my journey to China, I took several prominent cases that should be definitely implement in Ukraine as they are in demand. Some of them are ready to be implemented even considering the current level of ICT development; the others need some networks’ and IT infrastructure improvement first.

The first thing that it is easy to recognize in Beijing, as well as in Shenzhen, that all telecom infrastructure is very well integrated with the city infrastructure. In comparison to the Ukraine, where BTS antennas and other access network equipment is usually installed on special towers or buildings, in China I saw a lot of lighting poles, bridges and modern monuments equipped by BTS antennas. In my opinion, they are very harmonically blended to the city external appearance. Moreover, in some cases antennas could be disguised as the completely different things (trees, air conditioners, etc.). I think that this is a good idea not only from design view, but also from the point of security (if equipment is not shown vividly, the risk of vandalism is decreased for it). Therefore, I think that we should definitely take into account this approach while launching 4G in Ukraine. The second thing that I was impressed by was IoT in China. I tried to use two live IoT systems here. They are similar in their principles and, as for me, give very useful services to citizens. One of them is bicycles IoT system. There are several bikes operating companies in China that give bicycles for a rent. All the bicycles are connect into the one network, thus operating company is able to track them and to rent it via users' applications. The same service exists for the umbrellas rent.

I consider three main ICT technologies to be involved in such kind of systems: IoT, Cloud and payment via QR code. As for me, I am not sure that such kind of IoT system can be successfully deployed and used in Ukraine nowadays because of the lack of infrastructure (for bicycles riding) and security Reasons (there are too many ways to violate the rules of this type of rent, as I suppose). However, I do really appreciate the QR code payment technology and I wish we got it in Ukraine as popular as it is in China today.

Talking about Safe city concept that is very well develop in Chinese cities, I am very impressed by the huge scope of its usage. In my city, there are also some IP cameras on the crossroads to control the traffic and fix rules' violations on the street, but the scope of their usage is not so big. It is very fascinating to realize, how powerful Cloud part of Safe city system should be (from the point of storing so big amount of data and from the point of its processing), and how high requirements are for the network as well. Thus, developing IT infrastructure in Ukraine is a very important step to the further digital transformation in our country. To conclude, it is necessary to say, that ICT in Ukraine and in Kyiv particularly is constantly in progress, and I believe that its further development will bring new services, new values and new comfortable living environment for every Ukrainian.

HOW TO IMPROVE THE ICT TECHNOLOGY IN UKRAINE

I will start my essay with a few words about my native country. Nowadays Ukraine is one of the developing countries, where there is some progress in relation to the ICT and IoT technologies, but rather slow in comparison, for example, with China or Group of Seven. However, we are moving in the right direction and due to the young minds and perseverance will be able to catch up with all the latest technologies.

I have several years addicted to drones, even defended bachelor's project on “Advanced telemetry system in UAV”. So talking about about the IoT technology, I would like to highlight the Internet of Drones. Unlike most Internet of Things (IoT) devices, drones are deploy in smaller fleets, have large lithium-based batteries, and send a large amount of data over a short period and called as IoT Drones. Drone applications need real-time navigation, telemetry and payload access over a high-bandwidth secure link.

Drone technology abstract: Over last few years, drones have found applications across several verticals, such as agriculture, construction, industrial inspections, and surveys. You can find UAV also in energy, mining, mapping and quite a few government agencies like those responsible for transportation and infrastructure. Drone industry has been growing The Internet of Drones era is expect to further drive growth in this sector. Cloud services lowers the entry barrier, and provides ready tools for developers, to leverage this technology for building innovative products and for offering new services.

Features of Cloud services include:

- Real-time access to drone control, telemetry and payload data over the internet.
- Extensive API's for simple access and easy integration with third-party services.
- Easy integration of drones with hundreds of third-party business and social apps over the cloud, such as DroneDeploy, AirMap, Cisco Spark, Jira, Facebook, and Twitter.
- CloudSim: One-click access to cloud-based simulator instance for drone application developers.
- Designed to work with variable-bandwidth, variable-latency, Intermittent links between drone and cloud, including 4G/LTE, WiFi, etc.

Commercial drones are also connected devices. Therefore, they are ‘things in motion’. Most are accessible or controllable over the Internet, and the data they collect is push to various cloud services. Some drones are beginning to carry on-board processors as well and are now part of the growing trend of fog computing devices.

Even with this mass-produced systems you are be able to ‘talk to a drone’. For example, you are able to - from your smartphone in Ukraine - control a drone in China. In addition, it is because companies like DroneDeploy and U|g|CS have figured out how to make addressable drone management platforms that control multiple drones from anywhere on any device. DroneDeploy does it by marrying a simple 4G telemetry device to a drone’s avionics. This enables real-time data transmission, processing, and sharing. With this kind of hardware and software combination, you can plan missions (launch, go to point A, then point B, then to point C, etc.) in a browser, upload them to a drone anywhere, press start, and away it goes. You could do that with a fleet and monitor them all in flight.

To conclude, it is necessary to say, that ICT in Ukraine and in Kyiv particularly is constantly in progress, and I believe that its further development will bring new services, new values and new comfortable living environment for every Ukrainian.

Rohovyi Denys

*Taras Shevchenko National University of Kyiv
Kyiv*

CYCLES, WHICH PLACED ON THE STREETS

My name is Denys Rohovyi and I am from Ukraine. I live in Kyiv.

I like idea with cycles, which placed on the streets. And I chose this idea to improve my city.

Why?

From the childhood I always love to ride a cycle. On the street near my home, me and my friends have races all the time (who is faster cross the finish line).

Why is this currentidea?

Paying attention on greenhouse effect, cycles is good idea to tackle with this problem. Moreover, cycles can help to keep fit your body and have a less problem with your health. Less cars will be on the road, because 10 cars take more territory than 10 cycles. So, the difference is obvious.

My own experience

In theory it is very comfortable in usage because you can easy take cycle and explore the city, go to any place what you want or drive to the subway. But in real life I face with some problems.

First problem:Ofo application on my phone was on Chinese language and all my attempts switch to English were unsuccessful.

Second problem:I have Windows Phone and all my attempts to input special code from bike to the app was also unsuccessful.

The first two problems were not very problematic. People who passed near me help to unlock me the bike. I offered them money, but they didn't take it from me. I was pleasantly surprised.

Third problem: Lots of bikes were with broken pedals or wheels.

Fourth problem: Some of bikes are very heavy. In addition, it is very hard to pick up them on the pedestrian bridge when you want cross the road.

How to implement?

It is very easy just invite Chinese company like Ofo, Mobike and etc, and offer them favorable terms. Also, mayor of Kyiv Vitali Klitschko goes to work by bike and I think he will support this idea.

But it is easy only in theory, in practice it will be more difficult. When this companies faces with Ukrainian roads (they are in bad condition), with the lack of bike paths, with corruption and lastly with stealing bikes and putting them on the scrap. They will be shocked.

Some improvements

Using my own experience, I would like to make some improvements and advices. There are:

1. Make app for phone on different language for tourists from different countries.
2. Stable support on different mobile platforms
3. Some special form build-in app in which clients can write if some part of bike broken
4. Make bikes from plastic (maybe, you heart about Placha bike with a frame made of plastic). So, the bikes will have less weight. Also, this will help to recycle the mountains of plastic. Which is in Ukraine take out to the garbage dump. Moreover, it will solve a future problem with putting bikes on the scrap. Placha bike with a frame made of plastic
5. To solve future problem with stealing bikes I propose set bikes in magnetic parking like on picture.
6. About the tackle with corruption also like example, Ukrainian government can take the Chinese experience tackle with corruption. With roads the same.
7. About price it should be available to all segments of the population in Ukraine.

I hope that my essay will help to improve Kyiv and your cycle's infrastructure. And I think the bikes have all chances to become a popular transport in Ukraine.

АЛГОРИТМІЗАЦІЯ ЯК ОСНОВА ПРОГРАМУВАННЯ

Термін «інформатика» виник на початку другої половини ХХ століття, його ввів німецький інженер та кібернетик Карл Штайнбух, об'єднавши слова «Information» та «Automatik». Цей термін він описав у статті «Інформатика: Автоматична обробка інформації» для позначення області знань, що виконує автоматизовану обробку інформації за допомогою обчислювальної техніки. Отож, галузь знань, що вивчає структуру й загальні властивості інформації, закономірності, методи її створення, зберігання, перетворення, пошуку, передачі та використання у різних сферах людської діяльності, називається інформатика.

Виникнення інформатики обумовлене створенням та впровадженням нової технології накопичення, обробки та передачі інформації, пов'язаної з фіксуванням на електронних носіях. [2] На сьогодні інформаційні технології займають велике місце в нашому житті. Застосування електронно обчислювальних машин стало буденною справою, хоча не так давно робоче місце, обладнане комп'ютером, було великою рідкістю. Інформаційні технології дали нові можливості для роботи і відпочинку, багато в чому полегшили працю і життя сучасної людини. Теперішнє суспільство навряд чи можна уявити без інформаційних технологій.

Роль інформатики у сучасному світі постійно набирає обертів. Поняття «комп'ютерна грамотність» стало критерієм тієї необхідності, яку встановила науково-технічна революція. У якості мети, комп'ютерна грамотність містить потребу в спеціальній підготовці людини для становлення особливого стилю мислення, орієнтованого на роботу з електронною обчислювальною машиною, що істотно звужує традиційне поняття інформатики.

Інформатика дала змогу людству перенести у комп'ютерний вимір такі інформаційні процеси, як пошук та збирання інформації, її зберігання та накопичення, що стало значно зручнішим із розвитком електронних носіїв, передавання та поширення інформації, ключову роль у чому зіграла мережа інтернет, створення, використання та правильне й швидке опрацювання, оцінювання й захист інформації - усе це стало у багато разів простішим та ефективнішим, ніж було до виникнення комп'ютерних інформаційних технологій. [1]

Завдяки інформатиці, науці, яка зуміла перенести життєво необхідні інформаційні процеси у цілковито нову площину, у суспільства з'явилося почуття певної захищеності та впевненості у достовірному збереженні важливої

інформації. Враховуючи неперервний розвиток інформатики, надійність та безпечність покладання на неї найважливішого у житті кожної людини постійно зростає, що робить дану науку надзвичайно важливою та перспективною.

Інформатику рівною мірою можна віднести і до прикладних, і до фундаментальних наук. Така неоднозначна класифікація впливає із самої природи виникнення і розвитку інформатики як складної сукупності загальнотеоретичних і прикладних наукових дисциплін.

Від рівня розвитку інформатики залежить рівень зростання продуктивності праці в інших галузях, враховуючи величезну роль інформаційних технологій в сучасному суспільстві. Наприклад, правильне застосування інформатики може сприяти інтенсифікації економіки шляхом забезпечення зв'язків між галузями та вдосконалення управління, що ґрунтується на оперативній передачі даних. Тому розвиток інформатики повинен відбуватися випереджальними темпами в порівнянні з іншими галузями. Хоча у суспільстві значну частину інформації займає саме паперова інформація, а не у електронному форматі, але саме без паперова, електронна інформація все більше набирає ваги та важливості. Комп'ютерна пам'ять стає все більш надійною та використовується частіше.

Розвиток комп'ютеризації, що включає в себе і поширення мікропроцесорів та розширення сфери їх використання, викликає серйозну потребу в створенні нового програмного забезпечення, що матиме на меті розширення можливостей електронно обчислювальних машин в обробці інформації.

Можна зробити висновок, що інформатика є складною комплексною наукою, що включає в себе загальнотеоретичні та прикладні наукові дисципліни. Значне поширення інформаційних технологій, існування великої кількості комп'ютерів та технологій обробки різного роду інформації вплинуло на всі, без винятку, сфери людської діяльності та існування. Так, наприклад предмет "Інформатика" у школах діти вивчають раніше ніж фізику, що свідчить про те, що попит на ринку праці та необхідність володіння навичками ефективної роботи з комп'ютером тільки зростають, та комп'ютерна грамотність є важливим елементом сучасного життя будь-якої людини. Величезні надії та сподівання, які людство поклало на інформатику, на розвиток електронних інформаційних технологій штовхає вперед усі можливі проекти та інновації у даній сфері. При раціональному використанні інформатика має змогу створити порядок та ефективну організованість у важливих для існування суспільства сферах.

Разом із тим, стрімкий науково-технічний прогрес був неможливим без широкого використання обчислювальної техніки для автоматизації проектування найрізноманітніших процесів, для керування їхнього виготовлення й проведення наукових досліджень. Існує величезна кількість як простих, так і відносно складних задач, які мають частковий, прикладний характер і для рішення яких недостатньо навичок, отриманих при вирішенні типових задач.

Отже, алгоритмізація розвиває розуміння того, як необхідно правильно ставити та вирішувати прикладні задачі. Це важливо не лише з точки зору більш професійного програмування, але й має цінність у інтелектуальному плані, як навичка грамотно формулювати й ефективно вирішувати різні, у тому числі й некомп'ютерні, задачі. Основний крок до розуміння важливості вивчення алгоритмів – це необхідність давати точне визначення тому, що мається на увазі під цим словом. Алгоритм – чітко визначена послідовність правил та дій, виконання яких приводить до виконання задачі за кінцеву кількість кроків.

Вирішення будь-якої поставленої задачі поділяється на декілька етапів її реалізації:

Елементарна функція додавання двох чисел також є алгоритмом, хоч і дуже примітивним. Швидкість виконання алгоритму – найважливіша характеристика. Якщо створений алгоритм працює надто повільно, він відправляється на доопрацювання. Комп'ютерними спеціалістами прийнято говорити про найгірший і середній випадок виконання. Найгірший випадок виконання – це максимальний час виконання роботи алгоритму при «найгіршому» з усіх можливих введень даних. Середній випадок виконання – це середній час роботи алгоритму за будь-яких введень. Щоб використовувати алгоритми належним чином, необхідно знати всі типи алгоритмів. Якщо програмісту необхідно розробити важливу частину програми, то він повинен уміти оцінити швидкість роботи алгоритму. Точність оцінки залежить від уміння володіти аналізом часу виконання роботи. Можуть виникати проблеми, які не були пройдені на заняттях, та застосувавши набуті навички, з'являється можливість переробки програми, поклавши в основу більш підходящий алгоритм. Чим більше відомо про алгоритми, тим більша вірогідність знайти якісний вихід із ситуації. Застосовуючи фундаментальні розуміння можна вирішити будь-які складніші задачі шляхом спрощення.

Для того, щоб повноцінно та ефективно використовувати мову програмування, необхідно мати хоча б поверхневі знання про структури даних, що вони представляють і як впливають на виконання програми. Система «алгоритм» допомагає зрозуміти, як правильно будувати й вивчати конкретні моделі алгоритмів.

Разом із розвитком обчислювальної техніки та теорії програмування зростає необхідність створення нових економічних алгоритмів, змінюються їх будова, записи алгоритмів зрозумілою мовою для виконавця. Цим особливим виконувачем алгоритмів виступає комп'ютер, тому необхідно використовувати засоби, які б дозволили працювати розробнику в зручному вигляді, так і комп'ютеру розуміти написане. Цими засобами виступають мови програмування та алгоритмічні мови. [3]

Даний предмет необхідний для того, щоб бути висококваліфікованим спеціалістом у даній області, мати кар'єрний ріст і повагу колег. Він допомагає ефективно вирішувати поставлені задачі, правильно формувати та обирати

бібліотеки та методи вирішення складних ситуацій, писати короткі за змістом, але високоефективні програми, із максимальними можливостями використання мов написання кодів або алгоритмів.

Інформатика сміливо ввійшла в нашу повсякденну дійсність, адже вона може здійснювати серйозний вплив на інтенсифікацію економіки, шляхом забезпечення оптимальних зв'язків між галузями промисловості, окремими підприємствами, а також шляхом вдосконалення управління, що спирається на інформатику. Від чітко поставленої оперативної інформації значною мірою залежить дотримання виробничої дисципліни, тому вона відразу ж набуває виняткового значення. Сьогодні інформатика не тільки спрощує матеріальні основи багатьох соціально-економічних і науково-технічних процесів, але й змінює наші уявлення про навколишній світ, про методи його пізнання.

В Україні інформаційний сектор поки що розвинутий недостатньо, але певні надбання у сфері ІКТ усе ж мають місце. За кордоном визнаються можливості України щодо розвитку мобільного зв'язку, розробки програмного забезпечення, розвитку електронної промисловості та створення умов для поширення інформаційних послуг. [2]

Вирішення більшості задач зі шкільних курсів математики та фізики можливе із застосуванням програми алгоритму або будь-якої мови програмування. Для прикладу розглянемо задачу з механіки: визначити гальмівний шлях автомобіля залежного від швидкості руху (км/год), нахилу дороги (%), коефіцієнта тертя коліс по дорозі. Дану задачу представимо через систему алгоритм.

Необхідно сформулювати набір даних, які будуть необхідні при розв'язуванні:

- Вхідні дані:
 1. V_0 – швидкість руху авто до початку гальмування
 2. F – нахил дороги
 3. K – коефіцієнт тертя
- Результат:
 1. S – гальмівний шлях
- Проміжні дані:
 1. T – час гальмування
 2. G – прискорення вільного падіння
 3. A – уповільнення при гальмуванні

Для початку визначимо головну формулу, вона має вигляд:

$$S = V_0 \cdot T + A \cdot T^2 / 2$$

Залишається задати формули для часу T і уповільнення A . Отже, маємо:

$$A = -G \cdot (K \cdot \sqrt{1 - F^2} + F)$$

$$T = -V_0 / A$$

Формуємо алгоритм: будь-який алгоритм починається блоком «початок», позначається НАЧ; за ним необхідно зазначити блок, у якому ми будемо вводити дані та дамо номер блоку даного типу: П1; наступним кроком необхідно вивести попередні дані, використавши блок О1; для того, щоб знайти проміжні та шукані значення, необхідно, використовуючи блок присвоєння, задати їхні формули; маємо - $A1 \leftarrow A2, A3, A4$; для того, щоб вивести результати використаємо вже відомий блок виведення, але продовжимо його нумерацію О2; завершуємо алгоритм блоком «кінець», який позначається КОН. Використано простий лінійний алгоритм (рис.1).

Для $V0 = 5$ км/год, $F = 1$ %, $K = 0.04$, отримуємо $S = 1.98$ м.

Таким чином, розв'язання задач будь-якої складності можливе при написанні алгоритму або ж програмного коду. Із подібної універсальності застосування відкриваються широкі перспективи застосування та розвитку даних методів, адже із часом задачі та завдання, які постають у різних галузях нашого життя, стають дедалі складніші, у той час як період виконання цих має залишитись сталим або ж зменшитись взагалі. Саме тому застосування алгоритмів та програмних кодів тільки починає набирати своєї ваги та важливості поміж інших методів, що розвиваються.

На сьогоднішній день професія програміста все більше набирає популярності та захоплює все нові й нові ринки праці, при тому, що якість освіти, яка надається, не зменшується із кількістю попиту не неї, а навпаки – збільшується, покращується. Це дає змогу доступніше сформулювати розуміння принципів написання програм різного рівня та розширити знання та навички майбутнього програміста.

Інформатика сприяє формуванню нового наукового погляду, адже, усвідомлюючи можливості вирішення проблем та розв'язання надскладних математичних задач, про що кілька десятиріч тому й думки не було, науковцям та дослідникам випадає можливість розробки значно більшої кількості теорій, досліджень чи розрахунків, які можливо з легкістю перевірити за хвилини, а то й секунди, засобами програмування. Інформатика застосовує теоретичну основу інформації і обчислення, а також практичні методи для реалізації і впровадження цих основ. У інформаційну епоху кожна освічена людина повинна мати хоча б мінімальні знання в області інформатики, тому що вона починає набирати вигляду однієї з фундаментальних наук сучасності.

Список використаних джерел:

1. Попов І.І. Інформаційні ресурси, і системи: реалізація, моделювання, управління. М.: ТПК «Альянс», 2006. – 408 с.
2. Електронний ресурс: <https://dou.ua/lenta/columns/it-in-figures/>.
3. Степанова Е.Е., Хмелевская Н.В. Інформаційне забезпечення управлінської діяльності: Учбов. посібник. – М.: ФОРУМ:ИНФРА – М, 2005. – 154 с.

ДОСЛІДЖЕННЯ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЕКТУВАННЯ «РОЗУМНОЇ ТЕПЛИЦІ» НА БАЗІ МІКРОКОНТРОЛЛЕРІВ ARDUINO

Інтелектуальна (розумна) теплиця - це система автоматизованого контролю та керування інженерним обладнанням теплиці. Вона зв'язує всі прилади та системи (опалення, освітлення, вентиляція, кондиціонери, водопостачання, та ін.), які раніше функціонували незалежно один від одного, в єдину систему з централізованим керуванням.

Важливою властивістю «Розумної теплиці», що вирізняє її від інших способів організації виробничого простору є те, що це найбільш прогресивна концепція взаємодії людини з обладнанням, коли лише однією командою можливо задати бажаний результат, а вже автоматика у відповідності із зовнішніми та внутрішніми умовами обирає і відстежує режими роботи всіх інженерних систем і електроприладів. У цьому випадку час та зусилля на виконання роботи в теплиці зменшується до мінімуму а продуктивність до максимуму. У теплиці обладнаній системою «Розумна теплиця» достатньо одним натисканням на настінній клавіші (або пульті ДУ, сенсорної панелі і т. д.) вибрати один із сценаріїв. Система самостійно налаштує роботу всього обладнання у відповідності з часом доби, становищем в теплиці, погодою, зовнішньої освітленістю і т. д. для забезпечення оптимального мікроклімату.

Якщо у Вас встановлена система «Розумна теплиця», то вона ніколи не забуде увімкнути світло або опалення, не допустить надмірного поливання або засухи. За допомогою клімат-контролю можливо підтримувати постійний оптимальний температурний режим та вологість повітря, що сприятиме кращому росту культури. Вона може самостійно відкривати і закривати вікна для провітрювання, керувати поливом, вологістю, температурою, освітленням та іншими периферфйними пристроями.

ДОСЛІДЖЕННЯ ПОБУДОВИ СЕНСОРНІ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЇ ZIGBEE

Останні роки характеризуються широким розвитком систем зв'язку з метою збору і обробки дискретної інформації в автоматизованих системах управління (АСУ).

Інформацію, що виробляється чи отримується різними пристроями автоматизації прийнято називати даними. Передача даних, так само як і телеграфний зв'язок, базується на дискретних видах сигналів, але відрізняється від останнього в основному більш високою швидкістю і збільшеними вимогами по достовірності передачі інформації по каналах зв'язку. Існуючі канали зв'язку не забезпечують цих збільшених вимог по достовірності, тому задача вирішується шляхом застосування в кінцевій апаратурі передачі даних спеціальних способів підвищення достовірності.

На теперішній час розроблено велика кількість коректуючих кодів та різного виду систем передачі, забезпечуючих підвищення достовірності передачі дискретної інформації (ПДІ). Але, не дивлячись на це, до цих пір відсутні методики оцінки їх ефективності і вибору найбільш оптимальних умов передачі інформації по існуючим телеграфним і телефонним каналам зв'язку.

Раптовість процесів при передачі дискретної інформації по каналах зв'язку і велика кількість заважаючих факторів, причина яких не завжди відома, приводять до того, що дуже важко передбачити властивості каналу зв'язку, використовуючи тільки теоретичні методи. Виходячи з цього актуальним являються роботи по дослідженню, математичному опису і математичному моделюванню реальних каналів зв'язку.

Квідкус І.А.
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

РОЗВИТОК WLAN

Бездротові локальні мережі передачі інформації (WLAN) розвиваються за останні п'ятнадцять років неймовірно швидко. Простота розгортання таких мереж обмежена тільки необхідністю оформлення дозвільної документації (у тих країнах, де це потрібно). По пропускній здатності вони не уступають виділеним мідним лініям. Завадостійкість, надійність і захищеність сучасних протоколів

передачі зробили WLAN явищем повсюдним, а устаткування для них - масовим продуктом.

Відзначимо, що поняття «локальні мережі передачі інформації» досить умовно. Як правило, маються на увазі системи, локалізовані в радіусі сотні метрів. Однак технології локальних мереж з успіхом застосовують і на відстанях до декількох десятків кілометрів.

Зауважимо, що пристрої, які відповідають вихідній специфікації IEEE 802.11, не встигли отримати розвитку. Пропускна здатність проводових мереж Ethernet дуже зросла, і максимальна швидкість передачі 2 Мбіт/с, передбачена в IEEE 802.11, не задовольняла користувачів. Проблему вирішила поява стандартів (доповнень) IEEE 802.11b, 802.11n та 802.11g.

Рубанка Роман Сегрійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ RAKE, ЯК МЕТОДУ БОРОТЬБИ З БАГАТОПРОМЕНЕВИМ РОЗПОВСЮДЖЕННЯМ СИГНАЛУ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

В останній час все активніше розвиваються бездротові системи зв'язку, технології мобільних пристроїв, бездротових та мобільних мереж доступу. В свою чергу пропорційно зростає потреба абонентів у швидкісному і якісному зв'язку та доступі до мережі Інтернет. При цьому для кожного абонента повинна бути реалізована можливість залишатися мобільними, тобто отримувати однаково якісне обслуговування у будь якій точці зони покриття стільникової мережі «на ходу».

Основною проблемою, що найбільш відчутно впливає на швидкість передачі інформації і якість послуг, що надаються абоненту системами мобільного зв'язку – це ефект багатопроменевого розповсюдження сигналу. Даний ефект виникає при умові існування в точці прийому радіосигналу не тільки прямого, але і декількох або навіть цілого ряду відбитих променів. Іншими словами на антену приймача приходять не тільки прямі промені (безпосередньо від джерела), але і відбиті (від земної поверхні, будівель та іншого роду об'єктів). Усі прийняті промені складаються у приймачі. Відбиті промені при складанні з прямими можуть призводити до так званих «завмирань» у каналі (із за довшого часу розповсюдження по середовищу на відміну від прямих променів), що в свою чергу може привести до затухання і падіння рівня сигналу у випадку складання променів в протифазі та виникнення ефекту між-символьної інтерференції (накладання у приймачі символів інформаційної послідовності один на одного).

Як метод ефективної боротьби з ефектом багатопроменевого розповсюдження сигналу та його наслідками була створена технологія RAKE, яка в даний момент активно застосовується у системах мобільного зв'язку стандарту CDMA (Code Division Multiple Access).

Суть технології полягає в наступному. Для компенсації «завмирань» та між-символьної інтерференції використовується спеціальний пристрій – Rake-приймач. У своїй структурі він містить корелятори, що дозволяють розділити і окремо обробити кожен відбитий промінь, прийнятий на антену приймача (з урахуванням індивідуального часу затримки кожного променя), що при подальшому комбінуванні таких сигналів дозволяє не тільки значно знизити вплив «завмирань», але також і збільшити загальний рівень сигналу на виході приймача.

У даній роботі також розглянуті альтернативні методи боротьби з багатопроменевим розповсюдженням – OFDM-модуляція і технологія MIMO, що знайшли своє застосування у стандартах мобільного зв'язку четвертого покоління (4G).

OFDM (Orthogonal frequency-division multiplexing – мультиплексування з ортогональним частотним розділенням каналів) – це схема модуляції, що розроблялася як прямий «спадкоємець» технології RAKE. OFDM дозволяє швидко та ефективно передавати інформацію навіть у каналах з багатопроменевим розповсюдженням сигналу. Передача ведеться одночасно на великій кількості несучих частот. Рознесення по частоті та синхронізація несучих підібрані таким чином, щоб несучі були ортогональні між собою, тобто не впливали одна на одну не зважаючи на перекриття по спектру.

MIMO (Multiple Input Multiple Output) в свою чергу використовує зовсім інший підхід за рахунок частотного і просторового рознесення як на приймальній так і на передаючій стороні шляхом використання більшої кількості приймальних і передаючих антен. Також технологія MIMO дозволяє запобігти утворенню ефекту багатопроменевого розповсюдження сигналу шляхом використання антенних решіток, які мають дуже вузьку діаграму направленості (на відміну від стандартних секторальних антен базової станції мобільного зв'язку зі значно ширшими кутами діаграми направленості), що в свою чергу дозволяє реалізувати комутований промінь з адаптивним управлінням, направлений безпосередньо на мобільний пристрій абонента.

Результатом проведеної роботи став порівняльний аналіз описаних вище технологій. На основі отриманих даних був сформований висновок, в якому відображено основні переваги та недоліки технології RAKE як методу боротьби з багатопроменевим розповсюдженням сигнал, а також виділено деякі характерні особливості, притаманні лише даній технології на відміну аналогів, розглянутих у роботі.

INTERNET OF THINGS. ВАРІАНТИ ПІДКЛЮЧЕННЯ ІОТ

Спочатку Інтернет був мережею взаємодії між людьми за допомогою комп'ютерів. Згодом він став використовуватися для взаємодії пристроїв між собою, даний метод згодом отримав назву Інтернет речей. Технології взаємодії суворо пристроїв з пристроями отримали назву M2M (machine to machine). Концепція IoT має не лише об'єднати ці два підходи («Інтернет машин» та «Інтернет людей»), а й вивести їх на новий глобальний рівень взаємодії та можливостей. Ідея Internet of Things охоплює всі сфери сучасного життя – побут, освіта, бізнес, медицина, транспорт, промисловість, екологія тощо. Список можна продовжувати нескінченно. Недивно, що говорячи про ринок Internet of Things аналітичні компанії оперують сумами в трильйон доларів.

Безпроводові технології - інформаційні технології, призначені для безпроводової передачі інформації на відстань між двома й більше об'єктами. Для передачі інформації може використовуватися інфрачервоне випромінювання, радіохвилі, оптичне або лазерне випромінювання. На сьогодні існує безліч безпроводових технологій, відомих користувачам по їхніх маркетингових назвах, таким як Wi-Fi, WiMAX, Bluetooth, ZigBee, LTE та інші. Кожна технологія має певні характеристики, які визначають її область застосування.

Найновішою областю застосування безпроводових технологій є IoT (Internet of Things). В даний час розроблюються безпроводові технології під егідою робочої групи 802.11, в тому числі 802.11ah, також відомої як HaLow – стандарт для більш низької частоти для великих територій, призначений виступати в якості комірчастої мережі саме для Інтернету речей.

На сьогодні можна зустріти різні визначення як концепції IoT, так і різноманітні точки зору на те, які основні сфери вона охоплює. Найбільш показовим є розділення, запропоноване Harvard Business Review, в рамках якого розвиток Інтернету речей проводиться в п'яти напрямках: портативні пристрої, «розумний будинок», підключені автомобілі, «розумне» місто, промисловий Інтернет.

Є безліч варіантів підключення IoT і кожен з них має певні плюси і мінуси. Основні параметри з'єднання, які використовуються в загальному випадку, це Wi-Fi, Bluetooth та стільникового бездротовий зв'язок (4G). Але у кожного з них є недоліки: Wi-Fi використовує багато енергії; Bluetooth має обмежений

діапазон; 4G також енергоємний та може бути дорогим, особливо для передачі великих об'ємів даних.

Мережеві інновації зосереджені на вирішенні проблем підключення пристроїв на великій відстані та задоволення потреб з низьким енергоспоживанням, наприклад, для пристроїв, що працюють на батареях. Цілий ряд нових мережевих IoT-опцій існують, серед них:

- Sigfox - У 2009 році Sigfox, французький стартап, представив малопотужну мережу, з ультра-вузькою смугою пропускання, що працює на неліцензованій частині спектру. Базується на моделі обслуговування операторів безпроводового зв'язку. Sigfox доступний тільки в певних частинах Європи, великих містах США та вибірково в Латинській Америці.
- LoRA - Lora Alliance – це група індустріальний партнерів, що займаються розробкою протоколу з низьким енергоспоживанням, що називається LoRaWAN. Даний протокол працює на неліцензованих частотах.
- Стільниковий IoT – Це кілька стандартів, що базуються на специфікації 3GPP, такі як LTE-M, NB LTE-M, і NB-IoT. Ці стандарти мережі змінені і оптимізовані для пристроїв IoT.

У найближчому майбутньому більшість наших електронних або квантових пристроїв будуть підключені до Інтернету через унікальну IP-адресу (в полі IPv6-адрес, оскільки IPv4 уже скоро стане елементом минулого) і, таким чином, його можна буде контролювати власником з будь-якого місця в будь-який час.

В деяких країнах плануються проекти розумних міст, створених на основі смарт-інфраструктури в поєднанні з використанням технології IoT. Що стосується людей, то портативні пристрої і розумні будинки стануть ключем до розумного і сталого майбутнього.

IoT також допоможе урядам і великим підприємствам в моніторингу, зборі, аналізу і прийнятті рішення щодо будь-якої ситуації протягом короткого часу.

Проте слід пам'ятати, що постійний розвиток технології означатиме більше електронних відходів, проблема охорони навколишнього середовища з розвитком IoT набуде особливого значення.

Дві причини підштовхують українців до реалізації IoT-проектів, здатних підкорити місцевий ринок і весь світ. Перша - спроба заощадити внутрішні ресурси: електроенергію, час, воду, сили людини. Друга - бажання опинитися біля витоків багатомільйонного бізнесу.

Internet of Things - це підключення до Інтернету всіляких пристроїв, за винятком смартфонів, планшетів і комп'ютерів. Це можуть бути датчики світла і тепла, спеціальні пристрої в автомобілях, медичні прилади й просто будь-які інші звичні предмети. Дані, які вони збирають про людину і навколишній світ, пропускаються згодом через складні програми, які перетворюють хаотичний набір показників корисну інформацію і рекомендації.

IoT є відносно безпечним - ви навряд чи зіткнетеся з серйозною втратою або пошкодження через смарт-датчики, принаймні, не більше, ніж через свій домашній комп'ютер. Тим не менше, немає ніякої гарантії і досі робиться не достатньо для забезпечення захисту IoT від злону.

З кожним днем збільшується необхідність в додатковому обладнанні, яке дозволило б збирати і обробляти більший масив даних. Оскільки речей, здатних робити це, незліченна кількість, це відкриває новий необмежений ринок. За прогнозами, він буде стрімко зростати: з 656 млрд дол в 2014 році до 1,7 трлн дол в 2020 році.

Охременко В.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

ІННОВАЦІЙНИЙ ВНЕСОК 3G

Впровадження технології 3G в Україні - це в першу чергу інноваційний внесок в економіку країни та її комплексне пожвавлення.

Згідно з отриманими даними, початок використання 3G в країні призводить до збільшення ВВП на 10%, а зростання ВВП на душу населення збільшується на 0,15%.

Статистику легко пояснити. Використання в роботі гаджетів, підключених до Інтернету, робить працю більш ефективною. Можна виділити декілька ринків, які запрацюють по-новому з приходом 3G.

Сьогодні Україна є однією з найсильніших країн з виробництва інформаційних технологій у світі. За оцінками економістів, ринок ІТ в Україні вже перевищує \$ 2 млрд на рік. Еволюція зв'язку до 3G істотно збільшує кількість користувачів та виробників додатків, а українські програмісти нарешті стануть затребувані й зможуть реалізовувати ідеї в Україні.

Бердник Ірина Ігорівна

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ БЕЗПРОВОДОВИХ МЕРЕЖ ЗВ'ЯЗКУ

Стільниковий телефон стрімко увірвався в наше життя, перетворившись з предмету розкоші в недавньому минулому в повсякденний засіб комунікації, без якого в багатьох випадках не можна обійтися. Стільниковий радіотелефонний

зв'язок розвивається найбільш динамічно серед сучасних телекомунікаційних засобів. Цікаво, що кількість стільникових телефонів уже перевершила кількість персональних комп'ютерів. Поряд з поняттям стільниковий зв'язок часто використовується й інше поняття - мобільний зв'язок.

До недавнього часу основним фактором, який мав найбільший вплив на розвиток мобільного зв'язку, була традиційна передача голосу. Проте впровадження нових технологій високошвидкісної передачі даних дозволила операторам мобільного зв'язку надавати необмежені безпроводові мультимедійні послуги, наприклад, передача електронних листів, повідомлень, перегляд Web-сторінок, доступ до корпоративних мереж. Бурхливий розвиток безпроводових мереж передачі інформації в усьому світі зв'язано з такими їхніми перевагами:

- Гнучкість архітектури (можливості динамічної зміни топології мережі при підключенні, пересуванні та відключенні мобільних користувачів без значних втрат часу);
- Висока швидкість передачі інформації (1-1000 Мбіт/с та більше);
- Швидкість проектування та розгортання;
- Високий ступінь захисту від несанкціонованого доступу;
- Відмова від дорогої і не завжди можливої прокладки або оренди оптоволоконного чи мідного кабелю.

Розпочнемо огляд з Bluetooth, яка стала першою технологією, що дозволяє організувати безпроводову персональну мережу передачі даних (WPAN - Wireless Personal Network). Технологія Bluetooth спеціально розроблена для забезпечення дешевого, стійкого, ефективного, високоємного зв'язку, для роботи з голосом і передачею даних. Дозволяє здійснювати передачу даних і голосу по радіоканалу на невеликі відстані (10-100 м) у неліцензійному діапазоні частот 2,4 ГГц і з'єднувати ПК, мобільні телефони й інші пристрої при відсутності прямої видимості.

Наступна технологія Wi-Fi. Технологія безпроводової передачі даних, що допомагає з'єднати n-ну кількість комп'ютерів у мережу, або підключити їх до інтернету, з малим радіусом дії, що використовує радіохвилі. На даний момент існує чотири основні стандарти Wi-Fi - це 802.11a, 802.11b, 802.11g і 802.11i.

3G - IMT-2000 (UMTS / WCDMA, CDMA2000/IMT-MC, TD-CDMA/TD-SCDMA DECT і UWC-136).

Після екскурсу в історію перейдемо до розгляду покоління 4G, що означає "4rd Generation" - четверте покоління комунікаційних технологій мобільних телефонів. За час існування покоління 4G воно збагатилось великою кількістю технологій для передачі даних мобільними мережами.

Найпоширенішою версією 4G на даний час є LTE.

LTE – технологія побудови мереж безпроводового зв'язку на базі IP-технологій, що відрізняється високими швидкостями передачі даних.

Впровадження технології LTE дозволяє зменшити капітальні та операційні витрати, знизити сукупну вартість володіння мережею, розширити можливості в області конвергенції послуг і технологій, підвищити доходи від надання послуг передачі даних.

Бондаренко Микола Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Інформаційних технологій
м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПОДІЛУ РАДІОРЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ З M2M- ТРАФІКОМ

Стрімкий розвиток технологічних можливостей сучасних мереж мобільного зв'язку істотно випереджає попит на їхні послуги з боку користувачів і змушує операторів звертати увагу не тільки на традиційні (мова, передача коротких повідомлень, Інтернет), але і на суміжні ринки послуг, такі як M2M, SmartGRID, IPTV, RCS і ін.

Однак нарощування потенціалу технології мобільного зв'язку перешкоджає безліч бар'єрів, так як, на жаль, технологічні можливості завжди випереджають можливості більш консервативної системи регулювання операторської діяльності та надання послуг на ринку зв'язку.

Одним з бар'єрів, що знижують потенціал майбутніх мереж є використання смуг радіочастот в рамках розвитку перспективних технологій, що є одним з основних завдань розвитку наступного покоління, а саме оптимізація розподілу обмеженого числа радіоресурсів. Рішенням завдань планування радіоресурсів, призначення пріоритетів доступу в залежності від типу трафіку з заданими вимогами до якості обслуговування (QoS, Quality of Service) займаються модулі управління радіоресурсами.

Для аналізу характеристик обслуговування трафіку, таких як ймовірність блокування, середній час передачі та ін., Застосовуються моделі мультисервісних систем масового обслуговування. При побудові та аналізі таких моделей використовується апарат теорії ймовірностей і випадкових процесів [1], теорії масового обслуговування [2] і теорії телетрафіка [3].

На даний момент не існує загальноприйнятого підходу з обслуговування M2M-трафіку, в тому числі оптимального методу для розподілу обмеженої кількості радіоресурсів між H2H-користувачами і великою кількістю M2M-пристроїв. У зв'язку з цим існує безліч завдань ефективного планування і управління радіоресурсами [4].

Таким чином, для бездротових мереж наступних поколінь попереду стоїть завдання розробки нових моделей і методів аналізу їх функціонування для дослідження ефективності обслуговування M2M-трафіку. Існуючі методи розподілу радіоресурсів, які історично були оптимізовані для обслуговування користувачів традиційних послуг зв'язку, повинні бути доопрацьовані.

Література:

1. Башарин Г.П. Введение в теорию вероятностей: Учеб. пособие для студентов II-III курсов специальностей «Математика», «Прикладная математика». – М.: Изд-во РУДН, 1990. – 228 с.
2. Башарин Г.П., Бочаров П.П., Коган Я.А. Анализ очередей в вычислительных сетях. Теория и методы расчета. – М.: Наука, Гл. ред. физ.-мат. лит., 1989. – 336 с.
3. Лагутин В.С., Степанов С.Н. Телетрафик мультисервисных сетей связи. – М.: Радио и связь, 2000. – 320 с.
4. Dohler M, Alonso-Zarate J, Watteyne T. Machine-to-machine: an emergin communication paradigm // Tutorial, PIMRC 2010, 26 Sept. 2010, Istanbul, Turkey.

Сагайдак Виктор Анатольевич

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

БОТИЗАЦИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

Человек создание ленивое – с давних времен всегда стремился упростить себе жизнь: изобрел колесо, чтобы вместо того, чтобы толкать тележку катить её. Процесс упрощения происходит и до сегодняшнего дня – в телекоммуникациях раньше девушку переключали абонентов, а теперь это делают машины.

Бот – автоматическая программа, выполняющая автоматически какие-либо действия. Сейчас их применяют начиная от производственной до сферы обслуживания, потому как они уменьшают затраты на содержание персонала, так и на облегчение жизни обслуживающего персонала или клиентов.

К примеру, Сбербанк сейчас применяет чат-ботов в своих приложениях «Сбербанк-попутчик», платежный бот и т.п. «Сбербанк-попутчик» - это платформа, которая отправляет оповещения от одного сотрудника, которому нужно направиться в точку А в определенное время, другим сотрудникам, которые собираются выезжать. Если пункт и время сотрудника ищущего и отправляющего совпадают – бот информирует обе стороны. Платежный бот - через него можно было выбрать еду, при этом бот подсказывал оптимальные варианты под запрос пользователя, запоминал вкусы и потребительскую корзину и мог подсказывать блюда в следующем заказе. Фактически пилотный бот выполнял функции приложения службы доставки еды. Однако служб много — приложений много (под каждого поставщика приходится скачивать и устанавливать свое). А чат-бот — это лишь один из контактов в телефоне, по сути это просто новый канал получения той же услуги.[1]

Википедия использует ботов для правок статей. У них продвинутая функциональность: они умеют автоматически исправлять вандализм, отслеживать баны, проверять правописание, создавать ссылки между статьями

на разных языках, автоматически импортировать контент, осуществлять майнинг данных, определять нарушения копирайта, приветствовать новичков и т.д. Но среди ботов встречаются конфликты: Специалисты из Оксфордского института интернета недавно опубликовали результаты исследования, что происходит на страницах Википедии, когда на странице правок встречаются несколько ботов, предназначенных для внесения изменений в статью. По статистике, 15% всех правок в Википедию вносят именно боты. Исследование показало, что если правки ботов отклоняются, то обычно это происходит по инициативе других ботов, а не людей. Наибольшее количество правок ботов, которые исправляются другими ботами, а затем исправляются обратно, относится к **«несогласию между ботами, которые специализируются на создании и исправлении ссылок между различными языковыми редакциями энциклопедии»**. По мнению авторов исследования, «отсутствие координации может быть связано с тем, что в разных языковых редакциях немного различаются правила именования и соглашения».[2]

Также ботов используют в образовательных целях: в приложении Telegram подтянуть речь, грамматику закрепить знания по иностранному языку с использованием тех же чат-ботов. Приложения могут отправить аудио-файл с правильным произношением того или иного слова или подобрать упражнения для улучшения грамматики после прохождения теста.[3]

Но как говорится: «Нет худа без добра». Боты могут быть использованы злоумышленниками для своих целей: накрутки популярности групп, сайтов в социальных сетях или приложениях, фишинге пользователей.

К примеру, Инбар Рац из PerimeterX проводил исследования по количеству ботов в приложении знакомств Tinder. Как показал результат - 70% прекрасной половины – являются ботами. Перед конференцией по информационной безопасности в Копенгагене зашел в Tinder и в течение часа получил восемь совпадений (matches), или пар, как это называется в русском интерфейсе Tinder, — все как на подбор привлекательные молодые женщины. Одна из них отправила ему сообщение на датском со ссылкой в конце. После этого Tinder предложил Рацу еще множество вариантов пар, и все они написали ему сообщения. Все эти сообщения были практически идентичными — различие состояло в четырех символах в конце ссылки.[4]

То есть, боты в данный момент как огонь – их используют как для улучшения жизни, так и для вредительства. Юридически сейчас это никак не регулируется, но в будущем ситуация может стать чуточку светлее, потому как при развитии одной области та тянет за собой другую.

Список использованных источников:

1. Хабрахабр [электронный источник]// Как чат-боты наделяют разумом ИТ-проекты Сбербанка – Режим доступа: <https://habrahabr.ru/company/sberbank/blog/337496/>

2. Geektimes[электронный источник]// О чём хорошие боты спорят в Википедии– Режим доступа: <https://geektimes.ru/post/286336/>

3. Newtonew[электронный источник]// 5 Telegram-ботов для изучения английского языка—
Режим доступа:
<https://newtonew.com/app/5-telegram-botov-dlya-izucheniya-angliyskogo-yazyka>
4. Блог лаборатории Касперского [электронный источник]// Приложение-ловушка:
удивительный мир ботов Tinder— Режим доступа:
<https://www.kaspersky.ru/blog/tinder-bots/14649/>

Скаба Світлана
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ЯК ТЕХНОЛОГІЯ IP/MPLS ЗМІНЮЄ СВІТ?

В даному докладі мова йде про еволюцію комунікацій - технологію IP/MPLS. Зацікавитимуться питання способу комутації, базової архітектури, і основне завдання даної технології.

На сьогоднішній день напрям телекомунікацій є однією з найперспективніших в світі. Одним з шляхів розвитку мультисервісної мережі є впровадження методів багаторівневої комутації. Основною ціллю було зіставити переваги IP-маршрутизації та АТМ-комутації при цьому залишаючись орієнтованими на застосування в IP – мережах, таким чином дозволяючи розвиватися мультисервісній мережі в сторону спрощення її структури, шляхом інтеграції функцій другого і третього рівнів.

У 1996 р. група інженерів з Ipsilon Networks розробила «Протокол управління потоком» (англ. потоку Management Protocol). Заснована на цьому протоколі технологія «Комутації IP-пакетів» (англ. IP Switching), що працює тільки поверх спрощеної АТМ мережі, не отримала комерційного успіху. Cisco Systems розробила схожу технологію «Коммутатції на основі тегів» (англ. тегів Switching), але не обмежену передачею поверх мережі АТМ. Дана технологія, згодом перейменована в «Комутацію міток» (англ. Label Switching), була закритою розробкою Cisco. Пізніше вона була передана в Спеціальну комісію інтернет-розробок (IETF) для відкритої стандартизації.

MPLS (англ. Multiprotocol Label Switching — багатопротокольна комутація за мітками) — механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів.

Основна особливість технології MPLS – відділення процесу комутації пакета від аналізу IP-адреси в його заголовку, що дозволяє здійснювати комутацію пакетів значно швидше.

У традиційній IP-мережі пакети передаються від одного маршрутизатора до іншого, й кожний маршрутизатор, зчитуючи

заголовок пакета, (адреса призначення) приймає рішення про те, за яким маршрутом відправити пакет далі.

У протоколі MPLS ніякого подальшого аналізу заголовків у маршрутизаторах на шляху проходження не проводиться, а переадресація керується виключно на основі міток.

Маршрутизатори MPLS мережі називаються LSR (label switching routers)- маршрутизатори комутації по мітках, а маршрутизатори які використовуються на кордонах MPLS мережі Edge LSR - крайові LSR.

Коли IP трафік надходить до MPLS мережі крайові LSR перетворюють IP-пакети на MPLS-пакети вставляючи мітки. А коли пакети лишають MPLS мережу крайові LSR перетворюють MPLS-пакети назад на IP-пакети видаляючи мітки. В середині ж MPLS мережі LSR маршрутизують пакети по значенням міток.

На сьогоднішній день можна виділити три основні області застосування протоколу MPLS. Це управління трафіком, підтримка класів і якості обслуговування і віртуальні приватні мережі.

1) Управління трафіком (Traffic Engineering, TE) - це можливість управління напрямом проходження трафіку з метою виконання певних умов (резервування каналів, розподіл завантаження мережі, балансування і запобігання перевантажень). Управління потоком інформації, що передається дозволяє направляти потоки даних не по найкоротшому шляху, обчисленому за допомогою традиційного протоколу маршрутизації, а через менш завантажені вузли і канали зв'язку.

2) одна з основних переваг наданих MPLS криється в можливості управління QoS. Саме комутація на основі міток робить MPLS настільки корисним і унікальним. Frame relay і ATM забезпечують QoS за рахунок вибору маршруту, протягом якого мережа буде підтримувати вимоги трафіку до QoS завдяки виділенню ресурсів на кожному вузлі лінії з метою гарантії того, що трафік отримає необхідні для досягнення необхідного QoS ресурсів.

3) віртуальна приватна мережа (Virtual Private Network, VPN) моделює роботу корпоративної територіально розподіленої мережі за допомогою інфраструктури пакетної мережі загального користування. Але передача корпоративних даних через публічну пакетну мережу, являє собою очевидну загрозу в рамках безпеки мережі будь-якого підприємства. Крім цього, в каналах публічної зв'язку досить складно домогтися необхідного рівня продуктивності, надійності і якості обслуговування. Для вирішення цих проблем використовують технологію віртуальних приватних мереж VPN. В її основі лежить ідея використання мереж загального користування для захищеної передачі трафіку територіально віддалених філій замовника, з використанням ідеології побудови приватних мереж.

На даний час технологія MPLS набирає популярності, і кожен великий провайдер вводить її в свою мережу. Тому перехід на технологію MPLS є на даний час найбільш розумним рішенням, і дозволить перенести якість інтернет послуг на новий рівень.

Література:

1. Бубенцова Л. В. Технология MPLS. – Одесса : ОНАС им. А. С. Попова, 2010. – 44с.
2. Олвейн В. Структура и реализация современной технологии MPLS / пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 480 с.
3. Магистральная технология XXI века.

Зайка Максим

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

СУЧАСНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ

Інформаційною технологією (ІТ) розуміють систему методів і способів збирання, накопичення, зберігання, пошуку і оброблення інформації на основі застосування засобів обчислювальної техніки. ІТ відповідають на питання “як, за допомогою чого?”.

ІТ залежать від різних компонентів, зокрема:

- технічних засобів;
- персоналу, здатного використовувати їх;
- організації, яка об'єднує засоби і персонал в єдиному процесі;
- інформаційних засобів, що здійснюють формування й видачу інформації.

Систему, що реалізує функції управління, називають системою управління. Найважливішими функціями, реалізованими цією системою, є прогнозування, планування, облік, аналіз, контроль і регулювання.

Управління пов'язане з обміном інформацією між компонентами системи, а також системи з навколишнім середовищем. У процесі управління одержують відомості про стан системи в кожен момент часу, про досягнення (або не досягнення) заданої мети для того, щоб впливати на систему й забезпечити виконання управлінських рішень.

Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. На її основі створено та створюються обчислювальні системи й мережі різних конфігурацій не тільки для нагромадження, зберігання, перероблення інформації, але й максимального зближення термінальних улаштувань до робочого місця спеціаліста та для підтримки прийняття рішення керівника.

Інформаційні технології можна класифікувати за рядом ознак:

- за способом реалізації в АІС: традиційні, нові, високі ІТ;
- за ступенем охоплення задач управління: електронне оброблення даних, автоматизація функцій управління, підтримка прийняття рішень, електронний офіс, експертна підтримка.

ПРИНЦИПИ ПОБУДОВИ ГЛОБАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Вагомими спонукальними причинами стрімкої побудови потужних глобальних комп'ютерних мереж стали нагальні потреби ринку інформаційних послуг. Створення і розвиток таких мереж є цілком закономірним і природним процесом. Розглядаючи сучасне суспільство як деяку складну динамічну систему, всередині якої постійно відбуваються процеси інформаційного обміну, необхідно особливо виділити як базовий елемент побудови інформаційної інфраструктури ,технології інформаційного обміну, технології передавання даних на великі відстані, технології побудови систем оперативного доступу до різноманітної інформації.

Глобальна мережа (ГМ) сполучає кілька локальних мереж або ПК, географічно віддалених один від одного. Для глобальних мереж характерний масштаб (як за площею мережі, так і за числом вузлів) та неоднорідність., тобто різний тип архітектури та програмного забезпечення їх вузлів.

Розвиток глобальних мереж розпочався наприкінці 60-х рр. XX ст. у США. Першою була створена мережа **ARPANET** для спілкування науковців різних інститутів, що працювали над військовими проблемами. Головним заданням було створення мережі, яка могла б розширюватися, щоб приєднання чи вихід з ладу одного з вузлів не впливало на функціонування інших. Однак протокол NCP, згідно з яким працювала ARPANet, не передбачав взаємодії між мережами різної архітектури, тому в 1973 році було створено новий протокол TCP/IP. Перехід мережі на новий протокол дав їй змогу в 1984 р. розділитися на дві: **MILNet** – для військового відомства і **ARPANET** – для невійськового використання. У 1990 р. ARPANet припинила своє існування .

Кожна з глобальних мереж (Internet, FIDONet, ALONA, Bitnet, DECnet та ін.) організовувалися для конкретних цілей, а в подальшому поширювалися за рахунок під'єднання локальних мереж, які використовували їх послуги та ресурси .

Залежно від розмірів охоплюваної мережею території ГМ поділяють на: *міжнародні*, які функціонують на території кількох країн чи континентів; *регіональні* або *національні*, які охоплюють територію країни, регіону, міста; *корпоративні* або *відомчі*, що зв'язують між собою локальні мережі одного підприємства, установи, відомства.

Першою технологією глобальних мереж стала **технологія E1...E4/T1...T4**, що була розроблена на початку 60-х рр. XX ст. Почали використовувати цифрові лінії для передавання телефонних повідомлень. Сигнали від різних джерел накопичувалися в мультиплексорі і передавалися одним кабелем. При прийманні сигналів відбувалося їх перетворення на початкову форму.

У 70-х рр. XX ст. почали розвиватися **XDSL-технології**. Принцип цих технологій заснований на тому, що мовний сигнал не використовує всієї смуги пропускання телефонної лінії. Отже, є можливість розмістити цифровий сигнал. Для цього використовується спеціальне обладнання фільтрування сигналів, що надходять телефонними лініями та DSL-модеми.

Найпоширеніша технологія – **технологія ISDN** (цифрова мережа з інтеграцією послуг). Вона передбачає перетворення всіх видів даних у цифрові з наступним їх передаванням одним каналом зв'язку. Це дозволяє швидко і якісно передавати мову, дані, музику, відео.

Технологія FDDI (розподілений оптичний інтерфейс даних) – це специфікація, що описує високошвидкісну мережу зі структурою типу «подвійне кільце» на основі оптоволокна. Вона забезпечує високошвидкісний зв'язок між мережами різних типів. Однак довжина кільця має обмеження – до 100 км.

FDDI базується на технології спільного використання мережі. Це означає, що одночасно можуть передавати дані кілька комп'ютерів (що може спричинити перевантаження мережі). FDDI використовує систему передавання маркерів у подвійному кільці. Трафік у мережі FDDI складається із двох подібних потоків, що рухаються в протилежних напрямках двома кільцями. Головна перевага топології типу «подвійне кільце» – надмірність. Одне кільце використовується для передавання даних, а друге є резервним. Зазвичай дані передаються лише основним кільцем. Якщо в основному кільці відбувається збій, то мережа автоматично переконфігурується і дані починають передаватися додатковим кільцем у протилежному напрямку.

Ця технологія має певні обмеження: загальна довжина кабелю об'єднаних кілець має бути не більшою ніж 200 км; довжина одного кільця не повинна перевищувати 100 км; до одного кільця не може бути підключено більше, ніж 500 комп'ютерів; щонайменше через кожні 2 км має бути встановлений репітер.

Комп'ютери можуть підключатися до одного чи до обох кілець FDDI. Комп'ютери, підключені до обох кілець, називаються станціями класу А, а ті, що підключені тільки до одного кільця, – станціями класу В. Якщо відбувається збій у мережі, то станції класу А беруть участь у переконфігуруванні мережі, а станції класу В – ні.

Ще відомі **сучасні технології** такі, як **X.25**, **Frame Relay** – протокол ретрансляції кадрів, **асинхронний режим передавання (ATM)**, на основі

яких будуються як локальні, так і глобальні мережі, а на основі TCP/IP працює мережа Internet.

Література:

1. Комп'ютерні мережі : навч. посіб. для студ. / К. О. Кобильнік. – Київ : НТУУ «КПІ», 2008.

О.А. Золотухіна, І.А. Бученко
Державний університет телекомунікацій
м. Київ

ВИКОРИСТАННЯ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ ЗАДАЧ АВТОМАТИЗАЦІЇ ОСВІТНІХ ПРОЦЕСІВ В СЕРЕДНІХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Освітні процеси в середніх навчальних закладах вимагають не тільки постійної взаємодії вчителів та учнів, а й залучення до цих процесів батьків. Електронні щоденники та журнали, спеціалізовані дошки оголошень, календарі та системи обміну повідомленнями широко впроваджуються в багатьох школах України. Однак, слід зауважити на те, що існуючі додатки практично не використовують мобільні технології.

Пропонується розробка мобільного додатку для полегшення роботи класного керівника з учнями та їх батьками. Функціональні можливості програмного продукту дозволять автоматизувати розсилки сповіщень про базові важливі події (інформація про причини відсутності учнів на заняттях, батьківські збори, виклик батьків до школи тощо) безпосередньо в додатку, а також забезпечити автоматичний збір статистики відповіді батьків. Використання вказаного мобільного додатку дозволить значно заощадити робочий час класного керівника та кошти на телефонні дзвінки і смс-повідомлення.

Борисенко Микола Борисович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ

ІВМ В ОБЛАСТІ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ

Інтелектуальна мережа - це трансформована система передачі електрики, яка базується і використовує переваги сучасних технологій.

Інтелектуальна мережа:

- Дозволяє активну участь споживачів в обміні інформацією за допомогою мережі
- Чи передбачає можливість використання всіх наявних опцій
- Сприяє створенню нових продуктів, послуг і ринків
- Забезпечує якість і кількість енергії, необхідне для споживачів

- Сприяє оптимізації активів і операційної ефективності
- Забезпечує умови для недопущення збоїв в роботі мережі
- Формує умови для забезпечення безпеки проти негативного зовнішнього впливу.

Теза 1: Трансформація традиційної мережі в інтелектуальну мережу - це більше, ніж застосування нових технологій. Це каталізатор для трансформації всього ланцюжка створення вартості вимагає:

Стратегія (фундаментальне переосмислення бізнес стратегії і моделей управління промисловістю).

Співробітництво (більш тісний контакт зі споживачами, регуляторами, фінансистами, дослідниками, постачальниками технологій і сервісів, і з іншими зацікавленими сторонами).

Люди (новий погляд на роль, компетенції співробітників і на структуру управління).

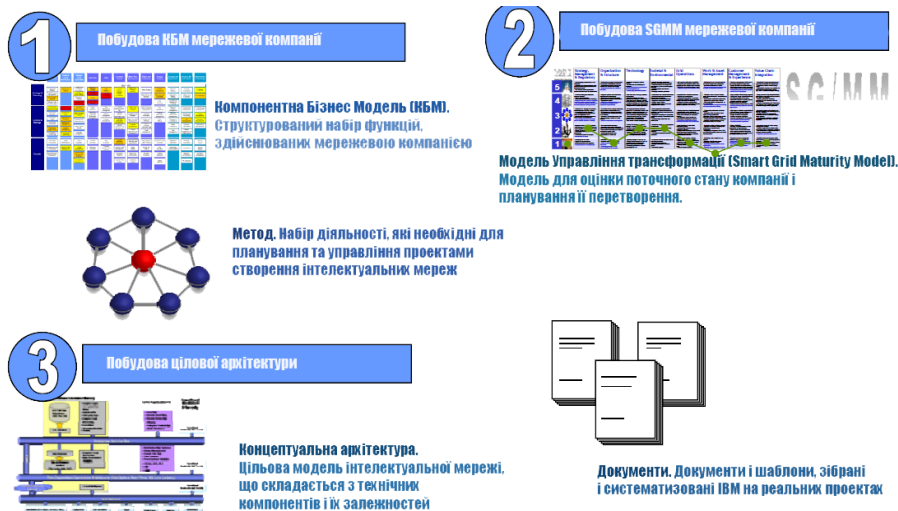
Процеси (новий дизайн бізнес процесів та програм по основними напрямками).

Теза 2: Пропозиція IBM в області побудови інтелектуальної мережі охоплює всі 4 основні елементи побудови інтелектуальної мережі: розумні прилади обліку, управління мережею, безпека мережі, комунікаційні мережі.

Теза 3: Основні етапи створення інтелектуальної мережі - рівні, опис і результати.



Теза 4: Програма впровадження рішення IBM в області побудови інтелектуальних мереж.



Теза 5: IBM - інтегратор для компаній енергетики та інтеграторів ... Побудова моделі інтелектуальної мережі на базі використання CIM моделі (Common Information Model) для забезпечення зв'язку з інформацією і системами генераторів, збутових компаній, СО ЦДУ і АТС на трьох основних рівнях. Це технологічний рівень, комерційний рівень, системний рівень.

IBM з власним програмним (і апаратним) забезпеченням для побудови мережі на SAFE (Solution Architecture for Energy Company):

Моніторинг і Управління Активами: IBM Maximo (управління активами), IBM Tivoli Netcool (моніторинг роботи лічильників, мережевий та іншої інфраструктури), IBM ILOG.

Управління Роботами: IBM Maximo (управління активами). IBM FileNet (управління документообігом), IBM ILOG.

Процесна інтеграція: IBM WebSphere Modeler (моделювання і оптимізація), IBM WebSphere Process Server (виконання), IBM WebSphere ESB (інтеграція), IBM WebSphere Message Broker (тиражування інформації та даних в реальному часі).

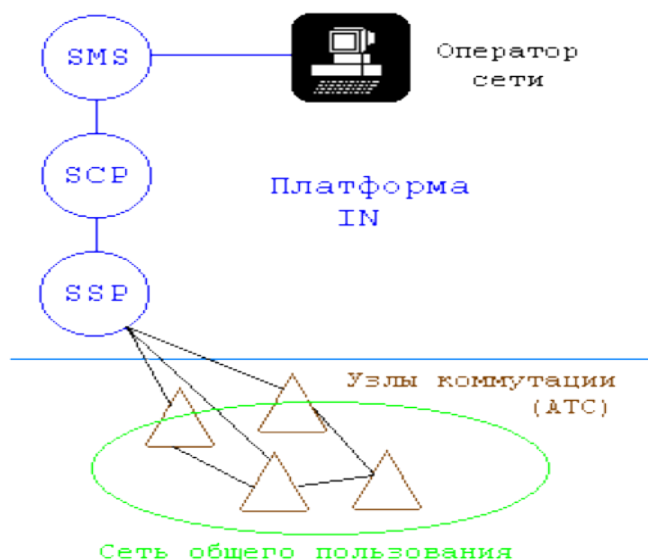
Активне Управління Споживанням: IBM WebSphere Portal, IBM Lotus Connections, IBM Lotus Expediter.

Ухвалення Рішення на основі Аналізу Інформації: IBM Cognos, IBM ILOG, IBM SPSS.

Управління Ризиками: IBM FileNet, IBM ILOG, IBM Tivoli Compliance Insight Manager.

Рішення по Забезпеченню Безпеки: IBM Tivoli Security Solutions, IBM DataPower.

Загальний спрощений вид "інтелектуальної мережі" наведено на малюнку:



Висновок: мета ідеї «Інтелектуальні мережі» полягає в відділенні процесу традиційної комутації викликів від процесу введення нових послуг. Для цього необхідно мати певні інтерфейси між комутаторами мережі і спеціальним пристроєм, званим "інтелектуальною надбудовою", "інтелектуальною платформою" або "платформою інтелектуальної мережі", і визначення типів даних, що передаються по ним. Модернізація послуг в цьому випадку проводиться лише модернізацією програмного забезпечення "платформи інтелектуальної мережі". Це дозволяє швидко і економічно впроваджувати на існуючих мережах будь-які послуги незалежно від виробників комутаційного обладнання.

Кононенко Владислав Вікторович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІОТ – РІШЕНЬ НА БАЗІ СТІЛЬНИКОВИХ МЕРЕЖ

Вплив технологій на наше життя важко переоцінити. Автомобілі дозволили швидко переміщатися, комп'ютери відкрили людству цифровий світ, в якому великі масиви даних можна зберігати, обробляти і передавати найрізноманітнішими способами, а стрімкий розвиток технологій дозволяє людям переосмислювати свою життєдіяльність.

Кожен з перерахованих винаходів, а також безліч інших - від холодильників і швейних машинок до телефонів, друкарських машинок і фотоапаратів - поступово влилися в суспільство і викликали величезну кількість політичних, соціальних і практичних змін. Вони перетворилися в речі, якими люди користуються щодня - і які здебільшого сприймаються як щось загальноприйняте і буденне. Також вони змінили

те, як люди вирішують свої численні повсякденні завдання, і дозволили їм переосмислити способи взаємодії, комунікації та виконання своєї повсякденної активності.

Свого часу Джо Болен, Джордж Біл і Еверетт Роджерс з Державного університету штату Айова ввели поняття кривої впровадження технологій (зараз вона вже є загальноприйнятою). Науковці висунули ідею про те, що будь-який новий продукт або рішення рухається відносно передбачуваній траєкторії, схожій на Гауссову криву. Така схема працює і в наш час, хоча за останні два десятиліття цей життєвий цикл технологій суттєво прискорився і продовжує набирати обертів.

В епіцентрі такого вибуху зараз знаходиться Інтернет речей - причому він тільки починається, але невдовзі він стане практичною основою життя та ведення бізнесу.

Взаємодіючи один з одним пристрої існували з часів появи перших комп'ютерних мереж і побутової електроніки. Однак поки не з'явився Інтернет, нікому не приходило в голову, що зв'язок може бути глобальним. У 1990-х дослідники масово розробляли теоретичні моделі про те, як поєднання людини і машини дасть абсолютно нову форму комунікації та взаємодії. А тепер ця реальність розгортається у нас на очах.

Хоч достовірно і не відомо, що саме стало тією іскрою, з якої розгорілося полум'я теперішньої технологічної революції, але можна із впевненістю стверджувати, що вирішальною подією став випуск провідними компаніями пристроїв, які від того часу почали називати смартфонами. Смартфони потрапили в руки мас. Завдяки цьому стала можливою взаємодія між двома об'єктами на карті за допомогою мобільного пристрою, який можна тримати в руці або покласти до кишені. За оцінками шведської компанії Ericsson, у 2021 році кількість таких пристроїв перевищить 28 млрд, 15 млрд з яких матимуть змогу взаємодіяти між собою без втручання людини [1, с. 2].

У кожен з таких портативних пристроїв вбудований набір мікросхем, які фіксують дані, голос, відео, аудіо, рух, розташування та багато іншого. Смартфони дозволили використовувати нові способи управління і аналізу подій в реальному світі.

В той же час досягли стрімкого розвитку технології радіочастотної ідентифікації (РЧІД), великий крок здійснили сенсорні технології, прискорилися процеси мінімізації обсягів, і вчинило гігантський стрибок програмне забезпечення. Зближення цих технологій - поряд з практично повсюдним поширенням бездротових мереж і хмарних комп'ютерних систем - призвело до появи ідеї про роботів-комах і роботів-тварин, нанороботів і мікророботів, які можуть функціонувати всередині людини, а також дронів, що виконують різні завдання на великій висоті. Немає ніяких сумнівів, що ми вступаємо в чудовий новий світ вбудованих технологій, що передбачають повне занурення у віртуальне середовище. Цей світ на перший погляд

більше схожий на наукову фантастику, ніж на науковий факт. Але все ж він залишається фактом.

Інтернет речей (IoT) дає нам поняття масиву фізичних об'єктів, машин, людей та інших пристроїв, що дозволяють встановлювати зв'язок та комунікації для обміну даними. Весь цей масив складається зі смартфонів, планшетів, побутової електроніки, транспортних засобів, двигунів та датчиків, які здатні до IoT зв'язку. Інтернет речей дозволяє дистанційно відстежувати та управляти об'єктами через існуючу мережеву інфраструктуру, створюючи можливості для прямої інтеграції між фізичним та цифровим світом, що дасть змогу підвищити якість та швидкість індустріального виробництва, а також до розв'язання повсякденних та побутових проблем.

Кількість IoT-комунікацій буде зростати протягом наступних років. З посиленням поширеності мобільного широкосмугового доступу стільниковий зв'язок стає однією з важливих методологій доступу для IoT. Значна частина комунікацій IoT планується в стільникових мережах. За даними досліджень та прогнозів GSMA, стільниковий зв'язок IoT прогнозує, що до 2020 року він становитиме більше 10 відсотків світового ринку. В наш час мобільні технології вже використовуються для IoT у деяких випадках, і очікується, що вони будуть використані ще в майбутньому, оскільки ці випадки використання вимагають повсюдної мобільності, стійких мереж, надійної безпеки, масштабованості мереж зв'язку, незалежно від різноманітності виробників IoT пристроїв.

Основне завдання для індустрії мобільного зв'язку зараз полягає в забезпеченні інтеграції з цими взаємозалежними мережами пристроїв таким чином, щоб вони були безпечними, гнучкими та легко масштабованими, забезпечуючи при цьому високу надійність та прийнятну затримку при передачі даних. Також необхідне забезпечення якісним покриттям, низьким рівнем споживання енергії для пристроїв, що потребують тривалого часу автономної роботи та оптимізація для підтримки великої кількості пристроїв. Метою є визначення основних перспективних рішень та охоплення набору інноваційних підходів та технологій як складових для вирішення цих проблем.

ЛІТЕРАТУРА:

1. Онлайн ресурс: <https://iot-analytics.com/internet-of-things-definition/>
2. Ericsson, Ericsson Mobility Report, November 2015, available at: <http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf>
3. Онлайн ресурс: https://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf

КАК ПОСТРОИТЬ КАРЬЕРУ В ИТ

В докладе сделано анализ рынка ИТ-сферы в Украине за параметрами объёма, экспорта-импорта продуктов и качества специалистов. Обозначены необходимые требования по соответствию студента уровню современного конкурентноспособного специалиста.

Обозначены и проработаны первейшие необходимые навыки, как то: умение говорить, знание английского языка, знания по специальности:

- проведён анализ и выделены разъяснения касательно умения говорить. Обозначены конкретные пункты для достижения требуемого уровня студентом по данному пункту путём тренировок (артикуляция, жестикуляция), работы над словарным запасом, увеличение эрудиции и, как следствие, снижение страха ведения диалога с различными должностными лицами;
- проведён анализ и выделены разъяснения касательно знания английского языка. Обозначены конкретные пункты для достижения требуемого уровня студентом по данному пункту образование в университете, чтение профильной литературы, выбор интересного контента;
- проведён анализ и выделены разъяснения касательно знания по специальности. Обозначены конкретные пункты для достижения требуемого уровня студентом по данному пункту образование в университете, сертификация.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційного обслуговування, переробки величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, який грає роль підсилювача інтелектуальних можливостей людини і суспільства в цілому, а комунікаційні засоби, які використовують комп'ютери, служать для зв'язку і передачі інформації. суспільства.

Інформатизація. Поява і розвиток комп'ютерів - це необхідна складова процесу інформатизації суспільства є однією із закономірностей сучасного соціального прогресу. Цей термін все наполегливіше витісняє широко використовуваний до недавнього часу термін «комп'ютеризація суспільства». При зовнішній схожості цих понять вони мають істотну відмінність.

При комп'ютеризації суспільства основна увага приділяється розвитку і впровадженню технічної бази комп'ютерів, що забезпечують оперативне отримання результатів переробки інформації і її накопичення.

При інформатизації суспільства основна увага приділяється комплексу заходів, спрямованих на забезпечення повного використання достовірного, вичерпного і своєчасного знання у всіх видах людської діяльності.

Таким чином, «інформатизація суспільства» є більш широким поняттям, ніж «комп'ютеризація суспільства», і спрямована на якнайшвидше оволодіння інформацією для задоволення своїх потреб. У понятті «інформатизація суспільства» акцент треба робити не стільки на технічних засобах, скільки на сутності і меті соціально-технічного прогресу. Комп'ютери є базовою технічною складовою процесу інформатизації суспільства.

Інформатизація на базі впровадження комп'ютерних і телекомунікаційних технологій є реакцією суспільства на потребу в істотному збільшенні продуктивності праці в інформаційному секторі суспільного виробництва, де зосереджено більше половини працездатного населення. Так, наприклад, в інформаційній сфері США зайнято понад 60% працездатного населення, в СНД - близько 40%.

З сучасної точки зору використання телефону в перші роки його існування виглядає досить смішно. Керівник диктував повідомлення своєму секретарю, який потім відправляв його з телефонної кімнати. Телефонний дзвінок брали в аналогічній кімнаті іншої компанії, текст фіксували на папері і доставляли адресату. Знадобилося багато часу, перш ніж телефон став таким поширеним і звичним способом повідомлення, щоб його стали, використовувати, так, як ми це робимо сьогодні: самі дзвонимо в потрібне місце, а з появою стільникових телефонів - і конкретній людині.

У наші дні комп'ютери, в основному, застосовуються як засоби створення та аналізу інформації, яку потім переносять на звичні носії (наприклад, папір). Але тепер, завдяки широкому розповсюдженню комп'ютерів і створення Інтернету, вперше можна за допомогою свого комп'ютера спілкуватися з іншими людьми через їх комп'ютери. Необхідність використання роздрукованих даних для передачі колегам усувається подібно до того, як папір зникла з телефонних переговорів. Сьогоднішній день, завдяки використанню Web, можна порівняти з тим часом, коли люди перестали записувати текст телефонних повідомлень: комп'ютери (і їх зв'язок між собою за допомогою Інтернету) вже настільки широко поширені і звичні, що ми починаємо використовувати їх принципово

новими способами. WWW - це початок шляху, на якому комп'ютери по - справжньому стануть засобами зв'язку.

Інтернет надає безпрецедентний спосіб отримання інформації. Кожен, хто має доступ до WWW, може отримати всю наявну на ньому інформацію, а також потужні засоби її пошуку. Можливості для освіти, бізнесу та зростання взаєморозуміння між людьми стають просто приголомшливими. Більше того, технологія Web дозволяє поширювати інформацію всюди. Простота цього способу не має аналогів в історії. Для того щоб зробити свої погляди, товари або послуги відомими іншим, більше немає необхідності купувати простір в газеті чи журналі, платити за час на телебаченні і радіо. Web робить правила гри однаковими для уряду і окремих осіб, для малих і великих фірм, для виробників і споживачів, для благодійних і політичних організацій. World Wide Web (WWW) в інтернеті - це найдемократичніший носій інформації: з його допомогою будь-хто може сказати і почути сказане без проміжної інтерпретації, спотворення і цензури, керуючись певними рамками пристойності. Інтернет забезпечує унікальну свободу самовираження особистості та інформації.

Подібно до використання внутрішніх телефонів компаній для зв'язку співробітників між собою і зовнішнім світом, Web застосовується як для зв'язку всередині організації, так і між організаціями та їх споживачами, клієнтами і партнерами. Та ж сама технологія Web, яка дає можливість невеликим фірмам заявити про себе на Інтернеті, великою компанією може використовуватися для передачі даних про поточний стан проекту по внутрішній інтрамережі, що дозволить її співробітникам завжди бути більш обізнаними і, отже, більш оперативними в порівнянні з невеликими, моторними конкурентами. Застосування інтрамережі всередині організації для того, щоб зробити інформацію доступнішою для своїх членів, також є кроком вперед у порівнянні з минулим. Тепер, замість того, щоб зберігати документи в заплутаному комп'ютерному архіві, з'явилася можливість (під контролем засобів захисту) легко проводити пошук і опис документів, робити посилання на них і складати покажчики. Завдяки технології Web бізнес, так само як і управління, стає більш ефективним.

Сучасні інформаційні технології обробки даних. Інформаційна технологія обробки даних призначена для розв'язання добре структурованих задач, по яких є необхідні вхідні дані і відомі алгоритми та інші стандартні процедури їх обробки. Ця сучасна технологія застосовується на рівні операційної (виконавчої) діяльності персоналу невисокої кваліфікації з метою автоматизації деяких рутинних постійно повторюваних операцій управлінської праці. Тому впровадження сучасних інформаційних технологій і систем на цьому рівні істотно підвищить продуктивність праці персоналу, звільнить його від рутинних операцій, можливо, навіть призведе до необхідності скорочення чисельності працівників.

На рівні операційної діяльності вирішуються такі завдання:

- Обробка даних про операції, які здійснює фірма;
- Створення періодичних контрольних звітів про стан справ у фірмі;
- Одержання відповідей на всілякі поточні запити й оформлення їх у вигляді паперових документів або звітів.

Кравцова Майя Олегівна

Державний університет телекомунікацій

Факультет Інформаційних технологій

м. Київ

НОВІ СТАНДАРТИ WI-FI МЕРЕЖІ

Лише в кінці 2016 року на ринку почали з'являтися перші бездротові маршрутизатори з підтримкою стандарту 802.11ad (WiGig), а організація IEEE вже прийняла чорновий варіант специфікації 802.11ay. Вона не виступатиме окремим стандартом, а стане розширенням для 802.11ad.

Щоб повною мірою оцінити нововведення 802.11ay, давайте коротко згадаємо історію розвитку, починаючи з 802.11ac. У порівнянні зі своїм прашуром (802.11n), стандарт 802.11ac запропонував більшу ширину каналу на частоті 5 ГГц (80 / 160 МГц проти 40 МГц), більшу кількість просторових потоків (8 проти 4), модуляцію вищого порядку (256-QAM проти 64-QAM) і підтримку технології MU-MIMO. В результаті зараз можна знайти на ринку моделі класу AC5400 з пропускнуою спроможністю стандарту 802.11ac до 2167 Мбіт/с.

А ним послідував 802.11ad з підтримкою частотного каналу 60 ГГц, який не потребує ліцензування. Ширина цього каналу сягає 2,16 ГГц. Перші пристрої цієї категорії відносяться до класу AD7200 з пропускнуою спроможністю стандарту 802.11ad на рівні 4600 Мбіт/с. У свою чергу 802.11ay пропонує використовувати чотири таких канали на частоті 60 ГГц, тобто сумарна їх ширина сягне 8,64 ГГц (4 x 2,16 ГГц). Також реалізується підтримка 4 просторових потоків завдяки технології MU-MIMO, кожен з яких має пропускну спроможність 44 Гбіт/с. Тобто загальна пропускна спроможність сягає 176 Гбіт/с. Додайте до цього й розширену відстань передачі даних 300 – 500 метрів.

Очікується, що фінальна версія специфікації 802.11ay буде прийнята до кінця поточного року. В майбутньому вона може використовуватися, наприклад, для бездротового підключення моніторів і телевізорів з високою роздільною здатністю.

Список використаних джерел:

1. Електронний журнал «ІТ для бізнесу»: <http://ko.com.ua/>
2. Вільна енциклопедія «Wikipedia»: <https://uk.wikipedia.org/>
3. Електронний журнал «ІТ-новини» <http://gecid.com/>

МУЛЬТИМЕДІЙНІ ТЕХНОЛОГІЇ

Средства мультимедиа позволяют создавать базы, банки данных и знаний в сфере культуры, науки и производства. Такие продукты всё более завоёвывают рынок пользователей. Мультимедиа технологии широко используются в рекламной деятельности, при организации управления маркетингом средств и методов продвижения товаров и услуг, в обучении и досуговой деятельности.

К компьютерным средствам мультимедиа относят: специальное ПО, а также: CD и DVD драйверы и компакт-диски к ним; аудиокарты, аудио колонки, наушники и микрофоны; видеокарты; аудио- и видео периферийные устройства (цифровые кинокамеры и фотоаппараты и др.).

Технология мультимедиа позволяет вводить, сохранять, перерабатывать и воспроизводить текстовую, аудиовизуальную, графическую, трёхмерную и иную информацию. Свойство интегрировать эти виды данных, компактно и длительно хранить их на электронных носителях, не разрушающихся со временем и не ухудшающих свои характеристики при копировании, позволяет утверждать, что они могут отражать богатейшие национальные богатства России в мультимедийных БД, которые вместе с системами гипертекста, гипермедиа и WWW обеспечат пользователям почти моментальный доступ к любому их фрагменту.

Организации и подразделения, обладающие информационными ресурсами и средствами мультимедиа, использующими мультимедийные технологии порой называют медиатеками. В России медиатеки находят широкое распространение в библиотеках и учебных заведениях. В этом случае считается, что медиатека – хранилище информационных медиаресурсов.

Технические средства мультимедиа, как и любые компьютерные информационные системы, позволяют выполнять все виды информационных процессов.

1 Аудиовизуальные технические средства представляют устройства записи, воспроизведения, проецирования, отображения и полноценного использования зрительных, звуковых и зрительно-звуковых материалов. Современные аудиовизуальные средства ориентируются на использование компьютерных технологий.

Аудиовидеотехнические материалы – это документы, содержащие текстовую, звуковую, изобразительную или изобразительно-звуковую информацию, хранящуюся на видео- и магнитных лентах и дисках, оптических и магнитооптических дисках, плёнках, кинопленках и других носителях, воспроизводимую с помощью технических средств.

К техническим средствам аудиовизуальной информации могут быть отнесены: магнитофоны, диктофоны, проигрыватели, плееры, мультимедийные компьютеры, видеоманитоны, видеокамеры, телевизоры, проекционное и др. вспомогательное оборудование, информационные табло и т.д.

Попытки систематизировать аудиовидеотехнические средства предпринимались и ранее, однако, предложить единую классификацию затруднительно из-за значительного отличия этих средств друг от друга по параметрам, областям применения, разнообразию фирм изготовителей, появлению всё более новых технических средств, включающих в себя несколько видов, отличающихся по принципу действия и т.п. Поэтому для изучения данной проблемы предлагается некоторое условное их деление.

По видовому признаку рассматривают аудиовизуальные технические средства, как: визуальные (показывающие изображения); аудио (звуковые); аудиовизуальные(зрительно-слуховые).

При этом под визуальной информацией понимаются данные, отображаемые на информационных досках и табло, экранах дисплеев, телевизионных приёмников и т.п.

По функциональному использованию мультимедийные программно-технические средства можно разделить на:

1. Устройства оперативной внутренней связи – местная телефонная или иная, например, диспетчерская связь и радиотрансляция, системы оповещения. Они используются для эффективного управления, выполнения работниками различных заданий руководства, а также запросов пользователей. В организациях всё чаще используют такие виды связи, как электронная почта, видеоконференции, интернет-телефония, мобильная связь и др.

2. Оборудование для индивидуального использования и проведения культурно-массовых мероприятий – аудио, CD и DVD плееры, электрофоны (проигрыватели), магнитофоны, диктофоны, музыкальные центры и т.п., видеоманитоны и видеоплееры, телевизоры, видео и кинокамеры, фотоаппараты, специально оборудованные компьютеры, проекторы, устройства для работы с микроформами;

3. Средства информирования (различные информационные доски и табло, сенсорные экраны, видео и звуковые автоответчики, видеокубы, видеостены и т.п.);

4. Системы охранной и пожарной сигнализации (видеокамеры и телевизоры слежения, звуковая сигнализация и др. датчики).

По используемому оборудованию аудиовидеотехнические средства можно классифицировать как устройства:

1) радиотелефонии и связи, звукоусиления, звукозаписи и звуковоспроизведения;

2) видеовоспроизведения и записи;

3) информирования.

Данные деления достаточно условны, однако, они дают представление о многообразии и сложности существующих аудиовидеотехнических средств.

Оборудование радиофикации и связи, звукоусиления, звукозаписи и воспроизведения необходимо для оперативного оповещения работников организации и её посетителей о различных (штатных и нештатных) событиях, например, о проводимых выставках или культурно-массовых мероприятиях, чрезвычайных ситуациях и др. Устройства радиофикации представляют региональную радиотрансляционную сеть и местное оборудование усиления звука, используемые для оповещения о различных мероприятиях, а также нештатных ситуациях (оповещение в чрезвычайных ситуациях).

Средства местной телефонной и диспетчерской связи образуются на основе применения учрежденческих (офисных) АТС и коммутаторов оперативной (диспетчерской) связи, громкоговорящих переговорных устройств производственной связи. Громкоговорящая связь на предприятии оказывается порой единственным и незаменимым средством взаимодействия его работников и относится к поисково-вызывным системам (ПВС). Другими устройствами ПВС являются средства персонального телефонного, радиотелефонного и радиовызова, а также световой, зрительной и зрительно-световой сигнализации.

Аудиовизуальное оборудование записи и воспроизведения данных делится на устройства аудио, видео или комбинированно (аудиовидео) воспроизводящие и (или) записывающие машиночитаемую информацию.

К устройствам воспроизведения относятся громкоговорители, усилители звука, электрофоны, аудио, CD и DVD-плееры, телевизоры, видеоплееры, проекторы, голограммы, читальные аппараты для микроформ.

В качестве устройств записи используются фотоаппараты, видео и кинокамеры, аудио и видеоманитофоны, аппараты изготовления микроформ, устройства записи на CD-ROM и DVD.

К устройствам воспроизведения и записи принадлежат магнитофоны, диктофоны, музыкальные центры, видеоманитофоны, цифровые фотоаппараты и видеокамеры, специально оборудованные компьютеры и драйверы компакт-дисков.

К аппаратуре звукоусиления относят усилительные устройства, громкоговорители, звуковые колонки и микрофоны для передачи речи и музыки.

Оборудование видеовоспроизведения и записи – телевизоры, видеоманитофоны и видеоплееры, фотоаппараты и видеокамеры, проекторы, голограммы, системы охранной и пожарной сигнализации, различные визуальные и аудиовизуальные информационные системы, читальные аппараты для микроформ, устройства записи и воспроизведения машиночитаемых данных.

Для общения в Интернете (в том числе проведения видеоконференций) используют упрощённые, подключаемые к ПК, видеокамеры, называемые Web-камеры.

В крупных городах последнее время наметилась тенденция организации кабельного телевидения. Скорость передачи данных в них составляет 2–30 Мбит/с. К системам кабельного телевидения (СКТВ) относятся устройства, обеспечивающие приём и одностороннюю передачу сигналов

телевидения и радиовещания по радиочастотному кабелю с использованием прямого и обратного каналов для внутрисистемных сигналов.

Системы охранной и пожарной сигнализации представляют звуковые и (или) световые устройства, извещающие о различных нарушениях охранной или пожарной безопасности в организации.

Література:

1. <http://www.frontmanagement.org/fomants-880-1.html>
2. <http://ua.textreferat.com/referat-8195-1.html>
3. <http://posibnyky.vntu.edu.ua/azarova/p4.html>

Михалюк В.В.

Державний університет телекомунікацій

Факультет Інформаційних технологій

Студентка групи ІМД-61

м.Київ

ОЦІНКА ЯКОСТІ НАДАННЯ ПОСЛУГИ ФІЗІОЛОГІЧНОГО МОНІТОРИНГУ

Одним з найважливіших мереж концепції Інтернету Речей є медичні мережі [1]. У роботах МСЕ по стандартизації мереж зв'язку для надання послуг системи електронного здоров'я передбачається широко використовувати нові технологічних досягнення в області побудови мереж M2M. Традиційно проблеми якості обслуговування знаходяться в центрі уваги сектора стандартизації телекомунікацій МСЕ. У рекомендаціях МСЕ-Т за визначенням і розробці класів і параметрів якості обслуговування для мереж M2M, які використовуються для надання послуг в системі e-health [2] визначені нові класи обслуговування і параметри для мереж зв'язку (табл.1).

Таблица 1-Вимоги МСЕ-Т по класах і параметрам якості обслуговування для послуг системи електронного здоров'я (e-health)

Послуги системи електронного здоров'я (e-health)	Швидкість передачі	Затримка	Втрати пакетів
Фізіологічний моніторинг в реальному часі	10-100 кбіт/с	< 300 мс	10^{-6}
Аудіо і відео системи, в тому числі для оперативного втручання	10 кбіт/с - 1 Мб/с	10-250 мс	10^{-4}
Доступ до бази даних пацієнта (наприклад, з мобільного пристрою)	1-10 Мб/с	< 1 с	Послуга толерантна до втрат

Мережі зв'язку загального користування створюються на основі вимог до класів і параметрам якості обслуговування, запропонованим в рекомендації Y.1541.

Однак стрімкий розвиток нових технологій в ряді випадків призводить до відставання процесу стандартизації від процесу розвитку і впровадження нових послуг. Так, наприклад, в рекомендації Y.1541 відсутні вимоги до параметрів затримки для таких додатків як гри в реальному часі. Ця величина визначена тільки в документах 3GPP і становить 50 мс, що в два рази менше, ніж вимоги до мінімальних затримок в рекомендації Y.1541. З метою недопущення двоякого тлумачення вимог для системи e-health в МСЕ-Т була створена спеціальна група з розробки рекомендацій для міжмашинної взаємодії (M2M), в тому числі і для системи e-health. До теперішнього часу цією групою були розроблені тимчасові рекомендації по класах і параметрам якості обслуговування для підсистеми мобільного здоров'я [2].

У деяких публікаціях [3,4] в дослідженнях розглядаються параметри затримки, пікової та середньої швидкості передачі даних, що на наш погляд недостатньо через відсутність вимог до коефіцієнта втрат пакетів. У ререкомендаціях МСЕ-Т розглядаються наступні послуги підсистеми мобільного здоров'я: фізіологічний моніторинг в реальному часі, медичні системи аудіо і відеоконференц-зв'язку, доступ до баз даних про здоров'я пацієнта і медичних даних і файлів, віддалене управління медичними роботами.

Як параметри для надання послуги фізіологічного моніторингу в [2] запропоновано швидкість передачі інформації 10-100 кбіт/с, затримки не більше 300 мс і частка втрачених пакетів - не більше 10^{-6} , за допомогою яких контролюються об'єктивні показники якості надання послуг зв'язку.

Надання послуги фізіологічного моніторингу безпосередньо пов'язано з ризиками для правильної оцінки здоров'я пацієнта. Тому, необхідна об'єктивна комплексна оцінка якості надання послуги мережею, для чого в дипломній роботі пропонується використовувати можливості нечіткої логіки.

Література:

1. Кучерявый, А. Е. Самоорганизующиеся сети/ А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. – СПб.: Любавич, 2011. – 312 с.
2. Carugi, M. M2M enabled ecosystems: e-health. Chapter 9.2 / M. Carugi, C. Li, J.-Y. Ahn, H. Chen // ITU-T, FG M2M, San Jose. – 13-15 November, 2012. – 2 p.
3. Lee, H. Wireless LAN with Medical-Grade QoS for E-Healthcare / H. Lee, K.-J. Park, Y.-B. Ko, C.-H. Choi // Journal of Communications and Networks. – April 2011. – Vol.13, n.2. – PP. 149-159.
4. Park, K.J. IEEE 802.11 WLAN for Medical-grade QoS / K.J.Park, D.M.Shrestha, Y.-B.Ko, N.H.Vaidya, L.Sha // WiMD'09, New Orleans, Louisiana, USA. – May 18, 2009. – PP. 3-8.

ТЕХНОЛОГІЇ РІВНЯ ДОСТУПУ МЕРЕЖІ NGN

В даному докладі мова йде про мережі NGN, а конкретно про нові технології рівня доступу цієї мережі.

Загальні відомості про мережі наступного покоління NGN

Термін «мережі наступного покоління» NGN (Next Generation Networks) з'явився в телекомунікаційній літературі на початку нового тисячоліття. Ідею розробки NGN, запропоновану в 2001 р Європейським інститутом стандартів електрозв'язку ETSI (European Telecommunications Standards Institute), підтримав Сектор стандартизації телекомунікацій Міжнародного союзу електрозв'язку (МСЕ-Т). У липні 2003 р на спеціальному семінарі з NGN в рамках дослідницької комісії ІК 13 МСЕ-Т була утворена Змішана група доповідачів (Joint Rapporteur Group, JRG) по NGN, яка підготувала проекти перших рекомендацій по NGN. Перші дві рекомендації МСЕ-Т - Y.2001 і Y.2011 - були затверджені в кінці 2004 р в новій серії Y. 2000, спеціально виділеної для рекомендацій про NGN. На початок 2011 року в цій серії вже було 70 рекомендацій, які відносяться до так званої першої версії NGN (NGN release 1). Останнім часом в МСЕ-Т розпочаті роботи по другій версії (NGN release 2).

Основними об'єктивними передумовами виникнення ідеї мереж наступного покоління NGN є:

- успіхи пакетних технологій передачі інформації, що зумовили бурхливе зростання цифрового трафіку, перш за все за рахунок розширення використання Інтернет;
- збільшення попиту на рухомий зв'язок і на нові мультимедійні служби Triple Play (спільної передачі голосу, відео, даних);
- конвергенція (взаємопроникнення) мереж електрозв'язку та інформаційно-обчислювальних мереж, розвиток інформаційно-комунікаційних мереж.

Слід особливо відзначити одну з основних причин появи ідеї NGN - завершення життєвого циклу експлуатованих цифрових комутаційних станцій телефонної мережі і бажання не замінювати їх такими самими станціями, а радикально модернізувати мережу з метою надання всього комплексу послуг Triple Play. Таким чином, технологія NGN є новим способом розвитку і модернізації існуючих мереж зв'язку і, в першу чергу, телефонних мереж зв'язку загального користування.

Згідно з визначенням, наведеним в Рекомендації MCE-T Y.2001, мережа наступного покоління (NGN) - це мережа з пакетною комутацією, здатна забезпечити користувачів різноманітними вузькосмуговими і широкосмуговими послугами, включаючи послуги телефонного зв'язку, заснована на широкосмуговій мережі з пакетною технологією транспортування, що забезпечує необхідну якість послуг QoS (Quality of Service), в якій функції, пов'язані з наданням послуг, не залежать від технологій транспортування інформації. Мережа NGN дає користувачам необмежений доступ до різноманітних послуг провайдерів і підтримує узагальнену мобільність, яка дозволяє користувачам отримати доступ до послуг у будь-якому місці і в будь-який час.

Рівень доступу

Мабуть, з рівнем доступу найчастіше стикаються клієнти мережі. Під терміном "доступ" тут мається на увазі дуже широке поняття від цифрових абонентських ліній до прикордонних шлюзів і конвертерів сигналізації. Доступ в загальному випадку - це все те обладнання, яке пов'язує мережу NGN з традиційними TDM-мережами і навіть невеликими локальними мережами передачі даних. Природно, тут не можна забувати і абонентів мережі. Можна виділити кілька способів включення їх в мережу наступного покоління. Найцікавіший - це безпосереднє підключення користувачів до пакетної мережі через IP-термінали або IP-телефони. Таке підключення найбільш "зручно" з точки зору побудови NGN, надання мультимедійного трафіку, управління ресурсами мережі. Однак в силу багатьох технологічних труднощів, пов'язаних з неможливістю доставити до абонента мережу Ethernet або MPLS в чистому вигляді, оператори не можуть надати такої послуги. IP-телефонами найчастіше користуються корпоративні абоненти, які постійно працюють в інтегрованій локальній NGN-мережі, інші включаються через широкосмугову мережу доступу. Природа такого підключення може бути різною: DSL-системи, що використовують мідні кабельні пари (найбільш часто зустрічається тип), системи цифрового кабельного телебачення, активно розвиваються зараз бездротові системи (Wi-Fi і WiMAX), оптичні технології доступу, наприклад PON. Об'єднує їх усіх одне - в якості кінцевого інтерфейсу абоненту вони надають IP-підключення, ті дають можливість використовувати інтелектуальний термінал з доступом до великої кількості додаткових сервісів. Набагато складніша ситуація з підключенням абонентів TDM-мереж. Єдиний можливий варіант для них - це опосередковане включення в NGN через шлюзи стандартної телефонії. Природно абоненти "старої" мережі не можуть отримати всього переліку послуг, доступного IP-абонентам, але навіть тут NGN привносить свої позитивні моменти, так як деякі послуги цифрової мережі нового покоління доступні всім абонентам.

Література:

1. http://www.tssonline.ru/articles2/support/testir_setey_ngn_kommutat_shlyuzy_trafiki
2. http://ngn.psuti.ru/?page=information_01_user

Овчаренко М. С.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
Київ, Україна*

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ, ЩО НАДАЮТЬ ІНФОРМАЦІЙНІ ПОСЛУГИ

Пов'язаний з безперервним збільшенням обсягів зберігаємої та оброблюваної інформації, потребою в наданні безперебійного доступу до документів і файлів, та безперестанною роботою бізнес процесів – створення та розвиток ЦОД набули найвищого значення в світі за останні роки. Головною метою створення нових дата-центрів є безвідмовна робота інформаційної структури підприємства з заданими рівнями доступності, надійності, безпеки та керованості.

У широкому сенсі ефективність - це комплексна характеристика ЦОД, що відображає ступінь його відповідності потребам та інтересам її замовників, користувачів, інших зацікавлених осіб. Основні потреби і інтереси зацікавлених осіб в формалізованому та агрегованому вигляді можуть бути представлені у вигляді цілей створення ЦОД. Тому з певним ступенем точності ефективність можна представляти як ступінь відповідності ЦОД цілям його створення, тобто ефективність в широкому сенсі враховує аспект результативності.

Існують різні підходи до визначення ефективності ЦОД. Загалом, їх можна розділити на дві групи. До першої групи входять показники ефективності, що залежать від інженерної системи ЦОД і методи, що дозволяють ці показники поліпшити. Методи, що дозволяють поліпшити цю групу показників, пов'язані з дослідженнями в області вдосконалення інженерної інфраструктури ЦОД: енергоспоживання, систем охолодження, розподілу електроживлення і т. д. Другу групу складають показники якості ЦОД і відповідно методи, які сприяють поліпшенню показників якості ЦОД при тих же умовах його функціонування. До другої групи визначення ефективності ЦОД віднесені показники якості ЦОД.

Найбільш важливими та значимими об'єктами для підвищення інженерної ефективності ЦОД являються енергоефективність, використання електроживлення та охолодження дата-центру. Що до показників якості, то слід звернути велику увагу до таких показників як управління навантаженням, що надходить на ЦОД та розподіл пам'яті у кластері ЦОД.

КОНЦЕПЦІЯ «ПРИНЕСИ СВІЙ ВЛАСНИЙ ПРИСТРІЙ»

BYOD є повноцінним рішенням проблем, пов'язаних з управлінням підключення мобільних пристроїв співробітників до корпоративної мережі при використанні набору політик, що забезпечують безпеку компанії.

BYOD

(Bring Your Own Device) - концепція, як одна із напрямків розвитку сучасних ІТ.

Термін BYOD з'явився досить давно (як мінімум з 2004 року). Проте, вибухова популярність в цілому за рахунок впливають ІТ-послуг і стрімкого розвитку функціоналу і різноманітності хмарних сервісів.

Прикладом використання BYOD є робота співробітника на власному портативному пристрої з різними програмами компанії.

Переваги

Одна з очевидних переваг те що співробітники можуть працювати зі своїми девайсами, ця умова дозволяє оголосити такі переваги як економія бюджету, ефективність роботи та лояльність на робочому місці яка підвищує відносини між компанією та співробітником.

За даними дослідження, проведеного IDC, близько 95% співробітників компаній вже використовують принаймні одне індивідуальне обладнання для робочих цілей. За оцінками Gartner, близько 90% компаній планують підтримувати бізнес-додатки на пристроях, що належать кінцевим користувачам, оскільки це дозволить скоротити витрати на обладнання на 40%. Крім того, широке розповсюдження мобільних пристроїв допоможе "вийти на зв'язок" з співробітником навіть після закінчення робочого дня.

Які можуть виникати ризики при використанні цієї концепції в ІТ сфері?

Щоб на Ваш пристрій та пристрій співробітників не піддався фішинговим атакам та шкідливим програмам треба обов'язково використовувати антивірусний захист.

Також пристрій може бути викрадений або втрачений щоб запобігти значних втрат, заздалегідь треба знайти рішення як відстежити Ваш пристрій та забезпечити всі можливості блокування або знищення інформації в разі втрати пристрою.

Обов'язково треба провести інструктаж по підвищенню рівня захищеності корпоративних даних.

Це повинен знати кожен співробітник для значного покращення політики безпеки.

До них входять:

Використовуйте складні паролі і регулярно їх міняйте

Не переходити за підозрілими, на Вашу думку, посиланням які можуть приходити Вам на пошту або мобільний телефон, також варто прийняти до уваги заходи щодо безпеки зберігання даних на хмарі.

Висновок

Проаналізувавши переваги та ризики використання концепції BYOD, новий підхід до більш комфортної, злагодженої роботи з якою кожна компанія може спроектувати в закінчене рішення, відповідне своїм побажанням та поставленій задачі з метою покращення продуктивності співробітника, який отримає свободу вибору пристрою, тим самим Ви виконаєте свої зобов'язання перед ними, акціонерам і вашими клієнтами в забезпеченні середовища, безпечної для роботи і ведення бізнесу.

Ефективність політики BYOD дозволяє Вам мати впевненість в тому, що Ваші співробітники працюють в рамках розроблених правил, встановлених для них.

Література:

1. <http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf>
2. . <http://www.smarttech.com>.
3. <http://www.mimio.com>.

Пархоменко Єгор Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут заочного та дистанційного навчання

м.Київ

ГЛОБАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ

Глобальні мережі (WideArea Network, WAN) – це телекомунікаційні структури, що об'єднують локальні комп'ютерні мережі, які мають загальний протокол зв'язку, методи підключення і протоколи обміну даними. Кожна з глобальних мереж (INTERNET, BITNET, DECNET і ін.) організовувалася для певних цілей, а надалі розширювалася завдяки підключенню локальних мереж, що використовують її послуги і ресурси.

Найбільшою глобальною інформаційною мережею є Internet. Internet-глобальна всесвітня мережа інформаційного обміну, яка об'єднує кілька мільйонів людей із більш ніж 100 країн світу за допомогою сучасних і зручних засобів зв'язку. Своє існування Internet розпочала з 1969 року.

Архітектура мережі Internet розроблена на основі концепції взаємопоєднуваності або міжмережевого поєднання різнорідних мереж, побудованих на базі різних фізичних систем зв'язку і комунікаційних технологій.

Таким чином, Internet- це сукупність технічних засобів, стандартів і домовленостей, яка дає змогу підтримувати зв'язок між різними комп'ютерними мережами у світі.

Основою функціонування Internet є базовий протокол TCP/IP (TransmissionControlProtocol/InternetProtocol). Він становить сукупність протоколів – систем стандартів і правил зв'язку та передавання інформації у глобальній мережі. Протокол- це домовленості про сигнали, якими обмінюються комп'ютери під час встановлення зв'язку між собою і приймання чи передавання інформації.

снує декілька видів підключення абонентів до Internet:

1. On-line ("живе") – сполучення комп'ютера користувача з віддаленим комп'ютером в режимі реального часу. On-line – режими:

- а) тимчасове IP-підключення;
- б) постійне IP-підключення;
- в) тимчасовий (сеансовий) термінальний доступ в режимі on-line;

2. Off-line (поза лінією або в автономному режимі) – робота користувача ПК до початку сеансу зв'язку з іншим комп'ютером у мережі Internet. Off-line режим – це сеанси зв'язку з передачею електронної пошти за протоколом UUCP.

Служби Інтернету – це системи, що надають послуги користувачам Інтернету. До них відносяться: електронна пошта, WWW, телеконференції, списки розсипки, FTP, IRC, а також інші продукти, що використовують Інтернет як середу передачі інформації.

Послуги, що надаються Інтернетом, можна розділити на дві основні категорії:

1. Відкладені (off – line) – основною ознакою цієї групи є наявність тимчасової перерви між запитом та отриманням інформації.

2. Прямі (on – line) – відрізняються тим, що інформація за запитом повертається негайно. Якщо від одержувача інформації потрібна негайна реакція на неї, то така послуга носить інтерактивний характер.

Засоби і служби Internet (логічна схема глобальної мережі internet) представлена на рис. 5.1:

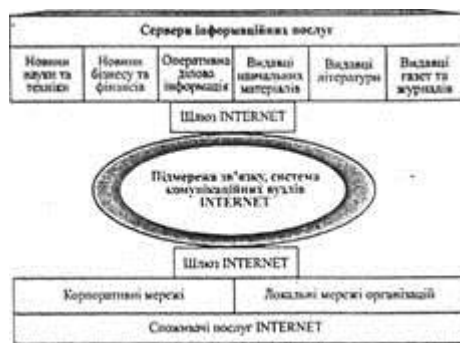


Рис. 5.1. Логічна схема глобальної мережі Internet

Глобальна обчислювальна мережа Internet надає такі послуги:

1. Електронна пошта (E-mail) – це просте й дешеве вирішення проблем підтримки постійних контактів між людьми. E-mail дає змогу скласти текстове повідомлення на комп'ютері й відправити його з допомогою мережі іншому користувачеві. Електронною поштою можна також пересилати будь-яку інформацію: відео- та аудіо-файли, фотографії, електронні таблиці в певному форматі, графічні файли, програми тощо. Недолік як традиційної (паперової) пошти, так і E-mail полягає в тому, що відправник ніколи не знає, коли його респондент прочитає повідомлення.

Електронний лист можна постачити цифровим підписом і зашифрувати. Швидкість пересилання складає в середньому кілька хвилин. При цьому вартість електронної пошти мінімальна і не залежить від відстані. Основними достоїнствами електронної пошти є простота, дешевизна і універсальність.

2. Телеконференції – друга за поширеністю служба Інтернету, що надає відкладені послуги.

Телеконференції – це послуга Internet, за допомогою якої абонент може залишити своє відкрите повідомлення у мережі. Його переглянуть зацікавлені в даній темі користувачі й зможуть так само відкрито на нього відповісти. Телеконференції – це колективна електронна пошта, тематичні електронні дискусії, призначені для обміну інформацією через електронні повідомлення. Телеконференції є найбільш економічним і поширеним засобом Internet для спілкування фахівців у конкретній галузі й просто зацікавлених людей.

Служба телеконференцій складається з безлічі тематичних телеконференцій – груп новин (newsgroup), підтримуваних серверами новин. Сервер новин – це комп'ютер, який може містити тисячі груп новин найрізноманітніших тематик. Кожен сервер новин, отримав нове повідомлення, передає його всім вузлам, з якими він обмінюється новинами. Група новин – це набір повідомлень з певної теми. Новини розподілені за ієрархічно організованими тематичними групами, й ім'я кожної групи складається з імен підрівнів. Існують як глобальні ієрархії, так і ієрархії, локальні для якої організації, країни або мережі. Набір груп, одержуваних сервером телеконференцій, визначається його адміністратором і їх наявністю на інших серверах, з якими даний сервер обмінюється новинами. Доступ до груп новин здійснюється через процедуру підписки, яка полягає у вказівці координат сервера новин і вибору цікавлять користувача груп новин. Слід зауважити, що кожен сервер новин має певний набір конференцій, і, якщо цікавить тематика на ньому не знайдена, можна спробувати використовувати інший сервер. Дана процедура, а також робота з групами новин здійснюється за допомогою програмного забезпечення, що підтримує ці функції, наприклад широко поширеним додатком компанії Microsoft – Outlook Express.

В обговоренні теми телеконференції може брати участь безліч людей, незалежно від того, де вони знаходяться фізично. Звичайно, хоча це і не є правилом, за порядком у конференціях стежать спеціальні люди, так звані

модератори. У їх обов'язки входить підтримка порядку в конференції відповідно до встановлених в ній правилами поведінки і тематикою. Поряд з описаною формою служб телеконференції широкого поширення набули WWW-телеконференції, також звані форумами. Відмінність полягає в тому, що вони працюють через web – інтерфейс і розміщаються не централізовано на серверах новин, а на web-сайтах.

3. Списки розсіпки (mail lists) – служба, яка не має власного протоколу і програми- клієнта і працююча виключно через електронну пошту.

Ідея роботи списку розсіпки полягає в об'єднанні під однією адресою електронної пошти адрес багатьох людей – передплатників списку розсіпки. Коли лист посилається на цю адресу, повідомлення отримують всі передплатники даного списку розсіпки. Ведучими списку розсіпки, як правило, є люди, що добре володіють його тематикою. Вони відповідають за підготовку та розсіпку чергових випусків. Одержувачами листів є люди, власноруч підписалися на список. Крім того, у них є право і можливість у будь-який момент скасувати свою підписку.

Існують відкриті розсіпки (для всіх бажаючих), закриті (для людей певного кола), безкоштовні (існуючі за рахунок ентузіазму творців, спонсорської підтримки, платних рекламодавців) і платні. Залежно від числа передплатників список розсіпки обслуговується на сервері програмами різної складності. Ці програми можуть забезпечувати або не гарантувати повну функціональність, яка полягає в автоматичній підписці клієнтів і прийомі їх відмови від підписки, перевірці коректності електронних адрес, веденні архіву повідомлень, обробці поштових помилок, підтримки роботи в режимі дайджесту (коли передплатник отримує не кожне повідомлення окремим листом, а всі повідомлення за якийсь термін в одному листі), перевірці повідомлень адміністратором списку перед розсіпкою і т.д.

4. Чати. Під словом чат (від англійського chat) маються на увазі служби Інтернету, що дозволяють проводити текстові дискусії в режимі реального часу. Від традиційної форми розмови їх відрізняє те, що вони ведуться в текстовому вигляді – шляхом набору тексту на клавіатурі. Найпопулярнішим відкритим стандартом, що лежить в основі чатів, є IRC (Internet Relay Chat).

IRC – це багатоканальна мережа, що розрахована на багато абонентів, за допомогою якої користувачі можуть розмовляти в режимі реального часу незалежно від свого місця розташування.

Свого часу чати, в основі яких лежав стандарт IRC, отримали досить широке поширення. Однак сьогодні все більш популярними стають чати, що проводяться на окремих web – сайтах та ґрунтуються або на мові HTML, або на мові Java. Це дозволяє користувачам Інтернету брати участь у них без установки додаткового програмного забезпечення, використовуючи тільки стандартний браузер, тим самим число потенційних учасників стає максимальним. З іншого боку, можливість установки на корпоративному сайті компанії системи, що забезпечує роботу чату, дозволяє широко використовувати цю службу в комерційних цілях, наприклад для обговорення з споживачами тих чи інших

питань діяльності підприємства, обговорення продукції, системи обслуговування і т.д.

5. Internet-пейджери. Проміжне становище між електронною поштою і чатами по динамічності та інтерактивності спілкування займають Інтернет-пейджери або служби миттєвих повідомлень. Служби миттєвих повідомлень дозволяють спілкуватися в режимі реального часу, поєднуючи в собі переваги електронної пошти та телефону. Представляє собою безкоштовні програми для безпосереднього спілкування у мережі. Зробив перелік контактів (усіх своїх ділових партнерів, друзів і знайомих) при натискуванні піктограми On-line у відповідній програмі можна дізнатися, хто з них у цей час перебуває на зв'язку з вами (тобто в Internet). Сучасні Internet- пейджери виконують функції: передавання файлів, електронної пошти, повідомлень голосом, новин тощо. Прикладом подібних програм служать ICQ, MSN, AOL Instant Messenger і інш. Однак ці програми мають суттєвий недолік: користувач Internet- пейджера компаній, наприклад YAHOO або MICROSOFT, може спілкуватися тільки з користувачем такої ж самої служби. В теперішній час, ведуться розробки єдиних стандартів для Internet-пейджерів. На нинішньому етапі найкращий Internet-пейджер це програма ICQ.

6. Skype – безкоштовне програмне забезпечення, що забезпечує текстовий, голосовий зв'язок і відео зв'язок через Інтернет між комп'ютерами (IP-телефонія), використовує технології пірінгових мереж, а також платні послуги для дзвінків на мобільні і стаціонарні телефони. Програма також дозволяє здійснювати конференц-дзвінки (до 25 голосових абонентів, включаю чи ініціатора), відео дзвінки (у тому числі відео конференції до 10 абонентів), а також забезпечує передачу текстових повідомлень (чат) і передачу файлів. Є можливість замість зображення з веб-камери передавати зображення з екрану монітора, а також створювати і відправляти відео повідомлення користувачам настільних версій програми.

7. FTP. FTP (file transfer protocol) – протокол передачі файлів, але, якщо FTP розглядається як служба Інтернету, мається на увазі не просто протокол, а саме служба доступу до файлів у файлових архівах. Одна з причин досить високою її популярності пояснюється величезною кількістю інформації, накопиченої в FTP- архівах за десятиліття експлуатації комп'ютерних систем. Інша причина криється в простоті доступу, навігації і передачі файлів по FTP.

FTP – служба прямого доступу, що вимагає повноцінного підключення до Інтернету.

WWW (World Wide Web) – служба прямого доступу, що вимагає повноцінного підключення до Інтернету і дозволяє інтерактивно взаємодіяти з представленою на web – сайтах інформацією. Це найсучасніша і зручна служба Інтернету. Вона ґрунтується на принципі гіпертексту і здатна представляти інформацію, використовуючи всі можливі мультимедійні ресурси: відео, аудіо, графіку, текст і т.д. Взаємодія здійснюється за принципом клієнт – сервер з використанням протоколу передачі гіпертексту (Hyper Text Transfer Protocol, HTTP). За допомогою протоколу HTTP служба WWW дозволяє обмінюватися

документами у форматі мови розмітки гіпертексту – HTML (Hyper Text Markup Language), який забезпечує належне відображення вмісту документів в браузерх користувачів.

Принцип гіпертексту, що лежить в основі WWW, полягає в тому, що кожен елемент HTML – документа може бути посиланням на інший документ або його частина, при цьому документ може посилатися як на документи на цьому ж сервері, так і на інших серверах Інтернету. Посилання WWW можуть

вказувати не тільки на документи, властиві службі WWW, але й на інші служби та інформаційні ресурси Інтернету. Більше того, більшість програм – клієнтів WWW – браузерів (browsers) – не просто розуміють такі посилання, але і є програмами – клієнтами відповідних служб: FTP, мережних новин Usenet, електронної пошти і т.д. Таким чином, програмні засоби WWW є універсальними для різних служб Інтернету, а сама інформаційна система WWW виконує по відношенню до них інтегруючу функцію.

Протокол World Wide Web – гіпертекстовий сервіс доступу до віддаленої інформації. Таким чином, World Wide Web – це одна з служб Інтернету, яка пропонує простий у використанні інтерфейс і дає можливість користувачам, навіть не дуже добре знають комп'ютер, отримувати доступ до web – службам в будь-якій частині Інтернету.

До WWW – або FTP- серверу користувач звертається безпосередньо, вказавши його мережеву адресу (URL), наприклад igex.org.

URL (Universal Resource Locator) – уніфікований покажчик ресурсу- це адреса інформаційного ресурсу в Internet, де вказаний протокол, за правилами якого передаються дані, ім'я серверу, на якому зберігається файл, а також може бути вказаний шлях до каталогу файлу і безпосередньо ім'я.

Доступ до певних послуг Internet залежить від місцеперебування користувача, пропозицій місцевих постачальників мережевих послуг і можливості користувача оплатити ці послуги.

8. Служби пошуку інформації. Особливу групу складають служби Інтернету, підтримувані однією з груп його учасників і зараховувані до даної категорії завдяки глобальному характеру наданих ними послуг з пошуку інформації. Пошук інформації є сьогодні однією з ключових проблем Інтернету, так як кількість представлених у ньому web – сторінок сьогодні оцінюється більш ніж в кілька сотень мільйонів. Крім того, в основі проблем пошуку інформації лежать такі причини, як множинність і фрагментарність джерел, велика кількість різних способів зберігання даних, дефіцит часу на вибірку та обробку інформації, вартість отримання інформації, ненадійність даних, постійне оновлення і додавання інформації.

Нижче перераховані основні інструменти пошуку інформації в Інтернеті, яким вдається в значній мірі долати вищезазначені проблеми:

– Пошукові машини (spiders, crawlers). Основна функція пошукових машин полягає в дослідженні Інтернету з метою збору даних про існуючі в ньому web – сайтах та видачі за запитом користувача інформації про web – сторінках, найбільш повно задовольняють введеному запиту. Одну з кращих пошукових

машин пропонують пошукові системи Yandex та Google (vandex.com.ua, google.com.ua), що індексує ресурси в українській зоні Інтернет. Із зарубіжних пошукових серверів один з відомих – AltaVista (altavista.com).

– Каталоги. Представляють собою ієрархічно організовану тематичну структуру, в яку, на відміну від пошукових машин, інформація заноситься з ініціативи користувачів. Додається сторінка жорстко прив'язується до прийнятих в каталозі категоріям. Один з найбільш відомих російських каталогів list.mail.ru.

– Мета-засоби пошуку. Дозволяють удосконалити процес шляхом запуску одночасно декількох пошукових засобів. Цей спосіб значно підвищує швидкість, однак не дозволяє скористатися можливостями побудови складних запитів, пропонованими більшістю сучасних систем пошуку.

Інтернет надає нові можливості розвитку бізнесу компанії. Комерційні організації розглядають Інтернет як загальнодоступний інформаційний і комунікаційний ресурс. За допомогою Інтернету фірми можуть розробляти нову продукцію, приймати замовлення, отримувати необхідну кореспонденцію та офіційні документи, вести спеціалізований інформаційний пошук у відповідних установах. Інтернет реально може послужити в проведенні маркетингових досліджень, спілкуванні з постачальниками і клієнтами, обміні комерційною інформацією.

Використання Інтернету дає можливість підприємцям і маркетологам досліджувати нові можливості ринку для своїх товарів, виділяти і вивчати різні сегменти ринку, такі як демографічний, географічний, організаційний, соціографічний, професійний, поведінковий і т.п. Відстеження відповідної інформації, що публікується в Інтернеті, також може бути корисним для прогнозування подальшого розвитку купівельного попиту і виявлення нових тенденцій у поведінці існуючих і потенційних клієнтів.

Якщо компанія в достатній мірі диверсифікована, то за допомогою Інтернету вона зможе проникнути в нові сфери бізнесу раніше за інших, замість того щоб намагатися вести конкурентну боротьбу в рамках своєї поточної діяльності.

Електронна пошта, об'єднана зі швидкими інтерактивними протоколами типу TELNET і протоколу передачі файлів (FTP), є досить ефективним засобом для здійснення продуктивної взаємодії через середовище Інтернет. FTP і TELNET надають клієнтам можливість зі своїх машин здійснювати доступ до ресурсів віддаленої машини-сервера в інтерактивному режимі (on – line). За допомогою FTP користувачі можуть з'єднатися з іншими комп'ютерами і здійснити пошук в їх каталогах публічного доступу, копіювати на свої носії зацікавила їх інформацію і програми і розміщувати власну кореспонденцію. TELNET – протокол з'єднує користувачів з віддаленою машиною і надає їм доступ до її програмних ресурсів.

Маючи доступ по комутованій лінії з використанням протоколів SLIP або PPP, що знаходяться на значній відстані бізнесмени, вчені, державні та

корпоративні службовці можуть обмінюватися проектами документів і коментарями до них і тим самим швидко приймати остаточні рішення.

Інформаційна система організації тісно пов'язана з Internet- технологіями. Internet-технології та їх спроможність економити час і гроші, підвищувати ефективність функціонування організацій усе більше позначаються на розгортанні корпоративних Intranet-мереж.

Intranet – внутрішня локальна обчислювальна мережа організації, яка створена і функціонує на основі Internet-технологій. Це організація компанії, яка базується на єдиній внутрішній інформаційній локальній мережі (Intranet). Впровадження Intranet підвищує ефективність взаємодії співробітників і оптимізує процеси планування й управління. У внутрішніх локальних Intranet-мережах організацій використовується те ж саме апаратне і програмне забезпечення, ті ж самі протоколи і підходи, що і в Internet. За сутністю, Intranet – це Internet в мініатюрі.

Ефективність колективної роботи у внутрішній Intranet- мережі організації у підсумку позначається на ефективності й прибутковості корпоративної діяльності. Результатом застосування Intranet в організації є:

- 1) значне зменшення обсягу паперових архівів;
- 2) легкість і простота публікації інформації;
- 3) універсальний і природний доступ до інформації з допомогою програм-браузерів;
- 4) істотне скорочення витрат на адміністрування програмних застосувань на робочих місцях користувачів;
- 5) швидка актуалізація будь-яких змін в інформаційному сховищі установи;
- 6) зміщення акцентів зі створення інформації на її ефективне споживання.

Зовнішня взаємодія компанії з партнерами, постачальниками і клієнтами здійснюється на основі Extranet-мереж. Extranet- дві або більше Intranet-мережі, що об'єднані з метою спільного використання ресурсів організацій; це сукупність бізнес-партнерів, що існує на основі мережі, яка контролюється провайдерами Internet за допомогою протоколу TCP/IP та Web-технології.

Оскільки Internet пропонує розмаїття методів комунікації і способів доступу до інформації, для значної кількості організацій вона швидко стає невід'ємною частиною їхньої інформаційної системи.

Література

1. <http://www.frontmanagement.org/fomants-880-1.html>
2. <http://ua.textreferat.com/referat-8195-1.html>
3. <http://posibnyky.vntu.edu.ua/azarova/p4.html>

ДОБРО ПОЖАЛОВАТЬ В SWIFT

Разработка языка Swift началась в 2010 году Крисом Латтнером, руководителем отдела разработки программного обеспечения Apple. Swift заимствовал идеи из: “Objective-C, Java, Ruby, Python, C#, и еще из стольких многих языков, что сложно перечислить”. 2 июня 2014 года на конференции WWDC Swift был официально представлен общественности.

Swift – открытый компилируемый язык программирования общего назначения. Создан компанией Apple в первую очередь для разработчиков iOS и macOS. Swift работает с фреймворками Cocoa и Cocoa Touch и совместим с основной кодовой базой Apple, написанной на Objective-C. Swift задумывался как более легкий для чтения и устойчивый к ошибкам программирования язык, нежели Objective-C. Программы на Swift компилируются в среде разработки Xcode.

Swift может использовать рантайм Objective-C, что делает возможным использовать обоих языков, а так же языка C, в рамках одной программы.

Swift – это надёжный и интуитивно понятный язык программирования от Apple, при помощи которого можно создавать приложения для iOS, Mac, Apple TV и Apple Watch. Он представляет разработчикам небывалую свободу творчества.

Swift заимствовал довольно многое из Objective-C, однако он определяется не указателями, а типами переменных, которые обрабатывает компилятор. По аналогичному принципу работают многие скриптовые языки. В то же время, он предоставляет разработчикам многие функции, которые прежде были доступны в C++ и Java.

Язык Swift добавлен в учебную программу. Не только разработчики заметили огромный потенциал Swift. Несколько ведущих университетов уже преподают его на уроках компьютерного программирования. Это значит, что даже новички могут легко перейти к программированию на профессиональном уровне.

НЕЙРОННЫЕ СЕТИ

Что такое нейронная сеть?

Нейронная сеть — это последовательность нейронов, соединенных между собой синапсами. Структура нейронной сети пришла в мир программирования прямиком из биологии. Благодаря такой структуре, машина обретает способность анализировать и даже запоминать различную информацию. Нейронные сети также способны не только анализировать входящую информацию, но и воспроизводить ее из своей памяти. Другими словами, нейросеть это машинная интерпретация мозга человека, в котором находятся миллионы нейронов передающих информацию в виде электрических импульсов.

Какие бывают нейронные сети?

Пока что мы будем рассматривать примеры на самом базовом типе нейронных сетей — это сеть прямого распространения (далее СПР). Также существуют рекуррентные нейронные сети. СПР как вытекает из названия это сеть с последовательным соединением нейронных слоев, в ней информация всегда идет только в одном направлении.

Для чего нужны нейронные сети?

Нейронные сети используются для решения сложных задач, которые требуют аналитических вычислений подобных тем, что делает человеческий мозг. Самыми распространенными применениями нейронных сетей является:

Классификация — распределение данных по параметрам. Например, на вход дается набор людей и нужно решить, кому из них давать кредит, а кому нет. Эту работу может сделать нейронная сеть, анализируя такую информацию как: возраст, платежеспособность, кредитная история и тд.

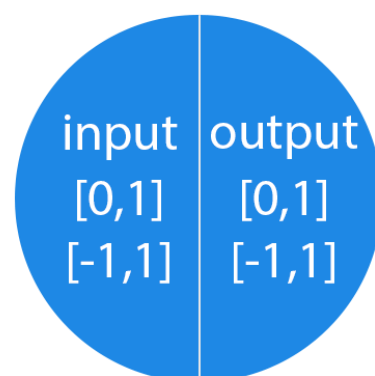
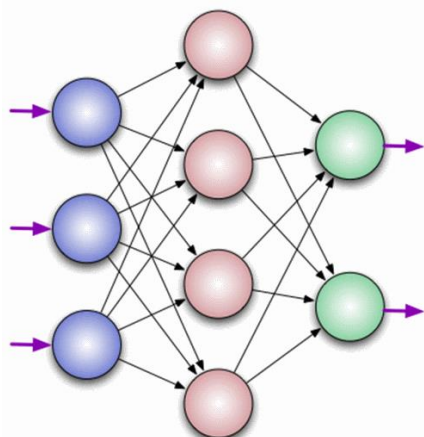
Предсказание — возможность предсказывать следующий шаг. Например, рост или падение акций, основываясь на ситуации на фондовом рынке.

Распознавание — в настоящее время, самое широкое применение нейронных сетей. Используется в Google, когда вы ищете фото или в камерах телефонов, когда оно определяет положение вашего лица и выделяет его и многое другое.

Что такое нейрон?

Нейрон — это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше. Они делятся на

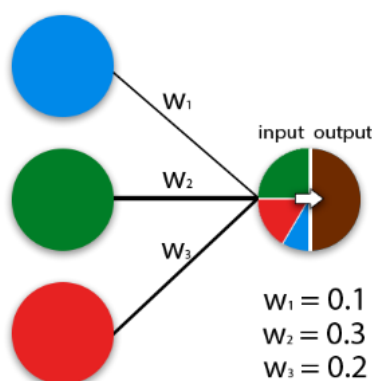
три основных типа: входной (синий), скрытый (красный) и выходной (зеленый). Также есть нейрон смещения и контекстный нейрон. В том случае, когда нейросеть состоит из большого количества нейронов, вводят термин слоя. Соответственно, есть входной слой, который получает информацию, n скрытых слоев (обычно их не больше 3), которые ее обрабатывают и выходной слой, который выводит результат. У каждого из нейронов есть 2 основных параметра: входные данные (input data) и выходные данные (output data). В случае входного нейрона: $\text{input} = \text{output}$. В остальных, в поле input попадает суммарная информация всех нейронов с предыдущего слоя, после чего, она нормализуется, с помощью функции активации (пока что просто представим ее $f(x)$) и попадает в поле output.



Нейроны оперируют числами в диапазоне $[0,1]$ или $[-1,1]$. Чтобы обрабатывать числа, которые выходят из данного диапазона нужно разделить 1 на это число.

Этот процесс называется нормализацией.

Что такое синапс?

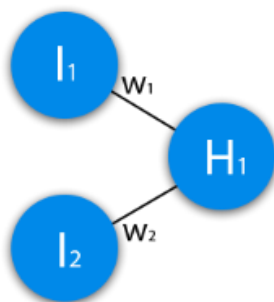


Синапс это связь между двумя нейронами. У синапсов есть 1 параметр — вес. Благодаря ему, входная информация изменяется, когда передается от одного нейрона к другому. Допустим, есть 3 нейрона, которые передают информацию следующему. Тогда у нас есть 3 веса, соответствующие каждому из этих нейронов. У того нейрона, у которого вес будет больше, та информация и будет

доминирующей в следующем нейроне (пример — смешение цветов). На самом деле, совокупность весов нейронной сети или матрица весов — это своеобразный мозг всей системы. Именно благодаря этим весам, входная информация обрабатывается и превращается в результат.

Важно помнить, что во время инициализации нейронной сети, веса расставляются в случайном порядке.

Как работает нейронная сеть?



$$1) H_{1input} = (I_1 * w_1) + (I_2 * w_2)$$

$$2) H_{1output} = f_{activation}(H_{1input})$$

В данном примере изображена часть нейронной сети, где буквами I обозначены входные нейроны, буквой H — скрытый нейрон, а буквой w — веса. Из формулы видно, что входная информация — это сумма всех входных данных, умноженных на соответствующие им веса. Тогда дадим на вход 1 и 0. Пусть $w_1=0.4$ и $w_2 = 0.7$. Входные данные нейрона H1 будут следующими: $1*0.4+0*0.7=0.4$. Теперь когда у нас есть входные данные, мы можем получить выходные данные, подставив входное значение в функцию активации (подробнее о ней далее). Теперь, когда у нас есть выходные данные, мы передаем их дальше. И так, мы повторяем для всех слоев, пока не дойдем до выходного нейрона.

Литература:

1. Саймон Хайкин Нейронные сети. Полный курс(Neural Networks: A Comprehensive Foundation) 2016.

НОВЫЕ ВОЗМОЖНОСТИ IBM DB2 EXPRESS 11.1

DB2 Версия 11.1 для Linux, UNIX и Windows предоставляет новые возможности, помогающие управлять стоимостями и упрощающие разработку различных программ

DB2 — семейство систем управления реляционными базами данных, выпускаемых корпорацией IBM

На сервере баз данных DB2 может размещаться несколько копий программного обеспечения DB2, отличающихся друг от друга версиями программного обеспечения и каталогами установки.

- Основные особенности DB2 Версия 11.1

IBM DB2 Версия 11.1 для Linux, UNIX и Windows предлагает эффективность, простоту и надежность баз данных в виде новых возможностей и усовершенствований, отвечающих широкому кругу бизнес-требований. Главные преимущества этой новой технологии - всесторонняя защита предприятия, упрощенная установка и внедрение, расширенная применимость и адаптируемость, ускоренная процедура обновления, усовершенствования для очень больших баз данных и значительные усовершенствования в BLU Acceleration.

- Усовершенствования управления

Версия 11.1 содержит усовершенствования, упрощающие управление средами DB2, сокращающие общую стоимость владения (total cost of ownership, TCO), уменьшающие влияние выполнения задач управления системой на производительность и расширяющие возможности автономных компонентов, добавленных в предыдущих выпусках.

- Усовершенствования производительности

DB2 Версия 11.1 содержит многочисленные усовершенствования производительности SQL, еще более укрепляющие позицию сервера данных DB2 в качестве промышленного решения сервера баз данных, подходящего для организаций любых размеров.

- Усовершенствования совместимости SQL

Если вы работаете с продуктами реляционных баз данных, отличными от продуктов баз данных DB2, DB2 Версия 11.1 содержит усовершенствования, которые уменьшают время и сложность подготовки прикладных программ, написанных для других продуктов реляционных баз данных, для работы в средах DB2.

- Усовершенствования защиты

С увеличением числа как внутренних, так и внешних угроз защиты становится важным отделить задачи защиты данных от задач управления и администрирования критических систем. Усовершенствования Версии 11.1, базирующиеся на предыдущих версиях и обеспечивают еще более лучшую защиту чувствительных данных.

- Усовершенствования клиентов и драйверов IBM Data Server

Для некоторых клиентов и драйверов IBM Data Server добавлены новые и улучшены старые возможности, повышающие производительность и надежность прикладных программ.

Дополнительные усовершенствования

- Усовершенствования перемещения данных

Версия 11.1 содержит усовершенствования в утилитах перемещения данных, таких как IMPORT, EXPORT, LOAD и INGEST.

- Усовершенствования установки и обновления

Версия 11.1 содержит усовершенствования, ускоряющие внедрение продуктов и упрощающие их поддержку.

- Усовершенствования возможности IBM DB2 pureScale

DB2 Версия 11.1 продолжает надстраивать поддержку возможности DB2 pureScale и предлагает ряд усовершенствований.

- Усовершенствования диагностики и устранения неисправностей.

DB2 Версия 11.1 содержит усовершенствования, позволяющие проще диагностировать и устранять неисправности в средах DB2.

- Усовершенствования высокой доступности, резервного копирования, ведения журналов, устойчивости и восстановления.

Версия 11.1 содержит усовершенствования, обеспечивающие постоянную доступность ваших данных.

Ставицкая Ю.В.

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

УСПЕХ ВНЕДРЕНИЯ СОВРЕМЕННЫХ ИТ В СТРОИТЕЛЬНЫХ КОМПАНИЯХ

Наиболее продвинутые компании в последние несколько лет стремятся использовать все, что могут предложить ИТ. Например, IP-телефонию, которая позволяет обеспечивать удаленные площадки телефонной связью в кратчайшие сроки и по экономичным ценам. Раньше все строительные предприятия пытались решать эту задачу на местах, посредством подключения местного телефона. Для этого они привлекали операторов связи, которые тянули провода к месту стройки, что зачастую было невозможно из-за труднодоступности и

отдаленности строительных площадок. Так, кстати, пытаются действовать многие до сих пор. Между тем канал связи можно организовать гораздо более простым и удобным способом, посредством технологий WiMAX и 3G. Также можно установить радиовышки, задействовать операторов спутниковой связи или протянуть оптический кабель. Хотя последний вариант самый дорогой и затратный, и имеет смысл только если объект рассчитан на долгий срок строительства и предполагает интенсивное использование кабеля или передачу кабеля заказчику, а затраты на его прокладку гарантированно окупятся. В любом случае обеспечение доступа в Интернет на стройплощадке — вполне решаемая задача. Далее с его помощью можно объединить все удаленные площадки посредством VPN с АТС в центральном офисе и обеспечить их внутренними корпоративными номерами. Благодаря этому можно звонить коллегам по внутренней связи бесплатно, а это позволяет строительным компаниям экономить расходы на связь, и чем в более удаленном регионе идет стройка, тем ощутимее экономия.

Помимо IP-телефонии, популярность в строительном бизнесе набирает видеоконференцсвязь, позволяющая сокращать затраты на командировки. К примеру, компания, имеющая офис в столице, для организации совещаний с работающими на объектах сотрудниками приходится постоянно отправлять менеджеров в командировки, или напротив, вызывать оттуда специалистов в центральный офис. Все это стоит больших денег. Однако благодаря современным ВКС-системам, таким как Polycom или CISCO даже, имея весьма узкий канал связи (например, организованный по технологии ADSL), можно организовать деловое общение между сотрудниками компании без необходимости их личного присутствия в офисе.

С точки зрения ИТ, современная строительная площадка фактически представляет собой мини-офис, требующий соответствующего уровня ИТ-обслуживания, поэтому изменений в подходе к ее организации много. В частности, в бюджет строительной площадки теперь, как правило, включаются все сопутствующие затраты на ИТ: например, расходы на связь и организацию компьютеризированных рабочих мест для управляющего персонала. Кроме того, при создании площадки выделяется время на то, чтобы наладить всю ИТ-работу. Дальнейшее его сопровождение также требует повышенного внимания. После запуска стройки необходимо обслуживать развернутую на объекте ИТ-инфраструктуру, а для этого там должны регулярно появляться ИТ-специалисты, способные решить все сопутствующие задачи. До недавних пор во многих строительных компаниях такого не было, а все ИТ-проблемы строители пытались решать своими силами, в лучшем случае привозя неисправные компьютеры в офис. Современный подход более рационален: после оснащения площадки за ней закрепляются выездные ИТ-администраторы, которые могут быть как штатными специалистами, таки аутсорсерами. В наиболее продвинутых компаниях существуют службы технической поддержки, специалисты которых готовы прийти на помощь удаленно, по первому же звонку

Трембовецький Максим Петрович
Д.т.н., старший науковий співробітник, зав.каф. ЕТ
Поливода Євгеній Григорович
Студент групи ТСДМ-62
Державний університет телекомунікацій
м. Київ, Україна

ДОСЛІДЖЕННЯ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СИСТЕМ МОНІТОРИНГУ МЕРЕЖ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

У галузі зв'язку відбуваються радикальні зміни: загострюється конкуренція на ринку, зростають вимоги до якості обслуговування з боку користувачів, відбувається технічне переозброєння мереж зв'язку, змінюється характер розподілу трафіку. Проходячи через призму експлуатації, ці зміни призводять до необхідності здійснення контролю та управління трафіком і якістю мереж різних технологій.

Тут на допомогу оператору приходять системи моніторингу мереж зв'язку. Вони не тільки змінюють уявлення про систему експлуатації, переходячи від експлуатації окремих станцій до експлуатації всієї мережі. Системи моніторингу мереж автоматизують багато рутинні процеси зі збору та обробки мережевих даних. Вони дають в руки операторів унікальні функції глибокого аналізу.

Для забезпечення високої якості послуг мережами зв'язку операторам доводиться постійно проводити тестування існуючих систем. Для тестування мереж використовуються апаратно-програмні комплекси від таких виробників як Ericsson, Huawei, ZTE, Alcatel. Дані комплекси здатні проводити вимірювання як в мережах 2,5 G так і в мережах 3G та 4G [1].

Одним з важливих параметрів, що впливають на якість зв'язку, є бітова швидкість Інтернет-з'єднання. Проблема забезпечення високих швидкостей Інтернет-з'єднання загострюється в зв'язку зі зростанням обсягів даних, що передаються через мережі Інтернет, які зараз дуже активно використовуються для перегляду фільмів в потоковому режимі, а також для відвідування соціальних мереж, де інформаційні сторінки сильно перевантажені графічною інформацією. Для комфортної роботи в мережі Інтернет на даний момент необхідні мінімум швидкості 1,5-2 Мбіт/с.

Актуальним завданням є моніторинг швидкості Інтернет-з'єднання, для забезпечення якого в даний час використовуються різні інтернет-ресурси, наприклад, тест швидкості, що надають різні компанії. Дані сервіси дозволяють досить швидко визначити швидкість Інтернет-з'єднання, але мають ряд істотних обмежень, наприклад: обмежене число запитів на добу, неможливість проводити тестування швидкості Інтернет-з'єднання без участі користувача (автоматизоване тестування), неможливість довільно змінювати розмір тестового пакета.

Таким чином виникає потреба постійного удосконалення, модернізації тестової системи не залежних від будь-яких зовнішніх сервісів.

У зв'язку з цим актуальним є огляд і аналіз нинішнього стану в світі взагалі, і в Україні зокрема, таких стандартів мобільного зв'язку, як GSM, CDMA, UMTS

(WCDMA), WiMAX, LTE [2,3]. Однак, більшість аналітиків як правило акцентують свою увагу переважно на одній з цих технологій, до якої вони мають найбільш близьке відношення. На мій погляд, враховуючи єдність телекомунікаційного простору України, більш правильним є комплексний підхід, коли перспективи кожної технології розглядаються в умовах її взаємозв'язку і взаємозалежності з іншими сучасними технологіями. Результати комплексного аналізу з урахуванням думок і висновків провідних українських і зарубіжних експертів в області систем зв'язку і передачі даних дозволили б спрогнозувати тенденції і подальші напрямки розвитку стандартів і систем зв'язку на їх основі, а також намітити шляхи вирішення зазначених вище проблеми стосовно українських реалій.

Література:

1. Терентьев В.О. Управление и качество услуг в сетях GPRS/UMTS/ Тихвинский В.О., Терентьев СВ.// Эко-Трендз. - 2007.
2. Попов В.И. Основы сотовой связи стандарта GSM / Попов В.И., В.В. Андреев// М.: ЭкоТрендз. - 2005. - 296с.
3. Ипатов В.П. Системы мобильной связи / В.П. Ипатов, В.К. Орлов, И.М.Самойлов, В.Н. Смирнов. - М.: Горячая линия-Телеком. - 2003.- 272с.

Черевик В'ячеслав Михайлович
Професор каф Комп'ютерної інженерії
Батіщев Сергій Олександрович
Державний університет телекомунікацій
Факультет Інформаційних технологій
м. Київ, Україна

АНАЛІЗ ІСНУЮЧИХ СТРАТЕГІЙ РЕЗЕРВУВАННЯ

Одним з важливих завдань при експлуатації обчислювальних систем є забезпечення цілісності і збереження даних, адже навіть в найнадійнішій з них існує ризик втрати життєво важливої інформації [1]. Тому необхідно мати механізм для швидкого відновлення втрачених даних. Це може бути забезпечено шляхом побудови розвиненої системи резервного копіювання, що періодично створює копії інформації з метою її подальшого відновлення у разі часткового або повного руйнування.

Крім того, така система може збирати і обслуговувати архів корпоративних даних. Часто вимагається, щоб система резервного копіювання функціонувала в обчислювальній мережі, причому уміла маніпулювати даними і пристроями незалежно від їх розташування в цій мережі.

Для підвищення рівня доступності інформації в межах традиційно виділяють три стратегії резервування [2]. При цьому у ролі вузла можуть розглядатися окремий сервер, серверний кластер, територіально-розподілений кластер, центр обробки даних.

Традиційно виділяють наступні основні стратегії резервування:

Стратегія 1. Використовується певна кількість копій масиву. При руйнуванні основного масиву використовується перша його копія. Якщо і вона зруйнувалася, то використовується наступна копія і т.д.

Стратегія 1 може використовуватися для масивів постійних і поточних даних.

Стратегія 2. При використанні цієї стратегії замість копій інформаційного масиву зберігаються його передісторії – попередні покоління масиву і відповідні їм масиви змін. При руйнуванні поточного масиву відбувається його відновлення по передісторії за допомогою програми оновлення.

Стратегія 3. Змішана стратегія, що передбачає зберігання як копій, так і передісторій. Резервування інформації проводиться методом поступового заміщення. Змінені частини масиву поміщаються в копію оригіналу. Оригінал видаляється лише після повного завершення оновлення і його підтвердження. Дві і більше ідентичні копії є тільки у час оновлення.

Детальний аналіз показав, що для вибору стратегії відновного резервування в межах локальної мережі доцільно використовувати моделі, які використовуються для оптимізації відновного резервування в локальних мережах і окремих вузлах. При виборі оптимального режиму віддаленого резервного копіювання даних на майданчик резервного центру обробки даних слід враховувати імовірнісні і вартісні характеристики каналу зв'язку а для запобігання великого об'єму використаних ресурсів використовувати алгоритми стискування.

Література

1. П.Массиглиа. Технологии управления хранением данных компании VERITAS Software. М:- «Jet Info», №8(99), 2001
2. Кульба В.В., Сомов С.К., Шелков А.Б. Резервирование данных в сетях ЭВМ. Издательство Казанского университета, 1987

Бондаренко І.І.

Державний університет телекомунікацій

Аспірант ФІТ

м. Київ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРОГРАМНО КОНФІГУРОВАНИХ МЕРЕЖ ТА ВІРТУАЛІЗАЦІЇ МЕРЕЖЕВИХ ФУНКЦІЙ

Комп'ютерні мережі як основоположна інфраструктура - стратегічний чинник розвитку сучасних ІТ, проте архітектура мережі, основи якої закладалися ще наприкінці 60-х років, застаріла і вже не завжди здатна адекватно і ефективно реагувати на нові потреби. Зростання кількості і різноманітності мобільних пристроїв, розвиток різних технологій бездротового зв'язку призвели до того, що сьогодні число їх користувачів перевищила число користувачів мереж з фіксованим зв'язком. Однак зростання потужності мобільних терміналів стимулює збільшення обчислювальної ємності додатків, що, у свою чергу,

вимагає збільшення пропускної спроможності каналів зв'язку - обсяг мобільного трафіку зростає в геометричній прогресії, а види трафіку стають все більш різноманітними.

Подальша еволюція мереж зв'язку нерозривно пов'язана з такими технологіями, як програмно визначаються мережі (SDN) і віртуалізація мережевих функцій (NFV).

Одним із еволюційних напрямків організації ресурсів білінгових систем мереж Long Term Evolution (LTE) є підхід, який передбачає віртуалізацію мережевих функцій (Network Functions Virtualization, NFV) ядра мобільних мереж Evolved Packet Core (EPC) та системи IP Multimedia Subsystem (IMS) як платформи. Такий підхід дозволяє знизити сукупну вартість володіння для мобільних мереж, збільшити ефективність використання ресурсів, доступність сервісів для споживачів та забезпечити більш гнучку керованість мережі.

Побудова мереж на базі технології SDN дає ряд переваг, які в традиційній архітектурі відсутні або їх використання значно збільшує вартість інфраструктури.

Ключові переваги NFV - гнучке розгортання сервісів і контрольовані витрати. Дослідна експлуатація дає оператору можливість випробувати новий підхід і проаналізувати його придатність.

Завдяки віртуалізації мережевих функцій значно змінюються традиційні методи проектування та управління корпоративними мережами, а також мережевою інфраструктурою телекомунікаційних компаній.

Курочкіна Марина Георгіївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет інформаційних технологій
м.Київ

БЛОКЧЕЙНИ – НОВІТНЯ ТЕХНОЛОГІЯ КРИПТОГРАФІЇ В ЦИФРОВОМУ СВІТІ

Блокчейн - це багатогранна, молода і набираюча популярність технологія, обумовлена тим, що вона стоїть на перетині відразу декількох наукових дисциплін і сфер діяльності: розподілені обчислення, макроекономіка і навіть теорія ігор - методи теорії ігор знаходять широке застосування в математичному апараті криптовалют, стимулюючи різні дії учасників.

Блокчейн являє собою розподілену облікову книгу записів про події в цифровому світі. Ключовою складовою блокчейна є журнал транзакцій, а самі транзакції - це єдиний спосіб змінити стан реєстру.

Транзакція може виконатися або до кінця, або не виконатися ніяк («зависання» операції в проміжному стані неприпустимо). При цьому записи в

журнал транзакцій можуть вноситися тільки за згодою більшості учасників мережі. Важливою особливістю журналу транзакцій у блокчейні є його незмінність. Ця властивість означає, що не можна непомітно видалити транзакцію з журналу або додати нову в його середину. Властивість незмінності досягається за рахунок прийомів криптографії, а не за рахунок довіри до організації або людям. Два найпростіших криптографічних алгоритми, що використовуються в блокчейні, – це хеш-функції і електронний підпис, що забезпечують цілісність транзакцій і відповідають за авторизацію. Хоча блокчейн і є розподіленою системою, а формувати транзакції може кожен вузол, це не означає, що всі учасники блокчейн-мережі рівноправні – майже в будь-якій реалізації цієї технології введено розподіл ролей на валідаторів (учасників, які пишуть транзакції в журнал), аудиторів і легких клієнтів. Причому, такий поділ справедливий не тільки для приватних блокчейнів, але і для відкритих (наприклад, біткоін).

З глобальної точки зору, блокчейн є мережею для обробки транзакцій з набором правил («протокол»), слідуючи яким учасники можуть прийти до спільного бачення журналу транзакцій і встановити стан мережі в певний момент часу. При цьому блокчейн децентралізований: навіть якщо істотна частина вузлів випаде з роботи на тривалий час або буде зламана, система все одно продовжить працювати. Децентралізована, відкрита і математично обґрунтована природа блокчейна дозволяє людям і організаціям мінімізувати ризики взаємодії між собою і проводити P2P-транзакції, виключаючи посередників. Ще це позитивно позначається на безпеці.

Класичні хакерські атаки, які здатні завдати шкоди великим централізованим банківським системам, виявляються нереалізованими або, у всякому разі, миттєво виявленими в блокчейн-середовищі. Якщо зломисник захоче зламати певний блок в ланцюзі, то йому доведеться зламати і всі попередні йому блоки. При цьому модифікувати доведеться всі журнали мережі, кількість яких може досягати тисяч або навіть мільйонів (якщо брати до уваги легкі клієнти).

Як же працює блокчейн біткоїнів і як відбувається обробка блоків? Щоб відстежувати всі проведені транзакції в мережі, вони об'єднуються в блоки. Відзначимо, що блок являє собою набір цифрових транзакцій, які були сформовані за останні 10 хвилин (проте варто додати, що включення залежить від комісії в транзакціях і інших параметрів, тому в блок можуть входити не всі транзакції за останні N хвилин).

Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеші транзакцій і додаткову службову інформацію. В системі біткоін першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою майнеру, що вирішив блок. При вирішенні блоку транзакцій майнери обчислюють його хеш. Він являє собою випадкову послідовність цифр і букв і є

гарантією того, що якщо в блоці даних зміниться хоча б один біт, кожен вузол швидко зможе дізнатися про спробу фальсифікації історії транзакцій. Блокчейн біткоїнів використовує алгоритм шифрування SHA-256. Створений блок буде прийнятий іншими учасниками мережі, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується. Рівень складності адаптується до сумарної обчислювальної потужності майнерів. Це здійснюється шляхом поновлення граничного значення кожні 2016 блоків, що відбувається приблизно раз на два тижні.

Так як результат хешування (функції SHA-256) є незворотним, алгоритму отримання бажаного результату не існує - ця операція виконується випадковим перебором. Зазвичай потрібна велика кількість перерахунків. Коли варіант знайдений, вузол розсилає отриманий блок іншим підключеним вузлів, які перевіряють його. Якщо помилок немає, то блок вважається доданим в ланцюжок, а наступний блок включає в свій заголовок його хеш. Таким чином, ланцюжок блоків містить історію володіння, з якою можна ознайомитися, наприклад, на спеціалізованих сайтах.

Першим блокчейном вважається криптовалюта біткоїн, яка і на сьогоднішній день залишається найпопулярнішим блокчейном за економічними і технічними показниками. Початок технології заклав Сатоши Накамото (Satoshi Nakamoto), який опублікував у 2008 році статтю про принципи роботи біткоїнів. Сам блокчейн біткоїнів був закладений в січні 2009 року.

Також з'явилася можливість використовувати блокчейн не тільки для реалізації електронних грошей, а й для виконання довільних розподілених обчислень (смарт-контракти). Ідея в тому, що за рахунок виконання логіки на тисячах вузлів до неї виникає довіра, заснована на математичних законах. Такі можливості відкрили дорогу блокчейну в корпоративне середовище. ІТ-гіганти на кшталт IBM, Intel і Microsoft почали впроваджувати технологію в свої продукти. Також створюються внутрішньогалузеві і міжгалузеві консорціуми (R3, Hyperledger, PTDL Group), що займаються блокчейном і розподіленими реєстрами.

На технологію звернули увагу і дослідники, які бачать потенціал в різних сферах діяльності: **фінансовій сфері, охороні здоров'я, інтернеті речей**. З'являються все нові і нові гравці, які прагнуть популяризувати використання блокчейна.

Можна з упевненістю сказати, що нові проекти на блокчейні будуть базуватися на його головних перевагах - відкритості, захищеності, безпеці. Тому блокчейн стане гарною підмогою для будь-яких сервісів, де користувачів хвилюють проблеми шахрайства та збереження персональних даних.

ДОСЛІДЖЕННЯ МОДЕЛІ ВЗАЄМОДІЇ ІНТЕРНЕТ РЕЧЕЙ З ДОПОВНЕНОЮ ТА ВІРТУАЛЬНОЮ РЕАЛЬНІСТЮ

Термін "інтернет речей" ("Internet of Things" , IoT) вперше був сформульований ще у 1999 році. Саме поняття представляє цілу концепцію комунікаційної мережі об'єктів ("речей"), які мають технології для взаємодії між собою та з оточуючим середовищем. Крім того, вони покликані виконувати певні дії без втручання людини. Тобто усі пристрої в домі, в авто та інших середовищах, самі обробляють інформацію, обмінюються нею та здатні виконувати різні дії в залежності від цієї інформації.

Кількісний перехід від «Інтернету людей» до «Інтернету речей» відбувся в 2008-2009 роках. Саме в той період кількість пристроїв, підключених до Інтернету, перевищила кількість інтернет-користувачів, а тому світ поступово перейшов у нову фазу розвитку технологій – Інтернету речей.

На сучасному етапі розвитку Інтернет речей (Internet of Things) в світі приділяється надзвичайно велика увага. За прогнозами аналітиків у найближчі роки очікується справжній бум Інтернет речей. Так, за прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн. доларів. Найбільші світові ІТ компанії, зокрема Intel, Google та ін. вже почали масштабну роботу на цьому ринку. Так корпорація Intel у 2014 році створила власний підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку. Компанія «Google» на початку 2014 року за 3,2 млрд. доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів. Спеціалісти компанії «Google» займаються широким впровадженням на американському ринку технологій IoT. Виробники побутової техніки також працюють у цьому напрямку. Так на виставці CES 2014 у Лас-Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до Інтернет.

Ще чотири роки тому в Україні налічувалося приблизно 50 тисяч ІТ-фахівців. За підрахунками індійських фахівців їх влітку минулого року вже налічувалося 75 тисяч. За іншими оцінками на даний час, кількість ІТ- фахівців в Україні сягає 80-90 тисяч. Однак такі цифри стосуються організованого ІТ-ринку. Якщо врахувати частину фахівців, які працюють неформально, то в нашій країні кількість ІТ- фахівців сягає 100 тисяч. За реалістично- оптимістичними прогнозами кількість ІТ- фахівців в Україні до 2020 року може подвоїтися.

Необхідно відзначити, що світовим лідером за кількістю ІТ- фахівців є Індія, а у Європі – Україна.

Концепція технології IoT полягає в тому, щоб всі предмети побуту, товари, вузли технологічних процесів тощо, оснащені вбудованими комп'ютерами та сенсорами і мають змогу обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею та виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції може бути система «розумний будинок», яка вже застосовується у країнах Європи. Вона контролює параметри навколишнього середовища, в залежності від цього регулює температуру у приміщенні. У зимовий період нагріваючи прилади, в залежності від температури повітря ззовні, вітру, часу доби без втручання людини регулюють інтенсивність опалення, що дозволяє значно зменшити споживання енергоносіїв.

Середовище роботи таких пристроїв не обмежується лише розумним будинком, воно може охоплювати більш глобальний простір. Наприклад, керування транспортом в місті згідно інформації, зібраної з камер на вулицях, розумний кондиціонер, що може відстежувати місце розташування свого власника і включатися, коли той прямує додому, а домашній холодильник – стежити за кількістю та асортиментом продуктів.

Велике зацікавлення технологією IoT представляє використання її для опрацювання інформації рухомих об'єктів, в першу чергу для автомобільного транспорту. Такі технології дають можливість діагностувати роботу автомобілів в процесі експлуатації, попереджати аварійні ситуації, замовляти необхідні запчастини та здійснювати пошук необхідної станції і встановлення часу обслуговування автомобіля.

Для об'єднання повсякденних речей у мережу потрібні декілька технологій.

- Для ідентифікації кожного об'єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати інформацію про певний предмет. Такий функціонал можна забезпечити за допомогою чіпів RFID (Radio-Frequency IDentification). Вони здатні без власного джерела струму передавати інформацію приладам зчитування. Кожен чіп має індивідуальний номер. Як альтернатива для даної технології для ідентифікації об'єктів можуть використовуватись QR-коди. Для визначення точного місця знаходження речі може використовуватись технологія GPS, яка ефективно використовується вже сьогодні у смартфонах та навігаторах.

- Для відслідковування змін у стані елементу чи оточуючого середовища об'єкти оснащуються сенсорами.

- Для обробки та накопичення даних з сенсорів використовуються вбудовані комп'ютери.

- Для обміну інформацією між пристроями використовуються технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN).

Вже сьогодні існують рішення, здатні об'єднати різні програмні комплекси і різні пристрої в єдину екосистему. Інструментом для збору всього воедино є, наприклад, хмарні технології.

Виходячи з наведеного вище, виникає висновок, що на сьогодні вища освіта потребує перетворень направлених на задоволення потреб в інженерах і вчених, чия діяльність буде тісно пов'язана з технологією Інтернет речей.

Вже зараз основні роботи в області Інтернет речей ведуться за чотирма напрямками: розроблення технологій збору і обробки інформації, технологій передачі даних, створення можливостей для пристроїв приймати самостійні рішення і можливостей реалізації прийнятого рішення.

Яновський Д.А.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

ТЕЗИ НАУКОВО-ДОСЛІДНИЦЬКОЇ РОБОТИ «ТРИГОНОМЕТРИЧНА ПІДСТАНОВКА В АЛГЕБРІ»

Мета дослідження: застосувати тригонометричну підстановку при розв'язуванні задач із метою встановлення взаємозв'язку різних розділів математики: алгебри й тригонометрії, навести приклади використання її в складних задачах для спрощення розв'язання.

Предметом дослідження є тригонометрична підстановка, **об'єктом** – прийоми застосування тригонометричної підстановки як методу розв'язку різноманітних алгебраїчних задач.

Досягнення поставленої мети передбачає виконання таких **завдань**:

- виявити теоретичні основи можливості введення тригонометричної підстановки;
- навести приклади використання тригонометричної підстановки для розв'язування рівнянь, нерівностей та її систем;
- застосувати даний метод для розв'язування олімпіадних задач та задач підвищеної складності.

Практичне значення. Робота може використовуватися на парах математики та факультативах із метою формування інтересу до математики.

ДОСЛІДЖЕННЯ МЕТОДІВ ПЛАНУВАННЯ ТА ОПТИМІЗАЦІЇ СИСТЕМ АБОНЕНТСЬКОГО РАДІОДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ LTE

LTE - це еволюційний крок у розвитку технологій мобільного зв'язку. Архітектура мережі LTE розроблена таким чином, щоб забезпечити підтримку пакетного трафіку з «безшовною» мобільністю, мінімальними затримками доставки пакетів і високими показниками якості обслуговування. Основною метою розробників стандарту LTE було максимально можливе спрощення структури мережі і виключення дублюючих функцій мережевих протоколів, характерних для системи 3G UMTS.

Його основні особливості:

- Максимальна швидкість завантаження з мережі до 299,6 Мбіт / с і максимальна швидкість завантаження в мережу від абонента до 75,4 Мбіт / с залежно від категорії користувача (антена 4×4 з використанням спектру 20 МГц).
- Низька затримка при передачі.
- Підтримка та FDD і TDD систем зв'язку, а також полудуплексної FDD з однією й тією ж технологією радіодоступу.
- Підтримка як мінімум 200 активних клієнтів у кожній соті 5 МГц.
- Радіоінтерфейс комутації пакетів.

Особливості технології є те що радіус дії базової станції LTE може бути різним в залежності від потужності і використовуваних частот. В оптимальному випадку це порядку 5 км, але при необхідності дальність дії може складати 30 км або навіть 100 км (при достатньому узвишші антени). Дзвінок чи сеанс передачі даних, ініційований в зоні покриття LTE, технічно може бути переданий без розриву в мережу 3G (W-CDMA, CDMA2000) або в GSM / GPRS / EDGE. Таким чином, розвиток мереж LTE можливо на вже розвинених мережах як операторів так і операторів CDMA.

Всього під технологію LTE виділено понад 40 частотних діапазонів, при цьому використання спектра для LTE має регіональні особливості. В США найбільш популярними є діапазони 700 МГц (band 13 та band 17) та AWS (AWS band) – парні частоти в діапазонах 1710-1755 МГц (канали прийому) (поєднання діапазонів 1,7 ГГц / 2,1 ГГц), в Європейських країнах - діапазони 1800 МГц (band 3) і 2600 МГц (band 7), в перспективі – 800 МГц (band 20). В Японії перші запуски LTE відбулися в діапазоні 800 МГц / 850 МГц; 1,5 ГГц; 1,7 ГГц і 2,1 ГГц (в

залежності від оператора); також було виділено діапазон 700 МГц (стандарт АРТ700) для запуску майбутніх мереж LTE.

У режимі з частотним розподілом FDD кадр ділиться на 20 слотів, нумерується від нулевого до 19-го, кожен з яких має тривалість 0,5 мс. У режимі FDD часовий ресурс в межах кадра розділений навпіл для передачі у протилежних напрямках. Фізичні канали в режимі FDD у протилежних напрямках мають обов'язковий дуплексний розрив. Режим часового рознесення каналів TDD має асинхронну природу. Передача даних в режим TDD відбувається одночасно в обох напрямках в одній діапазоні частот.

При плануванні LTE потрібно дотримуватись такої послідовності дій: отримання вихідних даних, калібровка математичної моделі розповсюдження радіоволн на основі вимірювань напруженості поля в найбільш характерних точках зони обслуговування мережі, побудова мережі початкового наближення, привязка ділянок розгортання базових станцій, визначених планом побудови (мережі початкового наближення) до місцевості, ітеративна оптимізація мережі при широкому використанні засобів програмного забезпечення, що підтримують функції синтезу мережі та аналізу експлуатаційних характеристик.

LTE позиціонує себе в якості мережі, яка відповідає вимогам до мереж мобільного зв'язку наступного покоління - як для існуючих операторів 3GPP / 3GPP2, так і для початківців ринку. Ця технологія дозволить операторам надавати високопродуктивні послуги широкосмугового доступу для широкої аудиторії, використовуючи комбінацію високих пікових швидкостей і пропускної потужності системи, як у напрямку "вниз", так і в напрямку "вгору", причому з низьким часовим відгуком.

Живаго К.В.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

IoT

На сьогоднішній день дуже багато говориться про Інтернет Речей (Internet of Things, IoT). У зв'язку з великою доступністю Інтернету і появою певних технічних можливостей в світі відбувається все більше процесів управління фізичними об'єктами через Інтернет безпосередньо. Можна говорити вже про те, що фактично ми вже живемо в епоху інтернету речей, так як кількість пристроїв, пов'язаних між собою за допомогою інтернету перевищує кількість людей, що проживають на планеті.

Говорячи про інтернет речей, багато уявляю собі пілосос, який при наповненні фільтра, сам замовляє його на складі компанії-постачальника або холодильник, який замовляє закінчилися продукти в магазині.

Існують різні визначення IoT (від англ. Internet of Things - Інтернет речей).

Це провідна або бездротова мережа, що з'єднує пристрої, яка має автономне забезпечення, управляються інтелектуальними системами, забезпеченими високорівневою операційною системою, автономно підключені до інтернету, можуть виконувати власні або хмарні додатки і аналізувати зібрані дані. Крім того, вони мають здатність захоплювати, аналізувати і передавати (приймати дані) від інших систем (IDC)

LPWAN - «енергоефективна мережа далекого радіусу дії») - бездротова технологія передачі невеликих за обсягом даних на дальні відстані, розроблена для розподілених мереж телеметрії, між машинної взаємодії та інтернету речей. LPWAN є однією з бездротових технологій, що забезпечують середовище збору даних з різного устаткування: датчиків, лічильників та сенсорів.

В основі принципу передачі даних за технологією LPWAN на фізичному рівні РНУ лежить властивість радіосистем - збільшення енергетики, а значить і дальності зв'язку при зменшенні швидкості передачі. Чим нижче бітова швидкість передачі, тим більше енергії вкладається в кожен біт і тим легше виділити його на тлі шумів в приймальній частині системи. Таким чином, низька швидкість передачі даних дозволяє домогтися більшої дальності поширення радіосигналу, і, як наслідок, збільшення радіусу дії приймаючої станції.

Підхід використовується для побудови LPWAN-мережі схожий з принципом роботи мереж мобільного зв'язку. LPWAN-мережа використовує топологію «зірка», де кожен пристрій взаємодіє з базовою станцією безпосередньо. Мережі міського або регіонального масштабу будуються з використанням конфігурації «зірка із зірок».

Пристрій або модем з LPWAN-модулем передає дані по радіоканалу на базову станцію. Станція приймає сигнали від всіх пристроїв в радіусі своєї дії, оцифровує і передає на віддалений сервер, використовуючи доступний канал зв'язку: Ethernet, стільниковий зв'язок, VSAT.

Отримані на сервері дані використовуються для відображення, аналізу, побудови звітів та прийняття рішень.

Управління пристроями, оновлення програмного забезпечення відбувається з використанням зворотного каналу зв'язку.

Для передачі даних по радіоканалу, як правило, застосовується по не ліцензованому спектру частот, дозволених до вільного використання в регіоні побудови мережі: 2,4 ГГц, 868/915 МГц, 433 МГц, 169 МГц

IoT став всесвітнім трендом і скоро можливість «інтернетизації» стане обов'язковою вимогою для продуктів і послуг широкого вжитку. Пристрої будуть виходити з конвеєра з уже вбудованими інтелектуальними і комунікаційними можливостями.

За рахунок збільшення масштабу виробництва та здешевлення компонентної бази вартість розумних пристроїв знизиться до мінімуму. IoT

проникне в автомобілі, ґрунт, море і річки, в тіло людини. Датчики стануть настільки мініатюрними, що будуть міститися в дрібних побутових предметах або продуктах харчування.

Відповідно пристроїв, зменшаться в розмірах і акумулятори, а потім вони і зовсім зникнуть - «розумні» датчики навчатися отримувати енергію з навколишнього середовища: від вібрації, світла або повітряних потоків і стануть повністю автономними.

Інтернет речей стане гетерогенної середовищем, яка буде існувати як окремий живий організм. Настане час машин.

Бондаренко Микола Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПОДІЛУ РАДІОРЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ З M2M- ТРАФІКОМ

Стрімкий розвиток технологічних можливостей сучасних мереж мобільного зв'язку істотно випереджає попит на їхні послуги з боку користувачів і змушує операторів звертати увагу не тільки на традиційні (мова, передача коротких повідомлень, Інтернет), але і на суміжні ринки послуг, такі як M2M, SmartGRID, IPTV, RCS і ін.

Однак нарощування потенціалу технології мобільного зв'язку перешкоджає безліч бар'єрів, так як, на жаль, технологічні можливості завжди випереджають можливості більш консервативної системи регулювання операторської діяльності та надання послуг на ринку зв'язку.

Одним з бар'єрів, що знижують потенціал майбутніх мереж є використання смуг радіочастот в рамках розвитку перспективних технологій, що є одним з основних завдань розвитку наступного покоління, а саме оптимізація розподілу обмеженого числа радіоресурсів. Рішенням завдань планування радіоресурсів, призначення пріоритетів доступу в залежності від типу трафіку з заданими вимогами до якості обслуговування (QoS, Quality of Service) займаються модулі управління радіоресурсами.

Для аналізу характеристик обслуговування трафіку, таких як ймовірність блокування, середній час передачі та ін., Застосовуються моделі мультисервісних систем масового обслуговування. При побудові та аналізі таких моделей використовується апарат теорії ймовірностей і випадкових процесів [1], теорії масового обслуговування [2] і теорії телетрафіка [3].

На даний момент не існує загальноприйнятого підходу з обслуговування M2M-трафіку, в тому числі оптимального методу для розподілу обмеженої кількості

радіоресурсів між H2H-користувачами і великою кількістю M2M-пристроїв. У зв'язку з цим існує безліч завдань ефективного планування і управління радіоресурсами [4].

Таким чином, для бездротових мереж наступних поколінь попереду стоїть завдання розробки нових моделей і методів аналізу їх функціонування для дослідження ефективності обслуговування M2M-трафіку. Існуючі методи розподілу радіоресурсів, які історично були оптимізовані для обслуговування користувачів традиційних послуг зв'язку, повинні бути доопрацьовані.

Література:

1. Башарин Г.П. Введение в теорию вероятностей: Учеб. пособие для студентов II-III курсов специальностей «Математика», «Прикладная математика». – М.: Изд-во РУДН, 1990. – 228 с.
2. Башарин Г.П., Бочаров П.П., Коган Я.А. Анализ очередей в вычислительных сетях. Теория и методы расчета. – М.: Наука, Гл. ред. физ.-мат. лит., 1989. – 336 с.
3. Лагутин В.С., Степанов С.Н. Телеграфик мультисервисных сетей связи. – М.: Радио и связь, 2000. – 320 с.
4. Dohler M, Alonso-Zrate J, Watteyne T. Machine-to-machine: an emergin communication paradigm // Tutorial, PIMRC 2010, 26 Sept. 2010, Istanbul, Turkey.

Тимощук А.О.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

ЕРА КОГНІТИВНИХ ТЕХНОЛОГІЙ РАЗОМ ІЗ IBM WATSON

Когнітивні технології змінюють компанії, професії та цілі індустрії, і це відбувається прямо зараз! Разом із IBM Watson стало можливим застосовувати когнітивні технології в організаціях будь-якого розміру.

Що робить Watson унікальним? - Можливість отримувати знання з неймовірної кількості даних зі швидкістю світла. Включаючи 80% неструктурованих даних, які ми традиційно не використовуємо.

Когнітивні системи дозволяють вчитися та приймати найбільш ефективні рішення. Оскільки когнітивні системи розуміють мову й емоції, стало можливим спілкуватися з ними. Цей стрімкий розвиток створив нову еру: еру когнітивного бізнесу.

IBM Watson - одна з перших когнітивних систем в світі. Ця система вміє дуже багато, завдяки чому можливості Watson використовуються в багатьох сферах - від кулінарії до передбачення аварій в населених пунктах. Загалом, більшість можливостей Watson не є чимось унікальним, але в комплексі всі ці можливості є досить потужним інструментом для вирішення різноманітних питань.

З появою application programming interface або, якщо коротко, API, життя програмістів стала дещо легшим, ніж раніше. За мінімальний час тепер можна вбудувати в свій додаток певні функції, структури, процедури, що надаються

іншим додатком, операційною системою або сервісом. API своїх сервісів і додатків зараз відкривають багато розробників.

У 2013 році компанія IBM відкрила відразу три API когнітивної системи Watson в рамках "The Watson Ecosystem" - системи, яка на той час включала понад 40 різних технологій. Завдяки цим API розробники отримали можливість вбудовувати у власні додатки і сервіси можливості, пропоновані IBM Watson. Зараз відкритих компанією IBM API вже набагато більше, сервіси стали більш функціональними.

Існуючі API різних сервісів, до яких може отримати доступ розробник, поділяються на кілька груп відповідно до основних можливостей і сфер використання.

1. Мова (Language)
2. Мовлення (Speech)
3. Обробка зображень (Image Processing)
4. Робота з даними (Work with data)

Зараз IBM Watson є лідером у своїй сфері - можливості цієї когнітивної системи, звичайно, не безмежні, але це набагато більше того, про що людина могла мріяти нещодавно.

Вчені намагаються використовувати можливості системи для передбачення землетрусів або вивержень вулканів в певних регіонах. Бізнесмени оптимізують товарні потоки і з'ясовують, що буде найбільш популярним серед покупців найближчим часом. Медики вводять в практику індивідуальний підхід лікування раку та інших захворювань.

На основі IBM Watson створені різні додатки і сервіси, які полегшують людині роботу і роблять життя комфортнішим. Спробувати створити власний сервіс на основі Watson може практично кожен розробник, якому це цікаво. Мета IBM на даному етапі - створити якомога більш розвинену систему додатків і сервісів, що працюють з Watson, надавши всім зацікавленим людям, вченим і бізнесменам надійного помічника, який здатен впоратися з великою кількістю проблем і питань. І це вже не майбутнє, описане фантастами, а сьогодення.

Список використаних джерел:

1. Когнитивная система IBM Watson — будущее действительно здесь // Облачные вычисления, Блог компании IBM // <https://geektimes.ru/company/ibm/blog/271306/>
2. API от Watson и что эти инструменты могут дать вашему сервису или приложению // Облачные вычисления, Блог компании IBM // <https://habrahabr.ru/company/ibm/blog/331206/>
3. Кирило Корнільєв «Ваше когнітивне майбутнє. Як технології наступного покоління змінюють спосіб життя та роботи сьогодні» // Конференція IBM Watson 2017, Київ
4. Серджіо Саад «Роль IBM Systems у Когнітивній Інфраструктурі. Тенденції на напрямки розвитку» // Конференція IBM Watson 2017, Київ

ПОРІВНЯННЯ РІВНОМІРНОСТІ РОЗПОДІЛУ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ТАБЛИЧНИХ ГПВЧ ТА ЛЮДСЬКИХ РЕСУРСІВ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ R

Анотація

Метою написання даної статті є розгляд сучасних критеріїв оцінювання якості застарілих типів ГПВЧ та втілення процедур перевірки згенерованих дискретних випадкових величин у графічному інтерфейсі мови програмування R.

Випадкові числа – це один з елементів криптографії. Більшість систем комп'ютерної безпеки не зможуть обійтися без випадкових величин – для ключів, унікальних чисел у протоколах, тощо. Також випадкові числа необхідні для моделювання природничих процесів та у ході тестування комп'ютерних програм. До середини 40-х років 20 ст. людству знадобилася небагато більша кількість випадкових чисел. Американський аналітичний центр RAND створив машину, яка була здатна генерувати випадкові за допомогою використання генератора випадкових мінусів. Пізніше значуща кількість випадкових чисел була опублікована у книзі «Один мільйон випадкових чисел та сто тисяч нормальних відхилень».[1] Також була побудована інша машина, E.R.N.I.E., яку використовували у британській лотереї Premium Bond. У 1951 Аланом Тьюрінгом комп'ютерові(Ferranti Mark 1) [2]була надана можливість відтворити випадковість, використовуючи дробові шуми – хаотичні відхилення значень струму та напруги від їх середнього значення. Проте використання даного алгоритму ставало джерелом нестабільності роботи комп'ютерних систем. Тому набула поширення раніше висловлена ідея використання детермінованої функції для генерації випадкових значень. Через те, що за однакової ініціалізації такої функції, результат буде однаковим, тобто передбачуваним і не випадковим, з'явилися генератори псевдовипадкових чисел.

За роки використання ГПВЧ обмежилися основні критерії вимог до них.

Головним критерієм, що визначає право на існування даної ГПВЧ є тест на наступний біт.[3] Логічний зміст тесту полягає у тому, що не повинно бути такого поліноміального алгоритму, який при введенні перших k біт згенерованої ГПВЧ послідовності, зможе вирахувати $k+1$ біт із вірогідністю більшою за 0,5. На сьогодні існують дві логічні реалізації даного тесту - це практичний тест наступного біту(PNB) та алгоритм Садегіяна-Махаєрі.[2]

Як видно зі змісту тесту, та функція, що його пройшла, не є повністю захищеною від розкриття, проте є задовільно криптостійкою. Оцінити захищеність такої функції більш детально можна за допомогою багатьох методів

та критеріїв. Розглянемо їх у ході перевірки двох випадкових послідовностей – послідовність некорельованих первірених значень з таблиці випадкових чисел з книги І. Г. Венецького, В. І. Венецької «Основные математико-статистические понятия и формулы в экономическом анализе»[9] та складену самостійно послідовність.

1796	4250
9938	2105
2965	3781
0164	7509
5780	0341
3008	9270

Метод Монте-Карло використовується для рішення математичних задач за допомогою згенерованих випадкових значень, рівномірно розподілених інтервалом (0;1), та має вимоги до такого значення, що є рівномірно розподіленим.[7] Значення з будь-якого іншого інтервалу можна звести до даного наступною формулою, що використовує властивість проекції відрізка (тут – інтервалу).

$$x = a + (b - a) \cdot r$$

Де, r – число з інтервалу (0;1), a та b – межі інтервалу, до якого належить випадкове число x . Але через те, що ми вже маємо конкретну величину, то для перевірки рівномірного розподілу цифр вище вказаних значень, їх треба представити у вигляді

$$x \cdot 10^{-n}$$

Де n – кількість розрядів. Маємо :

0,1796	0, 4250
0,9938	0, 2105
0,2965	0,3781
0,0164	0,7509
0,5780	0,0341
0,3008	0,9270

За методом Монте-Карло, члени послідовності вважаються рівномірно розподіленими, якщо її характеристики як дискретної випадкової величини відповідають наведеним даним:

$$m_r = \frac{\sum_{i=1}^n r_i}{n} \approx 0,5 \text{ – Математичне сподівання}$$

$$D_r = \frac{\sum_{i=1}^n (r_i - m_r)^2}{n} \approx 0,0833 \text{ – Дисперсія}$$

$$\sigma_r = \sqrt{D_r} \approx 0,2887 \text{ – Середньоквадратичне відхилення}$$

Звіримо подані значення із результатами обрахунків, проведених у графічному інтерфейсі мови програмування R.

```

> R1<-c(0.1796, 0.9938, 0.2965, 0.0164, 0.5780, 0.3008)
> R2<-c(0.425, 0.2105, 0.3781, 0.7509, 0.0341, 0.927)
> Mr<-function(a)
+ {
+   M.r<-0
+   for(i in 1:length(a))
+   {
+     M.r<-M.r + a[i]/length(a)
+   }
+   return(M.r)
+ }
> Dr<-function(a, M.r)
+ {
+   D.r <-0
+   for( i in 1:length(a))
+   {
+     D.r <-D.r+((a[i]-M.r)^2)/length(a)
+   }
+   return(D.r)
+ }
> (M.r1<-Mr(R1))
[1] 0.3941833
> (M.r2<-Mr(R2))
[1] 0.4542667
> (D.r1<-Dr(R1,M.r1))
[1] 0.1000596
> (D.r2<-Dr(R1,M.r2))
[1] 0.1036696
> sqrt(D.r1)
[1] 0.3163219
> sqrt(D.r2)
[1] 0.3219776

```

Із наведених результатів видно, що перевірку на рівномірність розподілу дані послідовності не пройшли. Даний перевірка відноситься до типу перевірок якості роботи ГПВЧ(у якості якого виступають табличний ГПВЧ та людина). Одним з найвідоміших критеріїв перевірки якості ГПВЧ є «хі-квадрат». У основі критерію лежить прирівнювання рівномірності розподілу значень ГПВЧ у доцільно розбитих інтервалах до еталонних позначок.[7] Тобто отримана дискретна випадкова величина розбивається на k рівних інтервалів, розраховується n_i - заповненість i -того інтервалу. Нижче наведено формулу, що розраховує різницю між отриманим n_i та еталонним $N \cdot p_i$, тобто такими значеннями за якими функція розподілу випадкової величини $f(x)=const$.

$$\chi_{\text{експ.}}^2 = \frac{1}{N} \sum_{i=1}^k \left(\frac{n_i^2}{p_i} \right) - N$$

```

> phi.sq<-function(a)
+ {
+   counter<-rep(0,10)
+   for(i in 1:10)
+   {
+     for(j in 1:length(a))
+     {
+       if(a[j]==i-1)
+       {
+         counter[i]<-counter[i]+1
+       }
+     }
+   }
+   X.exp.1 <- 0
+   X.exp.2 <- 0
+   for(i in 1:length(a))
+   {
+     X.exp.2 <- X.exp.2+((counter[a[i]+1]^2)/(counter[a[i]+1]/10))
+   }
+   X.exp<-X.exp.2/length(a) - length(a)
+   return(X.exp)
+ }
> phi.sq(R2.2)
[1] 26
> phi.sq(R1.2)
[1] 16
> R1.2
[1] 0.1 0.7 0.9 0.6 0.9 0.9 0.3 0.8 0.2 0.9 0.6 0.5 0.0 0.1 0.6 0.4 0.5 0.7 0.8 0.0 0.3 0.0 0.0 0.8
> R2.2
[1] 0.4 0.2 0.5 0.0 0.2 0.1 0.0 0.5 0.3 0.7 0.8 0.1 0.7 0.5 0.0 0.9 0.0 0.3 0.4 0.1 0.9 0.2 0.7 0.0

```

Наступним кроком буде порівняння отриманих значень з табличними значеннями $\chi_{\text{теор.}}^2$.

$\chi_{\text{експ.}}^2$ першої послідовності(табличний ГПВЧ) на 3 одиниці більше за найбільше значення у ряді, тому можна стверджувати, що дана ДВВ не є такою. Але значення $\chi_{\text{експ.}}^2$ знаходиться між стовпцями $p=75\%$ та $p=95\%$ довірчих рівнів, з чого можна зробити висновок, що дана ГПВЧ, що є джерелом даної послідовності у 75 випадках з 100 дасть рівнорозподілену ДВВ.

Використані джерела:

1. <https://habrahabr.ru/company/infopulse/blog/329778/>
2. Кнут Д.Е. Искусство программирования. Том 2: Получисленные алгоритмы – Пер. з англ. Навч. пос. – Москва: Видавничий дім «Вільямс», 2001. – 832с.
3. <https://habrahabr.ru/post/151187/>
4. <http://www.intuit.ru/studies/courses/691/547/lecture/12383>
5. http://www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture2.pdf
6. https://www.e-reading.club/chapter.php/65865/65/Shnaiier_-_Sekrety_i_lozh%27._Bezopasnost%27_dannyh_v_cifrovom_mire.html
7. <http://stratum.ac.ru/education/textbooks/modelir/lection22.html>
8. <https://habrahabr.ru/company/securitycode/blog/237695/>
9. <http://stratum.ac.ru/education/textbooks/modelir/lection22-01.html>

Єкімов В.

*Державний університет телекомунікацій
Навчально-науковий інститут заочного та дистанційного навчання
м. Київ*

ЧИМ ВІДРІЗНЯЄТЬСЯ WI-FI ВІД WiMAX

З технологією Wi-Fi користувачі інтернету знайомі не з чуток, адже її підтримує практично кожне сучасне мобільний пристрій. Точки доступу Wi-Fi відкриті в більшості кафетеріїв, готелів; Wi-Fi роутер встановлюють у квартири, щоб позбутися від проводів. Але все частіше ми чуємо про більш новому стандарті – WiMAX. Що це: інтернет нового покоління, покликаний замінити Wi-Fi, або ж просто технологія, що має співзвучне назва? Очі розгортання WSN ніколи не передбачало повністю статичні мережі, мобільність спочатку розглядалася як має ряд проблем, які необхідно подолати, в тому числі зв'язку, охоплення і споживання енергії. Недавні дослідження показали мобільність в більш вигідному світлі. У цій статті наводиться огляд пропозицій, які оцінюють мобільні зв'язку представлені в WSNs.

WiMAX - стандарт бездротового зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівняною з кабельними з'єднаннями. Назву «WiMAX» було створено WiMAX Forum — організацією, яку засновано в червні 2001 року з метою просування і розвитку WiMAX. Форум описує WiMAX як «засновану на стандарті технологію, яка надає високошвидкісний бездротовий доступ до мережі, альтернативній виділені лініям;

Wi-Fi – це більш стара інтернет-технологія, ніж WiMAX. Вона з'явилася в 1991 році для використання в системах касового обслуговування і далі розвивалася для розгортання бездротових мереж будинку або в офісі. Сучасні стандарти Wi-Fi дозволяють підключитися до інтернету в радіусі 300 метрів (на практиці – в радіусі кількох десятків метрів).

Wi-Fi має декілька стандартів. Найбільш часто використовуваний в наш час має максимальну швидкість підключення 54 Мбіт / с. Більш нові стандарти пропонують швидкість до 450 Мбіт / с, а в перспективі будуть давати і до 600 Мбіт / с. Стандарт також визначає частоти, на яких здійснюється зв'язок: від 2,4 до 5 ГГц. Користувач може розгорнути Wi-Fi мережу самостійно завдяки досить довгої історії розвитку, порівняно недорогому обладнанню та простоті

установки. WiMAX, також як і Wi-Fi, має кілька стандартів, що визначають крім швидкості з'єднання (до 40-75 Мбіт / с) і частотних діапазонів (1,5-13,6 ГГц) ще й радіус дії (1-80 км).

Діючі на території нашої країни оператори мереж WiMAX використовують різні частотні діапазони і різне обладнання, несумісне один з одним. У Росії до цих пір немає WiMAX-мереж для кінцевих користувачів, мережі орієнтовані на компанії, причому тільки великі. Сьогодні в Росії комерційні WiMAX-мережі розгорнуті лише в декількох містах і регіонах. Проте, дана технологія є дуже перспективною. WiMAX не є прямим конкурентом Wi-Fi, так ці технології спрямовані на вирішення різних завдань.

Зважаючи на співзвучність назв технологій і більш пізніший час появи технології WiMAX, можна помилково припустити, що остання - удосконалена модель Wi-Fi. Ці технології різні, і, перш за все, вони мають різні області застосування:

- Wi-Fi призначена, в основному, для організації невеликих бездротових мереж усередині приміщень і створення бездротових мостів;
- WiMAX - для організації зв'язку поза приміщеннями й для створення великомасштабних мереж.

Технологічною основою WiMAX, яка розроблялася як міська обчислювальна мережа (MAN), є протокол IEEE 802.16, що дозволяє забезпечити одночасно високошвидкісний доступ в Інтернет і передачу даних, а також послуги телефонії без використання кабельних ліній. На відміну від інших технологій радіодоступу, WiMAX сприяє функціонуванню в умовах щільної міської забудови поза прямої видимості базової станції. Відсутність необхідності встановлювати спеціальні вишки актуальна для великих мегаполісів: достатньо установити базову станцію на дахах будинків або висотних споруд, що дозволить швидко розгорнути таку мережу на великі відстані.

На відміну від Wi-Fi, радіус покриття якої не перевищує 100 метрів, зона покриття WiMAX, за певних умов, досягає 50 км. Тому вона може бути корисна мешканцям віддалених районів, для яких недоступні Інтернет або навіть звичайна телефонія через неможливість проведення кабельної мережі або DSL.

Питання безпеки в мережах WiMAX (стандарт IEEE 802.16), як і в мережах Wi-Fi (стандарт IEEE 802.11), загострено легкістю підключення до мережі. Безпека WiMax - мережі забезпечується на фізичному рівні спеціально розробленими чипами ASIC, які убудовані в пристрої бездротового зв'язку й управляють процесом передачі даних радіоканалом, запобігаючи:

1. спробам порушення конфіденційності;
2. порушенню цілісності даних;
3. порушенню автентичності джерела – споживача;
4. відмови в обслуговуванні.

Якість зв'язку у WiMAX вища, чим в Wi-Fi. При підключенні декількох користувачів до точки доступу Wi-Fi виникає проблема черговості доступу до каналу зв'язку. Технологія WiMAX забезпечує кожному користувачеві постійний доступ, використовуючи алгоритм установлення обмеження на число користувачів для однієї точки доступу. При наближенні базової станції WiMAX до максимуму свого потенціалу, вона автоматично розподіляє «надлишкових» користувачів на іншу базову станцію.

Набір переваг властивий всьому сімейству WiMAX, однак його версії, фіксована і мобільна, істотно відрізняються. Розроблювачі стандарту шукали оптимальні рішення як для фіксованого, так і для мобільного застосування, але сполучити всі вимоги в рамках одного стандарту не вдалося. При збігу ряду базових вимог, націленість технологій на рішення різних завдань привела до створення двох окремих версій стандарту. Кожна зі специфікацій WiMAX визначає свої робочі діапазони частот, ширину смуги пропускання, потужність випромінювання, методи передачі й доступу, способи кодування й модуляції сигналу, принципи повторного використання радіочастот та інші показники. Основне розходження двох технологій полягає в тому, що фіксований WiMAX дозволяє обслуговувати тільки «статичних» абонентів, а мобільний орієнтований на роботу з користувачами, що пересуваються зі швидкістю до 120 км/ч. Мобільність означає наявність функцій роумінгу й перемикання між базовими станціями при пересуванні абонента, як відбувається в мережах стільникового зв'язку. В окремому випадку мобільний WiMAX може застосовуватися й для обслуговування фіксованих користувачів.

Технологія Wi-Fi — це набір глобальних стандартів. На відміну від стільникових телефонів, устаткування Wi-Fi може працювати в різних країнах по усьому світу, дозволяючи розгорнути мережу там, де не можна прокласти кабель, наприклад, поза приміщеннями й у будинках, що мають історичну цінність. Wi-Fi-пристрої поширені на ринку, і пристрої різних виробників можуть взаємодіяти на базовому рівні сервісів.

Як і в багатьох інших областях, у бездротовій передачі даних немає універсальної технології. Під кожні конкретні завдання більше підходить WiMAX або Wi-Fi. Якщо поставлено завдання надати ширококутовий доступ до мережі для користувачів, доцільніше використовувати WiMAX, тому що ця технологія була розроблена саме із цією метою. Однак, якщо завдання - надати ширококутовий доступ в обмеженому приміщенні, то технології Wi-Fi і WiMAX однаково добре підходять для вирішення, за умови низького рівня перешкод або їх відсутності. А для впровадження бездротових систем безпеки або відеоспостереження доцільніше скористатися технологією Wi-Fi.

Відмінності	WiMax	від	Wi-Fi:
Швидкість передачі даних по Wi-Fi – до 54 Мбіт / с, WiMAX – до 75 Мбіт / с.			

Радіус покриття Wi-Fi – 300 метрів максимум, WiMAX – 80 км.

Робота ведеться на різних частотах: 2,4 ГГц в найбільш поширеному стандарті.

Wi-Fi і частотний діапазон 1,5-11 ГГц у WiMAX. WiMAX дозволяє стабільно передавати дані, незважаючи на радіоперешкоди, фізичні перешкоди чи погані погодні умови, які в той же час сильно позначаються на роботі Wi-Fi.

Wi-Fi в даний час набагато ширше поширений і має більш різноманітний асортимент обладнання за цінами більш доступним, ніж WiMAX.

Література:

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks" IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
2. S. S. Dhillon and K. Chakrabarty, "Sensor placement for effective coverage and surveillance in distributed sensor networks" in IEEE Wireless Communications and Networking Conference, 2003, pp. 1609–1614.
3. G. Cao, G. Kesidis, T. L. Porta, B. Yao, and S. Phoha, "Purposeful mobility in tactical sensor networks" Sensor Network Operations, 2006.
4. S.A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, J. Ma, "Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing" In International Conference on Advanced Information Networking and Applications Workshops, vol. 2, pp. 113–120, 2007.
5. I. Amundson, X. Koutsoukos, J. Sallai, "Mobile sensor localization and navigation using RF doppler shifts" In 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments, MELT 2008.
6. L. Fang, P.J. Antsaklis, L. Montestruque, M.B. McMickell, M. Lemmon, Y. Sun, H. Fang, I. Koutroulis, M. Haenggi, M. Xie, X. Xie, "Design of a wireless assisted pedestrian dead reckoning system – the NavMote experience" In IEEE Transactions on Instrumentation and Measurement, vol. 54(6), pp. 2342–2358, 2005.

Шкаруба М.О.

*Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій та інформатизації
Факультет Інформаційних технологій
м. Київ*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Сукупність засобів і методів збору, обробки, зберігання та передачі даних для отримання інформації нової якості про стан об'єкту, процесу або явища.

Необхідно розуміти, що освоєння сучасної інформаційної технології і подальше її використання повинні звестися до того, що потрібно спочатку добре оволодіти набором елементарних операцій, кількість яких обмежена.

Інформатизація суспільства є однією із закономірностей сучасного соціального прогресу.

«Телекомунікаційні системи та мережі»

Сучасний і надійний обмін інформацією визначає потребу в побудові ефективної мережевої інфраструктури, яка повинна задовольняти зростаючим вимогам організації.

В умовах стрімкого зростання кількості користувачів інформаційних систем і обсягу обчислень, головними якостями корпоративних мереж передачі даних стають продуктивність, масштабованість, безпека і керованість мережі.

«Безпека інформаційно-телекомунікаційних технологій»

В даний час для забезпечення захисту інформації потрібна реалізація системного підходу, що включає комплекс взаємопов'язаних заходів.

Безпека операційних систем і баз даних, системи технічного захисту інформації, антивірусний захист, безпеку Web-сервісів і Cloud-систем, безпеку мережевих комунікацій.

«Соціально-економічні проблеми розвитку телекомунікацій»

Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу.

Прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень (радіотехнологій, волоконно-оптичних, пакетних технологій тощо).

Щетініна Дар'я Артурівна

Державний університет телекомунікацій

Навчально-науковий інститут заочного та дистанційного навчання

м.Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АВТОМАТИЗАЦІЇ ОФІСУ

Інформаційна технологія автоматизованого офісу включає організацію і підтримку комунікаційних процесів як усередині організації, так і із зовнішнім середовищем на базі комп'ютерних мереж і інших сучасних засобів передачі і роботи з інформацією.

Автоматизація офісу покликана не замінити існуючу традиційну систему комунікації персоналу (з її нарадами, телефонними дзвінками і наказами), а лише доповнити її. Використовуючись спільно, обидві ці системи дозволяють:

1. забезпечити раціональну автоматизацію управлінської праці;
2. надати якнайкраще забезпечення управлінців інформацією.

Офісні автоматизовані технології використовуються управлінцями, фахівцями, секретарями і конторськими службовцями. Причини привабливості автоматизованого офісу для менеджерів усіх рівнів управління можна назвати наступні:

1. Автоматизований офіс привабливий у фірмі тому що підтримує внутрішньофірмовий зв'язок персоналу;
2. Автоматизований офіс привабливий у фірмі том, що надає персоналу управлінців нові засоби комунікації із зовнішнім оточенням.

В інформаційній технології автоматизації офісу широко використовуються і некомп'ютерні засоби: аудіо - і відео конференції, зв'язок факсиміле, ксерокс і інші засоби оргтехніки.

Основні компоненти.

База даних. Обов'язковим компонентом будь-якої технології є база даних. В автоматизованому офісі база даних концентрує в собі дані про виробничу систему фірми. Інформація в базу даних може також надходити із зовнішнього оточення фірми. Фахівці повинні володіти основними технологічними операціями по роботі в середовищі баз даних. Наприклад: В базі даних фіксуються відомості про щоденні продажі, які подають торгові агенти фірми, а також відомості про щотижневі поставки сировини.

Можуть щодня по електронній пошті надходити з біржі зведення про курс валют або котирунки цінних паперів, у тому числі і акцій цієї фірми. Ці дані щодня корегуються у відповідному масиві бази даних.

Література

1. <http://www.frontmanagement.org/fomants-880-1.html>
2. http://pidruchniki.com/1819111861384/informatika/tehnologiyi_avtomatizatsiyi_ofisu

Щетініна Анастасія Артурівна

Державний університет телекомунікацій

Факультет Інформаційних технологій

м. Київ

СУЧАСНІ ТЕХНОЛОГІЇ WI-FI ТА LI-FI

Назва "Wi-Fi" - це скорочення словосполучення "Wireless-Fidelity", що в перекладі на українську означає "Бездротова Свобода". І це в якомусь сенсі відображає призначення даного бездротового інтерфейса.

Wi-Fi дуже швидкий, більш ніж у 100 разів швидше за модемне з'єднання. Зазвичай схема Wi-Fi мережі містить не менш однієї точки доступу та може легко масштабуватись.

Дальність передачі залежить від потужності передавача, наявності та характеристики перешкод, типу антени. Ядром безпроводної мережі Wi-Fi є так звана точка доступу, яка підключається до якоїсь наземної мережевої інфраструктури та забезпечує передачу радіосигналу. Для того, щоб підключитися до точки доступу й відчувати всі переваги бездротової мережі, власнику ноутбуку або мобільного пристрою з адаптером Wi-Fi необхідно просто потрапити в радіус її дії.

Потрібно відзначити, що технологія Li-Fi більш безпечна для здоров'я людини, ніж Wi-Fi. У Wi-Fi використовується випромінювання хвиль на тих же частотах, що в мікрохвильовій печі, а вони при достатній інтенсивності здатні

закип'ятити воду. Постійний і сильний вплив радіації від Wi-Fi може негативно впливати на репродукційну функцію людини. Хвилі Li-Fi не інтерферують з випромінюванням від інших приладів, а це значить, що на якість з'єднання не вплинуть сусідські роутери, радіоприймачі або телевізійні перешкоди.

Технологія передачі даних Li-Fi показує швидкість в 100 разів більшу ніж середній Wi-Fi.

Li-Fi – бездротова технологія, яка передає дані з високою швидкістю за допомогою каналу зв'язку видимого світла (visible light communication або VLC). Оскільки дослідники досягли швидкості передачі даних в 224 гігабіт на секунду, потенціал цієї технології обіцяє зробити переворот в сфері інтернету.

Зараз дослідники вперше вивели технологію Li-Fi з дослідницької лабораторії, протестувавши її в офісі і промислових умовах в естонському Таллінні. Повідомляється, що вдалося досягти швидкості в 1 гігабіт на секунду – що в 100 разів швидше середньої швидкості Wi-Fi.

Технологія Li-Fi була винайдена Харальдом Хаасом з шотландського Единбурзького Університету в Шотландії в 2011 році, коли він вперше продемонстрував, що за допомогою мерехтіння світла від одного-єдиного світлодіода можна передати набагато більше даних, ніж через вежу стільникового зв'язку. І якщо взяти до уваги лабораторні показники швидкості в 224 гігабіт на секунду, то це дорівнює скачуванню приблизно 18 фільмів об'ємом 1,5 Гб за одну секунду.

Переваги Li-Fi над Wi-Fi крім потенційно великих швидкостей в тому, що світло не проходить крізь стіни, і це робить процес передачі даних набагато більш захищеним, а також означає менше перешкод між пристроями.

Використані джерела:

1. <http://startupline.com.ua/hardware/li-fi-shows-the-rate-of-100-times-more>
2. Буров Є.В. Комп'ютерні мережі. Підручник / Є.В. Буров // Вища освіта в Україні. - Л.: "Магнолія-плюс", 2015. - С.262.

Міщенко Володимир

Державний університет телекомунікацій

Навчально-науковий інститут телекомунікацій та інформатизації

Факультет Інформаційних технологій

м. Київ

ЩО ТАКЕ ЦОД?

Дата-центр (ЦОД) являє собою сукупність спланованих певним чином територій, зовнішніх майданчиків (анклавів), будівель, приміщень, зі встановленими інженерними системами забезпечення та обслуговуючим персоналом, що утворюють загальний фізичний простір і технологічне середовище для розміщення комп'ютерів, електронних та інших засобів

прийому, передачі, обробки, зберігання інформації і забезпечують задану ступінь доступності (готовності), розміщеного обладнання в заданому режимі функціонування.

Будівництво та експлуатація дата-центрів здійснюється згідно з рядом жорстких стандартів. Дата-центр може бути підрозділом телекомунікаційної компанії або ж окремою організацією.

Основна діяльність дата-центру полягає у встановленні та подальшому обслуговуванні серверного та комунікаційного обладнання клієнтів згідно з умовами колокації або виділення серверів. Обладнання монтується до серверних стійок і/або шаф. Якість та пропускна здатність каналів зв'язку дата-центру на пряму впливають на якість послуг, які він надає, позаяк основним критерієм її оцінки є час доступності розміщеного в дата-центрі сервера (англ. uptime).

Найстарішим дата-центром України є ColoCall (працює з 1 серпня 2000 року). Найбільшим спеціалізованим дата-центром України є ЦОД De Novo, площею 2117 м² і потужністю 3,3 МВт.

У ряді країн є стандарти щодо обладнання приміщень дата-центрів, що дозволяють об'єктивно оцінити здатність дата-центру забезпечити той чи інший рівень сервісу. Наприклад, в США прийнятий американський (ANSI) стандарт TIA-942 (англ.), що несе рекомендації зі створенню дата-центрів, і ділить дата-центри на типи за ступенем надійності.

Фактично, TIA-942 сприймається в усьому світі як єдиний стандарт для дата-центрів, однак слід зазначити що він досить давно не оновлювався. У той же час, активно розвивається стандарт BICSI 002 2010 Data Center Design and Implementation Best Practices, що з'явився в 2010 і оновлений в 2011.

Кожен із стандартів, як правило має свою внутрішню класифікацію дата-центрів за сукупністю їх параметрів.

Комунікації дата-центру найчастіше базуються на мережах з використанням протоколу IP. Дата-центр містить кілька роутерів і світчей, які керують трафіком між серверами і «зовнішнім світом». Для надійності дата-центр іноді підключений до інтернету за допомогою безлічі різних зовнішніх каналів від різних провайдерів.

Деякі сервери в дата-центрі служать для роботи базових інтернет- і інтранет-служб, які використовуються всередині організації: поштові сервера, проксі-сервера, DNS-сервера і т.д.

Мережевий рівень безпеки підтримують міжмережеві екрани, VPN-шлюзи, IDS-системи тощо. Також використовуються системи моніторингу трафіку і деяких додатків.

Література

1. <https://valtek.com.ua/ua/system-integration/it-infrastructure/data-centers/engineering-infrastructure/data-center>
2. <https://www.infocom.ua/services/tsentr-obrobky-danykh>

АРХІТЕКТУРА БЕЗДРОВОЇ МЕРЕЖІ НА БАЗІ СТАНДАРТУ 802.11

При побудові бездротової мережі використовуються два типи архітектури мережі: розподілена (WDS) і централізована. Для організації розподіленої мережі необхідно встановити точки доступу AP.

AP об'єднують в одному пристрої функціональність мережевого контролера ірадіотрансивера, тобто може працювати як на прийом, так і на передачу. WDS технологія дозволяє AP для бездротового з'єднання не тільки з бездротовими клієнтами, а й між собою. З'єднання WDS ґрунтуються на MAC-адресах і використовують спеціальний тип кадрів, в яких задіяні всі чотири поля для MAC-адрес, певним стандартом 802.11, замість трьох, як при звичайній передачі даних між точкою доступу і клієнтом. Основний недолік такої мережі - це відсутність єдиного керуючого компонента. Тому застосування такої технології деколи буває обмежене. Крім того, WDS архітектура підтримує лише WEP-шифрування, яке забезпечує менший ступінь захисту мережі в порівнянні з WPA-шифруванням, а, отже, захищеність мережі знижується.

При централізованій архітектурі Wi-Fi мережу поділена на два рівні: рівень управління і рівень підключення.

Рівень управління реалізується на основі спеціалізованих контролерів доступу, які керують доступом з аутентифікацією і авторизацією користувачів, генерацією та зберіганням ключів шифрування.

Рівень підключення організовується на базі точок доступу, завдання яких полягає в шифруванні даних в радіоканалі і взаємодії з контролером доступу.
Складові мережі Wi-Fi:

Під компонентами мережі мається на увазі фізичне обладнання, яке необхідно для побудови архітектури мережі і забезпечення всіх її вимог.

На початковому етапі розвитку Wi-Fi мережі поширеним компонентом була точка доступу (AP). З розвитком технологій з'явилися пристрої, здатні об'єднувати в собі відразу кілька функцій. На зміну AP прийшов роутер, який має більш розширені можливості. Отже, основними компонентами Wi-Fi мережі є:

- ✓ контролер WiFi, який виконує функцію управління.
- ✓ роутер, або як його ще називають маршрутизатор.
- ✓ Wi-Fi адаптер.

Висновок. Потрібно відмітити, що централізована архітектура забезпечує високий рівень безпеки мережі, тобто на точках доступу не зберігається якась важлива конфіденційна інформація. Ще одна перевага полягає в тому, що при

переході від однієї точки доступу до іншої користувач не втрачає з'єднання з мережею, і йому не доводиться проходити аутентифікацію заново.

Література

1. Джим Гейер. Беспроводные сети. Первый шаг [Электронный ресурс]. URL: http://www.lan23.ru/books/Wi-Fi_2.pdf.
2. Rolf de Vegt. 802.11ac Usage Models Document. Qualcomm, Inc. Santa Clara. January 22, 2009.
3. R. Watson. Understanding the IEEE 802.11 ac Wi-Fi Standard . 2012, 10с.
4. 802.11ac Technology Introduction. Rohde & Schwarz GmbH & Co. KG Munchen 2012, 29с.
5. 802.11ac: The Fifth Generation of Wi-Fi. Cisco Systems. 2012, 25с.

Криворот І.А.

*Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій та інформатизації
Факультет Інформаційних технологій
м.Київ*

ДОСЛІДЖЕННЯ МОДЕЛІ ВЗАЄМОДІЇ ІНТЕРНЕТ РЕЧЕЙ З ДОПОВНЕНОЮ ТА ВІРТУАЛЬНОЮ РЕАЛЬНІСТЮ

Термін "інтернет речей" ("Internet of Things" , IoT) вперше був сформульований ще у 1999 році. Саме поняття представляє цілу концепцію комунікаційної мережі об'єктів ("речей"), які мають технології для взаємодії між собою та з оточуючим середовищем. Крім того, вони покликані виконувати певні дії без втручання людини. Тобто усі пристрої в домі, в авто та інших середовищах, самі обробляють інформацію, обмінюються нею та здатні виконувати різні дії в залежності від цієї інформації.

Кількісний перехід від «Інтернету людей» до «Інтернету речей» відбувся в 2008-2009 роках. Саме в той період кількість пристроїв, підключених до Інтернету, перевищила кількість інтернет-користувачів, а тому світ поступово перейшов у нову фазу розвитку технологій – Інтернету речей.

На сучасному етапі розвитку Інтернет речей (Internet of Things) в світі приділяється надзвичайно велика увага. За прогнозами аналітиків у найближчі роки очікується справжній бум Інтернет речей. Так, за прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн. доларів. Найбільші світові ІТ компанії, зокрема Intel, Google та ін. вже почали масштабну роботу на цьому ринку. Так корпорація Intel у 2014 році створила власний підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку. Компанія «Google» на початку 2014 року за 3,2 млрд. доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів. Спеціалісти компанії «Google» займаються широким впровадженням на американському ринку технологій IoT. Виробники

побутової техніки також працюють у цьому напрямку. Так на виставці CES 2014 у Лас-Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до Інтернет.

Ще чотири роки тому в Україні налічувалося приблизно 50 тисяч ІТ-фахівців. За підрахунками індійських фахівців їх влітку минулого року вже налічувалося 75 тисяч. За іншими оцінками на даний час, кількість ІТ-фахівців в Україні сягає 80-90 тисяч. Однак такі цифри стосуються організованого ІТ-ринку. Якщо врахувати частину фахівців, які працюють неформально, то в нашій країні кількість ІТ-фахівців сягає 100 тисяч. За реалістично-оптимістичними прогнозами кількість ІТ-фахівців в Україні до 2020 року може подвоїтися. Необхідно відзначити, що світовим лідером за кількістю ІТ-фахівців є Індія, а у Європі – Україна.

Концепція технології IoT полягає в тому, щоб всі предмети побуту, товари, вузли технологічних процесів тощо, оснащені вбудованими комп'ютерами та сенсорами і мають змогу обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею та виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції може бути система «розумний будинок», яка вже застосовується у країнах Європи. Вона контролює параметри навколишнього середовища, в залежності від цього регулює температуру у приміщенні. У зимовий період нагріваючи прилади, в залежності від температури повітря ззовні, вітру, часу доби без втручання людини регулюють інтенсивність опалення, що дозволяє значно зменшити споживання енергоносіїв.

Середовище роботи таких пристроїв не обмежується лише розумним будинком, воно може охоплювати більш глобальний простір. Наприклад, керування транспортом в місті згідно інформації, зібраної з камер на вулицях, розумний кондиціонер, що може відстежувати місце розташування свого власника і включатися, коли той прямує додому, а домашній холодильник – стежити за кількістю та асортиментом продуктів.

Велике зацікавлення технологією IoT представляє використання її для опрацювання інформації рухомих об'єктів, в першу чергу для автомобільного транспорту. Такі технології дають можливість діагностувати роботу автомобілів в процесі експлуатації, попереджати аварійні ситуації, замовляти необхідні запчастини та здійснювати пошук необхідної станції і встановлення часу обслуговування автомобіля.

Для об'єднання повсякденних речей у мережу потрібні декілька технологій.

- Для ідентифікації кожного об'єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати інформацію про певний предмет. Такий функціонал

можна забезпечити за допомогою чіпів RFID (Radio-Frequency IDentification). Вони здатні без власного джерела струму передавати інформацію приладам зчитування. Кожен чіп має індивідуальний номер. Як альтернатива для даної технології для ідентифікації об'єктів можуть використовуватись QR-коди. Для визначення точного місця знаходження речі може використовуватися технологія GPS, яка ефективно використовується вже сьогодні у смартфонах та навігаторах.

- Для відслідковування змін у стані елемента чи оточуючого середовища об'єкти оснащуються сенсорами.

- Для обробки та накопичення даних з сенсорів використовуються вбудовані комп'ютери.

- Для обміну інформацією між пристроями використовуються технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN).

Вже сьогодні існують рішення, здатні об'єднати різні програмні комплекси і різні пристрої в єдину екосистему. Інструментом для збору всього воедино є, наприклад, хмарні технології.

Виходячи з наведеного вище, виникає висновок, що на сьогодні вища освіта потребує перетворень направлених на задоволення потреб в інженерах і вчених, чия діяльність буде тісно пов'язана з технологією Інтернет речей.

Вже зараз основні роботи в області Інтернет речей ведуться за чотирма напрямками: розроблення технологій збору і обробки інформації, технологій передачі даних, створення можливостей для пристроїв приймати самостійні рішення і можливостей реалізації прийнятого рішення.

СЕКЦІЯ №3. БЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.

Перепелиця Ліна Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

При вирішенні другого завдання необхідно розрізняти визначення загроз інформаційній безпеці, наведені в навчальних джерелах, стосовно різних суб'єктів інформаційних відносин.

Загрози інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері.

До основних загроз інформаційній безпеці України, зазначають експерти, можуть бути віднесені обмеження свободи слова та доступу громадян до інформації, руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов, маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл, низький рівень інтегрованості України в світовий інформаційний простір тощо.

Всі загрози інформаційній безпеці поділяють на наступні основні групи:

- загрози шкідливого впливу відповідної інформації (недостовірної, шкідливої, дезінформації) на особистість, суспільство, державні інтереси;
- загрози несанкціонованого чи неправомірного впливу сторонніх осіб до інформації й інформаційних ресурсів фізичних та юридичних осіб, органів державної влади та місцевого самоврядування;
- загрози обмеженню інформаційних прав особистості, механізмам їх реалізації.
- Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають дестабілізуючими факторами.
- Джерелами дестабілізуючих факторів можуть бути:
- окремі особи, організації, різного роду об'єднання, інші держави та відповідно їх органи, організації, громадяни тощо;
- інформаційні системи та засоби, що є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин;
- природне середовище (катаклізми, природні стихії, катастрофи тощо).

- Види дестабілізуючих факторів можна поділити на:
- внутрішньодержавні дестабілізуючі фактори: правовий вакуум у більшості питань забезпечення інформаційної безпеки; порушення законодавства з питань інформаційної безпеки; політичні конфлікти; відмови, збої, технічні помилки інформаційних систем (засобів); природні явища, що ускладнюють передачу, прийом і зберігання інформації або руйнують інформаційні системи;
- міждержавні дестабілізуючі фактори, що виникли в результаті конфліктів міждержавних масштабів і проявів (між державами, організаціями та державами, організаціями чи особами різних держав): воєнні, економічні, політичні, терористично-ідеологічні тощо.

Підтримання національної безпеки є важливим напрямом державної діяльності, що актуалізується залежно від наявності та ступеня відповідних загроз. Виділяють (В.Є. Лепський) фактори, що впливають на складність забезпечення інформаційної безпеки.

Так, до політичних факторів відносять:

- зміну геополітичної обстановки внаслідок фундаментальних змін у різних регіонах,
- формування нових національних інтересів,
- становлення державності на основі демократичних принципів, законності, інформаційної відкритості,
- руйнування усталеної системи командно-адміністративного державного управління,
- інформаційну експансію розвинутих країн, які здійснюють глобальний інформаційний вплив, з метою поширення світогляду, політичних і духовних цінностей та ідеалів західного світу,
- посилення міжнародної співпраці на основі максимальної відкритості сторін,
- низький рівень політичної, правової та інформаційної культури в суспільстві.
- До соціально-економічних факторів відносять:
- труднощі переходу до ринкової економіки,
- продовження інфляційних процесів та падіння життєвого рівня населення,
- зростання безробіття, майнову поляризацію,
- поширення злочинності, криміналізацію суспільних відносин, погіршення показників здоров'я нації,
- зростання міжетнічної напруги.
- До духовних факторів належать:
- криза державної ідеології,

- деформація системи норм, установок та цінностей, що проявляється у неадекватності оцінки інформаційно-психологічного впливу,
- поява нових форм та засобів впливу на індивідуальну, групову й масову свідомість,
- поява й ріст нових форм міфологічної свідомості,
- недооцінка національних і культурно-історичних традицій та проникнення в суспільну свідомість шаблонів західної масової культури, науки, освіти, виховання та культури,
- послаблення важливих соціокультурних інститутів держави,
- недовершеність та недосконалість системи етичних норм в сфері інформаційної діяльності.
- Також вбачаються технологічні фактори, що значно ускладнюють забезпечення інформаційної безпеки:
- програмно-технічна неспроможність органів державної влади захистити власні інформаційні ресурси від несанкціонованого чи неправомірного доступу до них;
- технічна неспроможність інформаційної інфраструктури забезпечити інформаційні потреби всього населення держави тощо.

Література:

1. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.

Бойко Анна Александровна
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г. Киев

ТЕСТ НА ПРОНИКНОВЕНИЕ

Тест на проникновение или пентест — это попытка взлома информационного ресурса организации, направленная на получение объективной оценки уровня информационной безопасности исследуемого ресурса, обнаружение его уязвимостей и слабых мест. Тест на проникновение позволяет понять заказчику, эффективны ли используемые средства защиты, и какова вероятность взлома и получения информации злоумышленником.

Задача тестирования на проникновение — поиск всех возможных известных уязвимостей программного обеспечения (ПО), недостатков парольной политики, недостатков и тонкостей настроек конфигурации ИС. Во время подобного теста специалист-тестирующий устраивает псевдоатаку на корпоративную сеть, инсценируя действия реальных злоумышленников или атаку, проводимую вредоносным программным обеспечением без

непосредственного участия самого специалиста-тестировщика. Целью данных тестов является: выявление слабых мест в защите корпоративной сети от подобных атак и устранение найденных в ходе псевдоатак уязвимостей. [2]

Основные причины, по которым компании задумываются о проведении данного вида аудита следующие:

- Оценка существующей системы управления информационной безопасности;
- Оценка защищенности отдельных ресурсов или средств защиты организации;
- Анализ возможного ущерба от действий злоумышленников;
- Оценка действий персонала организации.

Основными объектами аудита являются внешние web-ресурсы и локальная сеть Заказчика.

При проведении теста помимо технических методик также используются методы социальной инженерии, позволяющие оценить уровень подготовки сотрудников в вопросах информационной безопасности. Может быть предпринята рассылка электронных писем, вынуждающих пользователей выполнить определенные действия, либо попытка узнать нужную информацию от сотрудников организации при помощи телефонного звонка в ИТ-службу. Все условия и действия заранее обговариваются и утверждаются с Заказчиком.

Основные этапы теста на проникновение:

- Анализ общедоступной информации о компании, и ее информационной среде;
- Проведение исследований связанных с социальной инженерией;
- Анализ уязвимостей внутренних и внешних ресурсов;
- Осуществление проникновения;
- Создание отчетной документации.
- По завершению работ формируется отчет, в котором представляется следующая информация:
- Детальное отображение выявленных уязвимостей и недостатков, представляющих угрозу для бизнес-процессов компании, уровень их рисков, оценка возможностей злоумышленника ими воспользоваться;
- Описание сценариев, при помощи которых проводилось проникновение;
- Подробное описание структуры объектов тестирования;
- Методы и средства, использованные во время проведения теста на проникновение;
- Рекомендации по устранению обнаруженных уязвимостей и недостатков.

Литература:

1. http://www.pointlane.ru/security_a/pentest/
2. <https://defcon.ru/penetration-testing/746/>
3. http://www.pointlane.ru/security_a/pentest/

SSL СЕРТИФИКАТ

Существует достаточно много цифровых сертификатов, каждый из которых служит для своих целей. Самые распространенный тип сертификатов это естественно SSL сертификаты, которые также имеют несколько подвидов. Также существуют Code Signing сертификаты, Website Anti Malware Scanner сертификаты и Unified Communications сертификаты.

SSL сертификаты самый распространенный на данный момент тип сертификатов в Интернет. Чаще всего они используются в интернет-магазинах, то есть на сайтах, где есть функция заказа и где клиент вводит свои персональные данные. Для того, чтобы эти данные в момент передачи из браузера на сервер невозможно было перехватить используется специальный протокол HTTPS, который шифрует все передаваемые данные. Для того, чтобы активировать возможность работы протокола HTTPS как раз и нужны цифровые SSL сертификаты (также потребуется выделенный IP для конкретного сайта).

Что такое SSL сертификат?

SSL — это сокращение от Secure Socket Layer — это стандартная интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером. SSL сертификат позволяет нам использовать https протокол. Это безопасное соединение, которое гарантирует, что информация которая передается от вашего браузера на сервер остается приватной; то есть защищенной от хакеров или любого, кто хочет украсть информацию. Один из самых распространенных примеров использования SSL — это защита клиента во время онлайн транзакции (покупки товара, оплаты).

Какие данные содержит в себе SSL сертификат?

В сертификате хранится следующая информация:
полное (уникальное) имя владельца сертификата

- открытый ключ владельца
- дата выдачи ssl сертификата
- дата окончания сертификата
- полное (уникальное) имя центра сертификации
- цифровая подпись издателя

Что такое центры сертификации (CA)?

Это организация, которая обладает правом выдачи цифровых сертификатов. Она производит проверку данных, содержащихся в CSR, перед

выдачей сертификата. В самых простых сертификатах проверяется только соответствие доменного имени, в самых дорогих производится целый ряд проверок самой организации, которая запрашивает сертификат. Об этом мы поговорим ниже.

Так вот, разница между самоподписными бесплатным и платными сертификатами, выданными центром сертификации как раз и заключается в том, что данные в сертификате проверены центром сертификации и при использовании такого сертификата на сайте ваш посетитель никогда не увидит огромную ошибку на весь экран.

Говоря в общем, SSL сертификаты содержат и отображают (как минимум одно из) ваше доменное имя, ваше название организации, ваш адрес, город и страну. Также сертификат всегда имеет дату окончания и данные о центре сертификации, ответственного за выпуск сертификата. Браузер подключается к защищенному сайту, получает от него SSL сертификат и делает ряд проверок: он не просрочен ли сертификат, потом он проверяет, выпущен ли сертификат известным ему центром сертификации (CA) используется ли сертификат на сайте, для которого он был выпущен.

Если один из этих параметров не проходит проверку, браузер отображает предупреждение посетителю, чтобы уведомить, что этот сайт не использует безопасное соединение SSL. Он предлагает покинуть сайт или продолжить просмотр, но с большой осторожностью. Это последнее, что вы должны увидеть ваши потенциальные клиенты.

Центров сертификации существует достаточно много, вот перечень самых популярных:

- Comodo — работает с 1998 штабквартира в Jersey City, New Jersey, США.
- Geotrust — основан в 2001, в 2006 продан Verisign, штабквартира Mountain View, California, США
- Symantec — бывший Verisign в состав которого входит и Geotrust. Купил всех в 2010 году.
- Thawte — основан в 1995, продан Verisign в 1999.
- Trustwave — работает с 1995, штабквартира Chicago, Illinois, США.

Как видим самый крупный игрок на рынке SSL сертификатов это Symantec, который владеет тремя крупнейшими центрами сертификации — Thawte, Verisign и Geotrust.

Между собой сертификаты отличаются свойствами и уровнем валидации. Типы сертификатов по типу валидации

Сертификаты, которые подтверждают только доменное имя (Domain Validation — DV).

- Сертификаты, которые подтверждают домен и организацию (Organization Validation — OV).
- Сертификаты, с расширенной проверкой (Extended Validation — EV).

Разберемся с ними по порядку:

Сертификаты, подтверждающие только домен.

Это самые простые сертификаты, это ваш выбор если сертификат вам нужен срочно, так как выпускаются они автоматически и моментально. При проверке такого сертификата отсылается письмо со специальной ссылкой, по которой нужно кликнуть, чтобы подтвердить выпуск сертификата. Сертификаты с валидацией организации.

В таком сертификате уже будет указано название организации. Такой сертификат частное лицо получить не может. Срок выдачи таких сертификатов как правило от 3 до 10 рабочих дней, зависит от центра сертификации.

Сертификаты с расширенной проверкой.

Это самые дорогие сертификаты и получить их сложнее всего. В таких сертификатах есть так называемый «green bar» — то есть при входе на сайт, где установлен такой сертификат в адресной строке браузера посетителя появится зеленая строка, в которой будет указано название организации, получившей сертификат.

Вот как это выглядит на сайте.

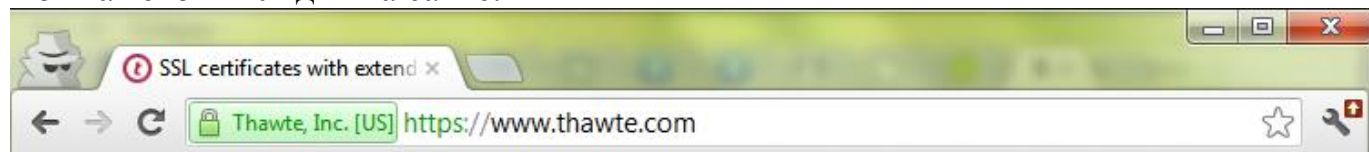


Рисунок 1. EV сертификат

Такие сертификаты обладают наибольшим уровнем доверия, среди продвинутых посетителей вашего сайта, поскольку сертификат указывает, что компания реально существует, прошла полную проверку и сайт действительно принадлежит ей.

SSL сертификаты с расширенной проверкой (EV) выпускаются только когда центр сертификации (CA) выполняет две проверки, чтобы убедиться, что организация имеет право использовать определенный домен плюс центр сертификации выполняет тщательную проверку самой организации. Процесс выпуска сертификатов EV стандартизирован и должен строго соответствовать правилам EV, которые были созданы на специализированном форуме CA/Browser Forum в 2007 году. Там указаны необходимые шаги, которые центр сертификации должен выполнить перед выпуском EV сертификата:

1. Должен проверить правовую, физическую и операционную деятельности субъекта.
2. Должен убедиться, что организация соответствует официальным документам.
3. Необходимо убедиться, что организация имеет исключительное право на использование домена, указанного в сертификате EV.

4. Необходимо убедиться, что организация полностью авторизована для выпуска EV сертификата.

Список того, что конкретно будут проверять такой же как и для сертификатов с проверкой организации EV сертификаты используются для всех типов бизнеса, в том числе для государственных и некоммерческих организаций. Для выпуска необходимо 10-14 дней.

Вторая часть правил актуальная для центра сертификации и описывает критерии, которым центр сертификации должен соответствовать перед тем, как получить разрешение на выпуск EV сертификата. Она называется, EV правила аудита, и каждый год происходит проверка на соответствие этим правилам.

Типы SSL сертификатов по своим свойствам.

Обычные SSL сертификаты

Тут все понятно, это сертификаты, которые выпускаются автоматически и подтверждают только домен.

SGC сертификаты

Сертификаты с поддержкой повышения уровня шифрования. Актуально для очень старых браузеров, которые поддерживали только 40 или 56 бит шифрование. При использовании этого сертификата уровень шифрования принудительно повышается до 128 бит. Wildcard сертификаты.

Нужны в том случае, когда вам кроме основного домена нужно обеспечить шифрование также на всех поддоменах одного домена. Например: есть домен domain.com и вам нужно установить такой же сертификат на support.domain.com, forum.domain.com и billing.domain.com SAN сертификаты.

Пригодится, если вы хотите использовать один сертификат для нескольких разных доменов, размещенных на одном сервере. Обычно в такой сертификат входит 5 доменов и их количество можно увеличивать с шагом в 5. EV сертификаты

Это те самые сертификаты с расширенной проверки и зеленой строкой в браузере, о которых мы говорили выше. Получить их может только юридическое лицо, коммерческая, некоммерческая или государственная организация.

Сертификаты с поддержкой IDN

Как правило, не у всех центров сертификации указана эта опция в описании сертификата, но не все сертификаты поддерживают работу с IDN доменами. Поэтому я просто приведу здесь список сертификатов, у которых есть такая поддержка

- Thawte SSL123 Certificate
- Thawte SSL Web Server
- Symantec Secure Site
- Thawte SGC SuperCerts
- Thawte SSL Web Server Wildcard

- Thawte SSL Web Server with EV
- Symantec Secure Site Pro
- Symantec Secure Site with EV
- Symantec Secure Site Pro with EV

Чем еще отличаются сертификаты между собой

- Скоростью выпуска. Быстрее всего выпускаются сертификаты с валидацией только домена, дольше всего с EV валидацией, от 7 рабочих дней.
- Количество перевыпусков сертификата — у большинства центров сертификации неограниченно. Требуется, если допустили ошибку в данных об организации.
- Гарантия — для некоторых сертификатов есть гарантия от 10.000 \$. Это гарантия скорее не для покупателя сертификата, а для посетителя сайта, где установлен сертификат. В случае если посетитель сайта с таким сертификатом пострадает от фрода и потеряет деньги, то центр сертификации обязуется их ему компенсировать до суммы указанной в гарантии. То есть центр сертификации как бы дает гарантию на свои сертификаты и что их невозможно установить на «левый» домен. На практике такие случаи мне не известны поэтому на этот параметр можно не обращать внимание.
- Бесплатный тестовый период — из платных сертификатов есть у symantec secure site, geotrust rapidssl, comodo positive ssl, thawte ssl web server. Также можете для тестов использовать бесплатные сертификаты: StartSSL™ Free
- Возврат средств — есть почти у всех сертификатов в течении 30 дней, хотя бывают и сертификаты без периода moneyback

Коваленко Елена Вадимовна
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

КРИПТОГРАФИЯ: БАЗОВЫЕ ЗНАНИЯ О НАУКЕ ШИФРОВАНИЯ

История

Формально криптография (с греческого — «тайнопись») определяется как наука, обеспечивающая секретность сообщения. Пионером, написавшим первый научный труд о криптографии, считается Эней Тактик, завершивший свой земной путь задолго до Рождества Христова. Свои данные пытались шифровать еще Индия и Месопотамия, но первые надежные системы защиты были разработаны в Китае. Писцы Древнего Египта часто использовали изощренные способы письма, чтобы привлечь внимание к своим текстам. Чаще всего

шифровка информации использовалась в военных целях: широко известен шифр «Скитала», примененный Спартой против Афин в V веке до н. э.

Криптография активно развивалась в Средние века, шифровками пользовались многочисленные дипломаты и купцы. Одним из самых известных шифров Средних веков называют кодекс *Scipiale* — изящно оформленную рукопись с водяными знаками, не расшифрованную до сих пор. Эпоха Возрождения стала золотым веком криптографии: ее изучением занимался Фрэнсис Бэкон, описавший семь методов скрытого текста. Он же предложил двоичный способ шифрования, аналогичный используемому в компьютерных программах в наше время. Значительное влияние на развитие криптографии оказало появление телеграфа: сам факт передачи данных перестал быть секретным, что заставило отправителей сосредоточиться на шифровке данных. Во время Первой мировой войны криптография стала признанным боевым инструментом. Разгаданные сообщения противников вели к ошеломляющим результатам. Перехват телеграммы немецкого посла Артура Циммермана американскими спецслужбами привел к вступлению США в боевые действия на стороне союзников.

Вторая мировая война послужила своеобразным катализатором развития компьютерных систем — через криптографию. Использованные шифровальные машины (немецкая «Энигма», английская «Бомба Тьюринга») ясно показали жизненную важность информационного контроля. В послевоенное время правительства многих стран наложили мораторий на использование криптографии. Ключевые работы публиковались исключительно в виде секретных докладов — таких, как, например книга Клода Шеннона «Теория связи в секретных системах», подходящая к криптографии как к новой математической науке.

Правительственная монополия рухнула только в 1967 году с выходом книги Дэвида Кана «Взломщики кодов». Книга подробно рассматривала всю историю криптографии и криптоанализа. После ее публикации в открытой печати стали появляться и другие работы по криптографии. В это же время сформировался современный подход к науке, четко определились основные требования к зашифрованной информации: конфиденциальность, неотслеживаемость и целостность. Криптография была разделена на две взаимодействующие части: криптосинтез и криптоанализ. То есть криптографы обеспечивают информации защиту, а криптоаналитики, напротив, ищут пути взлома системы.

Современные методы использования криптографии

Появление доступного интернета перевело криптографию на новый уровень. Криптографические методы стали широко использоваться частными лицами в электронных коммерческих операциях, телекоммуникациях и многих других

средах. Первая получила особенную популярность и привела к появлению новой, не контролируемой государством валюты — биткойна.

Многие энтузиасты быстро смекнули, что банковский перевод — штука, конечно, удобная, однако, для покупки таких приятных в быту вещей, как оружие или «вещества», он не подходит. Не подходит он и при запущенных случаях паранойи, ибо требует от получателя и отправителя обязательной аутентификации.

Аналоговую систему расчета предложил один из «шифропанков», о которых речь пойдет ниже, молодой программист Вэй Дай. Уже в 2009 году Сатоши Накамото (которого многие свято считают целой хакерской группировкой) разработал платежную систему нового типа — BitCoin. Так родилась криптовалюта. Ее транзакции не требуют посредника в виде банка или другой финансовой организации, отследить их невозможно. Сеть полностью децентрализована, биткойны не могут быть заморожены или изъяты, они полностью защищены от государственного контроля. В то же время биткойн может использоваться для оплаты любых товаров — при условии согласия продавца.

Новые электронные деньги производят сами пользователи, предоставляющие вычислительные мощности своих машин для работы всей системы BitCoin. Такой род деятельности называется майнинг (mining — добыча полезных ископаемых). Заниматься майнингом в одиночку не очень выгодно, гораздо проще воспользоваться специальными серверами — пулами. Они объединяют ресурсы нескольких участников в одну сеть, а затем распределяют полученную прибыль.

Крупнейшей площадкой купли-продажи биткойнов является японская Mt. Gox, через которую проводятся 67% транзакций в мире. Заядлые анонимы предпочитают ей российскую BTC-E: регистрация здесь не требует идентификации пользователя. Курс криптовалюты довольно-таки нестабилен и определяется только балансом спроса и предложения в мире. Предостережением новичкам может служить известная история о том, как 10 тысяч единиц, потраченных одним из пользователей на пиццу, превратились через некоторое время в 2,5 миллиона долларов.

Литература:

1. Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6
2. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
3. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.
4. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. СПб.: «Лань», 2000.

SYN FLOOD SPOOFING

Когда Сеть только зарождалась, большинство усилий программистов и разработчиков были направлены в основном на оптимизацию алгоритмов работы сетевых протоколов. Безопасность не была настолько критичной задачей, как сегодня, и ей, как часто это бывает, уделяли очень мало внимания. Как результат, получаем банальные и фундаментальные ошибки в сетевых протоколах, которые продолжают существовать и сегодня, несмотря на различного рода заплатки (ибо никакой заплатой не залатать логическую ошибку протокола). Здесь необходимы тотальные изменения, которые Сеть в существующем представлении просто не переживет.

Spoofed SYN — атака, при которой заголовки пакетов подделывается таким образом, что место реального отправителя занимает произвольный либо несуществующий IP-адрес. Клиент генерирует SYN-пакет, запрашивая новую сессию у сервера. Поскольку TCP сессия открыта (алгоритм “трехэтапного рукопожатия TCP” исполнен), хост будет отслеживать и обрабатывать каждую пользовательскую сессию, пока она не будет закрыта. Во время SYN-флуда атакуемый сервер с большой скоростью получает поддельные SYN-запросы, содержащие поддельный IP-адрес источника. SYN-флуд поражает сервер, занимая всю память таблицы соединений (Transmission Control Block (TCB) table), обычно используемую для хранения и обработки входящих пакетов. Это вызывает критическое падение производительности и, как итог, отказ в работе сервера.

Цель злоумышленника — поддерживать полуоткрытые соединения, ожидающие подтверждения, чтобы не допустить установления легитимных соединений.

Ввиду такой атаки, конечные пользователи не смогут установить связь с сервером, либо все-таки установят, но с некоторой задержкой. Все зависит от нагрузки сервера и мощности атаки.

Прошлое и настоящее спуфинга

Изначально термин «spoofing» использовался как термин сетевой безопасности, подразумевающий под собой успешную фальсификацию определенных данных с целью получения несанкционированного доступа к тому или иному ресурсу сети. Со временем этот термин начал употребляться и в других сферах инфобезопасности, хотя большинство так называемых old school специалистов и сегодня продолжают использовать слово «spoofing» только лишь для уточнения типа сетевых атак.

Литература:

IT-ресурс «Computerworld UK». URL: <http://computerworlduk.com/>

IT-ресурс «Хабрахабр». URL: <http://habrahabr.ru/>

СІМ СЕКРЕТІВ НАСТУПАЛЬНОЇ КІБЕРБЕЗПЕКИ

Звичні інструменти для забезпечення інформаційної і кібернетичної безпеки, такі як уніфіковані системи управління загрозами (UTM systems), брандмауери нового покоління та антивірусне програмне забезпечення часто занадто пізно приходять на допомогу, не мають користі для запобігання порушенням, і можуть лише «очистити місце злочину». Саме тому слід розглянути використання технік і моделей наступальної безпеки.

На відміну від антивірусного програмного забезпечення, яке реагує на факти експлуатації та зменшує шкоду після нападу, наступальна кібер-безпека (offensive cyber security) використовує проактивний підхід. Ця модель знаходить недоліки у Ваших системах, що підлягають обороні, і виправляє їх до того, як вони будуть використані для атаки ззовні.

Розглянемо сім тверджень, що допоможуть переосмислити безпеку Вашої організації.

1. Вся Ваша програмно-апаратна інфраструктура є вразливою.

Кібер-атаки переважно здійснюються на вразливості у Вашій інфраструктурі. Застарілі версії програмного забезпечення ПК, серверів, маршрутизаторів, операційних систем, браузерів, програм, плагінів, мережевих дисків часто мають серйозні вразливі місця.

Проте і сучасні технології несуть нові небезпеки. Інтернет речей (IoT) та мобільні додатки, такі, як Емої клавіатури, наразі є особливо популярними цілями для крадіжки даних. Наприклад, якщо Ви встановили клавіатуру смайликів і входите в свої облікові записи, Ваші ім'я користувача і пароль можуть бути перехоплені. Завжди перевіряйте правила конфіденційності та уважно перечитуйте всі дозволи, що Ви надаєте мобільним додаткам. В налаштуваннях пристрою Ви завжди можете перевірити, які дозволи мають встановлені додатки і змінити їх права. За можливості видаліть усі програми, яким Ви не можете повністю довіряти.

2. Якщо Ви не захиститеся від відомих вразливостей, вони будуть проексплуатовані.

На сьогодні існує більше, ніж 93 тисячі CVE (Common Vulnerabilities and Exposures) – загальних вразливостей та ризиків, і це число тільки зростає.

Необхідно досліджувати Ваші вразливі місця і, в першу чергу, позбуватись найкритичніших. Тут діє правило: «Якщо ти не захищаєш свої вразливості – вони будуть проексплуатовані».

Системи аудиту вразливостей від таких постачальників, як Trend Micro, Qualys, Rapid7 та Tenable, можуть допомогти Вам визначити їх. Також доступні безкоштовні альтернативи з відкритим вихідним кодом, наприклад, OpenVAS.

Виправляйте недоліки, які можна виправити, і перевіряйте свої системи постійно. Якщо немає доступного патча – переналаштуйте систему.

3. Постійні резервні копії – Ваша перша лінія захисту.

Вимагацьке шкідливе ПЗ (Ransomware) не може шкодити Вам, якщо Ваші дані можна швидко відновити. Інвестуйте в рішення безперервного захисту даних (CDP), яке створює резервні копії файлів у режимі реального часу. Вони автоматично зберігають копії всіх змін, внесених користувачем до даних.

Вибраний продукт повинен працювати на всіх Ваших операційних системах. Перевірте програмне забезпечення, щоб переконатись, процес що відновлення працює та відповідає Вашим потребам, перш ніж розгортати його в організації.

4. Всебічне використання стійкого шифрування.

Стійке шифрування з належним управлінням ключами є дуже важливим і може вирішити багато проблем.

Крадіжка даних є марною, якщо Ви завжди шифруєте інформацію. Це означає, що при витоку даних кіберзлочинці не зможуть отримати нічого цінного. Для того, щоб це було справді ефективно – шифрування потрібно встановлювати всюди, щоб захистити дані як під час передачі, так і під час зберігання. Для впровадження єдиної системи шифрування слід провести інвентаризацію всіх пристроїв та систем Вашої організації: від персональних смартфонів співробітників до баз даних компанії і обрати засоби шифрування, які можуть захистити їх усіх.

5. Постійний тренінг працівників.

Ефективна підготовка – єдиний спосіб забезпечення розуміння та дотримання працівниками політики безпеки своєї організації. Security awareness – обізнаність щодо безпеки – є особливо важливим засобом запобігання корупції, фішингу, поширення троянів та вимагацького ПЗ (ransomware).

Серед основних ідей, що необхідно донести персоналу: слід використовувати складні паролі; правильно зберігати свої паролі (не на стікері на моніторі комп'ютера); не клікати на посилання в електронних листах, отриманих від невідомих користувачів; не залишати комп'ютер незаблокованим без нагляду і т.п.

Необхідно регулярно навчати персонал як уникати порушень. Для цього використовувати цікаві, візуальні методи. Також важливо надсилати працівникам оновлення про нові загрози та перевіряти їх знання.

6. Більшість витоків могли бути зупинені ще до того, як вони сталися.

Випереджайте експлуататорів, визначаючи Ваші вразливості і закриваючи прогалини у Вашому захисті для запобігання кібер-атакам. Аналіз першоджерел допоможе визначити їх. Слідкуйте за всіма Вашими CVE і попереджайте можливі діри в безпеці, досліджуючи і виправляючи вразливості.

7. Секрет припинення порушень – модель наступальної безпеки «безпека на основі часу».

Що Ви могли б зробити, щоб уповільнити успішне проведення експлуатації таким чином, щоб воно зайняло більше часу, ніж запобігання експлуатації? Звучить безглуздо, чи не так? А от і ні. Це і є модель «безпеки на основі часу» (TBS – Time Based Security). Стратегію розроблено експертом із інформаційної безпеки Вінном Швартау (Winn Schwartau). Його концепція полягає в тому, що єдиною справжньою метрикою системи захисту інформації є час, за який нападник зламав би її.

Підхід «безпеки на основі часу» (TBS) забезпечує просту та логічну альтернативу традиційній безпеці і може доповнити тестування на проникнення.

Література:

IT-ресурс «Computerworld UK». URL: <http://computerworlduk.com/>

IT-ресурс «CVE Mitre». URL: <http://cve.mitre.org/>

Чабан Богдан Валентинович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ЕТАЛОННА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ МЕРЕЖ

Комп'ютерні мережі будуються за багаторівневим принципом. Для організації зв'язку між комп'ютерами, необхідно спочатку розробити набір правил їх взаємодії, визначити мову їх "спілкування", тобто визначити зміст сигналів, що посилають комп'ютери. Ці правила та визначення називаються протоколом.

Для коректної роботи мережі використовується цілий ряд протоколів: наприклад, протокол управління фізичним зв'язком, встановлення зв'язку в мережі, доступу до ресурсів, тощо. Багаторівневу систему було створено з метою спрощення і впорядкування такої величезної кількості протоколів та зв'язків. Багаторівнева модель взаємодії передбачає реальну взаємодію (інтерфейси) лише із сусідніми рівнями (верхнім та нижнім) і віртуальну - виключно із аналогічним рівнем приймача лінії зв'язку.

Під реальною взаємодією будемо розуміти безпосередню взаємодію - передачу інформації. В такому випадку інформація залишається незмінною - в пункт призначення вона надходить у вигляді, ідентичному вигляду у пункті відправлення. Віртуальна взаємодія передбачає опосередковану передачу даних, коли останні можуть обумовленим способом змінюватись.

Наведемо приклад для ілюстрації процесів реальної та віртуальної взаємодії. Нехай директор однієї фірми (директорі) написав лист директорові іншої фірми (директор_2). Секретарі вкладає цей лист у конверт, пише адресу і передає на пошту. Пошта здійснює доставку за зазначеною адресою. Конверт отримує секретар_2, розкриває його і кладе лист на стіл директорові_2. Реальною в даній

схемі є лише взаємодія на рівні поштового транспорту - тобто в процесі перевезення листа з однієї точки в іншу. Всі інші - віртуальні, починаючи із взаємодії поштових відділень і закінчуючи найвищим рівнем директорі <-> директор_2. В такій моделі взаємодії директора не хвилюють проблеми відправлення листа, а секретар не повинен знати про тонкощі перевезення поштової кореспонденції.

Саме такий підхід і є перевагою багаторівневої моделі взаємодії відкритих систем ISO OSI (International Standards Organization, ISO; Open System Interconnection, OSI), і саме він дозволяє встановлювати зв'язок із будь-яким комп'ютером мережі Інтернет, довільної конфігурації, і яку би ОС на ньому не було встановлено. Розглянемо детальніше зазначену модель із характеристикою рівнів

Рівень 0 (канал зв'язку) пов'язаний із фізичним середовищем - передавачем сигналу і містить характеристики посередників, що з'єднують кінцеві пристрої: кабелі, радіолінії і т.п. Як правило, рівень 0 не зазначається в моделі ISO OSI, проте, знання його особливостей дозволяє налагодити стабільний зв'язок з точки зору фізичних з'єднань.

Рівень 1 (фізичний) містить фізичні аспекти передачі двійкової інформації лінією зв'язку. Детально описує, наприклад, напругу, частоту, природу середовища передачі. Відповідає за підтримку зв'язку та приймання/передачу бітового потоку.

Рівень 2 (канальний) забезпечує безпомилкову передачу пакетів через рівень 1, що може спотворювати дані (використовується завадостійке кодування). Визначає початок та кінець пакету в бітовому потоці.

Рівень 3 (мережний) використовує можливості, що надаються рівнем 2 для забезпечення зв'язку двох довільних точок в мережі. Маршрутизація пакетів та обробка адрес відбувається на цьому ж рівні.

Рівень 4 (транспортний) завершує організацію передачі даних - контролює правильність передачі пакетів, правильність доставки в потрібний пункт призначення, їх збереженість та послідовність надходження. Відновлює повідомлення шляхом злиття пакетів. Містить надійну схему адресації для забезпечення зв'язку через величезну кількість мереж та шлюзів.

Шлюз - станція зв'язку із довільною мережею. Забезпечує зв'язок несумісних мереж, а також взаємодію несумісних компонентів у рамках однієї мережі. Транспортний рівень відповідає за всі деталі та проблеми передачі даних. Забезпечує взаємодію вищих рівнів моделі з інформацією незалежно від технічної реалізації самого процесу передачі.

Рівень 5 (сеансовий) координує взаємодію користувачів - встановлює зв'язок, відновлює аварійно завершені сеанси. Відповідає за картографію мережі - перетворює регіональні (доменні) комп'ютерні імена у числові адреси і навпаки. Підтримує процеси в мережі та їх взаємодію.

Рівень 6 (представлення даних) оперує синтаксисом та семантикою інформації, що передається, тобто встановлює "порозуміння" між двома комп'ютерами. Тут вирішуються задачі перекодування (всім, напевно, траплялись повідомлення у вигляді набору незрозумілих символів -наприклад, при передачі українського тексту без перетворення кодом Windows CP1251); підтримка зображень, стиск та розпакування файлів, підтримка мережних файлових систем (Network File System, NFS), тощо.

Рівень 7 (прикладний) забезпечує інтерфейс між користувачем і мережею, підтримує доступ користувача до різноманітних послуг мережі. На цьому рівні реалізуються, як мінімум, п'ять прикладних служб: передача файлів, віддалений термінальний доступ, електронна передача повідомлень, довідкова служба та управління мережею. Визначається користувачем відповідно до його потреб, можливостей та фантазії.

Література:

1. <http://petroonline.ho.ua/OSI.html>
2. http://pidruchniki.com/18301025/informatika/etalonna_model_vzayemodiyi_v_idkritih_merezh_sistem

Світлина Ольга Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ ТА ПРОБЛЕМИ ЇЇ РОЗВИТКУ

Сфера зв'язку та інформатизації є одним із пріоритетних і важливих напрямків економіки України. Вона створює інноваційну складову в соціально-економічному розвитку держави, демонструючи упродовж десятиліть стійку динаміку росту. Сталий розвиток інформаційно-телекомунікаційної інфраструктури є найважливішою передумовою для підвищення конкурентоспроможності економіки та інтеграції України у глобальне інформаційне суспільство, дозволяє розширити можливості людини отримувати доступ до національних та світових інформаційних ресурсів, поліпшити умови та якість життя.

Загальновідомим є той факт, що телекомунікації України значно відстають від телекомунікацій розвинутих країн як за обсягами, так і за рівнем технологій.

Взагалі, галузь телекомунікацій в Україні поділяється на два крупних сегменти: електрозв'язок та поштовий зв'язок. Електрозв'язок має два основні напрями: наземний (фіксований чи дротовий) та радіозв'язок. До першої групи, як правило, включають телефонний, телефонний міський, телефонний сільський, телефонний міжміський, телефонний міжнародний зв'язок. Сюди ж можна віднести Інтернет (хоча зараз Інтернет переміщується й у радіозв'язок). До другої групи належать супутниковий, стільниковий, пейджинговий, транкінговий зв'язок.

Основними проблемами розвитку ринків телекомунікацій є:

- повільне впровадження на мережах рухомого (мобільного) зв'язку радіотехнологій третього та четвертого поколінь (3G, 4G) для забезпечення держави та її громадян усіма перевагами сучасних телекомунікаційних мереж та послуг;
- нерівномірність забезпечення споживачів (особливо у сільській, гірській місцевості і депресивних регіонах) телекомунікаційними послугами, у тому числі загальнодоступними та послугами ШСД до Інтернету;
- необхідність модернізації телекомунікаційних мереж фіксованого місцевого зв'язку (наявність значної кількості аналогових комутаційних станцій), впровадження процедури встановлення внутрішньозонових з'єднань із використанням семизначних зонових абонентських номерів; затримка із впровадженням на мережах фіксованого та рухомого (мобільного) зв'язку послуги із перенесення абонентських номерів та неможливість забезпечити реалізацію права абонентів на вільний вибір постачальників послуг у повному обсязі;
- невідповідність існуючих нормативно-правових та нормативно-технічних документів галузі сучасному стану та перспективам розвитку телекомунікаційної мережі загального користування інформаційно-телекомунікаційних технологій та потребам ринку телекомунікацій України;
- втрата значного сегменту ринку телекомунікацій України внаслідок тимчасової окупації території Автономної Республіки Крим та м. Севастополь, зменшення доходів українських операторів від надання телекомунікаційних послуг та надходжень до державного бюджету;
- погіршення сталості функціонування телекомунікаційних мереж на тимчасово окупованих територіях та на території проведення антитерористичної операції, виникнення організаційних та технологічних проблем взаємодії таких мереж з іншими телекомунікаційними мережами на території України;
- порушення майнових прав суб'єктів ринку телекомунікацій України на тимчасово окупованій території, втручання у роботу телекомунікаційних мереж загального користування, збройне захоплення об'єктів і ліній зв'язку та перешкоджання здійсненню підприємницької діяльності.

Пропозицій до розв'язання проблеми може бути багато, але ми розглянемо саме такі, які є прийнятними для тих умов, що склалися на українському ринку телекомунікацій. Це такі пропозиції:

- підвищити технологічний рівень галузі.
- усунути монополію на ринку.
- створити належне законодавче підґрунтя функціонування галузі.
- підвищити рівень телефонізації по всій території країни.
- створити сприятливий інвестиційний клімат для залучення іноземних інвестицій у галузь.
- виділяти належні кошти на наукові дослідження всередині галузі.

Література:

1. В.Цхведиани. Телекоммуникации Украины – перспективы развития и основные проблемы // Фондовый рынок. - №16. – 2000.
2. Н. Васильева. Основні тенденції розвитку ринку інформаційних технологій та комунікацій // Економіст. - №10. – 2000.
3. С.О.Довгий. Стан та проблеми розвитку телекомунікаційної мережі України // Наука та наукознавство. - №3. – 2000.
4. KM-inform IT magazine (про українські телекомунікації) // www.km-inform.com.ua/communication/communication.shtml?4
5. О. Шевчук. О телекоммуникациях Украины // www.fas.com.ua/

Світліна Ольга Сергіївна

*Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

КОНЦЕПЦІЯ ТА АРХІТЕКТУРА ЗАХИСТУ ІНФОРМАЦІЇ

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленістю, довгостроковим збереженням великого об'єму даних на магнітних та оптичних носіях, одночасним доступом до ресурсів багатьох користувачів.

У цих сучасних умовах необхідність вживання заходів захисту, напевно, не викликає сумнівів. Однак існують певні труднощі:

- немає єдиної теорії захисту систем;
- виробники засобів захисту, в основному, пропонують окремі компоненти для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;
- для забезпечення надійного захисту необхідно розв'язати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

Для подолання перерахованих вище труднощів, необхідна координація дій всіх учасників інформаційного процесу як на окремому підприємстві, так і на державному рівні.

Концепція захисту інформації - офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її рішення з урахуванням сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів для її реалізації. На базі сформульованих у концепції цілей, задач і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки.

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту.

Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки:

- аналіз засобів захисту;
- визначення факту вторгнення.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації (рис.1.1).

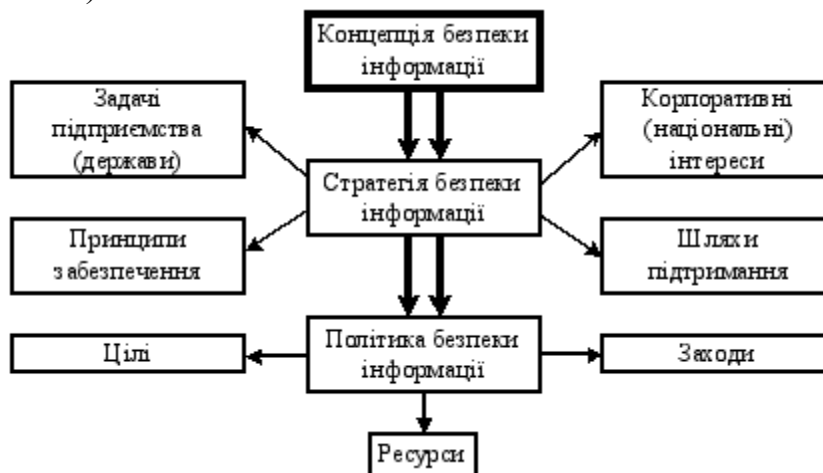


Рис. 1.1 Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендується проводити в три етапи (рис. 1.2).

На першому етапі повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільно диференціювати по значимості окремі об'єкти, що вимагають захисту.

На другому етапі повинен бути проведений аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту.



Рис. 1.2 Етапи розробки концепції захисту інформації

Головною метою третього етапу є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту.

Концепція захисту повинна містити перелік організаційних, технічних і інших заходів, що забезпечують максимальну безпеку при заданому залишковому ризику і мінімальні витрати на їх реалізацію.

Політика захисту - це загальний документ, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Сам по собі документ складається з декількох сторінок тексту. Він формує основу фізичної архітектури мережі, а інформація, що знаходиться в ньому, визначає вибір продуктів захисту. При цьому, документ може і не включати список необхідних закупок, але вибір конкретних компонентів після його складання повинен бути очевидним.

Політика захисту повинна обов'язково відображати наступне:

- контроль доступу (заборона на доступ користувача до матеріалів, якими йому не дозволено користуватися);
- ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);
- облік (запис усіх дій користувача в мережі);
- контрольний журнал (журнал дозволяє визначити, коли і де відбулося порушення захисту);
- акуратність (захист від будь-яких випадкових порушень);
- надійність (запобігання монополізації ресурсів системи одним користувачем);
- обмін даними (захист усіх комунікацій).

Один з найпростіших способів реалізувати захист - доручити зайнятися цим спеціалізованій компанії.

Література:

1.Гребенніков В.О *Аналіз розвитку телекомунікацій незалежної України.*

. "Зв'язок" №2 2010.

2.Звіт Національної комісії з питань регулювання зв'язку. // *Режим доступу:*

<http://www.nkrzi.gov.ua/uk/> ;

3.https://uk.wikipedia.org/wiki/Телекомунікації_в_Україні .

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян.

Комплексна система захисту інформації (далі КСЗІ) – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу. У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом. Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

У процес створення КСЗІ залучаються такі сторони:

- організація, для якої здійснюється побудова КСЗІ (Замовник);
- організація, що здійснює заходи з побудови КСЗІ (Виконавець);
- Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) (Контролюючий орган);
- організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);
- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації. Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх змінних параметрах. Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, заземлення та інші. Залежно від виду та форми подання інформаційних сигналів, які циркулюють в інформаційно-телекомунікаційній системі (ІТС), у тому числі і в автоматизованих системах (АС), при побудові КСЗІ можуть використовуватися різні засоби захисту.

У побудові КСЗІ можна виділити наступні етапи:

- підготовка організаційно-розпорядчої документації.
- обстеження інформаційної інфраструктури Замовника.
- розробка "Технічного завдання на створення КСЗІ".
- розробка "Плану захисту інформації".
- розробка "Технічного проекту на створення КСЗІ".
- приведення інформаційної інфраструктури Замовника у відповідність з "Технічним проектом на створення КСЗІ".
- розробка "Експлуатаційної документації на КСЗІ".
- впровадження КСЗІ.
- випробування КСЗІ.

Виконавцем робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення КСЗІ. Для проведення інших видів робіт з ТЗІ, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії. Якщо для створення КСЗІ необхідно провести роботи з

криптографічного захисту інформації, виконавець повинен мати ліцензію на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Література:

1. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
2. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005.-432 с.
3. Борсуковский Ю. Подходы и решения : Информационная безопасность // Мир денег. - 2001. - № 5. - С. 41-42
4. Інформаційна безпека України: проблеми та шляхи їх вирішення // Національна безпека і оборона. - 2001. - № 1. - С. 60-69
5. <http://altersign.com.ua/>
6. <http://www.dsszzi.gov.ua/dsszzi/control/uk/index>

Веселков Никита Леонидович
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

ЭЛЕКТРОННАЯ ПОДПИСЬ И СТАНДАРТЫ ЕЕ ПРИМЕНЕНИЯ В УКРАИНЕ

В 1976 году Уитфилд Диффи, Мартин Хеллманом и Ральф Меркле первыми предложили «одностороннюю функцию-ловушку» — теорию, которая позволяла передать зашифрованное сообщение без передачи ключа для разгадывания послания.

Электронная подпись — это реквизит электронного документа, который был образован в результате криптографического преобразования (чаще всего шифрования) с использованием закрытого ключа подписи для того, чтобы проверить целостность, авторство или неотказуемость электронного документа. По сути, электронная подпись является электронной печатью, которая скрепляет и заверяет документ. Чаще всего, для защиты информации, которая находится в подписи ее приходится шифровать.

Для построения электронной подписи используют схемы, основанные на:

- алгоритмах **симметричного** шифрования
- алгоритмах **асимметричного** шифрования

При создании подписи асимметричным методом (который является самым распространённым) генерируются закрытый и открытый ключи, при этом сначала подбирается из набора ключей закрытый, а потом в пару ему открытый. Закрытие ключи бывают двух форматов:

OpenPGP - ключи создавались на основе так называемых сетей доверия. Такая идея подразумевает, что обмениваются подписями люди, которым третья сторона для их взаимоотношений не нужна.

X.509 – ключ, сертификаты которого выдаются строго третьей стороной - гарантом вашей личности: Удостоверяющим Центром (УЦ).

Так как документы, на которые ставиться подпись, слишком большие, то подпись ставиться не на сам документ, а на его хэш, это ускоряет процесс обработки и сохраняет целостность документа, однако хэширование используется не всегда.

Электронные подписи являются “условно” безопасными. Это обусловлено тем, что любая подпись является уязвимой, однако воспользоваться этой уязвимостью крайне сложно, так как стоит учитывать, что при правильном (безошибочном) построении алгоритма подписи получение криптоаналитиком закрытого ключа алгоритма невозможна. Также для получения подписи можно подобрать коллизии первого и второго порядка, однако это также крайне сложно. Применение электронных подписей в Украине регулируется законом «**Про електронний цифровий підпис**», последняя поправка в который была внесена 02.11.2016. Данный закон мало чем отличается от зарубежных аналогов, однако в нем, как по мне, есть некоторые недочеты, к примеру не обозначено про манипуляции с подписями со стороны мошенников.

Литература:

- 1) *Интернет ресурс* ru.wikipedia.org
- 2) *Интернет ресурс* habrahabr.ru
- 3) *Интернет ресурс* www.docuSign.com
- 4) *Интернет ресурс* <http://zakon3.rada.gov.ua>

***Кравцов Олександр Анатолійович**
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ PORT-KNOSKING ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕКИ СЕРВІСУ ОБМЕЖЕНОГО ДОСТУПУ

Будь-який відкритий порт на веб-сервері представляє потенційну небезпеку. Зловмисники можуть сканувати сервер на відкриті порти за допомогою ПЗ nmap, дізнаватись версії запущених сервісів та їх найменування і здійснювати атаки на уразливі сервіси. Крім цілеспрямованих атак на сервіси зловмисники можуть застосовувати атаку на SSH, Telnet, FTP та HTTP-форми авторизації методом «грубої сили» (англ. bruteforce) . Такий тип атаки створює додаткове навантаження на сервер і без спеціального ПО, наприклад, fail2ban, яке блокуватиме невдалі спроби логіну, неможливо здійснити превентивні заходи для захисту сервера. Вибіркове блокування IP-адрес зловмисників в

IPTABLES або перенесення сервісу на інший порт буде лише тимчасовим рішенням.

Якщо відмовитись від деяких сервісів немає ніякої можливості, а підвищити безпеку системи все ж необхідно, можна використати програму knockd, яка дозволяє закрити взагалі всі порти, зберігши при цьому можливість роботи з усіма популярними сервісами, такими як SSH, FTP, HTTP і т.д.

Ідея knockd проста і геніальна. Наприклад, користувач хоче встановити зв'язок з іншим комп'ютером через SSH. Для цього на віддаленій машині повинен бути постійно відкритий порт 22. Knockd дозволяє за допомогою iptables закрити 22 порт для зовнішнього світу і відкрити в потрібний момент тільки потрібному IP. Як knockd визначає, коли відкрити порт і кому конкретно надати доступ?

У перекладі з англійської «to knock» - стукати. Щоб knockd впізнав «хазяїна» і відкрив потрібний порт потрібно «постукати» в заздалегідь обумовлені порти в заздалегідь обумовленій послідовності. Наведений нижче приклад конфігурації knockd добре ілюструє відкриття і закриття SSH:

[options]

logfile = /var/log/knockd.log

[openSSH]

sequence = 700,800,900 seq_timeout = 5 command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn

[closeSSH]

sequence = 900,800,700 seq_timeout = 5 command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn

В секції options потрібно вказати, куди зберігати логи підключень, в секції openSSH – умови для відкриття необхідного порту та сам порт в параметрах до команди IPTABLES, а в секції closeSSH – умови для закриття порту.

Якщо користувач спробує відкрити на віддаленій машині спочатку порт 700, потім 800, а потім 900, то knockd створить для фаєрвола нове правило, яке відкриває 22й порт для IP користувача. Після роботи користувач повинен закрити 22й порт, «постукавши» в зворотньому порядку: 900, 800, 700. Тепер про те, як «постукати». Зрозуміло, вручну відкривати будь-які порти не потрібно. Для зручності користувача існує команда knock. Приклад використання:

knock 127.0.0.1 700 800 900

Як перший аргумент вказується адреса сервера з knockd, всі інші аргументи є номерами портів, в які потрібно «постукати».

Примітки:

Для встановлення knockd на Ubuntu Server LTS 16.04 потрібно виконати команду в терміналі:

sudo apt-get install knockd

Конфігурація knockd на більшості серверних дистрибутивів Linux знаходиться за адресою /etc/knockd.conf. Після внесення змін в конфігурацію необхідно перезапустити демон knockd:

```
sudo /etc/init.d/knockd restart
```

Якщо потрібно налаштувати knockd для інших сервісів, потрібно openSSH, closeSSH в конфігурації замінити до прикладу на openFTP, closeFTP. Для повного розуміння принципу роботи knockd та більш детального налаштування (відкриття доступу для діапазону IP, відкриття доступу на певний час) бажано знати основи правил IPTABLES.

Література:

1. Інтернет-ресурси liberatum.ru, habrahabr.ru, wikipedia.org.

Мальгина Екатерина Вячеславовна
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРАТАКИ

Последние несколько лет на рынке информационной безопасности остро встал вопрос защиты от автоматизированных направленных атак, однако в общем понимании направленная атака в первое время представлялась как результат продолжительной и профессиональной работы организованной группой киберпреступников с целью получения дорогостоящих критичных данных. В настоящее время на фоне развития технологий, популяризации open-source форумов (напр. Github, Reddit) и Darknet, предоставляющих исходные коды вредоносного ПО и пошагово описывающих действия по его модификации (для невозможности его детектирования сигнатурным анализом) и заражению хостов, реализация кибератак значительно упростилась. Для реализации успешной атаки, сопровождающейся пагубными последствиями для владельцев автоматизированных и информационных систем, достаточно некомпетентного пользователя и энтузиазма в разборе предоставленного в сети Интернет / Darknet материала. Мотивом для осуществления подобной преступной деятельности является получение прибыли.

Вот основные шаги, которые позволят защитить себя от кибератаки:

1. Следите за тем, чтобы в системе были установлены все последние апдейты
Любая операционная система периодически получает обновления, многие из которых касаются сферы безопасности.

Желательно всегда использовать систему, которая получила самые свежие апдейты. Это может существенно снизить риски при вирусной атаке.

2. Задумайтесь о выборе операционной системе

Как бы не возражали сторонники Microsoft, но Windows значительно более уязвима для взлома и вирусов, чем Mac OS или различные дистрибутивы Linux.

И дело даже не в том, что *nix-системы имеют более совершенную архитектуру (хотя, многие уверены, что так и есть), а в том, что Windows больше распространена, а следовательно, является более интересной целью для злоумышленников.

Таким образом, можно с уверенностью утверждать, что купив MacBook или установив на свой компьютер Linux, вы снизите риск.

Также можно утверждать, что грамотно администрируемая сеть из Linux-компьютеров на предприятии является более защищенной от атак, чем сеть Windows-машин. Хотя тут, разумеется, возможно множество оговорок.

3. Используйте хорошие антивирусы

Эта информация в большей степени касается Windows-машин, хотя времена, когда антивирусы были совсем не нужны на Mac OS и Linux, давно прошли.

Не скупитесь на покупку хорошего антивируса, не доверяйте слепо тому, что встроен в Windows, и не пользуйтесь бесплатными антивирусами.

Компании, которые разрабатывают дорогие антивирусы, заботятся о своей репутации и стараются оперативно реагировать на угрозы, обновляя свои продукты.

4. Позаботьтесь о ликвидации последствий Petya.A

Вирус, атаковавший Украину в июне, был не финальным этапом атаки, а лишь подготовкой к последующим атакам. К такому выводу пришли некоторые эксперты, изучив механизм действия вируса.

В ходе кибератаки вирус активировал утилиту, которая использовала службу Kerberos в Microsoft Active Directory. Это давало злоумышленникам привилегированный доступ над ресурсами домена. Это “узкое” место в безопасности Microsoft Active Directory, поскольку ранее таких атак не было. И системные администраторы, как правило, даже не задумываются о смене пароля “юзера”, который отвечает за доступ к протоколу идентификации.

Теоретически, во время атаки Petya злоумышленники могли получать доступ к системе и генерировать бессрочный пароль на доступ к системе. Для этого даже не нужны административные права, подчеркивают эксперты.

Это значит, что у них может быть доступ и сейчас. И они лишь ждут подходящего момента для того, чтобы воспользоваться им. То был подготовительный этап, а настоящая атака еще может быть впереди.

Эксперты рекомендуют системным администраторам тех сетей, которые подвергались атаке, сменить все пароли к учетным записям в системе, а также обязательно сменить пароль пользователя krbtgt, который отвечает за доступ к службе Kerberos.

В настоящее время выпущены патчи, которые делают получение такого доступа к системе затруднительным. Это опять-таки указывает на необходимость регулярного обновления операционной системы.

5. Делайте бэкапы

Все важные данные должны иметь резервные копии. Причем, специалисты из CERT-UA рекомендуют хранить особо ценные данные в хранилищах, которые не подключены к интернету.

Это снизит шансы злоумышленников добраться до них, не имея физического доступа к хранилищам.

6. Пользователи должны быть осторожными

Рекомендация не открывать аттачменты в письмах от неизвестных адресатов существует едва ли не со времен появления сервиса электронной почты.

И тем не менее, это по-прежнему один из самых популярных способов распространения вирусов.

Представители украинского разработчика антивирусов Zillya рекомендуют системным администраторам вовсе запретить пользователям открывать из аттачментов файлы с расширением .zip и .exe.

Также стоит проявлять осмотрительность при переходе по ссылкам от неизвестных отправителей. Порой это тоже чревато последствиями.

7. Бдительность сисадминов

Очень велика роль системных администраторов предприятий. При первых появлениях признаков кибератаки, сисадмины должны обеспечить отключение сети от интернета. А также отключение хранилищ с важными данными. Порой физическое отключение является лучшим способом уберечь данные.

Литература:

- Овчинский В. С., Ларина Е. С. Кибервойны XXI века. О чём умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с. — ISBN 978-5-8041-0723-0.
- Киселёв В., Костенко А. Кибервойна как основа гибридной операции (рус.) // Армейский сборник : журнал. — 2015. — Ноябрь (т. 257, № 11). — С. 3-6.

Щебланин Александр Юрьевич

*Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г. Киев*

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сегодня искусственный интеллект сделала огромный скачок в своем развитии. За последние года эта технология стала очень популярной в различных сферах деятельности. К примеру, применение возможностей искусственного интеллекта (ИИ) позволит масштабировать бизнес и освободить сотрудников от множества повседневных задач чтобы перевести их на решение более комплексных проблем.

Для начала, что же такое ИИ? Искусственный интеллект — это свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. Так же существует 4 типа ИИ:

1. Реагирующий — основной вид ИИ, он воспринимает ситуацию или обстановку непосредственно такой, какая она есть и предлагает ответную реакцию. У него нет видения более широкого мира, выходящего за рамки этой ситуации. Он не формирует память и не может опираться на прошлый опыт,

чтобы выдать новое решение. И такой тип разрабатывается под одну конкретную сферу.

2. С ограниченной памятью - искусственный интеллект принимает во внимание части прошлой информации и добавляет их в запрограммированное ранее видение мира. Таким образом, он обладает достаточной памятью, чтобы принять нужное, правильное решение и выполнить надлежащее действие. Примеры этого типа интеллекта: самоуправляемые автомобили, чат-боты.

3. С теорией разума - тип может понимать мысли и эмоции, которыми руководствуются люди при своем поведении. Кроме того, он может распознать чувства, мотивы, намерения, ожидания, а также проявлять социальную вовлеченность. На самом деле такой тип находится еще в разработке. К примеру T-800 из фильма «Терминатор».

4. С самосознанием - тип может сформировать представление о самом себе. Как следующая ступень после 3 типа, он может осознавать внутреннее состояние, предсказать чувства других, составить картину ситуации и сделать логические выводы. Это - будущее ИИ, следующее поколение, "супер интеллект", обладающий чувствами и сознанием. К примеру робот из одноименного фильма «Робот Чаппи» [1].

В отличие от аналитиков и системных администраторов, которые могут просматривать только ограниченное количество случаев нарушения кибербезопасности, ИИ имеет возможность ежедневно анализировать миллионы событий и находить шаблоны, которые остаются незамеченными для людей. По данным IDG Research, фактически, 18% новых вредоносных программ остаются необнаруженными в течение первых 24 часов, а 2% остаются таковыми и спустя 3 месяца после первых случаев заражения. В этой ситуации искусственный интеллект становится стратегическим союзником безопасности предприятий, который позволяет сократить промежуток времени для обнаружения угроз и даже предвосхищать несостоявшиеся атаки. Использование интеллектуальных технологий повышает уровень обнаружения угроз, сокращая время реакции и совершенствуя техники, способные различать реальные попытки преодоления периметра безопасности вашей компании и инциденты, которые могут быть проигнорированы в силу отсутствия риска с их стороны. Однако искусственный интеллект еще не скоро заменит аналитиков по безопасности, но его преимущества очевидны.

Один из наиболее интересных способов применения ИИ – это машинное обучение, которое позволяет компьютерам анализировать огромные объемы данных и делать соответствующие выводы для выявления образцов поведения. Система всегда обучается и никогда не забывает, поэтому чем больше корпоративная система безопасности собирает информации, тем она будет более интеллектуальной [2].

Так же не мало важным является факт того, что аналитиков кибербезопасности недостаточно, что бы быстро выявлять угрозы и быстро разрешать эксплойт. В 2017 году 45% предприятий заявили, что у них «проблемный дефицит» специалистов кибербезопасности. Последние два года

этот критический уровень нехватки специалистов только растет. Тут ИИ может сыграть важную роль по замене рабочих мест.

Но есть и свой минус, человек, в отличие от алгоритма, может мыслить категориями из будущего. Поэтому нельзя рассчитывать, что ИИ будет делать сложную работу за людей. Хотя искусственный интеллект не заменит аналитиков по кибербезопасности совсем, но он может значительно упростить им работу. Например, исследователи из MIT Computer Science и лаборатории CSAIL разработали систему ИИ, которая использует контролируемое обучение для поиска угроз и представления отчета о них. После того, как аналитик в течение нескольких недель «учит» систему различать реальные угрозы безопасности и ложные тревоги, в конечном счете, она минимизирует количество ложных тревог, отмечая лишь значительные события, которые системный администратор потом может исследовать.

Компания IBM тоже занялась реализацией идей о ИИ используя за основу так называемый Watson (как говорится в официальных документах, программно-аппаратный комплекс, способный отвечать на вопросы на естественном языке, или некая реализация искусственного интеллекта). В IBM хотят научить Watson обрабатывать большой поток связанной с ИБ информации, так, чтобы суперкомпьютер мог «отличать вирусы от троянов». Для этого IBM будет сотрудничать с рядом американских университетов, студенты которых будут соответствующим образом готовить информацию для дальнейшей обработки. Данных получится много, речь идет о миллиардах записей [3].

От ИИ пользы конечно много, но не нужно забывать и то, что любая технология может стать оружием в информационных войнах. Она может использоваться как во благо, так и во вред. Не стоит забывать еще один очень важный момент, «Скайнет», из фильма Терминатор, был создан тоже во имя безопасности.

Литература:

- [1] <https://goldvoice.club/@marina-spring/vidy-iskusstvennogo-intellekta/>
- [2] <https://www.securitylab.ru/blog/company/PandaSecurityRus/342138.php>
- [3] <https://habrahabr.ru/company/kaspersky/blog/283536/>

*Ханун Анастасія Валеріївна
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

ПЕСИМІЗАЦІЯ. ЩО ЦЕ ТАКЕ І ЯК УНИКНУТИ?

На сьогоднішній день одним з найпопулярніших способів просування є оптимізація текстового контенту під пошукові системи. Це пояснюється досить високою ефективністю і відносною простотою. Але часто трапляються ситуації,

коли веб-майстри надмірно захоплюються оптимізацією текстів. Як результат, можна спостерігати переспам ключових слів або інші зловживання.

За такі провини пошукові системи передбачають покарання, саме воно має назву песимізація.

Головним змістом цих санкцій є зниження займаних позицій в пошуковій видачі. Крім того, в результаті песимізації може наступити ще один вкрай небажаний наслідок – сайт можуть відключити від посилання ранжирування.

Песимізація – це не новий термін в області пошукового просування. Його почали застосовувати розробники однієї популярної пошукової системи ще в 2003 році. Виділяють два типи песимізації: ручну і автоматичну. Розглянемо відмінності між цими явищами.

Автоматична песимізація відбувається в результаті перевірки сайту роботами пошукової системи. В ході перевірки, алгоритм визначає, що сторінка штучно переоптимізована. У підсумку місце сторінки в результатах пошуку істотно знижується.

Ручна песимізація передбачає накладання на ресурс певних санкцій, як відповідну реакцію на скарги користувачів про те, що Вам хтось продає рекламу. Зрозуміло, що недостатньо просто поскаржитися і сайт втратить позиції, – цією лазівкою б користувалися безліч недобросовісних конкурентів. Тому на скарги реагують компетентні кваліфіковані співробітники – модератори.

Песимізація не є незворотнім моментом. Всі негативні наслідки її застосування можна усунути. Але для цього веб-майстру доведеться виправити всі недоліки свого сайту. Після чого потрібно звернутися в службу підтримки для проведення повторного моніторингу.

Як уберегти сайт від песимізації?

Як ми визначилися, песимізація – це падіння рейтингу сайту у видачі. Це зниження є результатом накладання різних фільтрів. Пошукові системи використовують песимізацію для того, щоб зробити ТОП чистим від неякісних або недостатньо інформативних сайтів. Крім того, загроза песимізації тримає в рамках тих веб-майстрів, які тяжіють до сірих або чорних методів оптимізації.

Щоб не відчувати на собі і своєму ресурсі, що таке песимізація, потрібно користуватися тільки легальними методами розкрутки. Крім того, сайт повинен відповідати вимогам цільової аудиторії і бути корисним.

Ресурси максимально схильні до ризиків песимізації:

- Сайти з неунікальним контентом, який копіюється з інших сайтів.
- Сайти, які використовують сторінки з перенаправленням відвідувачів на сторонні ресурси.
- Ресурси, які наповнені переспамленими ключами вмістом.
- Сайти, які не несуть ніякої користі користувачеві.
- Сайти, які займаються бездумним обміном неревалентних посилань.

Слід відрізнити бан і песимізація. Перше означає, що пошукова система повністю виключає ваш сайт з індексу. Друге ж передбачає штучне «притримування» пошуковими системами, тобто сайт продовжує індексуватися, але результати ранжирування будуть занижені.

Література:

Welant.com. [SEO Glossary: Pessimization, Supplemental Results, Snippets](#)

Вовк Надія Ігорівна

Держаний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

РОЛЬ І МІСЦЕ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Із збільшенням кількості інформації в сучасному суспільстві збільшується потреба у висококваліфікованих фахівцях на ринку праці. Таким чином постає питання про компетентність сучасних спеціалістів в їхній галузі, вміння володіти, опрацьовувати та подавати інформацію з різних джерел. Особливо це питання стосується педагогів, які посідають важливе місце в навчанні майбутніх спеціалістів. Звідси впливає нова проблема про вміння користуватися та застосовувати в навчальному процесі інформаційних технологій[1].

Сучасні інформаційні технології навчання, що використовуються в навчальному процесі, значною мірою сприяють розв'язанню актуальних проблем активізації навчально-пізнавальної діяльності.

Сучасна інформаційна технологія в освіті – це комплекс навчальних і навчально-методичних матеріалів, технічних та інструментальних засобів обчислювальної техніки навчального призначення, а також система наукових знань про роль і місце обчислювальної техніки в навчальному процесі, про форми і методи їх застосування для вдосконалення праці викладачів та студентів

Використання сучасної інформаційної технології дає можливість розкрити гуманітарний потенціал природничих дисциплін, пов'язаний із формуванням наукового світогляду, розвитком аналітичного та творчого мислення, суспільної свідомості та свідомого ставлення до оточуючого світу .

Особливого значення при використанні інформаційних технологій у навчанні набуває врахування і розвиток неформалізованих, творчих компонентів мислення: реалізація проблемної ситуації чи постановка задачі; самостійне формування критеріїв добору потрібних операцій, що приводять до розв'язку задачі; генерація здогадок і гіпотез у процесі пошуку основної ідеї розв'язання (наукова, технічна фантазія, що не зводяться комбінаторних та генерації випадкових станів) [2].

Безумовним виміром якості продукції вищої освіти як сектора національної економіки є людський капітал як сукупність певних якостей людини: здоров'я, природних здібностей, освіти, професіоналізму і мобільності. У суспільстві зростає попит на висококваліфікованих спеціалістів-універсалів, котрі мають не лише спеціалізовану професійну підготовку, але й успішно оволодівають навичками інноваційної, підприємницької та управлінської діяльності, максимально використовують індивідуальні здібності. Про зв'язок якості освітньої системи із загальною конкурентоспроможністю країни свідчить те, що в першу десятку країн світу з найвищим загальним індексом конкурентоспроможності входить 7 країн-учасниць Болонського процесу [3].

Запорукою підвищення якості освіти та забезпечення конкурентоспроможності випускників вишу на ринку праці є безперервне оновлення змісту освіти на основі новітніх досягнень культури, науки, техніки, зокрема застосування інноваційних методів при використанні інформаційних технологій у навчальному процесі.

Аналіз розвитку передових у економічному відношенні країн показує, що однією з основних умов, яка визначає прогресивний розвиток економіки, науки і культури в державі є інформатизація системи вищої освіти. Знання і навички, якими сьогодні оволодівають майбутні фахівці, у подальшому визначатимуть шляхи розвитку суспільства. Саме у вишах зосереджена найбільша кількість прогресивних та відкритих до науково-технічних інновацій людей, що суттєво полегшує впровадження інформаційних технологій у навчальний процес.

Використання сучасних інформаційних технологій у навчальному процесі дозволяє підвищити якість навчального матеріалу й підсилити освітні ефекти від застосування інноваційних педагогічних програм і методик, оскільки дає викладачам додаткові можливості для побудови індивідуальних освітніх траєкторій учнів. Застосування інформаційних технологій дозволяє реалізувати диференційований підхід до студентів з різним рівнем готовності до навчання [4].

Адаптивна система навчання з використанням інформаційних технологій має ряд переваг:

- дозволяє зменшити непродуктивні витрати живої праці вчителя, який в цьому випадку перетворюється в технолога сучасного навчального процесу, в якому провідна роль приділяється не стільки й не тільки навчальній діяльності педагога, скільки навчанню самих учнів;
- дає слухачам широкі можливості вільного вибору власної траєкторії навчання в процесі набуття знань;
- припускає диференціальний підхід до слухачів, заснований на визнанні того факту, що у них різний попередній досвід і рівень знань у вивчаємій галузі знань, кожен слухач приходить до процесу оволодіння новими знаннями зі своїм власним інтелектуальним багажем, який і визначає ступінь розуміння ним нового матеріалу і його інтерпретацію, тобто здійснюється перехід від оволодіння всіма учнями того самого матеріалу до оволодіння різними учнями різного матеріалу;

- підвищує оперативність і об'єктивність контролю й оцінки результатів навчання;
- гарантує безперервний зв'язок у відносинах "слухач-викладач";
- сприяє індивідуалізації навчальної діяльності (диференціація темпу навчання, важкості навчальних завдань і т.п.);
- підвищує мотивацію навчання;
- сприяє розвитку у слухачів продуктивних, творчих функцій мислення, росту інтелектуальних здібностей, формуванню операційного стилю мислення [5].

Література:

1. Основи нових інформаційних технологій навчання: Посібник для вчителів / Машбиць Ю.І., Гокуль О.О., Жалдак М.І. та ін./ за ред. Машбица Ю.І./Інститут психології ім. Г.С. Костюка АПН України. К.: ІЗМН, 1997. - 264с.
2. Шатров А. О проблеме информатизации образования / А. Шатров, Ю. Цевенков // Информатика и образование. – 1989. – №5. – С. 3-10.
3. Болонський процес - структурна реформа вищої освіти на європейському просторі. <http://kpi.ua/bologna/>
4. Иванников А.В. Перспективные информационные технологии в концепции информатизации высшего образования / А.В.Иванников, Ю.Л.Ижванов, А.О.Кривошеев //Компьютерные технологии в высшем образовании. Вып.1. - М.: Изд-во Моск. ун-та, 1994. - С. 23.
5. Демкин В.П., Можаяева Г.В., Яковлева А.Г. Адаптивное обучение на основе информационных технологий // Телематика 2003. Труды X Всероссийской научно методической конференции.Т.2.с.400 - 401.

Добреля Виталий Алексеевич
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев

МЕЖСАЙТОВЫЙ СКРИПТИГ

XSS (Cross-Site Scripting — «межсайтовый скриптинг») — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницувредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «внедрение кода».

Специфика подобных атак заключается в том, что вредоносный код может использовать авторизацию пользователя в веб-системе для получения к ней расширенного доступа или для получения авторизационных данных

пользователя. Вредоносный код может быть вставлен в страницу как через уязвимость в веб-сервере, так и через уязвимость на компьютере пользователя. Для термина используют сокращение «XSS», чтобы не было путаницы с каскадными таблицами стилей, использующими сокращение «CSS».

XSS находится на третьем месте в рейтинге ключевых рисков Web-приложений согласно OWASP 2013. Долгое время программисты не уделяли им должного внимания, считая их неопасными. Однако это мнение ошибочно: на странице или в HTTP-Cookie могут быть весьма уязвимые данные (например, идентификатор сессии администратора или номера платёжных документов), а там, где нет защиты от CSRF, атакующий может выполнить любые действия, доступные пользователю. Межсайтовый скриптинг может быть использован для проведения DoS-атаки.

Безопасность в Интернете обеспечивается с помощью многих механизмов, в том числе важной концепцией, известной как правило ограничения домена. Это правило разрешает сценариям, находящимся на страницах одного сайта, доступ к методам и свойствам друг друга без ограничений, но предотвращает доступ к большинству методов и свойств для страниц другого сайта.

Межсайтовый скриптинг использует известные уязвимости в web-приложениях, серверах (или в системных плагинах, относящихся к ним). Используя одну из них, злоумышленник встраивает вредоносный контент в содержание уже взломанного сайта. В результате пользователь получает объединенный контент в веб-браузере, который был доставлен из надежного источника, и, таким образом, действует в соответствии с разрешениями, предоставленными для этой системы. Сумев внедрить необходимый скрипт в веб-страницу, злоумышленник может получить повышенные привилегии в отношении работы с веб-страницами, cookies и другой информацией, хранящейся в браузере для данного пользователя.

Выражение «межсайтинговый скриптинг» первоначально означало взаимодействие уязвимого веб-приложения с сайтом злоумышленника таким образом, чтобы в контексте атакуемого домена был выполнен javascript-код, подготовленный злоумышленником (отражённая или хранимая XSS уязвимость). Постепенно определение стало включать в себя и другие способы внедрения кода, включая использование устойчивых и не относящихся к javascript языков (например, ActiveX, Java, VBScript, Flash и даже HTML), создавая путаницу среди новичков в сфере информационной безопасности. XSS уязвимости зарегистрированы и используются с середины 1990-х годов. Известные сайты, пострадавшие в прошлом, включают такие сайты социальных сетей, как Twitter, Вконтакте, MySpace, YouTube, Facebook и др.

Классификация

По каналам внедрения скрипта

Ошибки в браузере

Из-за ошибок браузер может выполнять скрипты в SVG, нарушать правило Same Domain Policy. Это серьёзные ошибки; после обнаружения их быстро закрывают, однако в переходный период опасными становятся практически все сайты Веб 2.0: форумы, вики, имиджборды. Если такая ошибка обнаружилась, рекомендуется, пока не вышло обновление, пользоваться другим браузером.

Бывают и более тонкие ошибки, которые проявляются при очень специфичных условиях и крупного урона не наносят. Такие ошибки могут не исправляться годами и выгоднее исправить сайт, чем ждать обновления браузера.

Отсутствие экранирования спецсимволов HTML

Намного чаще встречаются ошибки на сайтах. Чтобы браузер гарантированно не принял строку за тег HTML, требуется заэкранировать пять символов: "&<>". Сервер может экранировать не все символы (известный недостаток PHP), либо веб-программист просто забывает заэкранировать строку.

Обычно в базах данных текст хранится неэкранированным, и экранировать требуется все пользовательские строки каждый раз, когда они встраиваются в HTML.

Многие сайты позволяют форматирование текста с помощью какого-либо языка разметки (HTML, BBCode, вики-разметка). Часто не проводится полный лексический анализ языка разметки, а лишь преобразование в «безопасный» HTML с помощью регулярных выражений. Это упрощает программирование, однако требует досконального понимания, какими путями скрипт может проникнуть в результирующий HTML-код.

Через внедрение SQL-кода

Основная статья: **SQL-XSS**

Если сайт допускает внедрение SQL-кода, и выводит содержимое БД без всякого экранирования (то ли по незнанию, то ли в БД хранится готовый HTML-код, то ли автор точно знает, что «плохих» символов в БД нет), можно провести необычную атаку.

Внедрением SQL-кода записываем в БД «отравленную» страницу. Если кто-то получит доступ к этой строке БД, ему в браузер попадёт вредоносный скрипт.

Література:

1. Seth Fogie, Jeremiah Grossman, Robert Hansen, Anton Rager, Petko D. Petkov. XSS атаки: эксплуатация и защита = XSS Attacks: Cross Site Scripting Exploits and Defense. — Syngress, 2007. — 464 p. — [ISBN 1597491543](#).

Шевчук Я.А., Марченко В.В.
*Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м.Київ*

ЗАХИСТ БАНКІВСЬКОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Система безпеки СЕП є багатоступеневою. Вона не тільки включає засоби шифрування інформації на різних її рівнях, а й вміщує цілий комплекс технологічних та бухгалтерських засобів контролю за проходженням платежів у СЕП. Технологічний та бухгалтерський контроль забезпечується програмно на всіх рівнях, що дає змогу персоналу і учасникам СЕП слідувати за порядком проходження платежів як протягом дня, так і за підсумками його завершення.

Система електронних платежів Національного банку (СЕП) – державна банківська платіжна система, що забезпечує проведення міжбанківського переказу через рахунки, відкриті в Національному банку України.

В міжбанківських платежах використовується нова для України форма платіжних інструментів — електронний платіжний документ. Такий документ має встановлену форму і відповідні засоби захисту, що надаються НБУ кожному учаснику СЕП. Крім того, кожний банк—учасник СЕП може мати власну систему захисту внутрішньобанківських розрахунків.

Система безпеки СЕП розроблена з урахуванням таких вимог [1]:
система захисту охоплює всі етапи розробки, впровадження та експлуатації програмно-технічного комплексу СЕП;
система безпеки включає організаційні, технічні, апаратні і програмні засоби захисту;
в системі чітко розподілена відповідальність за різні етапи обробки та виконання платежів.

В системі виділені такі основні задачі захисту СЕП:

захист від зловживань (несанкціоноване розшифрування повідомлень, поява фальсифікованих повідомлень);
автоматичне протоколювання використання банківської мережі з метою локалізації порушників технології роботи в СЕП;
захист від технічних пошкоджень та збоїв в роботі обладнання (вихід з ладу апаратних та програмних засобів, поява перешкод в каналах зв'язку).

Захист банківської інформації в СЕП включає комплекс дій, пов'язаних з шифруванням інформації, що циркулює в платіжній системі. Шифруванню підлягають усі файли СЕП: початкові і зворотні платіжні файли, файли

квитанцій, файли звітів, файли лімітів, файли стану коррахунку, файли нормативно-довідкової інформації.

Усі платіжні документи СЕП перед відправленням з банку обробляються апаратно-програмними засобами захисту інформації, що забезпечують виконання таких вимог з точки зору безпеки інформації:

інформація, що передається, має бути закритою, тобто повідомлення може бути прочитане лише тим, кому воно адресоване;

цілісність — випадкове чи навмисне пошкодження повідомлення на етапі його передачі буде виявлене під час його прийому;

автентичність відправника (під час прийому повідомлення можна однозначно визначити, хто його відправив).

Крім перерахованих основних вимог, необхідно виконувати низку допоміжних, що дає змогу більш детально аналізувати можливі нестандартні ситуації:

засобами захисту інформації ведеться шифрований арбітражний журнал, в якому зберігається протокол обробки інформації, а також вміст файлів, що обробляються;

у шифроване повідомлення включені поля дати та часу обробки.

В основу роботи засобів захисту інформації в СЕП покладено алгоритм шифрування із закритими ключами. Цей метод характеризується високою надійністю з точки зору його дешифрування, але ставить дуже високі вимоги до процедури транспортування та зберігання закритих ключів, секретність яких забезпечує на практиці стійкість системи шифрування.

Основними засобами захисту інформації в СЕП є апаратні засоби. Секретність ключів у них забезпечується технологічно:

ключі зберігаються в спеціальній електронній картці, прочитати їх можна тільки за допомогою спеціального блоку, що виконує процес шифрування інформації.

Прочитати ключі іншими засобами неможливо;

електронна картка видається банку з попередньою прив'язкою її до конкретного блоку шифрування цього ж банку; втрачена чи викрадена картка не буде працювати в іншому шифр-блоці (наприклад, в апаратурі іншого банку);

у випадку крадіжки одночасно блоку і картки у конкретного банку передбачено режим виключення цієї апаратури зі списку користувачів СЕП; банк може продовжити роботу в СЕП після вирішення юридичних та фінансових питань, пов'язаних з втратою апаратури та отриманням нового комплексу.

Найбільш слабким місцем з точки зору безпеки є ділянка підготовки платежів персоналом банку—учасника СЕП. Всі зареєстровані більш-менш успішні спроби НДС були з боку представників банків, що призводило до крадіжки коштів у власного банку, а не в держави чи в інших банках. В усіх цих випадках особи, які робили спроби НДС, мали легальний доступ до системи

підготовки та захисту платіжної інформації, причому їх повноваження були перевищені (доступ до багатьох чи навіть до всіх банківських ресурсів системи).

З метою гарантування безпеки інформації на цій ділянці від учасників СЕП вимагається виконання низки організаційних вимог:

допуск тільки довірених осіб до ключових операцій підготовки платіжних документів;

виконання відповідальними особами банку постійного, реального та достатнього контролю за станом бухгалтерського балансу та кореспондентського рахунку банку.

Для гарантування безпеки інформації на рівні банків—учасників СЕП пропонується впровадження перехресного накладення електронного цифрового підпису (реалізованого на основі алгоритму RSA) на платіжні документи.[3, с. 344]

Література

1. Міжбанківські розрахунки в Україні [Електронний ресурс]. – Режим доступу: <http://www.bank.gov.ua/control/uk/publish/>
2. Вступ до банківської справи: Навчальний посіб. / Савлук М. І., Мороз А. М., Коряк А. М. / Під ред. М. І. Савлука. — К.: Лібра, 1998. — 344 с

Сокол Антон Васильевич

*Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г.Киев*

МОДЕЛЬ OSI

Эталонная модель OSI, иногда называемая стеком OSI представляет собой 7-уровневую сетевую иерархию (рис. 1) разработанную Международной организацией по стандартам (International Standardization Organization - ISO). Эта модель содержит в себе по сути 2 различных модели:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах
- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной - соседние уровни обмениваются данными с использованием интерфейсов API.

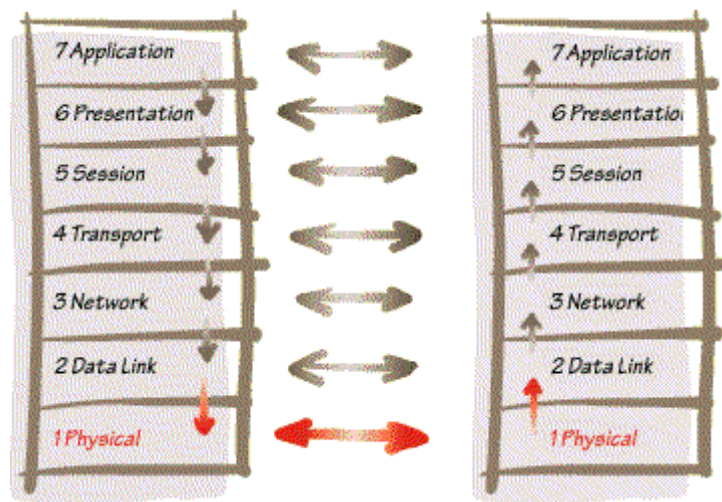


Рисунок 1 Модель OSI

Уровень 1, физический

Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

- Тип кабелей и разъемов
- Разводку контактов в разъемах
- Схему кодирования сигналов для значений 0 и 1

К числу наиболее распространенных спецификаций физического уровня относятся:

- EIA-RS-232-C, CCITT V.24/V.28 - механические/электрические характеристики несбалансированного последовательного интерфейса.
- EIA-RS-422/449, CCITT V.10 - механические, электрические и оптические характеристики сбалансированного последовательного интерфейса.
- IEEE 802.3 -- Ethernet
- IEEE 802.5 -- Token ring

Уровень 2, канальный

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.x делят канальный уровень на два подуровня: управление логическим каналом (LLC) и управление доступом к среде (MAC). LLC обеспечивает обслуживание сетевого уровня, а подуровень MAC регулирует доступ к разделяемой физической среде.

Наиболее часто используемые на уровне 2 протоколы включают:

- HDLC для последовательных соединений
- IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x
- Ethernet
- Token ring
- FDDI
- X.25

- Frame relay

Уровень 3, сетевой

Сетевой уровень отвечает за деление пользователей на группы. На этом уровне происходит маршрутизация пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Наиболее часто на сетевом уровне используются протоколы:

- IP - протокол Internet
- IPX - протокол межсетевого обмена
- X.25 (частично этот протокол реализован на уровне 2)
- CLNP - сетевой протокол без организации соединений

Уровень 4, транспортный

Транспортный уровень делит потоки информации на достаточно малые фрагменты (пакеты) для передачи их на сетевой уровень.

Наиболее распространенные протоколы транспортного уровня включают:

- TCP - протокол управления передачей
- NCP - Netware Core Protocol
- SPX - упорядоченный обмен пакетами
- TP4 - протокол передачи класса 4

Уровень 5, сеансовый

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью функций трех верхних уровней модели.

Уровень 6, уровень представления

Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня. Протоколы уровня представления обычно являются составной частью функций трех верхних уровней модели.

Уровень 7, прикладной

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних уровней относятся:

- FTP - протокол переноса файлов
- TFTP - упрощенный протокол переноса файлов
- X.400 - электронная почта
- Telnet
- SMTP - простой протокол почтового обмена
- CMIP - общий протокол управления информацией
- SNMP - простой протокол управления сетью
- NFS - сетевая файловая система
- FTAM - метод доступа для переноса файлов

Протоколы IEEE 802

IEEE (Institute of Electrical and Electronics Engineers) является профессиональной организацией (США), определяющей стандарты, связанные с сетями и другими аспектами электронных коммуникаций. Группа IEEE 802.X содержит описание сетевых спецификаций и содержит стандарты, рекомендации и информационные документы для сетей и телекоммуникаций.

Публикации IEEE являются результатом работы различных технических, исследовательских и рабочих групп.

Рекомендации IEEE связаны главным образом с 2 нижними уровнями модели OSI - физическим и канальным. Эти рекомендации делят канальный уровень на 2 подуровня нижний - MAC (управление доступом к среде) и верхний - LLC (управление логическим каналом).

Часть стандартов IEEE (802.1 - 802.11) была адаптирована ISO (8801-1 - 8802-11, соответственно), получив статус международных стандартов. В литературе, однако, гораздо чаще упоминаются исходные стандарты, а не международные (IEEE 802.3, а не ISO/IEC 8802-3).

Ниже приведено краткое описание стандартов IEEE 802.X:

- **802.1** - задает стандарты управления сетью на MAC-уровне, включая алгоритм Spanning Tree. Этот алгоритм используется для обеспечения единственности пути (отсутствия петель) в многосвязных сетях на основе мостов и коммутаторов с возможностью его замены альтернативным путем в случае выхода из строя. Документы также содержат спецификации сетевого управления и межсетевого взаимодействия.
- **802.2** - определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем. Прозрачные для вышележащих уровней функции LLC включают кадрирование, адресацию, контроль ошибок. Этот подуровень используется в спецификации 802.3 Ethernet, но не включен в спецификацию Ethernet II.
- **802.3** - описывает физический уровень и подуровень MAC для сетей с немодулированной передачей (baseband networks), использующих шинную топологию и метод доступа CSMA/CD. Этот стандарт был разработан совместно с компаниями Digital, Intel, Xerox и весьма близок к стандарту Ethernet. Однако стандарты Ethernet II и IEEE 802.3 не полностью идентичны и для обеспечения совместимости разнотипных узлов требуется применять специальные меры. 802.3 также включает технологии Fast Ethernet (100BaseTx, 100BaseFx, 100BaseFl).
- **802.5** - описывает физический уровень и подуровень MAC для сетей с кольцевой топологией и передачей маркеров. Этому стандарту соответствуют сети IBM Token Ring 4/16 Мбит/с.
- **802.8** - отчет TAG по оптическим сетям. Документ содержит обсуждение использования оптических кабелей в сетях 802.3 - 802.6, а также рекомендации по установке оптических кабельных систем.
- **802.9** - отчет рабочей группы по интеграции голоса и данных (IVD). Документ задает архитектуру и интерфейсы устройств для одновременной

передачи данных и голоса по одной линии. Стандарт 802.9, принятый в 1993 году, совместим с ISDN и использует подуровень LLC, определенный в 802.2, а также поддерживает кабельные системы UTP (неэкранированные кабели из скрученных пар).

- **802.10** - в этом отчете рабочей группы по безопасности ЛВС рассмотрены вопросы обмена данными, шифрования, управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.
- **802.11** - имя рабочей группы, занимающейся спецификацией 100BaseVG Ethernet 100BaseVG. Комитет 802.3, в свою очередь, также предложил спецификации для Ethernet 100 Мбит/с

Отметим, что работа комитета 802.2 послужила базой для нескольких стандартов (802.3 - 802.6, 802.12). Отдельные комитеты (802.7 - 802.11) выполняют в основном информационные функции для комитетов, связанных с сетевыми архитектурами.

Отметим также, что разные комитеты 802.X задают разный порядок битов при передаче. Например, 802.3 (CSMA/CD) задает порядок LSB, при котором передается сначала наименее значимый бит (младший разряд), 802.5 (token ring) использует обратный порядок - MSB, как и ANSI X3T9.5 - комитет, отвечающий за архитектурные спецификации FDDI. Эти два варианта порядка передачи известны как "little-endian" (канонический) и "big-endian" (неканонический), соответственно. Эта разница в порядке передачи имеет существенное значение для мостов и маршрутизаторов, связывающих различные сети.

Международный телекоммуникационный союз (ITU)

ITU представляет собой международную организацию в области стандартизации при ООН, ответственную за разработку стандартов для телекоммуникационного оборудования и услуг.

ITU включает три подразделения:

- **ITU-T** (телекоммуникационный сектор, ранее Международный консультативный комитет по телефонной и телеграфной связи - CCITT) отвечает за коммуникационные стандарты. Эта группа является наиболее активным разработчиком стандартов в сфере передачи данных по сетям.
- **CCIR** - международный консультативный комитет по радиосвязи.
- **IFRB** - международный комитет по регистрации частот, отвечающий за выделение радиочастот для телекоммуникаций.

Ниже приведен список наиболее распространенных стандартов ITU:

- **V.11** - электрические характеристики сбалансированных устройств при скоростях до 10 Мбит/с. Совместим с RS-422.
- **V.22** - работа синхронных и асинхронных модемов по выделенным и коммутируемым линиям при скоростях до 1200 бит/с.
- **V.22bis** - работа синхронных и асинхронных модемов по выделенным и коммутируемым линиям при скоростях до 2400 бит/с с возможностью снижения до 1200 бит/с.

- **V.24** - устройства физического обмена данными для подключения компьютерного оборудования. RS-232D является частью V.24. V.28 определяет электрические параметры устройства.
- **V.25bis** - процедура автоматических звонков (соединений) и ответа, реализующая командный протокол, подобный набору команд Hayes AT, но ориентированных на поддержку систем международной связи.
- **V.28** - электрические характеристики несбалансированного устройства обмена, используемого совместно с физическим устройством V.24. Напряжение от 5 до 15 В определяет двоичный 0; от -5 до -15 - двоичную 1. Стандарт совместим с RS-232D.
- **V.32** - работа синхронных и асинхронных модемов по выделенным и коммутируемым линиям при скоростях до 9600 и 4800 бит/с.
- **V.32ter** - версия стандарта V.32, предложенная AT&T; для скорости 19200 бит/с с возможностью снижения до максимальной поддерживаемой линией и устройствами скорости.
- **V.32 bis** - работа синхронных и асинхронных модемов по выделенным и коммутируемым линиям при скоростях до 14400 бит/с с возможностью снижения до максимальной поддерживаемой линией и устройствами скорости.
- **V.35** - физическое устройство обмена данными для подключения компьютерного оборудования при скоростях до 48 Кбит/с взамен устаревших V.36 и V.37. Сейчас V.35 является базовым термином для описания физического соединения и электрических параметров при скоростях до 2 Мбит/с.
- **V.42** - Стандарт CCITT для контроля ошибок при связи асинхронных модемов. Определяет протокол LAP-M.
- **V.42bis** - Стандарт CCITT для встроенного в модемы протокола коррекции ошибок и компрессии данных.
- **V.34** - работа синхронных и асинхронных модемов по выделенным и коммутируемым линиям при скоростях до 28800 бит/с.

Другие стандарты

Американский национальный институт стандартов (ANSI)

Представляет США в ISO. К числу наиболее важных стандартов ANSI относится FDDI.

ATM Forum

Некоммерческая организация (консорциум), задачей которой является обеспечение интероперабельности оборудования на базе международных стандартов и обеспечение кооперации производителей оборудования. К числу наиболее важных стандартов ATM Forum относятся:

- Эмуляция LBC (ATM LAN Emulation v. 1.0)
- Спецификация основанного на кадрах взаимодействия пользователь-сеть (FUNI)
- UNI 3.0, 3.1 и 4.0

Ассоциация электронной промышленности (EIA)

Наиболее важные стандарты EIA:

- Интерфейс RS-232D
- Кабельные системы EIA/TIA-568

Література:

1.А. Филимонов. Построение мультисервисных сетей Ethernet. — М.: BHV, 2007. ISBN 978-5-9775-0007-4.

2.Руководство по технологиям объединённых сетей. 4-е изд. — М.: Вильямс, 2005. ISBN 5-8459-0787-X.

3.Интернет ресурс: сервер book.itep.ru:

Дереча Наталія Андріївна
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КІБЕРБЕЗПЕКА-ПРОБЛЕМА СТОЛІТТЯ

На сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів. Щодня кожен з нас стикається із необхідністю користування інформаційними технологіями. Від соціальних мереж, розміщення інформації про свої персональні дані в інтернеті до користування банкоматами, банківськими рахунками і т. п. У зв'язку із цим виникає питання, чи врегульовано дану проблему вітчизняним законодавством і як себе захистити від кіберзлочинців.

Аналіз вітчизняного законодавства дав зрозуміти, що, на жаль, в Україні на сьогодні, навіть не визначено таких ключових понять: кіберзлочин, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист.

Водночас спостерігається вільне використання значної кількості термінів (та їх синонімів), що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», причому жоден з цих термінів не має свого визначення ані в цьому, ані в інших нормативних документах. В Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись прописані як складова частина поняття «технологічний тероризм». У «Стратегії національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007) комп'ютерні загрози не згадуються, а «кібербезпека» — лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України «Конвенції про кіберзлочинність». [1, с. 5–7; 2, с. 10]

В «Доктрині інформаційної безпеки України» також згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», знову ж таки — без жодних пояснень чи посилання на такі пояснення. Крім того, в Доктрині

згадуються і «кібератаки» без визначення терміну. Отже, можна констатувати, що в більшості своїй вітчизняне нормативно-правове поле в сфері інформаційної (кібернетичної) безпеки оперує термінами визначень яких фактично немає.

Варто відмітити, що дане питання повільно, але все ж таки вирішується. Станом на 21.05.13 за основу прийнято законопроект (реєстр. №2483), яким пропонується запровадити до термінології національного законодавства нові поняття, зокрема, «кібернетична безпека» та «кібернетичний простір».

Згідно із проектом, **«кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; кібернетичний простір (кіберпростір) – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем».** [3, с. 8]

Стержневою основою в українському законодавстві стосовно кіберзлочинів є передбачені кримінальним законом суспільно небезпечні діяння і закріпленні в окремому Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинів відносяться тільки злочини, передбачені розділом XVI КК України.

Таким чином, робимо висновок, що національне законодавство щодо кіберзлочинності знаходиться у зародковому стані, а українці з їх низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки в Україні – ідеальні мішені для кіберзлочинців.

Належний захист від кіберзлочинців залежить від самих громадян, які часто легковажно та необережно відносяться до електронних платежів і своїх персональних даних. Саме персональні дані, які ви надаєте банку, є найбільш затребуваними шахраями, а саме: прізвище та ім'я, номер мобільного телефону, адреса електронної пошти. Зазвичай таку інформацію продають на «чорному» ринку, а згодом використовують для розсилок смс, спаму, телефонних дзвінків рекламного характеру. Часто зазначені дані перехоплюються в місцях із відкритим Wi-Fi доступом під час користування ел. поштою або соціальними мережами.

Що стосується банківського сектору, то необхідно дотримуватися декількох простих правил щодо безпеки з користування платіжними картками. По-перше, не слід давати стороннім у руки свою платіжну картку. По-друге, ніколи не носити разом із карткою PIN-код. Останнім часом поширилося викрадення особистих даних з банкоматів. Таких шахраїв називають «кардери». Вони встановлюють на банкомати спеціальні пристрої: скіммери і накладки. Перший приклеюють на карткоприймач банкомату, другий – на клавіатуру. В їх приладах вмонтовані спеціальні передавачі, які пересилають всю отриману інформацію на мобільний телефон чи електронну пошту. Фахівці з IT-безпеки радять прикривати долонею цифри коду, які ви вводите у банкомат, оскільки поряд може бути вмонтовано злочинцями відеокамеру. Серед організаційних

заходів пропонується користуватися послугами смс-інформування та установити ліміт на використання грошових коштів, а також надати банку телефон, за яким із вами можна швидко зв'язатися.

На жаль, кіберзлочинність постійно удосконалюється і йде в ногу з технологіями, що, у свою чергу, ускладнює виявлення та протидію зазначеним протиправним діям. Варто пам'ятати, що на практиці втрачені кошти дуже важко відшкодувати, адже винну особу в такій ситуації знайти не просто, банк несе відповідальність тільки в тому разі, якщо буде доведено, що злочин було скоєно з його вини. Завдання кожного громадянина для власної безпеки — бути пильним і ставитись до своїх персональних даних і платіжних карток із особливою обережністю та уважністю.

Література:

1. ЗАКОН УКРАЇНИ «Про основи національної безпеки України» (Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351)
2. Конвенція про кіберзлочинність
3. http://zakon2.rada.gov.ua/laws/show/994_575

***Хоменко Тетяна Анатоліївна**
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

ЦЕНТРИ СЕРТИФІКАЦІЇ. ПРОТОКОЛ SSL

Сертифікати існують для підтвердження того факту, що даний відкритий ключ належить конкретній особі і нікому іншому. Це необхідно для запобігання спроб шахрайства.

Сертифікати видаються спеціальними компаніями (Центрами Сертифікації) і підписуються електронним цифровим підписом цих компаній. Будь-хто бажаючий може ознайомитися з сертифікатом, виданим Центром Сертифікації, і переконатися, що даний відкритий ключ належить саме тій особі, що у ньому зазначена. Компанія, що є Центром Сертифікації, повинна мати високий авторитет, оскільки користувачі повинні їй довіряти.

Для отримання сертифікату зацікавленій особі необхідно звернутися до Центру Сертифікації та надати необхідну інформацію про себе. Центр Сертифікації здійснить перевірку цієї інформації і, у випадку її правильності, видає сертифікат. Це платна послуга і кожний Центр Сертифікації встановлює свої ціни. Як правило, сертифікат видається на рік з можливістю продовження після оплати чергового внеску.

Особи, що володіють сертифікатами, можуть укладати між собою угоди через інтернет, підписуючи документи електронним цифровим підписом і не побоюючись відмови один одного від зобов'язань по угоді.

Найбільш відомими Центрами Сертифікації є компанії VeriSign (www.verisign.com) і Thawte (www.thawte.com). Протокол SSL (Secure Socket

Layer) використовується для захисту даних при передачі їх через інтернет. Цей протокол базується на комбінації алгоритмів асиметричного та симетричного шифрування.

Протокол може працювати в трьох режимах:

- при взаємній автентифікації сторін;
- при автентифікації сервера і анонімності клієнта;
- при взаємній анонімності сторін. При встановленні з'єднання за протоколом SSL для даної сесії зв'язку генерується разовий ключ, що використовується для симетричного шифрування даних, що передаються протягом даної сесії. При цьому використовуються асиметричні алгоритми шифрування. Процес передачі даних від клієнта до сервера з використанням SSL протоколу складається з двох стадій. На першій стадії встановлюється зв'язок.

Клієнт надсилає до сервера дані, що містять номер версії SSL клієнта, обраний шифр і певні випадково генеровані дані.

Сервер у відповідь надсилає аналогічні дані і свій цифровий сертифікат. Якщо обмін даними потребує представлення цифрового сертифікату, то сервер запрошує клієнта надати сертифікат.

Клієнт автентифікує сервер. У випадку збою клієнта інформують.

З використанням даних, які були генеровані при встановленні контакту з сервером, клієнт створює набір даних, відомих як попередній секрет хазяїна (premaster secret). Цей набір даних потім використовується при встановленні зв'язку.

Сервер автентифікує клієнта. Це відбувається лише у тому випадку, якщо транзакція потребує автентифікації обох сторін. SSL може використовуватися і тоді, коли автентифікується лише сервер. Отже, цей крок може бути пропущеним, що у більшості випадків і відбувається.

Якщо автентифікація клієнта і сервера успішно завершується, то обидві сторони здійснюють процес генерації іншого набору даних, відомих під назвою секрет хазяїна (master secret). При генерації цього набору частково використовується попередній секрет хазяїна. Секрет хазяїна представляє собою величину довжиною 48 біт, яка використовується при створенні ключів для передачі основної інформації між клієнтом і сервером після завершення встановлення контакту.

Тепер клієнт і сервер генерують пару ключів на основі секрету хазяїна. Один з ключів використовується для шифрування і дешифрування даних, що пересилаються від клієнта до сервера. Інший ключ використовується для шифрування і дешифрування даних, що пересилаються від сервера до клієнта.

Після завершення процесу встановлення зв'язку клієнт і сервер можуть розпочинати обмін зашифрованими даними із застосуванням одного з алгоритмів, включених до робочої версії SSL. Після завершення сесії обміну контакт розривається. Якщо дві сторони бажають зв'язатися повторно, вони знову повинні здійснити всю процедуру встановлення зв'язку. І кожного разу при

встановленні контакту генеруються різні пари ключів для шифрування і різні секрети хазяїна.

Література:

1. <http://nereff.ru/0400812.html>
2. <http://polka-knig.com.ua>

Марченко В.В., Шевчук Я.А.
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м.Київ

ЗАХИСТ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Визначено основну форму ведення аналітичної роботи. Висвітлено важливість проведення такої роботи на підприємстві в умовах сьогодення.

Захист інформації на підприємстві – це вироблення ефективних заходів, пропозицій і рекомендацій керівництву підприємства, спрямованих на недопущення витоку конфіденційної інформації про діяльність підприємства і проведені роботи [1].

Основою ефективного захисту інформації є аналітична робота, яка повинна включати елементи прогнозування можливих загроз. Основні напрямки аналітичної роботи на підприємстві такі:

аналіз об'єкта захисту;

- аналіз внутрішніх і зовнішніх загроз інформаційної безпеки підприємства;
- аналіз можливих каналів несанкціонованого доступу до інформації;
- аналіз системи комплексної безпеки об'єктів;
- аналіз порушень режиму конфіденційності інформації;
- аналіз передумов до розголошення інформації, а також до втрати носіїв конфіденційної інформації.

Функції аналізу на підприємстві покладаються на спеціально створений у його структурі аналітичний підрозділ, який комплектується кваліфікованими фахівцями в галузі захисту інформації [1]. Разом з тим такі фахівці повинні повною мірою володіти інформацією за всіма напрямками діяльності підприємства: знати види, характер і послідовність виконання виробничих робіт, взаємодіючі організації, специфіку діяльності структурних підрозділів підприємства і т. ін. Переважно аналітичний підрозділ включається до складу служби безпеки підприємства. Аналітичний підрозділ повинен забезпечувати керівництво підприємства достовірною та аналітично обробленою інформацією, необхідною для прийняття ефективних управлінських рішень в усіх напрямках захисту інформації.

Основними функціями аналітичного підрозділу є: забезпечення своєчасного надходження достовірних і всебічних відомостей з проблем захисту інформації; облік, узагальнення та постійний аналіз матеріалів про стан справ у системі захисту інформації підприємства (його філій та представництв); аналіз можливих загроз захисту інформації, моделювання реального сценарію можливих дій конкурентів (зловмисників), які зачіпають інтереси підприємства; забезпечення ефективності роботи з аналізу наявної інформації, виключення дублювання при її зборі, обробленні та розповсюдженні; моніторинг ситуації на ринку продукції, товарів і послуг, а також у зовнішньому середовищі з метою виявлення подій і фактів, які можуть мати значення для діяльності підприємства; забезпечення безпеки власних інформаційних ресурсів, обмеження доступу співробітників підприємства до аналітичної інформації; підготовка висновків і пропозицій, спрямованих на підвищення ефективності планованих і здійснюваних заходів щодо захисту інформації, а також уточнення (коригування) організаційно-плануючих документів підприємства та його структурних підрозділів; вироблення рекомендацій щодо внесення змін і доповнень у методичні документи, які регламентують алгоритм дій співробітників підприємства щодо захисту інформації (стандарти підприємства) [2].

Наявність постійної аналітичної роботи, її характер і результати визначають необхідність, основи організації, структуру та зміст системи комплексного захисту інформації, вимоги до її ефективності та напрямки її розвитку і вдосконалення [3].

Найбільш типові завдання аналітичного дослідження:
отримання даних про стан системи захисту інформації на підприємстві (його конкретних об'єктах, у філіях, представництвах);
виявлення можливих каналів витоку інформації, що підлягає захисту;
визначення обставин, причин і факторів, що сприяють виникненню каналів витоку і створенню передумов для витоку інформації;
підготовка для керівництва підприємства (філії, представництва) та його структурних підрозділів конкретних рекомендацій щодо закриття виявлених каналів витоку.

Під об'єктом дослідження розуміється все те, що вивчається та аналізується у ході дослідження.

Предмет дослідження – та сторона об'єкта, яка безпосередньо підлягає вивченню у ході аналітичного дослідження.

Проведення аналітичної роботи в галузі захисту інформації дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки підприємства, виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки підприємства, знизити потенційні втрати підприємства чи організації через підвищення стійкості функціонування корпоративної мережі, розробити

концепцію та політику безпеки підприємства, а також запропонувати плани захисту конфіденційної інформації підприємства, що передається по відкритих каналах зв'язку, захисту інформації підприємства від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання чи використання.

Література

1. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : Диасофт, 1999. – 480 с.
2. Тардаскін М. Ф. Технічний захист комерційної таємниці підприємства зв'язку : навч. посіб. / М. Ф. Тардаскін; за ред. М. В. Захарченка, М. Ф. Тардаскін, В. Г. Кононович. – Одеса : ОНАЗ, 2002. – 76 с.
3. Ткач Ю. М. Окремі аспекти інформаційно-аналітичної діяльності у процесі навчання математики фахівців з інформаційної безпеки / Ю. М. Ткач / Дидактика математики: проблеми і дослідження : міжнародний збірник робіт. – Донецьк, 2013. – Вип. 40. – С. 151–158.

Кукишин Дарія Вікторівна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Соціальні мережі давно вже стали невід'ємною частиною нашого життя. Вони допомагають нам спілкуватися один з одним і обмінюватися повідомленнями, фотографіями, аудіо- та відео-файлами. У кожного є сторінка в соціальній мережі, де можна розмістити різну інформацію про себе, а, також, дізнатися більше про своїх друзів, знайомих та різних людей, з якими потім можна познайомитись.

В соціальних мережах користувачі розміщують різні персональні дані про себе, наприклад: ПІБ, дата народження, та навіть інформацію про улюбленого співака або, яку музику ви слухаєте. Такий великий обсяг різних даних потрібно оберігати, бо вона у вільному доступі і кожен може прочитати, а потім і використовувати цю інформацію. У зв'язку з тим, що є ризик взлому аккаунтів в соціальних мережах, а потім зловмисники можуть використовувати ваші персональні дані. І від цього не застрахована жодна мережа, томи ми, користувачі, повинні самі захищати свої персональні дані, коли ми користуємося соціальними мережами.

Одним з найактуальніших завдань безпеки в цьому контексті є забезпечення конфіденційності, тобто, надання своїх персональних даних тільки заздалегідь визначеному колу осіб у рамках соціальної мережі (наприклад, тільки друзям). Це право дається тільки користувачу, і він сам вирішує, яку інформацію він робить загальнодоступною, а до якої обмежити доступ.

Також комп'ютерні шахраї зламують аккаунти для використання у власних цілях. Вони діють дуже обережно, щоб користувач не відразу запідозрив, що щось не так. В більшості випадків такі «зламані» сторінки використовують для вступу у різні групи, додавання коментарів або лайків. Це дуже зручно і так проводиться монетизація чужого аккаунту, бо більшість користувачів не перевіряє, в які спільноти вони вступили, та і перевіркою коментарів і лайків у соціальних мережах взагалі ніхто не займається.

Зараз послуга вступу до різних груп та додавання лайків та коментарів масово пропонується реальним користувачам. Але так ви нічого не зможете продати, бо хакери запрошують в такі спільноти замовників нецільову аудиторію, а розсилка спаму від невідомих спільнот розлючує людей, що не є плюсом для іміджу компанії.

Існує два найпоширеніших методів монетизації аккаунтів:

1. Розсилка спаму на стінку аккаунта, в особисті повідомлення
2. друзям, тощо. Спам розсилається у вигляді промоакцій та рекламних повідомлень.
3. Розсилка особистих повідомлень з проханням проголосувати або просто допомогти. В них повідомляється, що така допомога буде коштувати недорого, а на практиці виходить по-іншому.

Отже, щоб ваш аккаунт не виявився в руках зловмисників, потрібно дотримуватися декількох базових рекомендацій, так званої мереженої гігієни.

Так, до загальних механізмів безпеки, які не прив'язані до соціальних мереж, відноситься, наприклад, використання захищеного протоколу взаємодії з Web-серверами. Тобто, при вході і перебуванні в соціальній мережі повинен використовуватися лише протокол https. Це гарантує безпечну передачу інформації у мережі (але при цьому знижується швидкість передачі даних), у тому числі зв'язки логін – пароль.

Необхідно стежити і регулярно очищати дані про профіль користувача соціальної мережі, що залишається браузером у вигляді файлів або відповідних записів на комп'ютері. У деяких випадках такі дані можуть використовуватися шкідливим програмним забезпеченням для несанкціонованого отримання персональних відомостей (наприклад, тієї ж зв'язки логін – пароль).

Персональні дані на сторінці в соціальних мережах потрібно розміщувати з розумом. Не потрібно виставляти інтимну інформацію, відверті фото, дані про вашу сім'ю. Це все для того, щоб не потрапити в зону ризику і не привертати увагу шахраїв.

Варто періодично змінювати паролі, використовуючи якомога більше символів, щоб ускладнити автоматичний підбір. Слід вигадати складний пароль мінімум з 8 символів, з урахуванням регістру (користуватись великими і малими літерами), також слід увімкнути двофазну авторизацію через телефон (до аккаунту в особистих налаштуваннях додається телефон, і при вводі логіну та паролю сайт відправляє код через SMS, який додатково потрібно ввести).

Не залишайте номер свого мобільного на жодному з сайтів, коли розміщуєте інформацію про себе. Його легко відслідкувати, просто використавши пошук по

фото. Використовуйте це правило, якщо не хочете, щоб номер вашого телефону дізналися шахраї. Вам можуть приходити SMS-повідомлення різного змісту, або навіть вони можуть телефонувати Вам і вимагати грошей. Таким методом користуються телефонні шахраї, які обманом вимагають гроші від простих людей, які мали необережність залишити свій номер телефону в спільному доступі.

Не використовуйте в соціальних мережах геолокацію. Так зловмисники можуть дізнатися точну вашу адресу проживання, і це допоможе квартирним злодіям обстежити та оцінити ваше помешкання. Таким чином людина, сама того не розуміючи, повідомляє шахраям всю інформацію про те, де і як вона живе. Так злодії обирають собі наступну жертву. Отже, так через соціальні мережі можна привабити до себе навіть і квартирних злодіїв.

Остерігайтесь переходити за посиланнями, які вам надсилають на пошту і в соціальні мережі. Кожне з них може бути використане для зламу вашої сторінки. Також такі посилання можуть призвести до взлому вашого персонального комп'ютера, або хакери так можуть переносити різні віруси.

Зрештою, до одного із дієвих механізмів безпеки необхідно віднести установку на ваш персональний комп'ютер антивірусів і інших засобів захисту. Але не варто також забувати про мобільні пристрої, з яких останнім часом багато користувачів заходять в соцмережі. Ці пристрої локально зберігають персональні дані, отримані із соцмереж, та схильні до дії шкідливого програмного забезпечення.

На жаль, мережева гігієна, як і будь-яка інша, не зможе повністю захистити ваш аккаунт від вірусного захворювання. Навіть якщо враховувати, що соціальні мережі захищені безпечними протоколами, на сьогодні не існує стовідсоткових способів захисту облікового запису. Це, у першу чергу, пов'язано з тим, що соціальна мережа – це непідконтрольне нам середовище, і захистити її можуть тільки її співробітники за допомогою додаткових внутрішніх систем безпеки.

До того, як ваш аккаунт буде взломаний, майже неможливо виявити його слабкості, але вже після цього можна змінити логін і пароль, що зменшить доступ зловмисників до ваших персональних даних. В соціальній мережі набагато легше вирішувати проблеми по факту їх появи, ніж намагатися передбачити можливі варіанти атаки, бо ми не можемо покращити міри обережності стороннього середовища.

Як зрозуміти, що аккаунт було взломано? Перерахуємо основні ознаки взломаного аккаунта, щоб користувачі могли своєчасно змінити свої контактні дані. Також рекомендуємо змінити пароль не лише від аккаунта в соцмережі, а й від скриньки електронної пошти.

Основні ознаки взломаного аккаунта в соцмережі:

- Друзі пишуть Вам, що Ви були online, коли Ви впевненні, що в зазначений час Ви не заходили до Інтернету;
- З Вашого аккаунту почалась розсилка дивних листів та посилань;
- Ви виявляєте у себе в аккаунті спільноти, в які не вступали і друзів, яких не додавали;

- Ви заходите до себе в аккаунт, але ваш пароль не підходить.

Таким чином, існують лише базові поради щодо запобіжних заходів, дотримуючись яких ви зможете, якщо не повністю убезпечити, то хоча б максимально ускладнити несанкціонований доступ до ваших персональних даних.

Зараз почали використовувати соціальні мережі для різних видів інтернет-шахрайства. Тому, щоб протистояти такій небезпеці, потрібно знати, з чим маємо справу.

І перший вид такого інтернет шахрайства - фішинг. Це вид інтернет-шахрайства, мета якого полягає в отриманні доступу до персональних даних користувача – паролів, логінів тощо. В процесі цього виду хакер використовує фішинговий лист, який він надсилає в особисті повідомлення користувачу, де є прохання проголосувати за щось або просто прохання перевести гроші на допомогу. Наївний користувач переходить по посиланню в такому листі та вводить персональні дані, які потім використовує зловмисник. Але це не один сценарій. В іншому - користувач заходить на даний фішинговий сайт і відразу виходить. При таких діях починає працювати спеціальний скрипт, який визначає версію вашої операційної системи та використовуваного браузера. Виходячи з одержаних даних, встановлюється експлойт за допомогою якого отримується правка файлу HOSTS, встановлюється і активізується троян, який може зчитати всі дані користувачів з ПК.

Як захиститися від фішингу в соціальних мережах? По-перше, листи, які прийшли від невідомих користувачів, не потрібно навіть читати, а відразу відправляти в «спам» і повідомляти про це адміністрації сайту. Але не потрібно всі листи відправляти туди, якщо користувач брав участь в конкурсах, і організатори можуть надіслати вам повідомлення, але переходити по посиланням дуже обережно. Потрібно пам'ятати, що адміністрація не буде просити у користувача пароль, бо він у неї і так є. Також адміністрація не буде просити вислати SMS-повідомлення на якийсь номер.

Ще один тип загроз, що перейшов до соцмереж, - програми для крадіжки паролів. Вони впроваджують частини коду в ваш комп'ютер, щоб викрасти ваші дані для реєстрації до того, як вони будуть відправлені на сервер. Після цього зловмисник починає використовувати ваші дані, то він почне також відправляти посилання знайомим та друзям жертви, то кількість постраждалих буде рости, як снігова куля.

Існує ще один вид загроз – фармінг, який більш небезпечний, ніж фішинг. Спочатку з'явився фішинг, а потім, в результаті еволюції, фармінг. Що ж представляє із себе цей вид інтернет – шахрайства? Фармінг – це замасковане перенаправлення користувача–жертви на фальшивий IP-адрес.

В чому ж криється відмінність фішинга від фармінга? В обох випадках становищу жертви не позаздриш. Користувача перенаправляють з красивого справжнього сайту на красивий фальшивий сайт. Але якщо у випадку з фішингом назва сайту змінюється, то у випадку з фармінгом назва сайту залишається та сама, змінюється тільки IP-адреса, тобто, якщо сайт знаходиться в Україні, то його

двійник буде знаходитись, наприклад, в Японії. Навіть найуважніший користувач не в змозі відрізнити, коли потрапляє на фармінг-сайт, а коли – на справжній, якщо у нього, звичайно, немає змоги перевіряти IP-адреси сайтів. Якщо адреси двох сайтів ідентичні, то можна починати бити на сполох.

Отже, захист персональних даних в соціальних мережах – справа рук самого користувача. Тому краще сто разів подумати, перед тим, як викласти якусь інформацію про себе або фотографію. Ніхто не може гарантувати того, що саме Ваші дані не будуть використовуватися зловмисниками в особистих цілях.

Література:

- 1.Захист персональних даних в соціальних мережах [Електронний ресурс] – Режим доступу: <http://www.vaas.gov.ua/news/zaxist-personalnix-danix-v-socialnix-merezhax/>
- 2.Як захистити персональні дані в мережі – поради спеціалістів [Електронний ресурс] – Режим доступу : <http://universe.zp.ua/?p=4505>
- 3.Способы защиты персональных данных в социальных сетях [Електронний ресурс] – Режим доступу : <http://www.prima.ru/node/351>
- 4.Виды защиты информации в социальных сетях [Електронний ресурс] – Режим доступу : <https://sites.google.com/site/socialnyeseti94/zasita-informacii-v-socialnyh-setah/vidy-zasity-informacii-v-socialnyh-setah>

Перепелиця Ліна Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

КІБЕРБЕЗПЕКА, ЇЇ СТРУКТУРА ТА РОЗВИТОК В УКРАЇНІ ТА СВІТІ

Сьогодні актуальність проблеми кібербезпеки не викликає ніяких сумнівів. Щодня кожен з нас стикається з необхідністю використання інформаційних технологій.

Кібербезпека – це набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до керування ризиками, дій, професійної підготовки страхування та технологій, які використовуються для захисту кіберсередовища, ресурсів організацій та користувачів.

Основними завданнями забезпечення користувачів вважають:

- доступність;
- цілісність з врахуванням автентичності;
- конфіденціальність.

Створення безпечних комп'ютерних систем і додатків є метою діяльності мережесистемних інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики, так і економіки.

Згідно із загальноприйнятим визначенням, безпечна комп'ютерна інформаційна система — це ідеальна система, яка коректно і у повному обсязі реалізує ті і лише ті цілі, що відповідають намірам її власника.

У 2007 році тодішній секретар МСЕ (2007-2014) доктор Хамадун І. Туре створив Глобальну програму кібербезпеки МСЕ (GCA), яка є основою для міжнародного співробітництва, спрямованого на зміцнення довіри та безпеки в інформаційному суспільстві.

GCA сприяла таким ініціативам, як захист дітей онлайн, та партнерство між МСЕ та ІМРАСТ (міжнародне багатостороннє партнерство проти кіберзагроз), а також за підтримки провідних світових гравців з усіх груп зацікавлених сторін, розгортанню рішень кібербезпеки по усьому світу.

GCA побудована на 5 стратегічних напрямках, також відомих як робочі зони.

Аналіз законодавства України дав зрозуміти, що, на жаль, в Україні на сьогодні навіть не визначено таких ключових понять, як кіберзлочинність, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист. Разом з тим спостерігається вільне використання значної кількості термінів.

В Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись прописані як складова частина поняття «технологічний тероризм».

В «Доктрині інформаційної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», без жодних пояснень чи посилання на такі пояснення.

Варто відмітити, що дане питання повільно, але все ж таки вирішується.

Згідно з інформацією від 27 січня 2016 року указом Президента України була затверджена стратегія кібербезпеки України, прийнята на засіданні РНБО, і указ був оприлюднений 16 березня 2016 року на сайті Президента.

Метою стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави.

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору і досягнення сумісності з відповідними стандартами ЄС і НАТО. Крім цього, Стратегія передбачає залучення експертного потенціалу наукових установ, професійних і громадських об'єднань до підготовки проектів концептуальних документів у цій сфері.

Крім того, РНБО доручила Кабінету міністрів разом з СБУ, Службою зовнішньої розвідки та за участю Національного інституту стратегічних досліджень затвердити у двомісячний строк план заходів на 2016 рік щодо реалізації Стратегії кібербезпеки України.

Належний захист від кіберзлочинців першочергово залежить від самих громадян, які дуже часто легковажно та необережно відносяться до електронних платежів і своїх персональних даних. Спеціалісти радять користуватися засобами захисту інформації, які пропонуються поштовими серверами або соціальними мережами.

Що стосується банківського сектору, то необхідно дотримуватися декількох певних правил щодо безпеки з користування платіжними картками. Фахівці з IT-безпеки радять прикривати долонею цифри коду, які ви вводите у банкомат, оскільки поряд може бути вмонтовано злочинцями відеокамеру.

На жаль, кіберзлочинність постійно удосконалюється і йде в ногу з технологіями, що, у свою чергу, ускладнює виявлення та протидію зазначеним протиправним діям.

Завдання кожного громадянина для власної безпеки – бути пильним і ставитись до своїх персональних даних і платіжних карток із особливою обережністю та уважністю.

Література:

- 1.Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.
- 2.Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
- 3.Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
- 4.Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с. — ISBN 5-94074-383-8

Вовк Надія Ігорівна

*Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

СИСТЕМА «РОЗУМНИЙ БУДИНОК»:

ВИСОКОІНТЕЛЕКТУАЛЬНЕ ЖИТЛО

Будинок, в якому самі по собі відкриваються двері, включаються побутові прилади, регулюється температура і засуваються жалюзі, схожий на кадр з фільму про далеке майбутнє. Однак майбутнє набагато ближче, ніж нам здається. Система «розумний будинок» дозволяє повною мірою відчувати блага технічного прогресу і позбавляє людину від вирішення безлічі побутових завдань.

Перше поняття «розумний будинок» з'явилося в 50-х роках минулого століття. Прародителькою системи, здатної контролювати обстановку в цілому будинку, є технологія Java. Розробники цієї технології намагалися впровадити її в побутові прилади, тим самим зробивши їх більш «інтелектуальними».

Наприклад, вже в той час почали з'являтися перші вбудовувані мікрохвильові печі, кондиціонери, здатні регулювати мікроклімат приміщення залежно від погоди за вікном і т. д.

Однак поняття «розумний будинок» включає в себе не тільки інтелектуальну побутову техніку. Якщо пояснювати простими словами, то ця система координує роботу всіх технічних пристроїв, що знаходяться в будинку.

Причому управління системою може здійснюватися як за допомогою пульта, так і дистанційно, за допомогою сучасних девайсів — айфона, смартфона, планшета і т. д.

Розумний будинок - це інтелектуальна система управління, яка об'єднує в єдиний комплекс все обладнання, вирішальне різні завдання у сфері забезпечення безпеки, життєзабезпечення, розваг і зв'язку.

Системи і підсистеми «розумного будинку»

Система «розумний будинок» умовно ділиться на кілька самостійних підсистем: безпека, освітлення, multiroom та клімат-контроль.

Система безпеки розумного будинку включає в себе такі елементи, як сигналізація, протипожежні датчики, а також датчики, що реагують на несправність комунікативних ліній. Під час відсутності господаря в домі автоматично включається сигналізація та протипожежні датчики, а в разі виникнення небезпечної ситуації, будь то небажане вторгнення або загоряння, система сповістить вас про це на віддалене пристрій — мобільний телефон, планшет або комп'ютер. Також програма негайного оповіщення зреагує і в тому випадку, якщо в будинку несподівано протечуть труби чи станеться витік.

Система освітлення розумного будинку управляє всіма освітлювальними елементами об'єкта. При необхідності вона відключає непотрібні в даний момент джерела світла, автоматично регулює ступінь освітленості в залежності від часу доби і навіть пори року, а також включає світло, як тільки ви з'являєтесь в будинку. Крім того, щоб відвернути увагу зловмисників, у системі можна встановити програму періодичного включення/вимикання світла у якому-небудь приміщенні під час вашої відсутності в будинку. Система multiroom відповідає за розподіл аудіо — і відеосигналу по всій квартирі. Вона може включати і вимикати техніку, передавати сигнал на всі пристрої, регулювати звук, а також створювати оптимальні умови для перегляду відео або прослуховування музики. Крім того, якщо інтегрувати систему multiroom з системою безпеки, то запис з камер відеоспостереження можна переносити на будь-який підключений до програми пристрій. Наприклад, якщо ви знаходитесь далеко від дому, ви завжди можете спостерігати за тим, що відбувається під час вашої відсутності з допомогою допоміжних пристроїв комп'ютера або мобільного телефону, підключеного до системи.

Система клімат-контроль в «розумному будинку» керує пристроями, що відповідають за опалення, кондиціонування, очищення і зволоження повітря. Вибравши необхідний режим, ви можете налаштувати систему так, щоб вона нагрівала приміщення до вашого приходу, періодично очищала повітря, а також зволожувала його до оптимальних показників. Крім своєї зручності, ця система приваблива ще і можливістю заощаджувати енергоресурси. Клімат-контроль самостійно визначає необхідний рівень температури, вимикає прилади в разі перегріву і реагує на погоду за вікном. Крім вищезазначених підсистем, «розумний будинок» має масу інших допоміжних функцій. Наприклад, ви можете

автоматизувати роботу системи так, щоб обмежити доступ дітей до небезпечних елементів, встановити режим поливу 6 секретів осіннього догляду за газоном: допоможемо йому перезимувати і прокинутися навесні красивим, включити цілодобове внутрішнє і зовнішнє відеоспостереження, налаштувати роботу техніки на необхідні режими і т. д.

Як виконується робота по установці

Що необхідно зробити для створення системи «розумний будинок» своїми руками:

- обладнати сервер
- налаштувати веб-сервер
- організувати комп'ютерне відеоспостереження для підвищення рівня безпеки
- підключити охоронні аналогові веб-камери і систему сигналізації
- налаштувати інтернет-з'єднання
- змонтувати мережу за допомогою підключених датчиків і інших виконавчих пристроїв
- підключити температурні датчики і системи освітлення
- створити управління опалювальною системою
- підключити всі інженерні мережі до єдиної системи «розумний будинок»

Перш ніж приступити до створення «розумного будинку», необхідно вибрати центральний блок управління (бажано комп'ютер). Цей пристрій допоможе забезпечити універсальність і простоту використання системи. За допомогою комп'ютера можна виконувати велику кількість різнопланових завдань у межах однієї системи, а також дрібних підсистем. Завдяки розвиненості сучасного обладнання, а також оснащення його найбільш поширеними протоколами, інтеграція підсистем в єдину систему «розумний будинок» стає дуже простий.

Після того як ви визначилися з пристроєм керування, необхідно підключити до нього камери, що забезпечують запис відео для підвищення безпеки мешканців. Після таких процедур підключитися до відеоспостереженню можна за допомогою віддаленого робочого столу, навіть не перебуваючи вдома. Крім камер, необхідно підключити сигналізацію і спеціальні датчики. Також до сервера можна підключити 1-wire датчики, за допомогою яких можна автоматизувати включення і відключення прибудинкового освітлення в залежності від кліматичних особливостей; отриману інформацію можна використовувати для контролю температурного режиму всередині квартири або будинку.

Висновок:

Система «розумний будинок» робить житло максимально зручним, комфортним і безпечним. Завдяки технічній досконалості, вона значно спрощує життя людини, економлячи при цьому час і енергетичні ресурси.

Література:

1. <http://bud-porada.in.ua/sistema-umnyj-dom.htm>
2. <http://yakrobiremont.pp.ua/sistema-rozumnij-budinok-visokointelektualne-zhitlo/>
3. <http://ukrbukva.net/page,5,81947-Intellectual-naya-sistema-upravleniya-Umnyiy-dom.html>

Кисіль Владислав Андрійович
Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації
м.Київ

ВІРУС ШИФРУВАЛЬНИК ЯК ОДИН З ВИДІВ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто порівняння двох вірусів-шифрувальників, їх основні цілі, способи розповсюдження, способи шифрування. Наведено основні методи запобігання інфікування вірусом комп'ютера користувачів. Оскільки за останній час було зафіксовано низку масштабних кібератак вірусів-шифрувальників, які були спрямовані на шифрування даних, що знаходяться на жорстких дисках користувач з подальшим вимаганням коштів.

Віруси-шифрувальники, також їх ще називають криптографічні віруси – це особливий вид програмного забезпечення, який здійснює шифрування всіх файлів на жорсткому диску. Після того як вірус зашифрував всі файли вірус активізується та блокує доступ до всіх даних, до того вірус не видає своє існування.

За останні пів року на території України сталося 4 масштабних кібератаки за участі вірусів-шифрувальників, а саме: PetyaA, Locky, Bad Rabbit та Scarab. За офіційними даними кіберполіції вірус PetyaA вразив по всій території України більше ніж 12500 комп'ютерів. На територію України припало 12,2% всієї атаки вірусів Locky та Bad Rabbit.

Вірусні атаки Locky та Bad Rabbit були здійснені в один день, хоч кінцева мета кіберзлочинців і була ідентична – шифрування даних на жорсткому диску, але способи поширення шкідливого коду були різними.

Вірус Locky поширювався через фішингові розсилки електронних листів, зворотна адреса яких асоціювалася зі службою підтримки Microsoft, в яких містилися документи з розширенням .doc та .rtf. Після відкриття цих документів користувачем починалося інфікування комп'ютер, шкідлива програма завантажувала та виконувала файл вірусу, експлуатуючи вразливість у функції DDE офісного пакету. Далі вірус шифрував файли на диску і вимагав викуп для зловмисників..

Для поширення вірусу Bad Rabbit зловмисники скомпрометували популярні сайти, запровадивши в них шкідливий JavaScript код. Як тільки користувач заходив на заражений сайт з'являлося впливаюче вікно з пропозицією завантажити оновлення для Flash Player. Але впливаюче вікно з'являлося не завжди, а лише для користувачів, які були обрані за особливим алгоритмом. Далі

поширення вірусу в локальній мережі відбувалося через сканування внутрішньої мережі на наявність SMB-файлів з відкритим доступом, також через протокол HTTP WebDAV, який заснований на HTTP і дозволяє використовувати Web як ресурс для читання і запису.

За даними антивірусних аналітиків ESET, Bad Rabbit — це модифікована версія вірусу Win32 / Diskcoder.C, більш відомого як Petya/NotPetya. У новій шкідливої програми виправлені помилки в шифруванні файлів. Тепер воно здійснюється за допомогою DiskCryptor — легітимного ПЗ з відкритим вихідним кодом, призначеного для шифрування логічних дисків, зовнішніх USB-накопичувачів і образів CD/DVD, а також завантажувальних системних розділів диска. Ключі генеруються з використанням CryptGenRandom і захищені жорстко закодованим відкритим ключем RSA 2048. Як і раніше, використовується алгоритм AES-128-CBC.

Кінцевою метою Bad Rabbit було шифрування жорсткого диску комп'ютера і друк на екрані повідомлення з вимогою викупу. Вірус вразив ряд популярних ЗМІ та деякі державні підприємства.

Успішність кібератак, що були спрямовані проти підприємств, свідчить про те що бізнес та держоргани приділяють недостатньо уваги інформаційному захисту. Важливо регулярно оновлювати антивірусне програмне забезпечення та прикладні програми, не відкривати вкладення електронної пошти, що прийшла від неперевіреного відправника. Також одним з основних аспектів захисту від кібератак є своєчасне створення резервних копій критично важливої інформації.

Література:

1. Повідомлення департаменту кіберполіції Національної поліції [Електронний ресурс] – Режим доступу: <https://www.facebook.com/cyberpoliceua/posts/601564659967701>.
2. Повідомлення департаменту кіберполіції Національної поліції [Електронний ресурс] – Режим доступу: <https://www.facebook.com/cyberpoliceua/posts/602125623244938>
3. Звіт аналітиків ESET [Електронний ресурс] – Режим доступу: <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/>

Вовк Надія Ігорівна

*Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації
м.Київ*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОРГАНІЗАЦІЙНОЇ КУЛЬТУРИ

Під інформаційними технологіями слід розуміти комплекс взаємозалежних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і зберіганням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим устаткуванням, їх практичні додатки, а також зв'язані з усім цим соціальні, економічні та культурні проблеми.

Самі інформаційні технології вимагають складної підготовки, великих первісних витрат і наукомісткої техніки. Їх введення повинно починатися зі створення математичного забезпечення, формування інформаційних потоків у системах підготовки фахівців.

На сьогодні інформаційні технології займають велике місце в нашому житті. Застосування ЕОМ стало буденною справою, хоча ще зовсім недавно робоче місце, обладнане комп'ютером, було великою рідкістю. Інформаційні технології дали нові можливості для роботи і відпочинку, багато в чому полегшили працю і просто життя кожної сучасної людини. Теперішнє суспільство навряд чи можна уявити без інформаційних технологій.

Інформаційні технології дуже швидко перетворилися на життєво важливий стимул розвитку не тільки світової економіки, а й інших сфер людської діяльності. Сьогодні практично неможливо знайти сферу, в якій не використовуються інформаційні технології.

Інформація є одним з чинників формування організаційної культури. Різний підхід до використання інформаційних ресурсів є однією з основних ознак відмінності організаційних культур. Принципово кращим варіантом використання інформації є її загальнодоступність при ухваленні рішень, виконанні необхідних розрахунків та підготовки науково обґрунтованих прогнозів.

Оскільки організаційна культура є одним з елементів внутрішнього середовища організації, то вона формується управлінням значною мірою залежно від того, наскільки ефективним є обмін інформацією між працівниками. Від рівня використовуваних інформаційних технологій залежить і вирішення питань, пов'язаних з підтримкою та розвитком організаційної культури.

Вільний доступ до інформації характеризує сильну організаційну культуру, яка й відрізняється від слабкої культури тим, що працівники відчують себе невід'ємною частиною могутнього єдиного колективу, що має загальні устремління та цінності, добре поінформованого про діяльність один одного.

Організація може використовувати при цьому такі сучасні інструментальні інформаційні технології: гіпертекстові технології, машинну графіку, телекомунікаційні методи доступу, структурні й об'єктно-орієнтовані технології, мультимедіа.

Гіпертекст. Ця технологія дає змогу працювати з великими об'єктами семантичної (понятійної) інформації. Актуальність та значимість гіпертексту зростають в епоху якісних перетворень. Методологія гіпертекстового інформаційного моделювання та відповідні інструментальні засоби дають можливість формалізувати текстові описи систем, що реформуються, проектувати і обробляти інформаційні моделі різних економічних об'єктів і процесів у їх взаємозалежності та взаємообумовленості. Корисність цієї технології особливо виявляється тоді, коли створюється нова цілісна соціально-

економічна концепція, і є необхідна упевненість у тому, що величезна кількість нормативно-правових документів відповідатиме основним принципам розвитку.

Графіка. Накопичення знань про світ, вирішення завдань, що виникають перед фахівцями, можливо здійснити двома способами: алгебраїчним та геометричним. Алгебраїчний — дає змогу запроваджувати на практиці алгебраїчні моделі, які спираються на ідею символічних перетворень. Геометричний — генерує у людини певні асоціації, за допомогою яких формуються інтелектуальні підказки. Для особи, яка ухвалює рішення, важливо, робити вибір самостійно на основі запропонованої їй інформації, власного досвіду та знань. В умовах ринку велика увага приділяється науковій візуалізації даних з метою демонстраційного представлення наукових та комерційних результатів. Демонстраційна машинна графіка дає змогу вирішувати три основні типи завдань: робота з діаграмами; редагування зображення; підготовка та планування демонстраційного матеріалу. Інтенсивний розвиток технології цього напрямку свідчить про актуальність тих завдань, які вони допомагають вирішувати.

Телекомунікації. Останнім часом активно запроваджуються комп'ютерні системи громадського доступу: комерційні бази даних тематичного характеру; системи електронних бірж та рекламних дошок; системи віддаленої обробки інформації; засоби надання інформаційних та інших видів послуг. Основними формами реалізації цих систем є локальні обчислювальні мережі та телекомунікаційні системи. Можливості локальних обчислювальних мереж жорстко обмежені територіально. Найбільшу гнучкість і широту можливості мають засоби телекомунікаційних систем. Наявні телекомунікаційні середовища відрізняються як за номенклатурою та характером функціональних можливостей, що надаються (електронна пошта, факси, послуги економічного банку даних), так і за вартістю своїх послуг.

CASE-технології. У зв'язку з тим, що проектування економічних інформаційних систем є трудомісткою, складною та тривалою роботою, виникла необхідність у розробці програмно-технологічних засобів спеціального класу — CASE-систем. Первинне значення терміну CASE — комп'ютерна розробка програмного забезпечення. Більшість наявних CASE-систем орієнтована на автоматизацію проектування програмного забезпечення та заснована на методологіях структурного проектування та програмування. Ці методології використовують специфікації у вигляді діаграм або текстів для опису системних вимог, зв'язків між моделями системи, динаміки поведінки системи та архітектури програмних засобів. Стратегія вибору CASE-системи для конкретного застосування залежить від: цілей і потреб самого проекту; кваліфікації залучених у процес проектування фахівців.

Мультимедіа. Це інтерактивна система, що забезпечує роботу з текстами, нерухомими та рухомими зображеннями, анімаційною комп'ютерною графікою,

мовою та високоякісним звуком. Для реалізації мультимедіа був розроблений новий тип персонального комп'ютера — NEXT. Організація роботи з NEXT — особлива форма спілкування людини з ЕОМ. Якщо раніше взаємодія здійснювалася за допомогою інтерфейсу WIMP (вікно, образ, меню, покажчик), то комп'ютер типу NEXT дає можливість працювати з інтерфейсом SILK (усна мова, образ, мова, знання). Поява систем мультимедіа призвела до кардинальних змін у таких сферах, як бізнес, комп'ютерний тренінг, освіта. Це, у свою чергу, дало змогу динамічно відстежувати індивідуальні запити світового ринку, створювати відеокаталоги виробів, що продаються, комерційні бази, довідники, проводити ділові відеоконференції.

Викорастана література:

<http://westudents.com.ua/glavy/47487-94-suchasn-nformatsyn-tehnolog-organzatsyno-kulturi.html>
<http://libr.rv.ua/ua/virt/133/>

Бердник Олена Василівна
*Державний університет телекомунікацій,
Навчально-науковий інститут захисту інформації
кафедра Інформаційної та кібернетичної безпеки
Київ*

ІНТЕРНЕТ РЕЧЕЙ, ЯК ОСНОВНА СУЧАСНА УРАЗЛИВІСТЬ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРИСТУВАЧІВ

Розглянуто основні принципи, сфери використання та проблеми використання IoT

(Internet of Things- Інтернет речей). Через розвиток IoT, ростуть ризики безпеки для організацій та користувачів, також постає проблема у складності моніторингу. При створенні IoT-пристроїв безпека, як правило, не стоїть на першому місці, хоча спеціалісти служб інформаційної безпеки повинні розуміти потенціальні слабкі місця IoT. Встановлено, що необхідно використовувати динамічний підхід до забезпечення безпеки, а також впроваджувати стратегію багаторівневого захисту IoT-пристроїв.

Інтернет речей (Internet of Things, IoT) — це міжмережева взаємодія фізичних пристроїв, транспортних засобів, будівель й інших предметів (які ще часто називають «підключені пристрої» чи «розумні пристрої»). Вони мають вбудовану електроніку, програмне забезпечення, датчики, привідні механізми і здатні підключатися до мережі, що дозволяє їм збирати дані і обмінюватися ними. Прийнято вважати, що IoT включає три основні елементи – інформаційні технології, експлуатаційні технології та технології користувача.

Промисловий Інтернет речей (Industrial Internet of Things, IIoT) визначає тільки підключені пристрої в рамках мережі управління промисловим процесом, на відміну від корпоративної мережі чи центру обробки даних.

IIoT відкриває великі можливості для співробітництва та інновацій у різних сферах. З розвитком IIoT, ростуть й ризики безпеки для організацій та користувачів. Однією із проблем є складність моніторингу. Більшість спеціалістів служби безпеки не знають, які IIoT-пристрої підключені до їх мережі. При створенні IIoT-пристроїв безпека, як правило, не стоїть на першому місці. Підключені пристрої не мають необхідного рівня безпеки, на відміну від настільних систем, та мають уразливості, на усунення яких можуть витрачатися місяці, а то і роки. Крім того, для них є характерним:

- Звітність про уразливості, ризики та оновлення практично чи повністю відсутні.
- Запуск відбувається на спеціалізованій архітектурі.
- Наявність неоновлених пристроїв чи застарілих додатків, що мають уразливості – наприклад, Windows XP.
- Оновлення використовуються дуже рідко.

Крім того, у випадку атаки на систему доступ до IIoT-пристроїв для їх безпосередніх власників ускладнений чи взагалі неможливий, що не дає виконувати відповідні реакції. Тому ці пристрої несуть великий інтерес для зловмисників.

На питання безпеки IIoT-пристроїв впливає той факт, що спеціалісти служби інформаційної безпеки можуть не розуміти характер сигналів тривоги, що надходять з цих пристроїв. Крім того, не завжди зрозуміло хто із співробітників організації несе відповідальність у випадку атаки на IIoT.

Спеціалісти служб інформаційної безпеки повинні розуміти потенціальні слабкі місця IIoT, оскільки зловмисники орієнтуються на необізнаність при спробах запустити зловмисні програми, викрадення конфіденційної інформації, скомпрометовану мережу.

Вдала масова атака на ці пристрої здатна суттєво підірвати діяльність як комерційних підприємств, державних організацій, так і всього Інтернету в цілому. DDoS-атаки з використанням IIoT-пристроїв вже стали реальністю, і поява IIoT-ботнетів дозволяє припустити, що зловмисники можуть нанести шкоду в більших масштабах.

Для того щоб впоратись з проблемами безпеки, які створені стрімким розвитком і все менш контрольованим IIoT, спеціалістам служби інформаційної безпеки необхідно дотримуватись наступних рекомендацій:

- Продовжувати використання застарілих сигнатур.
- Захищати IIoT-пристрої за допомогою систем запобігання вторгнень.
- Уважно відстежувати мережевий трафік (особливо в IIoT-середовищах, де легко прогнозувати профіль мережевого трафіку).
- Відстежувати, як IIoT-пристрої з'єднанні з мережею і взаємодіють з іншими пристроями (наприклад, якщо IIoT-пристрій сканує інший пристрій, це може вказувати на дії зловмисника)

- Своєчасно використовувати виправлення.
- Працювати з постачальниками, які забезпечують безпеку продукту (дотримуються вимог PSB — Product Security Baseline) і публікують бюлетні по безпеці (Security Advisories).

Отже, для захисту IoT-пристроїв від компрометації та атак (чи хоча б для зменшення наслідків у випадку вдалої атаки зловмисника) необхідно використовувати динамічний підхід до забезпечення безпеки, а також впроваджувати стратегію багаторівневого захисту.

Література :

1. Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року. [Електронний ресурс] – Режим доступу: <https://communities.cisco.com/docs/DOC-76212>
2. IoT Security Foundation [Електронний ресурс] – Режим доступу: <https://www.iotsecurityfoundation.org>
3. "Умная" электроника: какие угрозы таит "Интернет вещей" [Електронний ресурс] – Режим доступу: <https://bin.ua/news/interesting/it/150328-umnaya-yelektronika-kakie-ugrozy-tait-internet.html>

***Дорохін Орест Олександрович**
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

РОЗВІДКА УРАЗЛИВОСТЕЙ ЯК ПЕРШИЙ ЕТАП КІБЕРАТАКИ

Першим етапом будь-якої кібератаки є розвідка, в ході якої зловмисник збирає якомога більше інформації про компанії, що стала мішенню для злому. Знайдені відомості необхідні для виявлення вразливостей, атакуючий виконує аналіз сайту компанії і її інформаційних систем, а також розглядає способи взаємодії мети з іншими організаціями. Як тільки уразливість знайдена, починається підбір інструментів для злому і підготовка до їх застосування.

Тестування безпеки - оцінка уразливості програмного забезпечення до різних атак, визначається тип і кількість тестованих систем. Найбільш часто визначаються наступні параметри для зовнішнього тестування:

Опції тестування можуть включати:

- Тестування внутрішнього периметра мережі. Повний тест на проникнення або ж проведення автоматизованого сканування вразливостей внутрішніх ресурсів компанії. Визначається кількість IP адрес, веб-сайтів і додатків.
- Аналіз змін мережевих пристроїв, додатків і серверів на відповідність стандартам безпеки. Виробники, що випускають обладнання та додатки, визначають власні рекомендації з безпеки. Аналіз проводиться з метою виявлення відхилень у рекомендаціях.

- Аналіз коду веб-сайтів. Код перевіряється на наявність вразливостей типу: SQLinjection, command injection, file inclusion, DoS, на наявність несанкціонованих закладок, недоліків в архітектурі та ін.
- Аналіз коду додатків. Код перевіряється на наявність вразливостей типу: Bufferoverflow, DoS, на наявність несанкціонованих закладок, недоліків в архітектурі і ін.
- Аудит мобільних пристроїв. Аналіз безпеки використання телефонів, смартфонів, планшетів, також устрій ств хр Аненій даних, таких як USB, плесрів і інших мобільних пристроїв.

Також важливо визначити порядок надання звітності. Кваліфікований аудитор зможе надати розгорнуту інформацію про виконану роботу для менеджменту в зрозумілій формі.

З найбільш доцільних варіантів:

- один результуючий звіт після закінчення тестування;
- надання окремого звіту відразу при виявленні критичної уразливості;
- проміжні звіти раз в 2-3 дня.

Необхідно також визначити наступні організаційні моменти:

- канали зв'язку для обміну інформацією між замовником і тестерами. Цілком очевидно, що вони повинні бути зашифровані;
- відповідальність осіб з боку виконавця і замовника;
- порядок дій у разі виникнення інцидентів, пов'язаних з проведенням тестування;
- обмеження тестування (наприклад, тільки у вихідні дні, тільки безпечні перевірки для певних систем і т.д).

Всі заходи з тестування проводяться тільки після підписання договору, а також угоди про нерозголошення з виконавцями. Виконавець зі свого боку проводить внутрішню підготовку до тесту: інструктаж персоналу, організацію спільної роботи, підготовку необхідного устаткування і ПО, каналів зв'язку та інше.

Збір інформації

Першочерговим завданням аудиторів на даному етапі є збір якомога більшої кількості інформації про тестованих системах і про співробітників компанії. Пошук інформації відбувається в доступних джерелах вручну, а також за допомогою спеціалізованих інструментів. У обсяг робіт, як правило, входить пошук інформації в таких джерелах:

- пошукові системи;
- соціальні мережі і сайти знайомств;
- каталоги підприємств;

- новинні сайти;
- корпоративні сайти компанії замовника, сайти клієнтів і партнерів;
- сайти пошуку роботи;
- бази даних WHOIS;
- DNS сервера компанії;
- аналіз маршрутів і виявлення мережевого обладнання;
- чорні списки спамерів;
- аналіз e-mail листів;
- Дзвінківcall центр компанії з метою отримати інформацію про ключових співробітників компанії, про структурі компанії і технологіях;
- безпосереднє сканування мережі різними інструментами для виявлення IP адрес, портів, версій працюють сервісів і операційних систем
- аналіз метаінформації в документах, розміщених на сайтах компанії;
- «Дайвінг» в сміттєві_баки компанії з метою знайти конфіденційну інформацію і інші методи.

Сканування - це набір процедур, що дозволяють ідентифікувати вузли, порти і сервіси цільової системи. Сканування мережі дозволяє зловмисникові зібрати профіль організації, що атакується.

Варто зазначити, що сканування не завжди зловмисна дія, фахівці з IT-безпеки використовують в своїй роботі спеціалізоване апаратне або програмне забезпечення, скануючий мережу і її пристрої на предмет виявлення слабких місць в системі безпеки.

Таким чином, мережеві сканери спрямовані на вирішення наступних завдань:

- ідентифікація та аналіз вразливостей;
- інвентаризація ресурсів, таких як операційна система, програмне забезпечення та пристрої мережі;
- формування звітів, що містять опис вразливостей і варіанти їх усунення.

Згідно керівництву по етичному хакінгу (Ethical Hacking and Countermeasures EC-Council) розрізняють такі типи сканування:

- мережеве сканування – визначення розташування вузлів в мережі;
- сканування портів - виявлення відкритих портів і функціонуючих сервісів;
- сканування безпеки системи - виявлення відомих вразливостей системи.

Сканери уразливостей мережі під час своєї роботи використовують два основних механізми. Перший — *зондування* — не дуже оперативний, але точний. Це механізм активного аналізу, який запускає імітації атак, перевіряючи таким чином уразливість. При зондуванні використовуються методи реалізації атак, які допомагають підтвердити наявність уразливості та виявити досі не виявлені «провали».

Другий механізм — *сканування* — більш швидкий, але надає менш точні результати. Це пасивний аналіз, при якому сканер шукає уразливість без підтвердження її існування, використовуючи непрямі ознаки.

В загальному випадку алгоритм роботи сканерів наступний:

- **Перевірка заголовків.** Найшвидший і найпростіший спосіб на основі сканування, однак вододіючий рядом недоліків. Так, виведення про «провал» робиться лише по результатам аналізу заголовків.
- **Активні зондуючі перевірки (active probing check).** Це сканування, при якому не перевіряється версія ПО, а порівнюється «цифровий зліпок» фрагмента програми із «зліпком» уразливості. Таким чином функціонують антивірусні програми, порівнюючи ПО з наявними в базі сигнатурами вірусів. Теж доволі швидкий метод, хоча і повільніший за перший, з більшим коефіцієнтом надійності.
- **Імітація атак (exploit check).** Це зондування, яке експлуатує дефекти програмного забезпечення. Таким чином подається своєрідний імпульс деяким уразливостям, які не помітні до певного моменту. Ефективний метод, однак його не завжди можна використати. Так, вірогідна ситуація, коли навіть імітована атака просто відключить вузол мережі, що перевіряється або уразливість виявиться непридатна для реалізації атаки. Більшість сучасних сканерів безпеки мережі функціонує по

нижчепереліченим принципам:

- збір інформації про мережу, ідентифікація усіх активних пристроїв та сервісів, завантажених на них;
- виявлення потенційних уразливостей;
- підтвердження обраних уразливостей, для чого використовуються специфічні методи і модулюються атаки;
- формування звітів;
- автоматичне усунення уразливостей. Не завжди даний етап реалізується в мережевих сканерах безпеки, але часто зустрічається в сканерах системних. Існує можливість створення резервного сценарію, який може відмінити виконані зміни, — наприклад, якщо після усунення уразливості буде порушено повноцінне функціонування мережі.

ЛІТЕРАТУРА І ПОСИЛАННЯ

1. https://ru.wikipedia.org/wiki/Тестирование_безопасности
2. <http://auditagency.com.ua/?r=blog&p=Pentest>
3. <http://www.kp.ru/guide/setevye-skanery-bezopasnosti.html>
4. <http://citforum.ck.ua/security/internet/vulnerability/>
5. «Информационная безопасность: защита и нападение»
Автор: Андрей Бирюков. Глава №4.

ЕТАПИ РЕАЛІЗВЦІЇ АТАКИ

В час розвитку й ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від рівня безпеки інформаційних технологій. Одним з найважливіших кроків для забезпечення безпеки інформаційних ресурсів є розуміння всіх етапів реалізації атаки.

1. Розбір уразливостей, можливість реалізації атак

В час розвитку й ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від рівня безпеки інформаційних технологій.

Вразливість автоматизованої системи – властивість системи, що робить можливим виникнення і реалізацію загрози.

Розглянемо можливі уразловості та загрози:

По меті впливу вразливості розділяються на три основні порядки:

- вразливості першого порядку – загрози порушення конфіденційності інформації;
- вразливості другого порядку – загрози порушення цілісності інформації;
- вразливості третього порядку – загрози порушення працездатності системи (відмовлення в обслуговуванні) .

При розгляді наслідків атаки на вразливість системи, модель характеризує успішність атаки, але не вартісні наслідки, викликані розкриттям, порушенням цілісності інформації чи відмовленням в обслуговуванні.

Оцінкою наслідків використання вразливості є оцінка кількості користувачів, задіяних в результаті успіху атаки на вразливість ЗАС. Якщо вразливість присутня в ЗАС, що захищає інформацію від загрози розкриття, то можливі наступні варіанти несанкціонованого доступу:

- до визначеної інформації користувача;
- до всієї інформації користувача;
- до всієї інформації групи користувачів;
- до всієї інформації всіх користувачів у системі.

2. Розробка методів реалізації атак, підбір технічних і програмних заходів

Перш ніж виконувати атаку на комп'ютерну систему, створюється стратегічний план. Сюди входить розвідка сил противника, його оборони, формування відповідного складу сил, розробка (якщо потрібно) додаткових атакуючих резервів.

Для успішної реалізації атак на систему, хакеру необхідно дізнатися:

- 1) тип атакуючої системи;
- 2) рівень знань користувача системи (жертви)
- 3) заходи захисту;
- 4) слабкі місця даної системи;
- 5) усвідомлювати мету атаки,
- 6) оцінити ймовірність успіху,
- 7) дізнатися, чи не зламувалася подібна система раніше і чи має вона типові проблеми безпеки.
- 8) що робити після успішного проникнення / виконання мети атаки.

3. Проникнення в систему будь-якими способами

Існує декілька основних методів проникнення в систему:

1. *Соціальна інженерія*
2. *Технічні методи*

a. Мережеві хробаки

Хробаки можуть розповсюджуватись наступними способами:

- i. Електронні листи
- ii. FTP
- iii. ICQ або його сучасні аналоги
- iv. P2P
- v. Напрямку через порти
- vi. USB та інші носії

vii. Трояни

- b. Сніффери**
- c. DoS атаки**
- d. Bruteforce**

3. Комбіновані методи

- a. Фішинг**
- b. Антивірусні програми, що мають у собі шкідливий код**
4. *Фізичний підхід*

4. Автоматичний збір інформації, обман системи

Електронне шпигунство, інтернет шпигунство - види збору інформації, в основі яких лежать інформаційно-комп'ютерні технології. За масштабами цей вид шпигунства вже далеко перевершив всі інші способи отримання інформації.

Можна виділити три рівні кібершпionaжу: державний, корпоративний, особистісний. Шпигунство завжди супроводжувало державну діяльність.

Автоматичний збір інформації передбачає автоматичне виділення інформації та її перетворення в необхідну форму.

Автоматичний збір інформації здійснюється за допомогою таких методів:

- Переповнення буфера

- Троянські коні, черв'яки, сніффери, руткіти та інші спеціальні програми
- Сніффінг пакетів
- Man-in-the-Middle

5. Реалізація цілей атак

Кібератака — спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі.

Характерна особливість кібератак — миттєвість їх здійснення (протягом секунд, хвилин). Класифікують кібератаки за наведеними далі ознаками.

За принципом впливу на об'єкт атаки поділяються на:

- використання прихованих каналів;
- застосування прав суб'єкта системи до об'єкта;

За характером впливу на об'єкт атаки поділяються на:

- активний вплив;
- пасивний вплив;

За способом впливу на об'єкт атаки поділяються на:

- систему дозволів (захоплення привілеїв),
- безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв.

За засобами впливу на об'єкт атаки поділяються на ті, що передбачають:

- використання стандартного ПЗ;
- спеціально розроблених програм.

За об'єктом атаки: напад може здійснюватися на:

- систему в цілому;
- дані і програми, що містяться на зовнішніх або внутрішніх пристроях системи, а також у каналах передавання даних;
- процеси і підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях).

За станом об'єкта: безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися. Наприклад, у ході передавання інформації лініями зв'язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації через перехоплення пакетів на ретрансляторі мережі або прослуховування з використанням прихованих каналів.

Зауважимо, що абсолютна більшість зазначених видів кібератак на практиці не застосовується. Натомість набула поширення класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши кількість можливих категорій кібератак до п'яти, фахівці компанії умовно виокремили з них такі, що мають на меті:

- 1) сприяти збору інформації;
- 2) сприяти спробам несанкціонованого доступу до інформації;

- 3) досягти стану відмови в обслуговуванні;
- 4) імітувати підозрілу активність;
- 5) чинити вплив на операційні системи.

Згідно з міркуваннями фахівців компанії, перші чотири категорії охоплюють вилучені (можливо, віддалені) кібератаки, а остання стосується локальних кібератак (вони реалізуються на вузлі, що зазнає атаки). При цьому всі кібератаки можуть бути як автоматизованими, так і неавтоматизованими.

Цілі хакерських атак:

- Готовий веб-хостинг
- Розміщення ботів
- Збір поштових адрес.
- Крадіжка особистості
- Розкрадання віртуальних цінностей
- Розкрадання фінансової інформації

Данні користувачів які цікавлять хакерів:

- Акаунти у соціальних мережах..
- Електронна пошта.
- Номер мобільного.
- Паспортні дані / ідентифікаційний код / фото.
- Особисте листування / фотографії / відео.
- Дані платіжних карт.

Методи викрадання інформації

1.Методи отримання паролів:

1. Підбір пароля онлайн
2. Підбір пароля оффлайн
3. Повторне використання пароля
4. Викрадення або підглядання пароля
5. Відновлення пароля через email або SMS
6. Перехоплення пароля по мережі

2. Викрадення даних в компанії

3.Викрадання персональних даних

6. Формування скритого каналу передачі вкраденої інформації

Прихований канал – це спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації.

За допомогою прихованих каналів можуть бути реалізовані наступні порушення політики безпеки:

- Загроза застосування шкідливих програм і даних.
- Загроза подачі порушником команд агентом для виконання його функцій.

- Загроза витоку криптографічних ключів, паролів (несанкціонований доступ до них) або окремих інформаційних об'єктів.

7. Приховування слідів присутності в системі

Є два аспекти завдання приховування слідів у системі:

- По-перше, це локальна безпека. Слід мати на увазі, що всі дії в віртуальному комп'ютерному світі залишають сліди і у системі суб'єкта також, що може стати джерелом великих проблем, адже це може стати доказами протизаконних дій
- По-друге, це глобальна безпека. Будь-які дії, в Інтернеті відслідковуються веб-серверами і фіксуються в лог-файлами як на серверах провайдера Інтернету, так і на відвіданих серверах.

Кроки для зачистки перебування системи: локально:

- Очистка реєстру.
- Очистка log-файлів програм авто-запуску
- Відключення аудиту.

Кроки для зачистки перебування системи: в Інтернеті:

Основний метод приховування діяльності в мережі «Інтернет» - підміна IP адреси.

Список використаних джерел

1. xaker.ru/2001/02/21/12020/
2. kaspersky.ru/internet-security-center/threats/viruses-worms
3. <http://conference.uapa.ru/attachment.php?aid=83>
4. <https://blog.kaspersky.ru/>

Пояркін Ігнатій Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м.Київ

ОСНОВНІ МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ

1. Шифр заміни, перестановки, комбіноване шифрування

На першому етапі розвитку криптології існувало два основних типу перетворень відкритих текстів – заміни й перестановки. Головна ідея шифрів заміни є заміна місця розташування символів відкритого тексту. Шифрів заміни було значне більше, але всі вони будувалися на заміні символу відкритого тексту символом зашифрованого тексту. До таких шифрів належать шифруючі таблиці, азбука Морзе, полібіанський квадрат, шифр Цезаря.

Існують різновиди шифрів заміни. Наприклад, шифр однозначної заміни. Максимальна кількість ключів для будь-якого шифру цього виду не перевищує $n!$, де n - кількість символів в алфавіті. Зі збільшенням числа n значення $n!$ росте дуже швидко

Шифр Цезаря - це шифр однозначної заміни. Тобто кожному символу відповідає єдиний символ з шифротаблиці. Для шифра Цезаря- кожний символ алфавіту замінюється на символ алфавіту, зміщений на деяке число.

Поліграмні шифри заміни - це шифри, в яких одна шифрозаміна відповідає відразу декільком символам вихідного тексту.

Біграммний шифр Порти. Шифр Порти, представлений ним у вигляді таблиці, є першим відомим біграммним шифром. Розмір його таблиці становив 20 x 20 осередків; нагорі горизонтально і зліва вертикально записувався стандартний алфавіт (в ньому не було букв J, K, U, W, X і Z). В осередках таблиці могли бути записані будь-які числа, букви або символи - сам Джованні Порти користувався символами - за умови, що вміст жодної з осередків не повторювалося.

Інший напрямок підвищення стійкості шифрів заміни полягає в тому, щоб кожна множина шифрозначень M_i містило більше одного елемента. При використанні такого шифру одну і ту ж букву (якщо вона зустрічається кілька разів в повідомленні) замінюють на різні шифрозаміни з M_i . Це дозволяє приховати справжню частоту зустрічальності букв відкритого повідомлення.

Поліалфавітні шифри складаються з декількох шифрів однозначної заміни і відрізняються один від одного способом вибору варіанта алфавіту для шифрування одного символу.

Шифр перестановки можна уявити як матрицю, в яку записується відкритий текст, потім переставляються стовпці та рядки матриці, и вже зчитується зашифрований текст.

Кобіноване шифрування - шифрування, при якому для зашифровки інформації використовується не один, а декілька різних по своїй сутності та складності шифрів. Як правило, в "чистому" вигляді шифри не зустрічаються, так як комбіноване шифрування більш криптостійке.

2 Квантове шифрування

Квантова криптографія - метод захисту комунікацій, заснований на принципах квантової фізики. На відміну від традиційної криптографії, яка використовує математичні методи, щоб забезпечити секретність інформації, квантова криптографія зосереджена на фізиці, розглядаючи випадки, коли інформація переноситься за допомогою об'єктів квантової механіки. Процес відправлення та прийому інформації завжди виконується фізичними засобами, наприклад, за допомогою електронів в електричному струмі, або фотонів в лініях волоконно-оптичного зв'язку.

Головною її особливістю, а заодно і особливістю будь-якої квантової системи є неможливість розкриття стан системи протягом часу, так, при першому ж вимірі система змінює свій стан на квантовому рівні. Наприклад, неможливо виміряти один параметр фотона, що не спотворивши інший (принцип невизначеності Гейзенберга). Іншими словами, використовуючи квантову криптографію, можна створити таку систему зв'язку, яка ЗАВЖДИ виявляє

підслуховування. Тобто, прихований злом або дешифрування неможливі, так як будь-який вплив на систему спотворює дані.

По своїй суті, квантова криптографія використовує особливості корпускулярно-хвильового дуалізму та поляризації фотонів, що являється великим скачком в захисті інформації.

3.Шифрування по ключу: Симетричні алгоритми шифрування

Симетричні алгоритми шифрування – спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же криптографічний ключ. До винаходу схеми асиметричного шифрування єдиним існуючим способом було симетричне шифрування. Ключ алгоритму повинен зберігатися в секреті обома сторонами. Алгоритми шифрування і дешифрування даних широко застосовуються в комп'ютерній техніці в системах приховування конфіденційної і комерційної інформації від не коректного використання сторонніми особами. Головним принципом у них є умова, що та приймає заздалегідь знають алгоритм шифрування, а також ключ до повідомлення, без яких інформація є всього лише набір символів, що не мають сенсу. Симетричні криптоалгоритми виконують перетворення невеликого (1 біт або 32-128 біт) блоку даних в залежності від ключа таким чином, що прочитати оригінал повідомлення можна тільки знаючи цей секретний ключ.

У міру розвитку криптологія в симетричних криптологічних системах виділяються два головних напрямки шифрування: **блокові й потокові шифри**. У блокових шифрах відкритий текст розбивається на блоки фіксованої довжини й зазнає шифруванню. Причому кожний блок зашифровується своїм шифром, але алгоритм перемішування залишався однаковим для всіх блоків. На цьому принципі побудовані велика кількість шифрів, включаючи американський стандарт DES і національний стандарт ДЕРЖСТАНДАРТ 28147-89. У блокових шифрах широко використовується перемішування.

Блокові шифри в ході своєї роботи роблять перетворення блоку вхідної інформації фіксованої довжини і одержують результуючий блок того ж обсягу, але недоступний для прочитання стороннім особам, що не володіють ключем. Таким чином, схему роботи блокового шифру можна описати функціями $Z = \text{EnCrypt}(X, \text{Key})$ і $X = \text{DeCrypt}(Z, \text{Key})$. Ключ Key є параметром блокового алгоритму і являє собою деякий блок двійкової інформації фіксованого розміру. Вихідний (X) і зашифрований (Z) блоки даних також мають фіксовану розрядність рівну між собою, але необов'язково рівну довжині ключа.

Скремблерами(або поточним шифруванням) називаються програмні або апаратні реалізації алгоритму, що дозволяють шифрувати побітно безперервні потоки інформації. Сам скремблер представляє із себе набір бітів, що змінюються на кожному кроці по певному алгоритму. Після виконання кожного чергового кроку на його виході з'являється біт, що шифрує, – або 0, або 1, що

накладається на поточний біт інформаційного потоку . Основним недоліком алгоритмів скремблювання є їхня нестійкість до фальсифікації.

При використанні поточкових шифрів кожний символ відкритого тексту зашифрується незалежно від інших. Також головною проблемою створення поточкового шифру є створення послідовності, що шифрує. Вимоги до таких послідовностей досить тверді.

Враховуючи двійкову систему можна сказати, що поточкові шифри дозволяють шифрувати інформацію побітово, а блочні працюють з деяким набором біт даних(зазвичай розмір блоку - 64 біта) і шифрують цей набір як єдине ціле.

Як тільки ми починаємо говорити про шифри, перед нами встає проблема їх передачі до одержувача. При використанні поточкових шифрів вони можуть вироблятися як на передавальному, так і на прийомному кінцях лінії зв'язку. Слід зазначити той факт, що в цей час практично жоден шифр не є чистим, у тому розумінні, що ставиться до одного з видів. Найчастіше використовується комбінація декількох шифрів.

Наступним більшим класом є асиметричні криптологічні системи або системи з відкритим ключем. Головною ідеєю при створенні цього класу шифрів є генерація двох ключів. Один відкритий ключ поширюється по відкритих каналах зв'язку й використовується при шифруванні повідомлень. На прийомній стороні за допомогою секретного ключа проводиться розшифрування повідомлення. Основою при створенні таких шифрів, як сказано вище, є задачі з важким розв'язком.. У якості таких задач у цей час використовуються задачі факторизації, дискретного логарифмування й методи теорії завадостійкого кодування.

4. Шифрування по ключу: Асиметричні алгоритми шифрування

Асиметричні алгоритми шифрування – алгоритми шифрування, які використовують різні ключі для шифрування та розшифрування даних. Головне досягнення асиметричного шифрування в тому , що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпала. Процедура шифрування обрана так, що вона необоротна навіть по відомому ключу шифрування. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення – прочитати його можна тільки за допомогою другого ключа – ключа дешифрування. А раз так, то ключ шифрування для відправлення листів якій-небудь особі можна взагалі не приховувати – знаючи його однаково неможливо прочитати зашифроване повідомлення. Тому, ключ шифрування називають в асиметричних системах “відкритим ключем”, а от ключ дешифрування одержувачеві повідомлень необхідно тримати в секреті – він називається “закритим ключем”. Алгоритми

шифрування й дешифрування створюються так, щоб знаючи відкритий ключ, неможливо було обчислити закритий ключ.

Порівняння асиметричних і симетричних криптоалгоритмів:

Асиметричні криптоалгоритми:

- Криптосистема з відкритим ключем;
- Для шифрування повідомлення використовується відкритий ключ, а при дешифруванні – закритий. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення;
- При порушенні конфіденційності k -ої робочої станції зловмисник довідається тільки “закритий” ключ k : це дозволяє йому читати всі повідомлення, що приходять абонентові k , але не дозволяє видавати себе за нього при відправленні листів;
- В асиметричних системах кількість існуючих ключів пов’язане з кількістю абонентів лінійно (у системі з N користувачів використовуються $2 \cdot N$ ключів).

Симетричні криптоалгоритми

- Криптосистема з секретним ключем;
- Секретний ключ використовується і для шифрування, і для дешифрування. Тобто, знаючи ключ шифрування й зашифрований текст, ви зможете дешифрувати повідомлення;
- При порушенні конфіденційності якої-небудь робочої станції зловмисник одержує доступ до всіх ключів цього користувача й може відправляти, нібито від його імені, повідомлення всім абонентам, з якими “жертва” вела переписку;
- В симетричних системах число ключів зростає квадратично із збільшенням числа користувачів.

Література:

1. <https://habrahabr.ru>.
2. http://www.dut.edu.ua/uploads/l_491_94183247.pdf
3. <https://sites.google.com/site/anisimovkhv/learning/kripto/lecture>
4. <http://files.school-collection.edu.ru/dlrstore/28399747-3cbc-6ad7-b265-807b7918559a/1008585A.htm>
5. <http://ua-referat.com/%D0%86%D1%81%D1%82%D0%BE%D1%80%...>
6. <http://www.furfur.me/furfur/culture/culture/166567-kriptografiya>
7. <http://algolist.manual.ru/defence/intro.php>
8. http://kryptography.narod.ru/istoria_kratko.html
9. <https://books.google.com.ua>

КАДРОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В УКРАЇНІ

Аналіз сучасних масштабних кібератак, свідчить про зменшення часу між їх проведенням і збільшенням їх негативних наслідків. У таких умовах суттєвого значення набувають питання підготовки та кадрового забезпечення кіберзахисту інформаційних ресурсів і систем, вимоги щодо захисту яких установлені законодавством України.

У роботі, на підставі огляду відповідних нормативно-правових документів, запропоновано назви професій, пов'язаних з кібербезпекою та кіберзахистом, а також загальні завдання та обов'язки посадових осіб, відповідальних за забезпечення кібербезпеки та кіберзахисту.

За результатами аналізу сучасних кібератак, висвітлених на сайті CERT-UA (скор. – Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) спеціалізованого структурного підрозділу Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України, зазначимо найбільш масштабні та найнебезпечніші:

DDoS-атаки та злам сайту Центральної виборчої комісії України під час президентських виборів 21-25 травня 2014 року;

виявлення на серверах приватних компаній України і країн НАТО шкідливих програм, серед яких Turla/Uroburos/Snake, RedOctober, MiniDuke і NetTraveler, що призначені для кібершпionaжу, у червні 2014 року;

відключення близько 30 підстанцій одного з обленерго, внаслідок чого більш ніж 200 тисяч мешканців залишилися без електроенергії на термін від однієї до п'яти годин, а також хакерські атаки на інші обленерго за допомогою троянської програми BlackEnergy3, що відбулися 23 грудня 2015 року;

хакерська атака 6 грудня 2016 року на внутрішні телекомунікаційні мережі фінансових та деяких інших установ України, в результаті якої було виведено з ладу ряд комп'ютерів і знищено критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень;

хакерська атака 17 грудня 2016 року на електричну підстанцію однієї з енергетичних компаній, яка призвела до збою в автоматичі управління, через що більше години знеструмленими залишалися райони у північній частині правобережного Києва і прилеглі райони Київської області;

хакерська атака 27 червня 2017 року за допомогою вірусної програми Petya.A, що порушила роботу численних українських державних і приватних підприємств;

масова розсилка у серпні 2017 року банківського трояна Zeus;

розповсюдження у вересні 2017 року в українському сегменті мережі Інтернет повідомлень із шкідливим програмним забезпеченням, яке є оновленою версією GlobeInposter Ransomware;

непоодинокі випадки враження (Одеський аеропорт, Київський метрополітен та ін.) інформаційних ресурсів України 24 жовтня 2017 року з використанням техніки DDE, що активувала виконання шкідливого коду шифрувальника файлів Locky та Bad Rabbit на комп'ютерах користувачів завдяки drive-by download атаці;

розсилання 22-23 листопада 2017 року через спам-ботмережу «Necurs» електронних повідомлень з метою завантаження на комп'ютер користувача вірусу-шифрувальника файлів Scarab.

Це далеко неповний перелік спрямованих (навмисних) дій у кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій і спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту; та які з високою вірогідністю будуть відбуватися у майбутньому.

В Україні приділяється певна увага забезпеченню кібербезпеки як захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

5 жовтня 2017 року ухвалено Закон України «Про основні засади забезпечення кібербезпеки України», в якому узаконено терміни з префіксом «кібер» (-простір, -атака, -злочин, -тероризм, -розвідка, -шпіонаж тощо); встановлено, що політику в сфері кібербезпеки формує і реалізує Кабмін; визначені відповідальні за кібербезпеку в рамках своїх повноважень – міністерства, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні органи, органи розвідки і контррозвідки, суб'єкти оперативно-розшукової діяльності та інші; забезпечення кібербезпеки країни покладено на Збройні сили України, Національний банк, підприємства, які відносяться до об'єктів критичної інфраструктури, суб'єкти господарювання, громадян та їх об'єднання, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [1].

Також зазначеним Законом встановлено, що функціонування національної системи кібербезпеки забезпечується, серед іншого, шляхом підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням

в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів.

Так, у Державному університеті телекомунікацій до Переліку спеціальностей освітнього ступеня бакалавра і магістра уведено спеціальність «Кібербезпека», що здобувають у Навчально-науковому інституті захисту інформації за спеціалізаціями «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації, автоматизація її обробки» та «Управління інформаційною безпекою».

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, кіберзахист критичної інфраструктури має полягати, насамперед, у створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту. Важливим є подальший розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав-членів НАТО [2].

З метою залучення на державну службу кращих фахівців постановою Кабінету Міністрів України від 9 серпня 2017 року № 572 «Про внесення змін у примітки до схеми посадових окладів на посадах державної служби за групами оплати праці з урахуванням юрисдикції державних органів у 2017 році» підвищено на 20% посадові оклади державних службовців, які виконують функції із забезпечення кібербезпеки, кіберзахисту та безпеки інформаційних технологій.

Назви посад підрозділів кіберзахисту і професій у документах (трудових книжках, штатному розписі, посадових (робочих) інструкціях тощо) мають відповідати Національному класифікатору України ДК 003:2010 «Класифікатор професій», затвердженому наказом Держспоживстандарту України від 28 липня 2010 року № 327, який призначений для застосування центральними органами виконавчої влади, органами місцевого самоврядування, Федерацією роботодавців України, всіма суб'єктами господарювання [3].

Єдиною професійною назвою роботи з префіксом «кібер» згідно додатку А ДК 003:2010 є «Професіонал з економічної кібернетики» (код Класифікатора професій 2419.2). Водночас, професійні назви робіт, які наведені у класифікаторі, рекомендовано застосовувати під час утворення нових назв професій і посад у зв'язку з розвитком нових видів економічної діяльності та технологій.

Перелік основних робіт, що властиві тій або іншій посаді, визначається у Довіднику кваліфікаційних характеристик професій працівників, який забезпечує єдність у визначенні кваліфікаційних вимог щодо певних посад. Довідник – нормативний документ, обов'язковий з питань управління

персоналом на підприємствах, в установах і організаціях усіх форм власності та видів економічної діяльності. У жодному з випусків довідника, які систематизовані за видами економічної діяльності класифікацією професій, зазначеною у ДК 003:2010, не згадуються професії працівників із префіксом «кібер» (перелік випусків і посилання на їх зміст можна знайти в Інтернеті, наприклад на сайті електронного журналу «Кадровік-01» у статті від 3 квітня 2017 року).

Кваліфікаційні характеристики професій, пов'язаних з інформаційною безпекою, визначені у випуску 99 Довідника кваліфікаційних характеристик професій працівників «Безпека господарської діяльності підприємства, установи, організації», розробленому Державною установою Науково-дослідний інститут соціально-трудових відносин Міністерства соціальної політики України за участю фахівців Всеукраїнської організації Український союз промисловців і підприємців, Університету економіки та права «КРОК», Київського національного економічного університету ім. В. Гетьмана, Національної академії Служби безпеки України, Інституту стандартів безпеки, Інституту Управління державної служби охорони України Київського національного університету ім. Тараса Шевченка та ТОВ «ДТЕК» і затвердженому наказом Всеукраїнської організації Українського союзу промисловців і підприємців від 3 жовтня 2011 року № 99. У цьому випуску встановлені кваліфікаційні характеристики таких професій, пов'язаних з інформаційною безпекою:

керівник (директор, начальник) підрозділу (служби, управління, департаменту) з інформаційної безпеки;

керівник (начальник) підрозділу (відділу, сектору, групи) з інформаційної безпеки;

менеджер (управитель) систем з інформаційної безпеки;

професіонал з організації інформаційної безпеки;

професіонал з організації захисту інформації з обмеженим доступом;

фахівець з організації інформаційної безпеки;

фахівець з організації захисту інформації з обмеженим доступом [4].

Особливості забезпечення кібербезпеки обумовлюються об'єктами кібербезпеки та кіберзахисту, суб'єктами забезпечення кібербезпеки, а також їх функціями, серед яких:

1) здійснення заходів щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснення інформаційного обміну щодо реалізованих і потенційних кіберзагроз;

4) розроблення і реалізація запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

б) здійснення інших заходів із забезпечення розвитку та безпеки кіберпростору.

Зважаючи на особливості забезпечення кібербезпеки, вбачається за доцільне внести встановленим порядком і погодити з Міністерством соціальної політики України доповнення до Довідника [4], наприклад:

керівник (директор, начальник) підрозділу (служби, управління, департаменту) з кібербезпеки;

керівник (начальник) підрозділу (відділу, сектору, групи) з кібербезпеки;

менеджер (управитель) систем з кібербезпеки;

професіонал з організації кібербезпеки;

професіонал з організації кіберзахисту;

фахівець з організації кібербезпеки;

фахівець з організації кіберзахисту.

Ураховуючи викладене вище, можна запропонувати такі загальні завдання та обов'язки посадових осіб, відповідальних за забезпечення кібербезпеки та кіберзахисту:

забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура);

створення і розвиток нормативно-правової та організаційно-розпорядчої бази документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки;

організація своєчасного виявлення, запобігання та нейтралізації кіберзагроз, оперативне реагування на кібератаки та кіберінциденти, у тому числі за рахунок упровадження сучасних технологій кіберзахисту;

забезпечення ефективної боротьби із кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю;

удосконалення системи зберігання, передачі та обробки державних інформаційних ресурсів із застосуванням сучасних інформаційно-комунікаційних технологій (включаючи мережу Інтернет і технології онлайн-доступу);

організація та забезпечення кіберзахисту об'єктів критичної інфраструктури, здійснення захисту технологічних процесів на таких об'єктах, в яких управління або моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

організація взаємодії та налагодження співробітництва між суб'єктами забезпечення кіберзахисту щодо запобігання кіберзагрозам, реагування на кібератаки та кіберінциденти, усунення їх наслідків.

Інші завдання та обов'язки посад керівників, професіоналів і фахівців, мають ураховувати специфіку та сферу діяльності підприємств, установ і організацій.

У подальшому потребують визначення і розмежування завдання та обов'язки, необхідні знання та кваліфікаційні вимоги для запропонованих посад.

Література:

1. Про основні засади забезпечення кібербезпеки України : Закон України, 5 жовтня 2017 р. [Електронний ресурс] // Голос України від 09.11.2017. – № 208. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/2163-19>. – Назва з екрана.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України, 15 березня 2016 р. № 96/2016 [Електронний ресурс] // Урядовий кур'єр від 18.03.2016. – № 52. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/96/2016>. – Назва з екрана.

3. Класифікатор професій ДК 003:2010 : Держ. установа наук.-досл. ін-т соціал.-труд. відносин М-ва праці та соціал. політики України; Ін-т укр. мови НАН України; Держкомстат. України. – К. : «Соцінформ», 2010. – 745 с.

Довідник кваліфікаційних характеристик професій працівників «Безпека господарської діяльності підприємства, установи, організації». Випуск 99 [Електронний ресурс] // Український союз промисловців і підприємців, Університет економіки та права «КРОК», ДУ НДІ соціально-трудових відносин тв. ін. – 2011. – Режим доступу :

<http://zakon.medsprava.com.ua/regulations/1521/8196/8197/461210/>

Починок Максим Олексійович

Держаний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

РОЗВИТОК СИСТЕМИ BLOCKCHAIN В УКРАЇНІ

Блокчейн - це безперервний ланцюг блоків, за якими можна відстежити інформацію. Цією інформацією найчастіше стають транзакції криптовалюти (біткоїни, етеріум та інші). Але це зовсім не єдине застосування технології.

Особливість блокчейна полягає в його «прозорості». Просто уявіть, що кожен крок і кожен процес записаний і зафіксований. Його легко відстежити і практично неможливо зламати. Вся інформація при цьому децентралізована. Саме тому непідкупність блокчейн відкриває перед технологією величезні можливості в державному секторі.

Розподілений реєстр дозволить вибудувати таку систему, де держава не матиме потреби в додатковій довірі. Його монополія буде передана містам і частково автоматизована - в ланцюжку державних сервісів не буде особи, якій

ми ексклюзивно передаємо свої дані. Чиновники будуть виконувати функції страхових агентів системи з елементами моніторингу.

Меморандум про співробітництво з Bitfury

8 червня, Державне агентство з питань електронного уряду України і компанія Bitfury підписали меморандум про співпрацю в сфері інтеграції технології блокчейн в базові реєстри і в систему продажу конфіскованого майна «СЕТАМ».

За словами прем'єра, документ передбачає залучення передового досвіду американської компанії до створення ефективної екосистеми для розвитку блокчейн в Україні. В рамках партнерства компанія надасть широкий спектр рішень на базі блокчейна для сфери державного управління.

Угода України з компанією Bitfury розпочнеться проектом щодо впровадження блокчейн на цифрову платформу в країні. Дослідницькі області для проекту включають державні реєстри, державні послуги, соціальне забезпечення, охорону здоров'я та енергетику.

Як тільки впровадження проекту буде завершено, програма блокчейн пошириться на всі області, включаючи кібер-безпеку.

Перспективи блокчейну в сфері фінансів

Найпопулярніша криптовалюта, створена на базі цієї технології - Bitcoin - рідко використовується для платежів. Хоч цей показник і буде рости, біткоіни не стане масовим засобом платежу в дворічній перспективі, як багато від нього очікували.

Павло Кравченко розповів, чому блокчейн насправді потрібен в фінансах і будь переваг варто чекати банкам від впровадження цієї технології:

- підвищення безпеки
- здешевлення інфраструктури
- підвищення надійності і швидкості верифікації

Сергій Васильчук, керівник Attic Labs вважає, що фінансова система майбутнього буде складатися з безлічі блокчейнів. А банки будуть виконувати функцію передачі цінностей з одного розподіленого реєстру в інший. Це дозволить різним бізнесам випускати свої електронні гроші. А користувачам - легко конвертувати кошти, випущені одним магазином, в цінності, випущені іншим, в разі необхідності.

У Attic Labs вже розробили рішення для управління електронними гаманцями - OpenbankIT. Першою установою, яке почало працювати з цим проектом, став Альпарі Банк. Але Сергій Васильчук стверджує, що банки - не єдині гравці ринку електронних грошей на блокчейн.

Блокчейн в українських проектах

- **Електронні аукціони на блокчейн**

23 березня 2016 року в Києві було підписано Меморандум про розвиток і впровадження системи децентралізованих онлайн-аукціонів в державних галузях. У розробці платформи eAuctoin 3.0 брали участь IDF Reforms Lab, Distributed Lab, Ощадбанк, ПриватБанк, Microsoft, Unitybars.

На початку липня відбувся перший блокчейн-аукціон, а через ще три місяці до прозорих торгів підключилось шість майданчиків і два банки - Ощадбанк і ПриватБанк. Аукціон дозволяє здавати в оренду державне майно.

- **Відкрита платформа електронної демократії**

E-Vox - ініціатива, спрямована на підвищення прозорості в державному управлінні за рахунок використання блокчейну в організації голосувань, референдумів, підписання петицій. Так, команда E-Vox в серпні 2016 року домовилася встановити систему голосування в мерії міста Балта (Одеська область) - депутати змогли голосувати прямо зі своїх смартфонів і планшетів, залишаючи запис в блокчейн. Очікується, що через пару років системою будуть користуватися близько п'яти установ.

- **Блокчейн в НБУ**

9 листопада 2016 під час конференції Cashless Ukraine Summit в Києві НБУ представив дорожню карту розвитку безготівкової економіки. У документі зазначено, що регулятор планує за допомогою Blockchain провести революцію в електронних грошах.

З метою створення альтернативи картковим платежам, вже в 2017 регулятор може зайнятися випуском електронних грошей на базі Blockchain. Революція в роботі з електронними грошима буде відбуватися в рамках розвитку національної платіжної системи простір.

- **Банки на Блокчейн**

В кінці минулого року один з українських банків оголосив про початок роботи з електронними грошима на блокчейн. За допомогою розподіленої банківської системи SmartMoney банк побудує інфраструктуру для процесингу операцій з електронними грошима. Проект реалізується відповідно до вимог Національної платіжної системи «ПРОСТІР».

Фінустанова вже підписало угоду з IT-компанією Attic Lab.

У березні поточного року стало відомо, що ще один український банк готується до випуску активів на блокчейні. Таким чином, як мінімум дві українських фінустанови серйозно зацікавлені можливостями, які відкриває Blockchain для емісії електронних грошей.

- **Електронний уряд**

Концепція порталу електронного уряду на блокчейн - E-Ukraine - була презентована на Blockchain Conference Kiev ще 19 березня 2016 року. Тоді

платформа перебувала на стадії написання ТЗ і повинна була стати точкою взаємодії громадян, бізнесу та держави. Об'єднавши на одній платформі аукціони, голосування, ведення держреєстрів і інші розподілені сервіси.

Література:

1. <https://www.reuters.com/article/us-ukraine-bitfury-blockchain/ukraine-launches-big-blockchain-deal-with-tech-firm-bitfury-idUSKBN17F0N2>
2. <https://www.facebook.com/volodymyrgroysman/posts/529818137187105>
3. <https://psm7.com/reportage/ukraina-idealnaya-platforma-dlya-kriptotekhnologij.html>
4. <https://psm7.com/reportage/ukraina-idealnaya-platforma-dlya-kriptotekhnologij.html>

Загиней Антон Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

ЗВІДКИ ДІЙСНО ПОХОДИТЬ КІБЕРЗЛОЧИННІСТЬ?

Кіберзлочинність не контролюється. Це скрізь. Ми чуємо про це кожен день. Цього року, більше двох мільярдів записів втрачено або вкрадено. Тому, якщо ви дивитеся вечірні новини, ви думаєте, що більша частина цього це шпіднаж, чи національна діяльність. Шпигунство, як бачите, є прийнятною міжнародною практикою. Але в цьому випадку це лише невелика частина проблеми, з якою ми маємо справу.

Отже, де все це відбувається? Організація Об'єднаних Націй, заявила, що 80 відсотків цього є з високоорганізовані злочинні банди. На сьогоднішній день це являє собою одну з найбільших нелегальних економік у світі, що становить 445 мільярдів доларів. Щоб це краще уявити: 445 млрд. доларів більше, ніж ВВП 160 країн, зокрема Ірландії, Фінляндії, Данії та Португалії, та інших. Так як це працює? Як діють ці злочинці? Ну, дозвольте мені розповісти вам маленьку історію. Близько року тому дослідники з безпеки досліджували не такий простий, але в одночас складний банківський троянець, який мав назву Dyre Wolf. Dyre Wolf потрапляв на ваш комп'ютер через вас, натиснувши на посилання в фішинговому електронному листі. Тоді буде сидіти і чекати, поки ви не зайдете на ваш банківський рахунок. І коли ви це зробите знайдуться люди, що викрадуть ваш пароль, а потім використають це, щоб вкрати ваші гроші. Це звучить жахливо, але реальність є, реальністю. В індустрії безпеки ця форма атаки є дещо повсякденним явищем. Проте, Dyre Wolf мав чітко різні особистості - для цих невеликих транзакцій викорисовувалися рахунки інших людей. Ось що станеться, коли ви починаєте процес про видачу банківського

переказу, і в вашому браузері з'явиться окреме вікно із вашого банку, що є проблема з вашим рахунком і що вам потрібно зателефонувати в банк негайно, поряд з цим вікном номер до відділу шахрайства банку. Тож ви піднімете телефон і дзвоните. І після проходження звичайних голосових підказок, ви зустрілися з оператором. І ви проходите процес, як ви робите кожен раз, коли ви телефонуєте своєму банку, даєте їм своє ім'я і номер вашого рахунку. Проходить перевірку безпеки, щоб переконатися, що ви, це дійсно ви. Більшість з нас може не знати цього, але у багатьох великомасштабних дротових переказах, це вимагає підтвердження двох осіб на банківський переказ, тому оператор запитує вас, щоб отримати другу особу на лінії, і проходить через той же набір перевірок. Звучить нормально, чи не так? Тільки одна проблема: ви не розмовляєте з банком. Ви говорите з злочинцями. Вони побудували довідкову службу завдяки підробленим накладкам на банківський веб-сайт.

І це було бездоганно виконано, що вони рухали майже півмільйоном доларів за спробу. Ці злочинні організації діють, як сильно регламентований законний бізнес. Їхні співробітники працюють з понеділка по п'ятницю. Вони беруть вихідні. Як ми це знаємо? Ми знаємо це тому, що дослідники безпеки бачать неодноразові шипи зловмисного програмного забезпечення в п'ятницю вдень. Ці люди, після довгих вихідних з дружиною та дітьми повертаються, щоб побачити, як було добре.

Темний Інтернет це саме те місце, де вони проводять вільний час. Цей термін, використовується для опису анонімного нижнього інтернету, де злодії можуть працювати з анонімністю і без виявлення своїх справжніх імен. Там вони продають свою атаку на програмне забезпечення і обмінюються інформацією на нові методи нападу. Ви можете все купити там все: від атаки на базовому рівні, до набагато більш просунутої версії. Фактично, у багатьох випадках ви навіть бачите золотий, срібний та бронзовий рівні обслуговування. Ви можете перевірити посилання. Ви навіть можете купити атаки, що приходять із гарантією повернення грошей - якщо ти не досягнеш успіху. Тепер ці середовища, ці ринки - вони виглядають, як Amazon, або eBay. Ви бачите продукти, ціни, рейтинги та відгуки. Це не інше, ніж перевірка на Yelp або TripAdvisor перед тим як їхати в новий ресторан.

Це відбулося пів року тому. Дослідники дивилися нову програму, яка належить до шкідливих програм Android що вони виявили. Вона називалася Bilal Bot. У блозі вона позиціонувала Bilal Bot як нову, недорогу та бета-версію до набагато більш просунутого GM Bot, це було звичайним явищем в кримінальному підпіллі. Цей огляд не подобався авторам Bilal Bot, тому вони написали їм (аторам блогу) саме це повідомлення, заявляючи про свою справу і зробили аргумент, що у блозі було використано стару версію програми. Вони попросили їх оновити блог з більш точною інформацією і навіть запропонував

зробити співбесіду, докладно описавши програму. І тому зараз їхня програма атакує краще ніж їхні конкуренти.

Так як це можна зупинити? Це не так, як ми зможемо визначити , хто відповідальний за це - пам'ятайте, вони працюють з анонімністю і поза досяжністю закону. Ми, звичайно, не зможемо переслідувати злочинців. Я б запропонував, що нам потрібно абсолютно новий підхід. І потрібен такий підхід, щоб бути зосередженим на ідеї, що нам потрібно змінити економіку для хакерів. І дати собі перспективу - про те, як це може працювати. Давайте подумаємо про відповідь, яку ми бачимо до пандемії в галузі охорони здоров'я: SARS, Ebola, пташиний грип, Zika. Який головний пріоритет? Це знати, хто заражений і як розповсюджується хвороба. Тепер уряди, приватні установи, і тому подібне - кожен відповідає відкрито і швидко. Це колективні та альтруїстичні зусилля щоб зупинити розповсюдження у своїх системах і інформувати будь-кого, хто не заражений: як захистити або прищепити себе. На жаль, це не зовсім те, що ми бачимо у відповідь на кібератаку. Організації набагато частіше зберігають інформацію про цю атаку для себе.

Чому? Тому що вони хвилюються, про конкурентну перевагу, судовий процес та іншу тяганину. Нам потрібно ефективно демократизувати дані про загрозу розвідки. Нам потрібно утримувати всі ці організації відкритими і щоб вони поділитися своєю приватною інформацією про атаки. Хакери рухаються швидко - ми повинні рухатися швидше. І найкращий спосіб це зробити – відкрити і ділитися даними про те, що відбувається. Давайте подумаємо про це в конструкції фахівців з безпеки. Ми повинні зрозуміти мислення в його голові. Спеціальні служби повинні отримати інформацію з різних компаній, як приватних, так і державних. І вони повинні також бути готовими обмінюватися інформацією. І ось чому: якщо ви ділитесь інформацією, це еквівалентно інфуляції. І якщо ви не поділяєте цю думку ви насправді є частиною проблеми, тому що ви збільшуєте шанси щоб інші люди могли постраждати за тими ж методами атаки. Але є ще більша користь. Знищуючи пристрої злочинців ближче до реального часу ми розбиваємо їх плани. Ми інформуємо людей, яким вони намагаються заподіяти біль, набагато раніше, ніж вони коли-небудь очікували. Ми руйнуємо їх репутацію, ми знижимо їх рейтинги та відгуки. Ми не сплачуємо кіберзлочинність. Ми змінюємо економіку для хакерів. Але щоб зробити це, був потрібний перший рушій - хтось змінить мислення в галузі безпеки в цілому. Близько року тому спеціалісти з кібербезпеки видумали радикальну ідею. Що робити, якщо IBM візьме їхні дані - вони мали одну з найбільших загроз бази даних розвідки в світі - і відкриє це? Вона мала інформацію не просто на те, що сталося в минулому, але що відбувалося в найближчому часі. Що робити, якщо ми повинні опублікувати все це? Що робити якщо воно буде відкрито в інтернеті? Як ви можете собі уявити це отримало досить різку реакцію. Спочатку прийшли юристи: Що таке законне та які наслідки цього? Тоді прийшов бізнес:

Який бізнес? наслідки цього? І це теж зустрічалось дуже часто. Вони розпочали публікацію. Більше 700 терабайт можна застосувати у даних про загрозу розвідки, включаючи інформацію про атаки в реальному часі, що можна зупинити кіберзлочинність у своїх слідах. І на сьогоднішній день понад 4000 організацій використовують ці дані, включаючи половину 100 Fortune. І наша надія як наступний крок це переконати всі ці організації приєднатися до нас у боротьбі і робити те ж саме і поділитися своєю інформацією на коли і як на них також нападуть.

У всіх нас є можливість зупинити це, і ми всі вже знаємо, як це зробити. Все, що нам потрібно зробити - це подивитися на відповідь, яку ми бачимо у світі охорони здоров'я і як вони реагують на пандемію. Простіше кажучи, ми повинні бути відкритими та спільними.

Література:

1. <http://lingualeo.com/ru/jungle/where-is-cybercrime-really-coming-from-506342#>
2. https://www.ted.com/talks/caleb_barlow_where_is_cybercrime_really_coming_from/transcript

Кушнір Дмитро

*Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

HOW CYBERSECURITY SOLUTIONS CAN HELP WITH GDPR COMPLIANCE

Technical (protection) measures, means, technologies, rules and resources are mentioned multiple times throughout the GDPR text. The Regulation does not, however, specify any security technology implementation as obligatory (a few methods are suggested as optional solutions for the specific usage). Choice and evaluation of adequacy is the sole responsibility of the data controller and processor.

The range of possible technical mechanisms and safeguards for processing personal data depends primarily on the existing business processes and underlying ICT systems. Cybersecurity (or ICT security) solutions present a subset of possible technical approaches to ensuring compliance, characterized by its scope (digital domain) and purpose of application (preserving availability, authenticity, integrity, confidentiality, non-repudiation and privacy).

A saying, especially appropriate for GDPR, states that “there is no privacy without security” (not necessarily vice versa). So, what does InfoSec have in store for the GDPR buyer?

Before, during, and after

To put it bluntly, the purpose for cybersecurity protection lies in the very act of compromise. Since there is no way to eliminate threats altogether, only thing that's left to do is strengthening the defences and then wait.

Security controls can be classified into one or more of the three groups: **preventive, detective and corrective controls**. Even if the division is not already familiar to the reader, their context can be inferred intuitively: certain measures can help minimize the risk of an incident and/or detect its occurrence and/or conduct an appropriate response; i.e. mitigate the consequences.

Most of the cybersecurity solutions today fall within more than one of the categories. For example, network and endpoint protection solutions prevent unauthorized access, but at the same time constantly monitor the systems' usage and can detect anomalous behaviour, as well as block certain activities. An insider threat management portfolio provides a psychological barrier for the potential inside perpetrator, while storing a forensics audit trail and providing additional remediation functions.

On the other hand, some solutions are limited to a single domain. Most notable, but only on account of a specific mention in the GDPR, are encrypting and pseudonymising data. Inherently preventive, these solutions provide protection in two directions: rendering the data unreadable to the unauthorized user (not a member of the encryption chain of trust) or altering/masking the data in order to remove its ability to identify an individual (pseudonymising or data tokenization).

Cybersecurity maturity

A different perspective on ICT security posture offers several focuses, which could somewhat relate to the maturity of the security model of the organization.

The traditional basic approach to InfoSec was confined to **network perimeter and endpoint focus**, including primarily network firewall, antivirus and patch management solutions. Further need for protection and control lead to the **infrastructure and service focus**, offering implementations of Security Incident and Event Management (SIEM), Intrusion Detection/Prevention Systems (IDS/IPS), vulnerability management, Web Application Firewall (WAF), etc. Third is the **user focus**, which provides secure identity management mechanisms and monitoring of individual behaviour. This is achieved through tools and methods such as multi-factor authentication (MFA), Single Sign-on (SSO), Privilege Access Management (PAM), User Behaviour Analysis (UBA) and other solutions. Finally, data-centric focus concentrates on the data itself, by providing classification, encryption/pseudonymising, Data Leakage Protection (DLP) and others.

Although all four categories undergo constant progress and new types of solutions emerge, progression from the first to the fourth focus roughly resembles growth of cybersecurity maturity for most organizations. Adequate protection of (personal) data should therefore meet the corresponding qualities of all four security focuses.

Caveat emptor (“Let the buyer beware”)

This short list of possible mapping of cybersecurity functionalities to GDPR requirements is by no means an exhaustive one. The security landscape is always widening—albeit one step behind the threat agents. An organization’s InfoSec budget is the bottom line and risk management steers the wheel.

However, while prioritization of possible combinations of vulnerabilities, threats and mitigation measures will point to the specific technological direction, adequacy of the solution doesn’t just depend on the requirements & specification matrix. Ongoing delivery and upgrade/maintenance of the solution bears as much importance to the continuous compliance as the functional and operational features.

To conclude: security is not perfect, and privacy has many difficulties. However, we simply can’t afford to put up a Great Wall to keep our people’s data in. Respecting their privacy via legally based business processes is not enough. In order to secure the data, organizations have to invest in the security technology (and continue to do so in a constant manner).

Bibliography

1. <https://www.helpnetsecurity.com/2017/12/05/cybersecurity-solutions-gdpr-compliance/>
2. <https://www.csoonline.com/article/3240245/security/cybersecurity-professionals-arent-keeping-up-with-training.amp.html>

Ліщук Інна

*Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ*

РОЗБІР УРАЗЛИВОСТЕЙ,МОЖЛИВІСТЬ РЕАЛІЗАЦІЇ АТАК

В час розвитку й ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від рівня безпеки інформаційних технологій.

Характеристика наслідків атаки на вразливість – опис та структуризація методів реалізації вразливості. Модель, що характеризує наслідки атаки на вразливість забезпечує характеристику та визначення цілей атаки.



Вразливість автоматизованої системи – властивість системи, що робить можливим виникнення і реалізацію загрози.

По меті впливу вразливості розділяються на три основні порядки:

- вразливості першого порядку – загрози порушення конфіденційності інформації;
- вразливості другого порядку – загрози порушення цілісності інформації;
- вразливості третього порядку – загрози порушення працездатності системи (відмовлення в обслуговуванні) .

При розгляді наслідків атаки на вразливість системи, модель характеризує успішність атаки, але не вартісні наслідки, викликані розкриттям, порушенням цілісності інформації чи відмовленням в обслуговуванні.

Наприклад, система, призначена для запобігання загрози розкриття, не захищає від загрози цілісності інформації в системі, за винятком цілісності програмного забезпечення системи, що відображено у вимогах. Аналогічні твердження справедливі і для загроз цілісності і відмовлення обслуговуванні.

Таким чином, розроблювана система повинна мати у своєму складі параметр, що відбиває ступінь значимості наслідків атаки на вразливість системи стосовно загроз.

Наслідки атаки, що порушують безпеку інформації, у відношенні загрози, від якої захищає компонент безпеки, що лежить в основі проектованої захищеної автоматизованої системи (ЗАС) повинні прийматися з максимальним значенням рівним одиниці. Наслідки атак на безпеку інформації, пов'язаних з загрозами, від яких проектована захищена автоматизована система не захищає (атаки й вразливості «другого порядку»), варто враховувати в проектованій захищеній автоматизованій системі.

Оцінкою наслідків використання вразливості є оцінка кількості користувачів, задіяних в результаті успіху атаки на вразливість ЗАС. Якщо вразливість присутня в ЗАС, що захищає інформацію від загрози розкриття, то можливі наступні варіанти несанкціонованого доступу:

- до визначеної інформації користувача;

- до всієї інформації користувача;
- до всієї інформації групи користувачів;
- до всієї інформації всіх користувачів у системі.

Прикладом є одноразовий несанкціонований доступ до інформації користувача, одержання зловмисником пароля користувача системи і використання його для одержання повного контролю над користувачем системи, несанкціоноване одержання порушником пароля користувача більш високого ступеня довіри в системі мандатного розмежування доступом. При цьому скомпрометованими виявляються всі користувачі з даним ступенем довіри.

Максимальна шкода безпеки системи може бути досягнута порушником у випадку одержання ним прав адміністратора системи, тобто несанкціонованому доступу до всієї інформації всіх користувачів у системі. Адміністратор системи має права доступу до всієї інформації в системі. Він може створювати нових суб'єктів у системі, а також надавати їм права доступу до об'єктів. Також адміністратор системи може контролювати всі можливі характеристики функціонування системи.

Рыжков Дмитрий Олегович
Государственный университет телекоммуникаций
Учебно-научный институт защиты информации
г. Киев

РОЛЬ СМИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ВОЙНАХ

Наше время ознаменовывается глобализацией информационной сферы и приводит к изменениям в жизни социума. В связи с этим ученые констатируют переход цивилизации в новую информационную эру с появлением характерного ему информационного общества, для которого приоритетной является сфера массовых коммуникаций.

Средства массовой информации (СМИ) и степень их влияния на общественные процессы привлекает повышенное внимание представителей различных сфер деятельности. СМИ выполняют различного рода функции: информируют о чем либо, сообщают о фактах и событиях, удовлетворяют потребность в получении необходимых сведений, просвещают, распространяют культуру, развлекают, а так же являют собой платформу для распространения рекламы.

В современных психологических процессах особую роль играет информационная война, высокая значимость и актуальность которой подтверждается частыми дискуссиями, а так же ее непосредственными проявлениями в военно-политических конфликтах по всему миру. К настоящему

времени накоплен большой опыт применения различных приемов, способов, методов и технологий информационно-психологического воздействия.

Широко известна практика использования в качестве инструмента политического воздействия технологий пропаганды, психологического манипулирования, шантажа, направленных слухов и самым явным объектом реализации этих методик является СМИ.

Одним из примеров влияния информации на ведение войны является начало Второй мировой войны, когда поводом для вторжения Германии на территорию Польши стали сообщения о нападении польских военных на немецкую радиовышку. Информация об этом была распространена в газетах и на радио. Каждый немец считал вторжение правильным и необходимым, однако в действительности это оказалась хорошо спланированная операция Германии по оправданию своей агрессии.

В современном мире остались те же методики, но существенно усовершенствованы новыми подходами и возможностями. Появилась возможность постоянного непрерывного вещания через телевидение и интернет, демонстрация видеоряда о каком либо происшествии для формирования ассоциаций у человека, постоянная «подпитка» новыми фактами. Так же не обходится одними лишь СМИ – над новостями работают так же так называемые пиарщики, политтехнологи и психологи. Часто проводится отсылка к статистике и социальным опросам. Замечена тенденция подключать мнения авторитетных личностей, а именно: политики, известные люди и ученые. Вызывают доверие так же люди, которые всячески дискредитируют деятельность той стороны конфликта, к которой они приписаны, "разоблачая" и демонстрируя эту политическую силу в невыгодном для нее свете, при этом зачастую не сообщается какую сторону на самом деле поддерживает человек и насколько значимую роль он выполняет в деятельности своей стороны. Обычно достаточно того, что человек является гражданином государства-противника или был членом определенной политической силы в прошлом.

Обращаясь к методикам важно заметить, что эффективную роль в ведении любой информационной борьбы играет фальсификация, перекручивание фактов, имеет место подмена понятий, навешивание ярлыков (например "фашист", "террорист"). Обычному человеку внушается огромное количество явно неправдивой информации, которая ввиду объема, а так же большого количества информационных источников, по которым она распространяется, постепенно кажется правдоподобной и формирует определенное мнение.

В конечном итоге, нередко достигается ситуация, когда среднестатистический читатель информационного ресурса или телезритель скорее с легкостью поверит сведениям из СМИ, чем словам непосредственного участника событий или даже собственным наблюдениям. Это говорит об очень серьезном влиянии на сознание человека и об основательном подходе специалистов в сфере психологии и нейролингвистического программирования, которые и сами нередко становятся источником новостей, не вызывающих сомнения.

Современное положение дел в информационном поле сложилось так, что верят преимущественно тому, кто больше, громче и правдоподобнее отстаивает свою позицию, а не тот, кто действительно прав и способен оперировать доказательствами. Любая другая позиция, которая не соответствует убеждениям конкретного индивидуума, воспринимается враждебно и всячески отрицается ее объективность. Человек перестает анализировать и объективно оценивать ситуацию и все мировоззрение формируется не путем собственных наблюдений и анализов, а исходя из изложенных в информационном ресурсе сведений.

Масс-медиа с одной стороны являются элементом глобализации мира, который действует по законам социального пространства, с другой стороны масс-медиа участвуют в процессе формирования социальной реальности. В этой связи представляется необходимым подчеркнуть ключевую роль СМИ в процессе трактовки тех или иных событий, очень многое зависит от действий журналистов, редакторов, блогеров и различного рода экспертов.

Таковой является сегодняшняя реальность. Важно понимать то, насколько сильную роль играют средства массовой информации в повседневной жизни и в принятии важных решений. Современный журналист должен осознавать огромную степень своей ответственности за слова, используемые при описании события, которые имеют решающее значение в восприятии информации.

Роль информационно-психологического метода ведения информационной войны является, пожалуй, не менее значительной, нежели кибернетического, ведь человек гораздо более уязвимая система, чем ЭВМ и отличается возможностью мыслить и принимать те решения, которые не способен принимать компьютер.

Литература:

1. Дмитрий Шурхало. *СМИ в вооруженных конфликтах современности*. — Киев 1999.
2. Панарин И.Н. *Общественное мнение и вооруженные конфликты*. - <http://www.panarin.com/doc/41> 2009.02.26.
3. Панарин И.Н. *Информационная война и геополитика*. - М.: 2006, Поколение, 560 с.
4. Бурдые П. *О телевидение и журналистике*. — М.: Фонд научных исследований «Прагматика культуры», Институт экспериментальной социологии, 2002. — 149 с.
5. Бенедиктов К. С. *Инфовойны. Новая реальность* [Электронный ресурс] К. Бенедиктов/vip premier — 2014 - №1. — Режим доступа:<http://www.vip-premier.ru/inside.php?action=statia&id=7411&pid=788>

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ. КЛАСИФІКАЦІЯ, СТАТИСТИКА

В 21 столітті сучасна людина не уявляє свого життя без комп'ютера, так званого «друга», але людство не стоїть на місці і цей «друг» в будь-який момент за певних умов може стати нашим ворогом. Для людини особисто чи для якогось підприємства це може становити величезну небезпеку.

Цю небезпеку загалом становлять люди, щоб заподіяти шкоду. Вони переслідують якусь особисту, моральну чи фінансову вигоду, використовуючи шкідливе ПЗ та віруси, які працюють за своїм призначенням, цим самим шкодячи будь-кому.

З кожним днем загроз існує все більше і більше, про які деякі навіть і не здогадуються, але з кожним днем інформація стає все більш та більш ціннішою. Інформацію можна використовувати як для добрих, так і для поганих намірів. В цій роботі буде детальніше йти мова про те, що саме може нашкодити інформації, а тобто і нам.

Шкідливий програмний засіб, шкідливе програмне забезпечення (англ. malware — скорочення від malicious — зловмисний і software — програмне забезпечення) — програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді коду, скрипта, активного контенту, і іншого програмного забезпечення. Шкідливий — це загальний термін, який використовується для позначення різних форм ворожого або непроханого програмного забезпечення.

До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плагіни та інше зловмисне програмне забезпечення. Зловмисні програмні засоби відрізняються від дефективного ПЗ тим, що останнє є легальним ПЗ, але містить шкідливі помилки, які не були виправлені до випуску. Програмне забезпечення, яке може бути віднесене до

«шкідливих програм» може бути заснованим на різних технологіях, володіти абсолютно різним набором функцій і можливостей. Єдине, що об'єднує всі типи шкідливих програм — це мета, з якою вони створюються.

В сучасній літературі можна знайти декілька варіантів класифікації шкідливого ПЗ. Один з них я опишу.

Отже, шкідливе ПЗ можна поділити на 2 категорії. Перша група – це програми, що потребують програм-носіїв. В основному, до них відносяться фрагменти програм, що не можуть існувати незалежно від програм-носіїв. В цій ролі можуть виступати програмні додатки, утиліти чи системні програми.

До другої категорії відносять програми, що є незалежними. До них відносяться окремі незалежні програми, які можуть плануватися і запускатися ОС.

Україна не ізольована від інших країн, а це означає, що ми також стикаємося з проблемою комп'ютерних шкідників. Згідно з діаграмою статистики української антивірусної лабораторії Zillya!, щороку українці найбільше страждають від програм, що демонструють рекламу.

Найбільше страждає від цього Закарпатська, Івано-Франківська, Дніпропетровська області та Київ.

Література:

1. <https://ru.wikipedia.org/wiki/>
2. <https://studfiles.net/preview/3904449/page:15/>
3. <http://ua-referat.com/>
4. <http://zillya.ua>
5. <https://uk.wikipedia.org/wiki>
6. <https://sites.google.com/site/zagrozu/project-updates>

Шумлянська Аліна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

МОДЕЛІ ПОРУШНИКІВ

За порушників на АТС розглядаються суб'єкти, внаслідок навмисних або випадкових дій котрих, і (або) випадкові події, внаслідок настання яких можливі реалізації загроз для інформації.

Розглядаються три групи моделей порушників на АТС. Перша група містить у собі моделі порушників, що реалізують загрози на одній підсистемі АТС (див. розділ 6) з боку іншої підсистеми. Друга група містить у собі моделі порушників, що реалізують загрози на підсистемі керування станцією. Третя група містить у собі моделі порушників, що реалізують загрози на підсистемі КАЗЛ АТС.

Передбачається, що порушник - суб'єкт є кваліфікованим фахівцем, володіє всією технічною інформацією про АТС і, зокрема, про системи і можливі засоби її захисту, а порушник - випадкова подія має найгірший (із позицій власників інформації, що захищається) закон розподілу.

Кодифікатор моделей порушників на АТС наданий у таблиці

Код моделі порушника	Найменування моделі порушника
	Перша група моделей (для порушників, які створюють загрози на одній підсистемі АТС при впливах з боку іншої підсистеми)
MН1.01	Модель порушника ПРД до інформаційних ресурсів підсистеми керування станцією, який діє з боку абонентських ліній
MН1.02	Модель порушника, який використовує помилки або некоректні дії суб'єктів, що допущені на будь-якій із стадій життєвого циклу АТС, з метою реалізації загроз на підсистемі керування шляхом впливу на інформацію з боку підсистеми КАЗЛ
MН1.03	Модель порушника, який використовує програмні і (або) технічні позаштатні пристрої, що встановлені на підсистемі керування АТС, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми КАЗЛ
MН1.04	Модель порушника, який використовує програмно-технічні позаштатні пристрої, що встановлені на підсистемі КАЗЛ АТС, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми керування
MН1.05	Модель порушника, який використовує якісну недостатність інформаційно-уразливих режимів, функцій і послуг, що надаються АТС, для реалізації загроз на підсистемі КАЗЛ з боку підсистеми керування
	Друга група моделей (для порушників, які створюють загрози на підсистемі керування АТС)
MН2.01	Модель порушника ПРД
MН2.02	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції (але не штатні засоби доступу) на елементи підсистеми керування АТС
MН2.03	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації АТС з метою порушень доступності до підсистеми керування
MН2.04	Модель порушника, що впливає позаштатними засобами на елементи підсистеми керування АТС
MН2.05	Модель порушника, який використовує закладні пристрої і (або) програмні закладки, що встановлені на елементах підсистеми керування

MН2.06	Модель порушника через канали ПЕМВН
MН2.07	Модель порушника через канали побічних акусто-електричних перетворень на терміналах обслуговування АТС
MН2.08	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми керування або її документації, що допущені на передексплуатаційних стадіях життєвого циклу АТС
MН2.09	Модель порушника, який використовує помилки або некоректні дії персоналу АТС при збереженні критичної інформації на фізичних носіях
MН2.10	Модель порушника, який використовує випадкові збої і відмови в роботі підсистеми керування АТС
	Третя група моделей (для порушників, які створюють загрози на підсистемі КАЗЛ АТС)
MН3.01	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції на елементи підсистеми КАЗЛ АТС
MН3.02	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації АТС з метою порушень доступності до елементів підсистеми КАЗЛ АТС
MН3.03	Модель порушника, який впливає позаштатними засобами на елементи підсистеми КАЗЛ АТС
MН3.04	Модель порушника, який використовує програмні закладки і (або) апаратні закладні пристрої, що встановлені на підсистемі КАЗЛ АТС
MН3.05	Модель порушника через канали ПЕМВН
MН3.06	Модель порушника через канали побічних акусто-електричних перетворень в абонентських прикінцевих пристроях.
MН3.07	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми КАЗЛ або її документації, що допущені на передексплуатаційних стадіях життєвого циклу АТС
MН3.08	Модель порушника, який використовує випадкові збої і відмови в роботі елементів підсистеми КАЗЛ АТС

Приходько Владислав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м.Київ

КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ І ОБ'ЄКТИ КОМП'ЮТЕРНОЇ СИСТЕМИ

Комп'ютерна система, як правило, складається з безлічі компонентів. Деякі з компонентів можуть бути спеціально призначені для реалізації політики безпеки (наприклад, засоби ізоляції процесів або керування потоками інформації). Інші можуть впливати на безпеку опосередковано, наприклад, забезпечувати функціонування компонентів першого типу. І, нарешті, треті можуть взагалі не бути задіяні під час вирішення завдань забезпечення безпеки. Множина всіх компонентів перших двох типів називається комплексом засобів захисту.

Іншими словами, КЗЗ — це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки. Частина КС, що складає КЗЗ, визначається розробником. Будь-який компонент КС, який внаслідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина КЗЗ.

Комплекс засобів захисту розглядає ресурси КС як об'єкти і керує взаємодією цих об'єктів відповідно до політики безпеки інформації, що реалізується. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поведінням, яке визначає способи зміни стану. Для різних КС об'єкти можуть бути різні. Наприклад, для СУБД в якості об'єктів можна розглядати записи БД, а для операційної системи — процеси, файли, кластери, сектори дисків, сегменти пам'яті і т. ін. Все, що підлягає захисту відповідно до політики безпеки, має бути визначено як об'єкт.

При розгляді взаємодії двох об'єктів КС, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. Далі розглядаються такі типи об'єктів КС: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-користувача і об'єкта-процеса.

Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену — ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини. В інших доменах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим об'єктом-процесом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Іншими словами, об'єкти можуть знаходитись в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті.

Пасивний об'єкт переходить в стан об'єкта-користувача, коли індивід (фізична особа-користувач) «входить» в систему. Цей об'єкт-користувач виступає для КЗЗ як образ фізичного користувача. Звичайно, за цим процесом іде активізація об'єкта-процесу за ініціативою користувача. Цей об'єкт-процес є керуючим для пасивних об'єктів всередині домену користувача. Об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти далі позначаються просто як користувачі, процеси і об'єкти, відповідно.

Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об'єктами і/або зміни стану системи. Як потік інформації розглядається будь-яка порція інформації, що передається між об'єктами КС.

Література:

1. Каталог українських інтернет-ресурсів з ІТ-безпеки

ПЛАНУВАННЯ ЗАХИСТУ І КЕРУВАННЯ СИСТЕМОЮ ЗАХИСТУ

Для забезпечення безпеки інформації під час її обробки в АС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу АС. На стадії розробки метою процесу управління КСЗІ є створення засобів захисту, які могли б ефективно протистояти ймовірним загрозам і забезпечували б надалі дотримання політики безпеки під час обробки інформації. На стадії експлуатації АС метою процесу управління КСЗІ є оцінка ефективності створеної КСЗІ і вироблення додаткових (уточнюючих) вимог для доробки КСЗІ з метою забезпечення її адекватності при зміні початкових умов (характеристик ОС, оброблюваної інформації, фізичного середовища, персоналу, призначення АС, політики безпеки і т. ін.).

На кожному етапі мають бути виконані збирання і підготовка даних, їх аналіз і прийняття рішення. При цьому результати виконаного на певному етапі аналізу і прийняті на їх підставі рішення нарівні з уточненими вимогами слугують вихідними даними для аналізу на наступному етапі. На будь-якій стадії або будь-якому етапі може постати необхідність уточнення початкових умов і повернення на більш ранні етапи.

Створення КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси АС, що підлягають захисту. Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків. На підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. Ризик являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. Величина ризику може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.). На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень остаточного ризику до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформульованої політики безпеки розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу АС. Вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.

Література:

1. Новини, статті з IT-безпеки, захист інформації для бізнес

ФУНКЦІЇ І МЕХАНІЗМИ ЗАХИСТУ

Основними завданнями засобів захисту є ізоляція об'єктів КС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути віднесена до функцій ізоляції, перевірки або реєстрації. З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості КС і спостереженості дій користувачів.

Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної КС. Водночас одні й ті ж самі механізми можуть використовуватись для реалізації кількох послуг. Наприклад, для розробника слушно реалізувати і адміністративне і довірче керування доступом єдиним набором механізмів.

Реалізація механізмів може бути абсолютно різною. Для реалізації функцій захисту можуть використовуватись програмні або апаратні засоби, криптографічні перетворення, різні методи перевірки повноважень і т. ін. Вибір методів і механізмів практично завжди залишається за розробником. Єдиною вимогою залишається те, щоб функції захисту були реалізовані відповідно до декларованої політики безпеки і вимог гарантій.

Для реалізації певних послуг можуть використовуватись засоби криптографічного захисту. Криптографічні перетворення можуть використовуватись безпосередньо для захисту певної інформації (наприклад, при реалізації послуг конфіденційності) або підтримувати реалізацію послуги (наприклад, при реалізації послуги ідентифікації і автентифікації). Згідно із законодавством створення переліку вимог, сертифікація і атестація систем шифрування покладається на відповідний уповноважений орган виконавчої влади. Ця діяльність регламентується "Положенням про порядок здійснення криптографічного захисту інформації в Україні".

Література:

1. *Родичев Ю.* Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.
2. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.

КОНЦЕПЦІЯ ДИСПЕТЧЕРА ДОСТУПУ

При реалізації КЗЗ використовується концепція диспетчера доступу. Ця концепція не єдино можливий метод, проте є найбільш опрацьованою теоретично і перевіреною на практиці.

Диспетчер доступу характеризується трьома атрибутами:

- забезпечує безперервний і повний захист;
- достовірний (захищений від модифікації);
- має невеликі розміри.

Це означає, що диспетчер доступу має бути завжди активним і повинен контролювати всі запити на доступ до будь-якого захищеного об'єкта, який піддається впливу. Диспетчер доступу має бути захищений від модифікації, що для програмної реалізації звичайно вважається ізоляцією домену КЗЗ від доменів інших процесів. І, нарешті, диспетчер доступу повинен мати невеликі розміри, щоб код (реалізація) був зрозумілим і його можна було перевірити в процесі оцінки. Термін "невеликий" (або "мінімізований") є відносним. На практиці це означає, що диспетчер доступу не повинен складати весь КЗЗ, а повинен включати мінімально необхідний набір механізмів, що безпосередньо реалізують перевірку легальності запитів на доступ і, можливо, реєстрацію цих запитів.

Головна мета диспетчера доступу — забезпечення відомої точки проходження всіх запитів всередині КС і досягнення гарантії того, що потоки інформації між об'єктами-користувачами, об'єктами-процесами і пасивними об'єктами відповідають вимогам політики безпеки.

Класичний погляд на диспетчер доступу полягає в тому, що він служить бар'єром між інформацією, до якої хоче одержати доступ користувач, і самим користувачем. Диспетчер доступу дозволяє або забороняє доступ відповідно до того, чи є запит авторизованим. Рішення приймається на підставі перевірки атрибутів доступу користувача, процесу і пасивного об'єкта.

Узагальненням концепції диспетчера доступу є ідея герметизації, коли кожний об'єкт як би герметизовано диспетчером доступу, що утворює навкруги нього непрониклу оболонку. Кількість захищених (що знаходяться всередині оболонки) об'єктів може вар'юватись від одного об'єкта до всіх об'єктів системи. Таке подання є розширенням класичного підходу для розподілених і об'єктно-орієнтованих систем.

Методи реалізації концепції диспетчера доступу можуть бути різними. Незалежно від реалізації диспетчер доступу повинен забезпечити неможливість доступу до об'єкта в обхід механізмів захисту, перевірку наявності у користувача і/або процесу прав доступу до об'єкта і реєстрації подій, що відбуваються.

Найбільш широке розповсюдження одержала реалізація класичного погляду на диспетчер доступу, яка називається "ядром захисту".

Література:

1. *Борисов М. А., Романов О. А.* Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). № 2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014. — 248 с. — ISBN 978-5-9710-0837-8.
2. *Применко Э. А.* Алгебраические основы криптографии. № 9. Изд. стереотип. М.: Книжный дом «ЛИБРОКОМ», 2014. — 294 с. — ISBN 978-5-397-04457-8.
3. *Гуров С. И.* Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. Изд.2. М.: Книжный дом «ЛИБРОКОМ», 2013. — 352 с. — ISBN 978-5-397-03899-7.

***Хворостяний Родіон Віталійович**
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ*

КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АС

Повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в АС. Класифікація є підставою для визначення власником (розпорядником) інформації або АС методів і способів захисту кожного окремого виду інформації.

За режимом доступу інформація в АС має бути поділена на:

- відкрити;
- з обмеженим доступом.

Відкрити інформацію слід поділити на відкрити, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкрити, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну та конфіденційну.

До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю.

Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України "Про державну таємницю".

Правила доступу до конфіденційної інформації, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні, юридичні особи або держава, встановлює її власник. Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків. З метою встановлення ПРД до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за

ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).

Для встановлення правил взаємодії активних і пасивних об'єктів АС інформація повинна бути класифікована за типом її представлення в АС (для кожної з визначених категорій встановлюються типи пасивних об'єктів комп'ютерної системи, якими вона може бути представлена).

Ахтьоров Владислав Юрійович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕС УПРАВЛІННЯ СУСПІЛЬСТВОМ

Розвиток технологій та глобалізація призвели до необхідності створення нової моделі суспільства, яка б могла задовольнити потреби людей в світі інформаційних та телекомунікаційних технологій. Саме тому почало формуватися інформаційне суспільство.

Інформаційне суспільство – нова історична фаза розвитку цивілізації, в якій головними продуктами виробництва є інформація та знання, а відмінними рисами – зростання долі інформаційних комунікацій, продуктів, послуг у ВВП, створення глобального інформаційного простору, що забезпечує ефективну взаємодію людей, їх доступ до світових інформаційних ресурсів та задоволення їх потреб в інформаційних продуктах і послугах.

Особлива форма діяльності притаманна для інформаційного суспільства – інформаційна політика.

Інформаційна політика – особлива сфера життєдіяльності людей, пов'язана з відтворенням, розповсюдженням і споживанням інформації, яка задовольняє інтереси держави, громадянського суспільства і направлена на забезпечення творчого, конструктивного діалогу між ними [1, с.7-8].

Однією з основ інформаційного суспільства є концепція «електронного уряду». Ця концепція полягає в формуванні уряду, цілями якого будуть:

1. Надання населенню інтегрованих функцій в мережі Інтернет
2. Партнерство між державою та приватним сектором
3. Подолання інформаційної нерівності
4. Забезпечення доступу широких верств населення до інформації про діяльність органів влади, участь громадян в процесі прийняття управлінських рішень.

[2, с.5-6]

Концепція електронного уряду також включає в себе використання інформаційних технологій для вирішення певних адміністративних, економічних або соціальних проблем. Прикладом вирішення подібних проблем є використання гео-інформаційних технологій для територіального планування міст. [3, с.4-6].

Багато наукових та технічних розробок ведуться в напрямку реалізації , підтримки та розвитку інформаційного суспільства та концепції електронного уряду , проте навіть зараз наявні певні суперечності . Виникло дві протилежні точки зору :

перша з них полягає в тому, що широке застосування комп'ютерних технологій може спричинити зменшення ролі органів влади в процесі прийняття управлінських рішень, бо в умовах “електронної демократії” забезпечується можливість участі в прийнятті управлінських рішень широким верствам населення. Друга, навпаки, засвідчує що впровадження on-line технологій може призвести до збільшення ролі державних установ, підвищення результативності їх діяльності і відповідного збільшення значимості.

Система «електронного уряду має свої переваги та недоліки. Серед переваг можна виділити:

- підвищення ефективності публічної адміністрації у внутрішній організації своєї діяльності, підвищення якості адміністративних послуг;
- економія матеріальних та часових ресурсів, ефективніше використання бюджетних коштів, скорочення витрат на утримання державного апарату
- забезпечення умов для розвитку електронної демократії , створення умов для прозорості та відкритості публічної адміністрації, прийняття прозорих рішень.

Недоліки :

- слабку захищеність від нового класу соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій
- можливість здійснювати електронний контроль за життям, настроями, планами громадян, політичних організацій;
- можливість використання нових інформаційних технологій з політичною метою.[4 , с.5-8].

Отже впровадження інформаційних та телекомунікаційних технологій в управління державою має ряд переваг і задовольняє інформаційні потреби громадян , але через ряд недоліків та складність реалізації не є основою управлінням державами світу на даний момент часу.

Література:

- 1) *К.О.Линьов Інформаційне забезпечення державного управління та державної служби Навчальний посібник*
- 2) *І.В. КЛИМЕНКО, К.О. ЛИНЬОВ ТЕХНОЛОГІЇ ЕЛЕКТРОННОГО УРЯДУВАННЯ*
- 3) *Палеха Ю.Н Применение гис-технологий в денежной оценке и территориальном планировании городов Украины*
- 4) *Єганов В.В ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ*

ДОКАЗОВИЙ ПІДХІД ДЛЧ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПРИКЛАДИ ПОЄДНАННЯ ФУНКЦІЙ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Комплексна система захисту державних інформаційних ресурсів – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист державних інформаційних ресурсів, що підлягають захисту згідно визначеної політики безпеки й чинного законодавства в інформаційно-телекомунікаційних системах (інформаційних, телекомунікаційних, інтегрованих системах) держави, суспільства або громадян.

Аналізуючи основні принципи, які забезпечують інформаційну безпеку АС, можна узагальнити основні принципи побудови КСЗ ДІР та віднести до них: – системність; – централізоване управління системою; – комплексність; – своєчасність та безперервність захисту, послідовність їх рубежів; – резервування основних елементів системи; – розумну достатність та адекватність захисту; – гнучкість захисту; – прихованість захисту; – відкритість алгоритмів та механізмів захисту;

- простоту та зручність використання засобів захисту;
- захист засобів забезпечення безпеки системи;
- фізичний розподіл відомчих телекомунікаційних мереж та мережі загального використання;
- забезпечення безперервного виконання функцій, які покладені на КСЗ ДІР, при відмовах системи та її окремих елементів (підсистем);
- використання загальноприйнятих стандартів;
- масштабованість програмного забезпечення;
- багатоланковість;
- апаратно-платформенну незалежність і системність програмного забезпечення;
- комунікаційність;
- достатню ефективність захисту (визначається рівнем допустимого ризику порушення основних властивостей інформації).

Виходячи з принципів побудови КСЗ, можна запропонувати наступну узагальнену структурну схему системи захисту ДІР (рис.1).

Дана структурна схема є ієрархічною і до неї може застосовуватись доказовий підхід, ідея якого полягає в послідовній перевірці правильності описів системи

захисту на кожному з використовуваних рівнів та адекватності переходу від одного рівня опису до наступного.

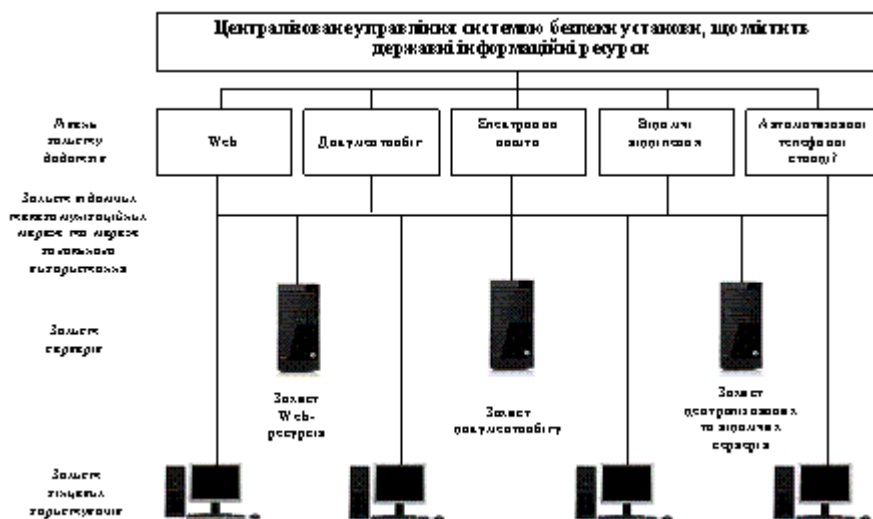


Рис.1. Структурна схема захисту ДІР

Одним із основних підходів до побудови КСЗІ є визначення та розвиток поняття «функції захисту інформації» з усіма його складовими. Це, наприклад, такі події, як оцінювання реальної можливості (або заходи) прояву порушень безпеки інформації, виявлення фактів їх прояву, вживання заходів до запобігання їх дії на інформацію, що захищається, виявлення, локалізація і ліквідація наслідків дій на інформацію, що захищається, і ін. В рамках такого підходу основне завдання теорії і практики захисту інформації в будь-якій ІТС можна розуміти як формування і обґрунтування повної множини функцій захисту S , яка повинна характеризуватися очевидною властивістю: множина S повинна містити такі функції, щоби при їх реалізації СЗІ ІТС могла протидіяти всім потенційно можливим порушенням безпеки інформації в процесі функціонування ІТС, а також при організації і забезпеченні захисту інформації.

Варто розглянути також о структуру множини S . Порушення інформаційної безпеки безпосередньо пов'язані з загрозами інформації. По суті порушення – це реалізація загроз інформації. А загрози інформації визначаються за результатом дії на основні властивості інформації, які визначають її цінність, тобто конфіденційність, цілісність, доступність і спостереженість. Таким чином, вводяться і розрізняються наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності (логічної або фізичної);
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

До цих загроз інформації необхідно додати ще загрозу несанкціонованого використання інформаційних ресурсів.

Ураховуючи, попередньо названі чинники(застосування яких можливе як теоретично, так і практично), для повноцінного аналізу функцій на кожному із ситуацій множини S , можна зобразити рівняннями:

$$F = x,$$

$$2 \ 1 \ 2 \ F = x \wedge x,$$

$$3 \ 1 \ 2 \ 3 \ F = x \wedge x \wedge x,$$

$$4 \ 1 \ 2 \ 3 \ 4 \ 5 \ F = x \wedge x \wedge x \wedge x \wedge x,$$

$$5 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 8 \ 10 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x \wedge x,$$

$$6 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 9 \ 11 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x \wedge x,$$

$$7 \ 1 \ 2 \ 3 \ 4 \ 6 \ F = x \wedge x \wedge x \wedge x \wedge x,$$

$$8 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 8 \ 10 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x \wedge x,$$

$$9 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 9 \ 11 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x \wedge x,$$

$$10 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 8 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x,$$

$$11 \ 1 \ 2 \ 3 \ 4 \ 5 \ 4 \ 6 \ 7 \ 9 \ F = x \wedge x \wedge x \wedge (x \wedge x \vee x \wedge x) \wedge x \wedge x.$$

http://www.rusnauka.com/32_PNR_2015/Informatica/4_200010.doc.html

УДК 004.056.5

СЕКЦІЯ №4. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Мирошниченко Наталія Володимирівна

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

ТЕЛЕКОМУНІКАЦІЇ - МЕНЕДЖМЕНТ СОЦІАЛЬНО ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

Під телекомунікаційними послугами маються на увазі будь-які послуги з передачі інформації за допомогою електромагнітних випромінювань (наприклад послуги телефонного зв'язку), в тому числі передача телевізійних і радіопрограм в ефір.

У багатьох країнах надання таких послуг іноземними підприємствами підпадає під цілу низку жорстких обмежень. В основі такого підходу лежить кілька причин:

1) у багатьох країнах держава традиційно володіла, контролювала і регулювала всі аспекти телекомунікацій, включаючи телефонний зв'язок, радіо, телебачення тощо. Вплив фінансових інтересів бюрократичних і комерційних структур призводить до того, що держави часто намагаються максимально обмежити або виключити доступ іноземних підприємств на ринок цих послуг;

2) у деяких випадках держави, громадські організації побоюються посилення іноземного (насамперед американського) культурного впливу;

3) деякі держави бояться, що іноземні підприємства, які поширюють теле- і радіопередачі на їхній території, будуть пропагувати фальсифіковані (на їхню думку) відомості й маніпулювати суспільною думкою.

Держави можуть обмежувати іноземну участь на ринку:

- забороняючи або обмежуючи участь іноземних підприємств. Такі обмеження можуть мати найрізноманітніші форми. Така розмаїтість пов'язана з особливостями самих телекомунікаційних послуг (наприклад, цензура, хоча її основу можуть становити політичні та інші "некомерційні" мотиви (суспільна мораль), також може обмежувати торгівлю телекомунікаційними послугами);

- забороняючи або обмежуючи показ реклами, розробленої за кордоном;

- забороняючи іноземним підприємствам контролювати вітчизняні об'єднання або обмежуючи це їхнє право (наприклад, забороняючи володіти значною часткою акцій таких підприємств).

Держави не тільки обмежують участь іноземних громадян і підприємств у наданні телекомунікаційних послуг, вони в деяких випадках обмежують діяльність вітчизняних підприємств на зовнішніх ринках. Наприклад, у США американським операторам телефонного зв'язку заборонено надавати послуги міжнародного зв'язку між США та іншими країнами.

Останнім часом ці обмеження повсюдно зменшуються. Зазвичай це відбувається "на основі взаємності" в обмін на зменшення обмежень іншими країнами.

Генеральна угода з торгівлі послугами (ГАТС) встановила правила переговорів між країнами - членами СОТ про зниження обмежень на торгівлю послугами. В рамках таких переговорів зниження обмежень у торгівлі послугами повинно відбуватися одночасно стосовно всіх країн - членів СОТ, без дискримінації.

Згідно з правилами ГАТС ведуться переговори і про зниження обмежень на торгівлю телекомунікаційними послугами. При цьому переговори про послуги телебачення і радіомовлення ("основні телекомунікації") ведуться окремо від переговорів про інші телекомунікаційні послуги. Останні розвиваються інтенсивніше перших.

Реклама

Реклама повсюдно визнається як дуже важлива послуга для інших секторів економіки.

Збільшення обсягів міжнародної торгівлі товарами і послугами спричиняє істотне зростання обсягів міжнародної торгівлі рекламними послугами.

У різних країнах існують різні обмеження і вимоги до рекламної діяльності. Частина цих обмежень стосується тільки іноземних "виробників" рекламної продукції, інші обмеження ставляться до рекламної продукції взагалі.

В одних країнах рекламну діяльність контролює й обмежує держава, в інших - цю функцію повністю покладено на фахові асоціації рекламних агентств.

У багатьох країнах діють обмеження на телевізійну і радіорекламу. Можна навести такі приклади:

- заборона рекламних оголошень, які переривають передачу;
- обмеження часу телевізійного або радіомовлення, який можна використовувати для реклами;
- заборона реклами на телебаченні;
- обмеження реклами алкогольних і тютюнових виробів;
- заборона використовувати в рекламі дітей.

У багатьох країнах діють норми, які забороняють недобросовісну рекламу. "Недобросовісна реклама" в різних країнах розуміється зовсім по-різному. Наприклад, те, що в Італії буде вважатися "кумедним перебільшенням", у Данії або Німеччині розглядатиметься як серйозний обман споживачів. Порівняння в рекламі якостей і властивостей різних товарів і послуг допускається в одних країнах

(наприклад у Великій Британії й Ірландії), але суворо заборонено в інших (країни Бенілюксу) або дозволено із серйозними обмеженнями (Інші країни Європейського Союзу).

У рекламному бізнесі в багатьох країнах обмежена або заборонена участь іноземних підприємств (як прямо, так і через створення дочірніх компаній або філій). Серед країн ЄС такі обмеження діють тільки у Франції і Швеції. В тих країнах, в яких подібних обмежень немає або є незначні обмеження, на ринку зазвичай домінують міжнародні рекламні агентства.

Література

1. Балабанов И.Т. *Внешиэкономические связи: Учеб. пособие для вузов. - 2-е изд., перераб. и доп. - М., 2001.*

2. Глобализация и либерализация. Процесс развития в условиях двух мощных тенденций. Доклад Генерального секретаря ЮНКТАД на девятой сессии Конференции ООН. - Е&ю-Йорк; Женева, 1996.
3. Закон України "Про єдиний митний тариф" // Відомості Верховної Ради України. - 1992. - 12 травня. - № 19.
4. Кириченко О.А., Панфілова Т., Меркотан К. Вибір моделі зовнішньоекономічної діяльності України в процесі приєднання до ГАТТ/СОТ // Підприємництво і право. - 1997. - № 7.
5. Кириченко СБ. Європейський Союз: штрихи до портрета // Зовнішня торгівля. - №3-4. -2001. -С. 8-15.
6. Мельник Т. Проблемні питання розвитку зовнішньої торгівлі та економічного зростання в Україні / Економіст. - № 4. - 2007. - С. 46-60.
7. Мировая экономика: Учеб. пособие для вузов / Под ред. И.П. Николаевой. - 2-е изд. - М., 2000.
8. Новицький В.Е. Міжнародна економічна діяльність України: Підручник. - К.: КНЕУ, 2003. - 948 с.
9. Плотников О.В. Ultima ratio економічних реформ. - К.: Кондер, 2003. - 240 с.
10. Посельський В. Європейський Союз: інституційні основи європейської інтеграції. - К.: Смолоскип, 2002. - 168 с.
11. Розширення Європейського Союзу: вплив на відносини України з центральнo-європейськими сусідами / Інститут регіональних та євроінте-граційних досліджень "Євро регіо Україна". - К: МК.І. С.* 2004. - 360 с.
12. Спиридонов И.А. Мировая экономика: Учеб. пособие для вузов. - М., 2001.
13. Устинов ИЛ. Мировая торговля: Стат.-аналит. справ. - М., 2000.

Мирошниченко Наталія Володимирівна

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

АНАЛІЗ МОДЕЛЕЙ УПРАВЛІННЯ РЕСУРСАМИ ТА НАВАНТАЖЕННЯМ КАНАЛІВ ПЕРЕДАЧІ В ТЕЛЕКОМУНІКАЦІЯХ

Проблема створення і забезпечення ефективного функціонування та управління ресурсами та навантаженням каналів передачі телекомунікаційних систем досить часто постає перед організаціями та корпораціями із розвиненою розподіленою інфраструктурою. Вкладаючи свої кошти ці компанії сподіваються на якісну роботу таких інформаційних систем та очікують зменшення витрат на експлуатацію, зниження вартості обслуговування користувачів, що дозволить закласти основу для більш ефективної діяльності самої компанії та їх клієнтів. Клієнти своє бачення роботи такої структури погоджують із компанією на рівні вимог, до яких належать: вартість таких послуг, доступність та керованість інфраструктури, цілісність даних, безпека, надійність. Досягнення такого рівня вимог користувачів із найменшими коштами та ресурсами становить сутність проблеми створення і забезпечення функціонування телекомунікаційної системи. Загалом таку комплексну інформаційну проблему розбивають на ряд проблем менших розмірів, хоча не набагато простіших. Однією із таких є проблема управління ресурсами і

навантаженням телекомунікаційної системи. Тут необхідні гнучкі рішення, які ґрунтуються на оцінюванні та прогнозуванні стану ресурсів, обсягів навантаження і полягають у правильному балансуванні навантаження та ефективному розподілі ресурсів телекомунікаційної системи. Для прийняття коректних правильних рішень необхідні інструментарій та комплекси методик для вирішення задач підтримки інфраструктури телекомунікаційної системи. Створення такої структури становить достатньо важливу проблему, розв'язання якої вимагає досить глибокого розуміння процесів, які відбуваються в телекомунікаційних системах, функціонування інфраструктури, чіткої постановки конкретних задач аналізу та дослідження, розроблення нових математичних моделей та відповідних методів вирішення задач і реалізацію розроблених методик.

Постановка проблеми

У статті досліджуються та розглядаються питання вирішення задачі аналізу моделей управління ресурсами та навантаженням каналів передачі в телекомунікаційних системах. Необхідно проаналізувати моделі та алгоритми управління телекомунікаційною інфраструктурою організацій і підприємств з урахуванням завантаженості каналів передачі системи. Оскільки моделі залежать від багатьох чинників, то в статті буде проаналізована класифікація потрібних для реалізації системи управління інфраструктурою моделей і алгоритмів із урахуванням цих чинників як ознак класифікації. Потрібні моделі визначаються комбінаціями необхідних параметрів.

Одна з ознак параметрів передбачає відмінність моделей у залежності від цілей роботи телекомунікаційної системи – управління інфраструктурою для підтримки власних процесів чи надання послуг зовнішнім клієнтам. Такий поділ буде впливати на вид критерію, який використовується у відповідній моделі. Іншою ознакою є технологічні особливості інфраструктури телекомунікаційної системи, які обумовлені архітектурою її побудови. Загалом ці ознаки будуть впливати на всі елементи моделі. Залежно від етапу життєвого циклу, на якому знаходиться телекомунікаційна система виникають різні задачі. Тому на етапі планування крім технологічних та ресурсних обмежень можуть використовуватись також і інші обмеження, наприклад вартість чи надійність. Рівень доступних ресурсів буде впливати на складність моделі задачі. Суттєво буде впливати на вид моделей остання ознака – це забезпечення ресурсами.

Література

1. Теленик С.Ф. Моделі і методи розподілу ресурсів в системах з серверною віртуалізацією /
2. С.Ф. Теленик, О.І. Ролік, М.М. Букасов, О.А. Косован, О.І. Кобец // Зб. наук. праць ВІТІ НТУУ «КПІ». – Київ : ВІТІ НТУУ «КПІ», 2009. – Випуск № 3. – С. 100–109. 2.
3. Теленик С.Ф. Моделі управління віртуальними машинами при серверній віртуалізації /
4. С.Ф. Теленик, А.И. Ролик, М.М. Букасов, А.Ю. Лабунський // Вісник НТУУ «КПІ»: Інформатика, управління та обчислювальна техніка. – К. : «БЕК+», 2009. – № 51. – С. 147–152. 3.

5. Хмельницький Ю.В. Система керування пристроями адаптивного діагностування /
6. Ю.В. Хмельницький //Вісник Хмельницького національного університету.
7. Технічні науки. – Хмельницький : ХНУ, 2009. – № 4 (137). – С. 127–131.

Лебедєва Ірина Сергіївна
Державний університет телекомунікацій
Навчально – науковий інститут менеджменту та підприємництва
м. Київ

МЕНЕДЖМЕНТ В ТЕЛЕКОМУНІКАЦІЯХ

Менеджмент - скоординована діяльність з керівництва та управління організацією.

Дисципліна «Менеджмент в телекомунікаціях» є дисципліною що грає важливу роль в освоєнні студентами навичок менеджменту, вивченні підходів до ефективної організації управління підприємством, отримання знань з побудови сучасних систем менеджменту. Ця дисципліна дає базові знання з основ теорії менеджменту, міжнародним стандартам систем менеджменту (якість, екологія, безпека) і менеджменту бізнес-процесами. Дисципліна «Менеджмент в телекомунікаціях» вивчається в десятому семестрі.

16 травня 2008 Україна вступила до СОТ (Світова організація торгівлі). У зв'язку з цим особливу роль набувають питання стандартизації, акредитації та сертифікації, які сприяють встановленню багатосторонніх торговельних відносин. Для забезпечення довіри виникає гостра потреба в широкомасштабному впровадженні сучасних систем менеджменту в різних сферах промисловості, високих технологіях і в сфері послуг (у тому числі і в сфері телекомунікацій). Для побудови та сертифікації сучасних систем менеджменту необхідні компетентні фахівці, від яких залежить ефективно розвиток цих систем в Україні. На даний період існує істотне відставання в розвитку в нормативній та методологічній бази від передових країн, а також існує потреба у підвищенні рівня підготовки фахівців в Україні у цій сфері. Для забезпечення підвищення кваліфікації та компетентності персоналу в області систем менеджменту пропонується активізувати роботу з підготовки фахівців в області систем менеджменту при навчанні студентів КПП. Кожен випускник КПП повинен володіти сучасними знаннями в області систем менеджменту і готовий на практиці виконувати роботи з впровадження, підтримання функціонування та розвитку сісти менеджменту в тих організаціях, де йому належить працювати.

Даний курс «Менеджмент в телекомунікаціях» спрямований на формування у слухачів комплексу знань, які забезпечують можливість проводити роботи в галузі менеджменту якістю на підприємстві, а також проектувати нові системи менеджменту якістю і вносити зміни в існуючі системи. Слухачі повинні знати основи теорії менеджменту, нормативні документи, необхідні для побудови систем менеджменту якістю, проведення

аудиту і процедур сертифікації, знати основні поняття в галузі менеджменту якістю, знати методи проектування систем і методологію впровадження результатів системних досліджень, формувати програми розвитку менеджменту якістю на підприємстві, розробляти і впроваджувати системи менеджменту якістю, оцінювати системи менеджменту якістю, проводити сертифікацію систем менеджменту якістю, проводити роботи з підготовки кадрів та навчання на підприємстві.

Метою дисципліни є отримання студентами базових знань щодо створення систем менеджменту в організаціях:

- формування базових знань у галузі менеджменту;
- оволодіння навичками побудови систем менеджменту в організаціях;
- отримання знань з підготовки документації з систем менеджменту в організаціях.
- У результаті вивчення навчальної дисципліни студенти повинні:
- ЗНАТИ:
- основи менеджменту;
- основні стандарти з систем менеджменту (якість, екологія, безпека).
- УМІТИ:
- розробляти політику якості в організації;
- кваліфіковано готувати необхідні документи для систем менеджменту в організаціях.

Література:

1. Амстронг Майкл. Основы менеджмента. Как стать лучшим руководителем. Серия "Учебники и учебные пособия". Ростов-на-Дону: "Феникс", 1998. - 512с.
2. Бовыкин В.И. Новый менеджмент: (управление предприятиями на уровне высших стандартов: теория и практика аффективного управления). - М: ОАО "Издательство "Экономика", 1997. - 368с.
3. Гевко І.Б. Методи прийняття управлінських рішень: Підручник. - К: Кондор, 2009. - 187с.
4. Герчикова Н.Н. Менеджмент: Учебник-3е изд. перераб. и доп. - М.: Банки и биржи, ЮНИТИ, 1997. - 501с.
5. Діденко В.М. Менеджмент: Підручник. - К.: Кондор, 2008. - 584с.
6. Дем'яненко СІ. Менеджмент виробничих витрат у сільському господарстві. - К.: КНЕУ, 1998. - 264с.
7. Завадський І.С. Менеджмент: Management. - У 3т. - Т. 1-3-вид., доп. - К.: Вид-во Європ. ун-ту - 2001. - 542с.
8. История менеджмента: Учеб. пособие I Под ред. Д.В.Валового. - М.: ИНФРА - М, 1997. - 256с.
9. Колпаков В.М. Теория и практика управленческих решений: Учеб. пособие. - К.: МАУП, 2000. - 256с.
10. Кредісов А.І., Панченко С.Г., Кредісов В.А. Менеджмент для керівників. - К.: Т-во "Знання", КОО, 1999. - 556с.
11. Менеджмент в АПК І Ю.Б.Королев, В.Д.Коротнев, Г.Н.Кочетова и др.. - М.: Колос С, 2007. - 424с.
12. Карнеги Д. Как завоевать друзей и оказывать влияние на людей: Как вырабатывать уверенность в себе в влиять на людей, выступая публично: Как перестать беспокоиться и начать жизнь: Пер. с англ.. - С. - Пб: Лениздат, 1992. - 708с.

РОЛЬ, ПРОБЛЕМА ТА СТРАТЕГІЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Роль і проблеми розвитку телекомунікацій. Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

У сфері телекомунікацій існують такі проблеми:

- 1) низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;
- 2) нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);
- 3) використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;
- 4) наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- 5) неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- 6) недостатній регуляторний вплив держави на ринок телекомунікацій;
- 7) недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Стратегія розвитку телекомунікацій спрямована насамперед на розв'язання зазначених проблем, крім того, передбачає здійснення заходів для подальшого забезпечення розвитку телекомунікацій в Україні на базі телекомунікаційних мереж наступного покоління.

Розвиток телекомунікацій повинен здійснюватися за такими основними напрямками:

- 1) прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень (радіотехнологій, волоконно-оптичних, пакетних технологій тощо);
- 2) сприяння реалізації регуляторної політики у сфері телекомунікацій, спрямованої на об'єднання (консолідацію) можливостей суб'єктів ринку

телекомунікацій з метою розв'язання основних проблем сфери, підвищення ефективності їх діяльності;

3) удосконалення нормативно-правової бази у сфері телекомунікацій

Важливою компонентою синтезу інтегрованих систем оперативного управління Міністерства надзвичайних ситуацій України (ІСОУ–МНСУ) є задача забезпечення надійного зв'язку. Здійснення заходів з запобігання надзвичайних ситуацій (НС), моніторингу та ліквідації вимагає надійного оперативного зв'язку для передавання команд і даних між органами управління МНС, цивільною обороною, органами влади, промисловими і транспортними та енергетичними компаніями, що залучаються до ліквідації загроз та місцями розташування об'єкта НС. Для забезпечення координації дій в цих ієрархічних структурах повинні використовуватись всі види зв'язку: комутовані телефонні лінії АТС, спеціальні виділені лінії і канали, урядові канали зв'язку і оповіщення, телетайпні, телеграфні і оптоволоконні лінії зв'язку, радіоканали та супутникові системи мобільного зв'язку, альтернативні системи зв'язку при руйнуванні кабельних магістралей, мобільні пункти передавання інформації та зв'язку на основі короткохвильових, ультракоротко- хвильових систем радіозв'язку, супутникового радіозв'язку.

Об'єкти телекомунікаційної та управлінської структур характеризуються різноманітністю інформаційних потоків, які циркулюють між його елементами, що вимагає введення єдиних систем уніфікації і стандартизації представлення документів та протоколів обміну. Відповідно, основними цілями функціонування телекомунікаційних систем та зв'язку в інформаційній структурі підтримки прийняття рішень будуть: підвищення оперативності прийняття рішень та надання інформаційно- аналітичної підтримки на всіх рівнях управління, моніторингу та ліквідації НС, забезпечення посадових осіб і органів влади достовірною інформацією про НС, забезпечення сумісності інформації на всіх рівнях ієрархії управління за рахунок використання єдиних класифікаторів, стандартів, принципів побудови інформаційних структур і систем, оптимізація координації організаційної та інформаційної взаємодії функціональних систем МНС, оптимізація і автоматизація процесів збирання та комплексного оброблення даних, отриманих від системи моніторингу і переданих по каналах зв'язку, комп'ютерних і телекомунікаційних мережах, підвищення достовірності та повноти циркулюючої інформації за рахунок інтелектуального оброблення даних і засобів захисту каналів, забезпечення оперативних потоків даних визначеними маршрутами до центрів оперативного управління МНС, підтримка регулярного інформаційного обміну через мережі зв'язку і телекомунікаційні системи.

Відповідно до наведених завдань стратегічного рівня сформулюємо принципи побудови інформаційного забезпечення оперативних центрів МНС каналами передачі даних і радіомережами: оперативні центри управління створюються на основі інтеграції функціональних, інформаційних і програмно-апаратних засобів, інтеграція орієнтована на цільове використання потоків даних від різних джерел і на основі інтелектуального опрацювання даних формується

в реальному часі об'єктивна оцінка НС та прогноз розвитку сценаріїв. Технологія збирання та накопичення даних передбачає автоматизацію вводу, алгоритмізацію та формалізацію, інформаційний обмін між структурними елементами по мережах і каналах зв'язку, передбачає автоматизацію передачі даних з врахуванням рівня доступу в інтегрованих структурах МНС.

Інформаційною основою інтеграції потоків даних в межах центру управління НС-МНС є типові протоколи і елементи лексичного та лінгвістичного забезпечення і зі спільним регламентом інформаційного обміну, всі елементи інтегрованої системи ЦУНС-МНС мають можливість безпосереднього зв'язку з центром ОУ, що підвищує відповідно його інформованість щодо ходу моніторингу і ліквідації НС. Первинне оброблення даних ґрунтується на структуруванні та формалізації, кваліфікації блоків даних після їх інтелектуального оброблення.

Інформаційна сумісність передачі пакетів даних в комп'ютерних мережах та аналогової інформації в каналах зв'язку забезпечується використанням єдиного лінгвістичного забезпечення лексичного і програмного, яке включає в себе уніфіковані інформаційні структури банків даних усіх рівнів системи, а також правил і протоколів передачі даних. Організаційні заходи забезпечують недоступність несанкціонованих осіб до апаратно-технічних засобів системи, магнітних носіїв даних, кабельних систем зв'язку та радіоканалів. Технічні засоби мають забезпечити відсутність електромагнітних випромінювань в апаратній і кабельній системах за межами зони контролю, однозначну ідентифікацію та аутентифікацію користувачів до роботи з найбільш критичними елементами системи і баз оперативної інформації, а також забезпечити безперебійне живлення критичних компонентів структури управління центрів оперативного керування МНС.

Аналітичне забезпечення інтегрованого опрацювання даних в ІС-ЦОУ МНС ґрунтується на комплексі сучасних прикладних програм з апробованими алгоритмами опрацювання даних, математичних моделях і картографічних засобах візуалізації, математичному забезпеченні процедур прогнозування розвитку подій при НС та оцінки наслідків НС. Програмне забезпечення повинно відповідати існуючим міжнародним стандартам в галузі баз даних та систем телекомунікацій (протоколи), графічних систем інтерфейсів користувача, дати можливість працювати в розподіленому, гетерогенному середовищах та в мобільному режимі, використовуючи потокові моделі обміну.

Технічне забезпечення ЦОУ–МНС повинно бути побудоване на основі стандартизації та уніфікації засобів обчислювальної техніки та електронного зв'язку, засобів телекомунікації та каналів зв'язку на основі використання математичного апарату теорії ігор, дослідження операцій, теорії графів.

Висновок:

Встановлено, що інформаційна сумісність передачі пакетів даних в комп'ютерних мережах та аналогової інформації в каналах зв'язку забезпечується шляхом використання єдиного лінгвістичного забезпечення, лексичного і

програмного, яке включає в себе уніфіковані інформаційні структури банків даних усіх рівнів системи, а також правил і протоколів передачі даних.

Література:

1. Малець І.О. Розроблення елементів математичного забезпечення регіональної системи оперативного управління підрозділами МНС / І.О. Малець // Пожежна безпека. – 2007. – № 10. – С.21–25.
2. Сікора Л.С. Управління ієрархічними техногенними структурами в умовах підвищеного ризику / Л.С. Сікора, І.Р. Манишин, І.О. Малець, М.С. Антоник // Моделювання та інформаційні технології. – 2008. – Вип. 47. – С. 131–140.
3. Малець І.О. Інтелектуальні аспекти забезпечення функціональної стійкості систем зв'язку / І.О. Малець, Л.С. Сікора // Сучасні проблеми телекомунікацій – 2007 // Мат. наук.-практ. конф., (Львів, 18–20 жовт. 2007 р.). – 2007. – С. 8-10.

Марчук Вікторія Ярославівна

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ

Нині особливого значення набуває галузь зв'язку, справляючи величезний вплив на соціально – економічний розвиток суспільства, що переходить від індустріальної до інформаційної фази свого розвитку. Інформація дедалі більше стає повноправним учасником виробничих процесів і вирішальним чинником науково – технічного й соціального прогресу.

Розвиток соціально – економічних систем привів до того, що людина дістала можливості формування в новому соціумі. Вона стає соціально – активним, суспільним суб'єктом – особою зі своїм психологічним складом, дієздатністю і роллю в суспільстві. В цих умовах важливе місце в житті людини, в її соціальній діяльності займає зв'язок. Він (зв'язок) не лише перестає бути галуззю економіки країни в системі суспільного розподілу праці, організаційних і економічних відносин, але й є безпосередньо включеним в органіку людини. “Людина як особа сама створює і будує свої відносини, бере участь у соціальному спілкуванні, управляє процесами. Зв'язок створює і матеріальні умови цього управління. За допомогою засобів зв'язку людина здійснює комунікацію як у сфері виробництва так і в соціальних відносинах. При цьому природа зв'язку проявляється передусім у характері його послуг, тобто його предмета. Саме через предмет долається простір. Зв'язок поєднує людей для спілкування...”, яке є однією з найбільш важливих потреб людини.

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися

випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.

Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Доходи від надання послуг зв'язку за 2007 – 2009 рр. зросли на 6414,7 млн. грн. або на 16,1 %.

Економічна діяльність сфери телекомунікацій характеризується рівнем доходів. Значне зростання доходів відбулось від надання таких послуг як надання комп'ютерних послуг (на 1730,2 млн. грн. або на 106 %), послуг кабельного телебачення (на 543,3 млн. грн. або на 73,3 %), проводового мовлення (на 83,6 млн. грн. або на 76,3 %). Відбулось зростання доходів від надання послуг мобільного зв'язку на 3419,8 млн. грн. або на 13,6 %

Таким чином, можна визначити, що розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вжити ще більших заходів щодо сприяння розвитку саме цієї галузі. Недостатній розвиток телекомунікацій загрожує конкурентоздатності економіки України та перспективам її розвитку.

Література:

1. Закон України «Про Телекомунікації». – К. : Державне видав-ничо-інформаційне агентство «Зв'язок», 2003. – 58 с.
2. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – М. : Инфра-М, 1996. – 493 с.
3. Кузьминов А.В. Проблемы и противоречия в управлении электросвязью региона и пути их разрешения / А.В. Кузьминов // Спеціалізований випуск матеріалів конференції «Проблеми управління та економічного розвитку підприємств зв'язку – Економіка'99» : збірник наукових праць. – О. : УДАЗ ім. О.С. Попова, 1999. – 98 с.
4. Економіка телекомунікацій [Текст] : навч. посіб. [для студентів вищих навчальних закладів] ; за заг. ред. В.М. Орлова. – О. : ОНАЗ ім. О.С. Попова, 2014. – 512 с.
5. Гранатуров В.М. Управління послугами зв'язку [Текст] : навч. посіб / В.М. Гранатуров, І.В. Литовченко. – К. : Освіта України, 2010. – 254 с.

СФЕРА ТЕЛЕКОМУНІКАЦІЙ: СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-ПОСЛУГ У СІЛЬСЬКИХ РЕГІОНАХ

Науково-технічна революція, що сталася у XX столітті, помітно змінила умови та характер економічного розвитку. Швидке розповсюдження в усьому світі наукових відкриттів, технічних винаходів, інформаційних технологій, нових засобів комунікацій – усе це чинить вагомий вплив на економіку, політику та культуру усіх країн світу. Зв'язок як складова інфраструктури суспільства є однією із необхідних умов функціонування і підйому економіки держави, відіграючи при цьому величезну роль в її збалансованому розвитку. Зв'язок є основним компонентом будь-якої географічно віддаленої системи. Однак через особливості технологічних процесів та інших факторів серед усіх видів зв'язку пріоритетну роль у ході формування інформаційного суспільства належить телекомунікаціям, які створюють фундаментальну технологічну платформу для більшості інформаційних процесів. Стратегічною метою телекомунікацій є необхідність забезпечення споживачів телекомунікаційними послугами. При цьому сфера телекомунікацій повинна, насамперед, передбачити порядок і терміни забезпечення доступу до загальнодоступної телекомунікаційної мережі людей у різних регіонах країни, а також таких груп, як малозабезпечені сім'ї, пенсіонери, інваліди.

Розвиток телекомунікацій повинен відповідати зростаючим потребам інформаційного суспільства щодо надання послуг споживачам з урахуванням існуючого економічного та соціального стану України. Виконання цього завдання забезпечується лібералізацією і дерегулюванням у сфері зв'язку та інформатизації України, які відбулися у кінці XX ст. та визначили перехід від монопольної структури ринку до появи конкурентного середовища.

Телекомунікаційні послуги за останні роки зазнали значних змін, пов'язаних з активізацією розвитку інфокомунікаційних технологій, тим самим створюючи ситуацію, яка характеризується присутністю на ринку послуг зв'язку традиційних загальнодоступних послуг (фіксована міська та сільська телефонія) і нових послуг (мобільний зв'язок, Інтернет тощо).

Проте впровадження нових телекомунікаційних послуг та розвиток існуючих стикаються з низкою проблем. Це пов'язано з тим, що багато країн вступають в нову еру соціально-економічних відносин. Завдяки загальному руху соціально-економічних систем до інформаційного суспільства відбувається набуття та розвиток нових форм відносин в економічній, соціальній та політичній сферах. Суспільство неухильно рухається до такої інформаційної епохи, в 72 Серія Економічні науки Випуск 14. Частина 4. 2015 якій більша частина бізнесу та економіки постають в електронному вигляді та здійснюються у глобальній мережі Інтернет.

Аналіз останніх досліджень і публікацій. Вирішенням проблем, пов'язаних з аналізом сучасних тенденцій, що призводять до формування основ інформаційного суспільства, переймалися такі зарубіжні вчені, як Д. Белл, Е. Тоффлер, І. Масуда, М. Кастельс, П. Дракер та ін. У нашій країні вирішенням проблем формування та розвитку послуг зв'язку присвячені останні публікації

вітчизняних учених П.П. Воробієнка, В.М. Гранатурова, В.М. Орлова, Г.А. Отливанської, С.В. Зяблова та інших. Але, на наш погляд, є ще такі питання, які потребують подальшого розгляду.

Постановка завдання. Метою статті є визначення соціально-економічних проблем у сфері телекомунікацій і шляхів впровадження інтернет-послуг у сільських регіонах та надання пропозицій щодо їх вирішення.

Виклад основного матеріалу дослідження. Розвиток телекомунікаційної сфери стримується за рахунок низки проблем, які виникають унаслідок науково-технічного прогресу, кризового становища економіки, зниження обсягу інвестування та доходів верств населення тощо.

Термін «проблема» нині набув широкого поширення як у практичній, так і в науковій діяльності. Проблема – це складне питання, розв’язання якого має важливе практичне або теоретичне значення, але цьому розв’язанню перешкоджає відсутність загальноприйнятих методів.

У широкому сенсі проблема розглядається як складне теоретичне або практичне питання, яке вимагає вивчення, дозволу.

У науці під проблемою розуміється суперечлива ситуація, що виступає як протилежні позиції в поясненні будь-яких явищ, об’єктів і потребує адекватної теорії її вирішення. Під проблемою також розглядається наявність істотної розбіжності між бажаним і фактичним станом системи, як концентроване вираження протиріч, що виникають у процесі суспільного розвитку, форму їх проявлення у господарській діяльності для соціально-економічних проблем. Ці протиріччя відображаються в суб’єктах управління, як відсутність позитивного наукового знання, як наявність диспропорцій у розвитку взаємопов’язаних сфер господарювання, як порушення фаз відтворювального процесу, як порушення динамічної рівноваги в системі «природа-суспільство-людина». Як перше, так і наступні розуміння «проблеми» не суперечать один одному і відображають головні сутнісні сторони: складність і протиріччя.

В умовах телекомунікаційної сфери необхідно виділити виробничий, науково-технічний, організаційно-економічний, соціальний та екологічний аспекти протиріч, які і формують відповідні проблеми. У зв’язку з цим слід розуміти поняття проблеми як концентроване вираження виробничих, науково-технічних, економічних та соціальних протиріч, що носять складний характер і вимагають свого вирішення.

Вирішення проблем забезпечується дією людей, що здійснюють управлінську діяльність, що вирішують завдання управління. Тому здійснення управлінської діяльності має бути націлене на виявлення і дозвіл наявних і виникаючих в ході розвитку об’єкта проблем («вузьких місць»). Без проблем не можуть існувати цілі, спрямовані на вирішення цих проблем. Цілі як бажаний досяжний стан об’єкта, як напрями розвитку об’єкта завжди повинні забезпечувати вирішення наявних проблем.

Проведення розбудови телекомунікаційної сфери не може бути здійснено без аналізу проблем і протиріч накопичених і знов виникаючих в старих

системах управління. Тому стає таке завдання як створити таку систему управління, яка буде підготовлена до вирішення наявних проблем і протиріч.

У роботі не представляється можливим розкрити весь перелік питань, пов'язаних з вирішенням усіх наявних проблем у сфері телекомунікацій. Для аналізу розглянемо лише деякий перелік протиріч, наявних в області задоволення послуг зв'язку, які носять різний характер.

- До них можна віднести:
- проблему цифрового розриву, яка пов'язана з недостатньо рівномірним розповсюдженням сучасних технологій;
- недоліки тарифної політики, у зв'язку з чим виникають проблеми зі взаєморозрахунками між телекомунікаційними підприємствами та споживачами послуг зв'язку, що спричиняє конфлікти, а, як наслідок, підвищуються тарифи на телекомунікаційні послуги. Крім того, існує проблема із забезпеченістю населення універсальними послугами зв'язку;
- фізичний та моральний знос обладнання, що спричиняє погіршення якості послуг зв'язку;
- недосконалість стратегії розвитку телекомунікаційної сфери, тобто відсутність єдиної збалансованої стратегії розвитку та планування у телекомунікаційній сфері;
- недосконалість нормативно-правової та законодавчої бази, немає узгодженості між нормативно-правовим документами, крім того більшість законодавчих документів не відповідають стану як ринкової економіки, так і державної політики;
- складність отримання та використання обчислювальних ресурсів за рахунок їхньої нерозвиненості;
- недостатність кількості висококваліфікованих фахівців та зменшення їхньої кількості у зв'язку з постійною еміграцією, що сприяє зменшенню кількості інноваційних, науково-дослідних та дослідно-конструкторських робіт;
- відсутність механізму підтримки вітчизняного виробника, що спричиняє неможливість забезпечити себе продукцією власного виробництва;
- нестабільну економічну і політичну ситуацію в країні, що сприяє збільшенню рівня інфляції та безробіття, зменшенню споживання послуг зв'язку.

Найважливішою передумовою є розв'язання соціально-економічних проблем щодо вирівнювання рівнів розвитку телекомунікацій у міській та сільській місцевості. Нині лише у країнах Західної Європи, Північної Америки та в Японії показники телефонної щільності в містах і сільській місцевості приблизно однакові.

У країнах Східної Європи, включаючи Росію, а також Центральну Азію, Латинську Америку і Центральну Африку, телефонна щільність у містах приблизно у 2,5 рази вища, ніж у сільській місцевості, а в Північній Африці, країнах Близького Сходу та Південно-Східної Азії такий розрив досягає 5-7 разів. У цих

регіонах проблема надання доступу до базових послуг усім громадянам незалежно від місця проживання постає найбільш гостро та належить до пріоритетних завдань розвитку національних телекомунікаційних мереж.

Те саме ми маємо змогу спостерігати і в Україні. В нашій країні треба більш уваги приділяти соціально-економічному розвитку сільських районів, Науковий вісник Херсонського державного університету 73 враховувати та впроваджувати світовий досвід у цій сфері.

Однією із обов'язкових умов розвитку соціальної інфраструктури села є оновлення і розширення мереж телекомунікацій. Якісний телефонний зв'язок у сфері матеріального виробництва сприяє економії часу, дозволяє поліпшити використання сільськогосподарської техніки та оперативне маневрування нею з урахуванням погодних умов, зменшити її простої і прискорити ремонт, забезпечити своєчасні поставки та заготівлі сільськогосподарської продукції.

Поширена думка, що експлуатація сільських мереж збиткова через низьку платоспроможність жителів аграрних районів та у зв'язку з високими капітальними витратами на один телефонний номер, що зумовлено більшою протяжністю ліній зв'язку (порівняно з міською мережею), а також низькою щільністю і нерівномірністю розподілу населення на селі. Тому протягом останніх двох десятиріч одним із актуальних завдань залишається побудова рентабельних мереж телекомунікацій у сільських регіонах країн як з розвиненою, так і з економікою, що розвивається. Увага, яку приділяють даному аспекту, обумовлена перш за все тим, що ефективність одного телефону, що вводить у сільській місцевості, значно вище, ніж у міській, хоча питомі капітальні вкладення на лінію в сільській місцевості можуть бути втричі-вчетверо більше.

Звичайна політика фінансування передбачала мінімальні інвестиції у створення телекомунікаційної інфраструктури в сільських і віддалених районах країн, що розвиваються. На жаль, ці інвестиції недостатні для гарантії загального доступу до основних телекомунікаційних послуг. Тому треба шукати інші способи фінансування.

Нині уже загальновизнано, що сфера телекомунікацій невід'ємна, по своїй сутності, від комерції. Надання якісних телекомунікаційних послуг – це підприємство, що по праву може і повинно бути рентабельним. Воно забезпечує коштовні і життєво важливі стимули для економічного розвитку, поряд із соціальним і культурним розвитком, особливо у сільських і віддалених районах.

Досвід розвинутих країн свідчить, що впровадження телекомунікаційних послуг, які віднесено до загальнодоступних телекомунікаційних послуг (ЗдТП) (у т.ч. інтернет-послуги), є комплексною задачею. Це залежить від низки соціально-економічних, технічних, демографічних та психологічних (ментальних) факторів, які мають широкий розподіл значень у різних країнах. На жаль, в Україні інтернет-послуги не входять до переліку ЗдТП.

Нині досі діє «Концепція розвитку телекомунікаційних мереж сільських районів України на 2003–2010 рр.» (затверджена Держкомзв'язку України), яка визначає головні технічні принципи розвитку, обсяги та рівні надання послуг,

необхідні обсяги фінансування. У 2006 році була прийнята «Концепція розвитку телекомунікацій України до 2010 року», яка підтвердила основні технічні принципи розвитку мереж (модернізація телекомунікаційної мережі району на базі цифрової автоматичної телефонної станції (ЦАТС) одного або сумісних типів обладнання) та уточнила необхідні обсяги фінансування в сучасних соціально-економічних умовах розвитку України. Між тим ці документи зі статуту не визначали усі проблеми розвитку телекомунікацій в сільській місцевості. Нижче приведено варіант класифікації проблем.

На наш погляд, до основних проблем щодо розвитку телекомунікацій у сільській місцевості можна віднести:

- розрив між існуючим і раціональним рівнем розвитку мережі (маємо 5-11% телефонної щільності, а необхідно 30-35%) (СЕ);
- розрив між існуючим рівнем якості послуг, що надаються, та необхідним для більшості користувачів з урахуванням витрат на його забезпечення (СЕ);
- моральний та фізичний стан основної маси обладнання телекомунікаційних мереж (лінійні споруди, автоматична телефонна станція (АТС), системи передачі), близько 60% парку обладнання є морально та фізично застарілим (Т);
- необхідність спеціальних рішень та засобів для побудови абонентської мережі малої ємності (одиниці абонентів) з довжиною ліній до 15 км (Т);
- однозначного визначення загальнодоступних телекомунікаційних послуг, затвердження механізму їх фінансування та реалізації з врахуванням сучасного стану економіки України (ОА);
- розрив між соціальною значущістю наявності повної номенклатури телекомунікаційних послуг для кожного населеного пункту і обсягів збитків для операторів, які повинні їх надавати (НПО);
- розрив між приведеними витратами на організацію послуги та можливими доходами від них (НПО).

Проблеми розвитку сільської телекомунікаційної мережі носять комплексний характер та визначаються такими факторами:

- соціально-економічними (СЕ);
- технічними (Т);
- організаційно-адміністративними (ОА);
- факторами «незрілих» ринкових відносин (НРО).

Судячи з вищезазначеного, можна констатувати, що оператору практично може бути не вигідно розвивати сільський зв'язок з сучасними телекомунікаційними послугами, а тим більш його модернізувати, але з точки зору суспільства – це вкрай необхідно, тим більше що Україна підписала Туніську Декларацію та заявила про необхідність ліквідації цифрового розриву для побудови інформаційного суспільства. Варто зазначити, що, якщо враховувати інтегральний соціально-економічний ефект, то впровадження сучасних

телекомунікаційних послуг з необхідною якістю може бути рентабельним навіть для оператора з урахуванням окремих пільг для нього від місцевої влади.

Належним чином протилежний характер мають і програми інформатизації сфер діяльності, що існують, у тому числі і в сільських регіонах, у різноманітних формах, якими передбачено вирішення первісних невідкладних питань, а саме:

- недосконалість нормативно-технічного обладнання (технічні стандарти, умови тощо) процесів інформатизації, що сильно ускладнює взаємодію та координацію між програмами інформатизації. Тут існує багато невирішених моментів: відсутність сталої термінології, стандартів, критеріїв систематизації засобів інформатизації;
- використання нестандартної або застарілої обчислювальної техніки, що не завдає перешкод виконанню функцій, які покладено на них чинним законодавством. Більшість персональних комп'ютерів, які використовуються на виробництві у якості робочих станцій, становлять Windows-сумісні комп'ютери класів 486DX2-80 – Intel Pentium 166-233. Незважаючи на їхню моральну застарілість (такі комп'ютери вже не виробляють), вони узгоджуються з новітніми моделями за обміном даними, а амортизаційний строк цієї техніки перевищує термін її морального старіння. Взагалі, ті, хто вважає параметри своїх телекомунікаційних мереж невідповідними, зрештою використовують набагато меншу пропускну можливість каналів. З іншого боку, потрібно відзначити, що визнаних нормативних критеріїв, завдяки яким можливо було б визначити достатність пропускну можливості й інші параметри телекомунікаційних мереж, не існує;
- усунення недоліків нормативно-правової бази, які стосуються форм, змісту та порядку обміну інформацією серед управлінських організацій, що призводять до повторення або повної втрати цієї інформації. Тобто невирішеним моментом залишається відсутність нормативно-правового становища електронних документів;
- можливість застосування наявних телекомунікаційних систем в інтеграції на державному рівні, які не знайшли найбільш прийнятної відповіді в інфокомунікаційних програмах. Потрібен чіткий розвиток інформаційних потоків з їхньою технічною реалізацією на платформі, яка буде належати до відкритих систем, щоб інтеграція сфери інформаційних систем стала загальнонаціональною;
- ухвалення низки нормативно-правових та законодавчих актів має посприяти вирішенню інтеграції програмного, інформаційного, технічного оснащення інформаційно-аналітичних систем різноманітного призначення та рівня, інженерії якості різних програмних систем;
- для всебічного розвитку соціально-економічних процесів повинні бути засновані інтегровані системи баз даних, має проводитися різнобічний моніторинг головних індикаторів протікання таких важливих процесів в цілому в країні, її окремих регіонів та сфер економіки. Повинна

продовжуватися побудова інших окремих інформаційно-аналітичних систем, вони дозволять значною мірою автоматизувати виконання різних функціональних задач;

- існує низка питань, які регулюють суспільні відносини та які пов'язані з поширенням використання мережі Інтернет – авторське право, сумлінність використання інформації, порушення у галузі використання товарних знаків, захист честі, вторгнення у приватне життя, регулювання ліцензованих ринків товарів та послуг, у тому числі банківських послуг, реклами, освіти тощо.

Висновки:

Таким чином, незважаючи на визначений обсяг соціально-економічних проблем, сфера телекомунікацій, яка займає значне місце в економіці країни (регіону, району), чинить значний вплив на її соціально-економічний розвиток. Проблеми складні, однак без їх вирішення неможливий подальший розвиток телекомунікацій та економіки країни в цілому та її окремих регіонів.

Література:

1. Воробієнко П.П. Проблеми використання закономірностей впливу ІКТ на економічний розвиток країни [Текст] / П. Воробієнко, В. Гранатуров // Економіка України. – 2011. – № 8. – С. 26-33.
2. Державна служба статистики України [Електронний ресурс]. – Офіційний веб-сайт. – Режим доступу: <http://www.ukrstat.gov.ua>.
3. Костіна О.В. Тенденції розвитку інформаційного суспільства: аналіз сучасних інформаційних і постіндустріальних концепцій / Електронний журнал "Знання. Розуміння. Уміння" 2009 № 4

Лазоренко Анастасія Вячеславівна
Державний університет телекомунікацій
Навчально- науковий інститут менеджменту та підприємства
м. Київ

ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ

Анотація.

Постійний розвиток та подальше становлення ринкових відносин ставить свої вимоги до стабільно функціонуючої системи управління на підприємстві. Досягнення бажаного рівня неможливе без розв'язання вже накопичених суперечностей і вирішення проблем в усіх сферах економіки України. Сфера телекомунікацій та її підприємства як складові являють собою стратегічне значення для сталого розвитку й подальшої інтеграції усіх сфер і галузей економіки у процеси світової глобалізації. Це підтверджується вже доведеним міжнародним суспільно-економічним явищем – становленням наступного інформаційно- технологічного способу виробництва.

Управління підприємствами телекомунікацій - складне системне утворення й пов'язане з багатьма змінними, що сприяє виникненню суперечностей і проблем усередині системи. Суперечності, в свою чергу, являють собою джерело економічного прогресу, відсутність яких зупинить саме життя людства та його еволюцію, але їх накопичення призводить спочатку до кризи, а потім – до

банкрутства підприємства. Виявлення суперечностей і подальше визначення структури проблем можна представити за допомогою принципів, які повинні враховуватись керівниками й фахівцями підприємства при реалізації своєї діяльності.

Принципи як основні положення, від вмісту яких залежать сутність і особливості планування цілей та окреслення бізнес-процесів у цілому, допоможуть сформувати модель структури проблем для їх аналізу та розв'язання; проте, керуючися принципами, можна коригувати дії на кожному етапі для досягнення кінцевого позитивного результату розв'язання проблеми чи зняття суперечностей. Ключові слова: проблеми, суперечності, модель структури проблем, телекомунікації, принципи, система управління.

Постановка проблеми. В умовах динамічного розвитку ринкової економіки зростають вимоги до соціально-економічної адаптованості та відповідного рівня функціонування усіх галузей та сфер економіки України. Прогресивний розвиток науки, техніки і технологій, інноваційність та висока науковість сучасного виробництва висувують особливі вимоги до шляхів розвитку інформаційно-телекомунікаційної сфери.

Сфера телекомунікацій як складова сфери зв'язку та інформатизації має стратегічне значення для сталого розвитку й стабільного функціонування виробничої і соціальної інфраструктури України, що призначена для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах. Це можливо зробити лише за умов стабільної роботи підприємств телекомунікаційної сфери, що спрямована на подальший успішний розвиток. Так підприємства телекомунікацій повинні бути динамічними, адаптивними, швидко реагувати на стрімкий, схильний до кардинальних змін телекомунікаційний ринок.

Унаслідок цього інформаційно-телекомунікаційні послуги не можуть ефективно поширюватись без налагодженого механізму управління даними послугами. Одним із елементів успіху в цьому процесі є правильно обрана, адаптована до сьогодення система управління й контролю за діяльністю об'єктів економіки, яка врахує всі можливі проблеми, недоліки, суперечності та кризові явища у майбутньому.

Економічна та соціальна політика потребує вивчення кола суперечностей і проблем, що виникли на даному етапі та гальмують подальший розвиток підприємств телекомунікацій в Україні. Формування моделі структури проблем управління телекомунікаційними підприємствами допоможе послідовно й детально проаналізувати суперечності та проблеми для їх подальшого розв'язання.

Інтеграція цієї структури у систему управління телекомунікаційним підприємством надасть можливість менеджменту підприємства своєчасно реагувати й швидко вирішувати проблеми, що постають у процесі управління життєдіяльністю об'єктом телекомунікаційного ринку. Незважаючи на велику кількість наукових досліджень, публікацій і накопичений практичний досвід у теорії і практиці структуризації й розв'язання суперечностей та проблем на

необхідному етапі розвитку підприємства, все ще залишаються аспекти, розглянуті недосить повно. Вони стосуються розробки моделі структури проблем для сприяння швидкісному та спрощеному їх вирішенню у сучасних динамічних умовах техніко-технологічного та інформаційного розвитку економіки.

Метою статті є формування моделі структури проблем та суперечностей, необхідної для подальшого вдосконалення системи управління телекомунікаційних підприємств України в сучасних економічних умовах. Виклад основного матеріалу. У сучасних умовах недостатній аналіз кола актуальних суперечностей та проблем не дає змогу підприємствам реалізувати весь потенціал виробничих, економічно-соціальних і науково-технологічних можливостей з точки зору ефективного виробництва й реалізації кінцевих продуктів телекомунікацій. Ця проблема безпосередньо пов'язана з відсутністю структурного підходу до формування ефективної моделі структури проблем та протиріч, що визначає необхідність вивчення останніх.

Сфера послуги телекомунікаційного ринку в Україні як складова сфери послуг країни на даному етапі відноситься до однієї з найдинамічніших за розвитком сфер економіки. Доходи від надання телекомунікаційних послуг за 9 місяців (січень-вересень) 2014 року порівняно з аналогічним періодом минулого року збільшилися на 2,9 % і склали 36289,0 млн. грн., що становить 92,3 % від загальної кількості доходів від надання послуг зв'язку.

Але, не дивлячись на вищезазначене, сьогодні в Україні існує, так званий, феномен цифрової нерівності, цифрової прірви – поділ окремих верств населення на основі нерівного доступу до сучасних технологій. Це особливо актуально для споживачів важкодоступних сільських, гірських районів та соціально вразливих груп споживачів: малозабезпечені сім'ї, пенсіонери та інваліди.

Для розв'язання окресленої проблеми Законом України «Про телекомунікації» (далі – Закон) було введено поняття «загальнодоступні телекомунікаційні послуги» які надаються споживачам на всій території України за тарифами, що регулюються державою і встановлені не тільки нижче їх реальної вартості, але інколи й нижче собівартості. Доконечність надання збиткових загальнодоступних телекомунікаційних послуг викликало низку нових техніко-економічних проблем телекомунікаційної сфери, які потребують вчасного вирішення.

У першу чергу, йдеться про мотивацію розвитку таких послуг. Із цією метою Законом передбачено необхідність компенсації збитків операторам, що надають загальнодоступні послуги. Створення відповідного механізму компенсації збитків покладено на Кабінет Міністрів України.

Після введення в дію Закону пройшло 10 років, проте такий механізм, який відповідав і ринковим принципам, і соціальним інтересам, з різних причин, на жаль, не створено, тому, як вказано, досить гостро стоять проблеми:

- визначення та обґрунтування загального обсягу витрат, необхідних для компенсації збитків операторам, що надають загальнодоступні послуги
- визначення джерел надходження цих коштів;
- визначення організаційних структур, які акумулюватимуть ці кошти, їх прав та обов'язків;
- визначення порядку надходження коштів у ці структури;
- визначення порядку розподілу коштів між операторами, які надають збиткові загальнодоступні телекомунікаційні послуги.

Питання розвитку широкосмугового доступу до мережі Інтернет становить ще одну з проблем, яка викликана швидким зростанням соціальної ролі телекомунікацій у житті українців. Ця проблема у світі вирішується вже відомим шляхом – ще на початок 2012 р. більш ніж 40 країн включили широкосмуговий зв'язок у склад загальнодоступних послуг .

За даними звіту Бюро розвитку електрозв'язку (ITU) за 2014 рік, більше 75 % телекомунікаційного потоку припадає на вільний широкосмуговий зв'язок Інтернету, тому стрімкий розвиток у світі широкосмугового зв'язку є самою значущою тенденцією у секторі інформаційно-комунікаційних технологій за останні кілька років . Він суттєво вплинув на способи спілкування, доступу до інформації, обміну досвідом і знаннями, ведення господарської діяльності тощо. Але такий стрімкий розвиток викликав низку проблем соціально-економічної безпеки. Телекомунікаційна сфера та її підприємства потребують, з одного боку, державного регулювання, а з іншого – допомоги, щоб максимізувати вигоди від нових технологій і послуг, але мінімізувати ризики для споживачів та економіки.

Специфічною характеристикою діяльності як руху є її усвідомленість і самоусвідомленість. Суть протиріч економічних інтересів виявляється через їх функції: Мотиваційну. Протиріччя є джерелом руху. В результаті вирішення суперечностей відбувається подальше вдосконалення не лише соціально-економічних, але й організаційно- економічних та техніко-економічних відносин.

Ці процеси – рушії прогресу, що супроводжують розвиток виробництва і стимулюють об'єктів телекомунікацій розв'язувати протиріччя. Стосовно техніко-економічних відносин, в умовах застосування високих технологій технологічна й маркетингова діяльність потребує від компаній істотно різних компетенцій персоналу й організації бізнес-процесів, тому на часі використання аутсорсингу в технічному обслуговуванні та підтримці мереж постачальникам обладнання, фахівці останніх є більш компетентними у прийнятті рішень

Література:

1. Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009. – № 1. – С. 83-89.
2. Кузьмінов А.В. Узгодження мотиваційних впливів на ефективність механізму управління телекомунікаціями регіону: дис. ... канд. екон. наук: 08.07.04 / А.В. Кузьмінов, Одеська національна академія зв'язку ім. О.С. Попова. – Одеса, 2005. – 224 с.
3. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.
4. Кравченко А.І. Історія менеджменту : підручник / А.І. Кравченко. – 3-тє вид., перероб. і

доп. – М. : КНОРУС, 2010. – 432 с.

5. Лігоненко Л.О. Антикризове управління підприємством: теоретико-методологічні засади та практичний інструментарій / Л.О. Лігоненко. – К. : КНТЕУ, 2001. – 580 с.

6. Чухно А. Сучасна фінансово-економічна криза: природа, шляхи і методи її подолання /

Лазоренко Анастасія Вячеславівна

Державний університет телекомунікацій

Навчально - науковий інститут менеджменту та підприємства

м. Київ

СОЦІАЛЬНІ ПРОБЛЕМИ МОЛОДІ В ОБЛАСТІ ІНФОРМАТИЗАЦІЇ СИСТЕМИ ОСВІТИ УКРАЇНИ

Сучасні суспільні процеси різко змінили соціальне, матеріальне і політичне становище молоді. До соціальних проблем українського суспільства, які, на думку української молоді, відносяться падіння престижу загального і професійно-технічної освіти, збільшення числа молоді, що починає трудову діяльність з низьким рівнем освіти, без бажання продовжувати навчання. Також окрема проблема - критична зношеність матеріально-технічної бази закладів освіти всіх рівнів і недостатні темпи її модернізації.

Сучасна державна молодіжна політика в повній мірі не вирішує соціально-психологічні проблеми вдосконалення системи виховання і освіти молоді, методів реалізації соціально-економічних і духовних потреб. Необхідно розробити програму національно-патріотичного виховання, спрямовану на подолання розрізненості молоді різних регіонів України та консолідації української нації.

Інформатизація системи освіти передусім передбачає появу нових ІКТ-орієнтованих педагогічних і освітніх технологій, новітніх засобів навчання, створення й використання в педагогічних системах сучасних комп'ютерно орієнтованих навчальних середовищ, поступове формування і розвиток комп'ютерно-технологічної платформи інформаційного освітнього простору, електронних інформаційних освітніх ресурсів (колекцій цифрових освітніх ресурсів) і мережних сервісів, що його змістовно наповнюють і процесуально підтримують [1]. На характер і темпи інформатизації системи освіти визначально впливає поширення найсучасніших й перспективних форм і технологій організації освіти, до яких, передусім, слід віднести відкриту освіту, системи електронної дистанційної освіти, електронні дистанційні технології навчання, що будуються на основі принципів відкритої освіти [2]. Саме впровадження в освіту України принципів відкритої освіти акумулює останні погляди вчених і практиків на перспективні шляхи розвитку освіти в інформаційному суспільстві, передбачає використання найсучасніших здобутків психолого-педагогічної науки, освітньої практики і науково-технічного прогресу, забезпечує наслідування і відтворення в освіті України світових тенденцій розвитку освітніх систем, зумовлює інтеграцію системи освіти України у світовий освітній простір.

Проблеми сучасного стану інформатизації освіти. Серед найгостріших з таких проблем є такі:

1. Значна цифрова нерівність надання ІКТ-послуг у різних регіонах України, особливо для населення великих міст і сільської місцевості, невідповідність комп'ютерного оснащення навчальних закладів та умов кадрової підтримки ІКТ-систем сучасним вимогам:

- недостатній рівень оснащення навчальних закладів сучасними загальносистемними програмно-апаратними засобами комп'ютерної техніки, включаючи підключення до Інтернет через широкосмугові канали зв'язку;
- вкрай низький рівень застосування освітніх ІКТ-систем, неготовність до їх ефективного використання в педагогічних системах;
- невідповідність якісного і кількісного складу ІКТ-підрозділів навчальних закладів складності підтримки функціонування і розвитку сучасних освітніх ІКТ-систем, слабе залучення до цієї роботи компаній – аутсорсерів.

2. Відсутність індустріального підходу, недостатній рівень і масштаби створення і впровадження в освітню практику якісних електронних освітніх ресурсів та їх колекцій.

3. Недосконалість системи оцінювання і сертифікації створених електронних освітніх ресурсів.

4. Значні масштаби використання в системі освіти не ліцензованого програмного забезпечення.

5. Психолого-педагогічні проблеми безпеки навчальної діяльності в загальнодоступних і корпоративних інформаційних мережах:

- користувачів у мережному середовищі комп'ютерної віртуальної реальності;
- збереження і конфіденційності доступу до мережних даних.

6. Проблема готовності учнів (студентів) і вчителів (професорів) до роботи у відкритих педагогічних системах.

7. Недостатня інтеграція у вищій школі навчальної, наукової та управлінської діяльності.

8. Слабкий зв'язок у ланцюгах «школа - університет» та «освіта - наука - виробництво».

9. Слабкий зв'язок між інвестиціями у створення, розвиток і підтримування програмно-апаратних засобів різнорівневих освітніх ІКТ-систем (в тому числі витратами на підвищення кваліфікації освітянських кадрів) і відповідним підвищенням якості освіти, ІКТ-компетентностей тих, хто навчається.

10. Відсутність в системі освіти дійових механізмів стимулювання інноваційних проектів із створення і впровадження ІКТ-систем, підвищення їх ефективності.

11. Недосконалість системи моніторингу процесу інформатизації освіти.

Вважаю за доцільне поліпшити доступність освіти через систему соціальної підтримки учнів, студентів та молодих вчених, прискорити темпи модернізації освітнього процесу та розширити мережу нових форм навчання, створити спеціальні програми з інформатизації навчальних закладів, підвищивши зацікавленість в отриманні інформації.

Ефективні засоби сприяння зайнятості молоді: по-перше, зобов'язати навчальні заклади забезпечити випускникам перше робоче місце (44%), а по-друге, встановити на підприємствах квоти для молоді (41%) [3].

Такий підхід до соціальних питань молоді дозволить їй пізнати і розвинути себе на основі власних умінь і, досягнувши зрілості, максимально реалізуватися, що є неодмінною умовою особистого щастя, динамічного і сталого суспільного прогресу.

Література:

1. Биков В.Ю. Відкрите навчальне середовище та сучасні мережні інструменти систем відкритої освіти // Науковий часопис НПУ ім. М.П. Драгоманова. Серія №2. Комп'ютерно орієнтовані системи навчання: 36. наук, праць / Редрада. - К.: НПУ імені М.П. Драгоманова, 2010. - №9(16). - С. 9-16.
2. Биков В.Ю. Упровадження інформаційно-комунікаційних технологій в освіті - імператив її модернізації // Національна доповідь розвитку освіти України, 2011. - С. 118-124.
3. Національна стратегія розвитку освіти в Україні на 2012-2021 роки // Науковий журнал. - 2011. - №6. - С. 25-43.

Лазоренко Анастасія Вячеславівна

Державний університет телекомунікацій

Навчально - науковий інститут менеджменту та підприємництва

м. Київ

АКТУАЛЬНІ ПРОБЛЕМИ СТРАТЕГІЇ ЕКОНОМІЧНОГО І СОЦІАЛЬНОГО РОЗВИТКУ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ

Нове суспільство називають постіндустріальним, постекономічним, оскільки мова йде про багатосторонні і кардинальні зміни у розвитку цивілізації. Але одним з найпростіших є назва "інформаційне суспільство", так як воно відображає докорінна зміна - перетворення інформації і знань в головний виробничий фактор. Всупереч усіляким домислів про неможливість постіндустріального розвитку для України, національні рухи за інформатизацію економік суспільства, які очолює і регулює ООН, придбали загальносвітовий характер.

Для цього розроблена Спеціальна програма створення інформаційного суспільства, що поєднує національні програми та направляючі рух всіх членів ООН з цього шляху.

Так, в Україні вже два роки діє затверджена урядом нашої країни та спеціалізованої Програмою розвитку ООН програма "Інноваційний трамплін: інформаційно-комунікаційні технології для добробуту України". Відповідно до цієї програми розробляється ється стратегія розвитку ІКТ. Все це дозволило підвищити частку власне інформаційного продукту до 12% загального валового продукту, хоча цього, безперечно, мало. Аналогічний показник у розвинених країнах перевищує 20%

За даний час більш ніж у 20 разів збільшився індекс активності української Інтернет-аудиторії, розширюється інформаційна мережа вузів. Україна першою серед країн СНД приєдналася до європейської освітньо-наукової мережі GEANT, яка охоплює понад 3000 науково-дослідних навчальних закладів та 3 млн. індивідуальних користувачів з 31 європейської країни. У рамках проекту

Міжнародного союзу електрозв'язку у ВАТ телекомунікацій створена філія Академії Cisco з питань підготовки фахівців на тов в області мережевих технологій. Одеська національна академія зв'язку здійснює проект "Система дистанційного навчання на базі сучасних телекомунікаційних та інформаційних технологій в галузі підготовки, перепідготовки та підвищення кваліфікації кадрів для країн СНД в кінці жовтня 2003 р. у Києві на базі Центру" Укрчастотнагляд "відкритий міжнародний центр підвищення кваліфікації кадрів для країн Європи та СНД. У світі діє 5 таких центрів: для Західної і Центральної Африки, Східної Європи, Південної Африки, Азіатсько-Тихоокеанського регіону, Америки і для Арабського регіону.

Як бачимо, вже на перших етапах поширення інформаційно-комунікаційних технологій неминуче виникає необхідність створення розробки та реалізації національних програм з налагодженням та поглибленням міжнародного співробітництва. Взаємодія загального, інтернаціонального, з особливим, національним, є необхідною умовою швидкого оволодіння ІТ-технологіями та їх широкого використання.

Складність цього процесу полягає в тому, що сучасні технології розвиваються одночасно вглиб і вшир. Характерна риса нинішнього етапу - цифрова трансформація всіх складових нових технологій. Цифрові технології стають рушійною силою підвищення продуктивності та конкурентоспроможності економіки, зростання рівня життя народів. Цифрову інформацію просуває Інтернет. Інфраструктура зв'язку стає цифровою і об'єднується з Інтернетом. У майбутньому почне здійснюватися бездротові підключення до Інтернету, що визначає його великі перспективи. Створюються інтегровані пристрої, що поєднують обчислювальні функції з бездротовою комунікаційною інфраструктурою, тобто буде відбуватися інтеграція обчислень з телекомунікаціями. Фахівці вважають, що в найближчі 20 років відбудуться прогресивні зміни в ІТ і їх потрібно своєчасно розпізнавати і вміло використовувати.

У той же час нові технології швидко виходять за межі розвинених країн, охоплюють все нові країни, проникають у різні сфери економіки та суспільного життя. Так, Інтернет сьогодні налічує 700 млн. користувачів, і найближчим часом їх кількість зросте до 1 млрд., а потім і до 2 млрд. У цей час у світі налічується близько 1 млрд. користувачів мобільних телефонів. Вони також стають цифровими, можуть фотографувати, здійснювати відеозапис, комп'ютерні розрахунки, відправляти короткі повідомлення. Обсяг торгівлі через Інтернет вже обчислюється кількома трильйонами доларів. У найближчі роки він досягне 10 трлн. дол., що еквівалентно всій економіці США.

Отже, зростання і вдосконалення ІТ-технологій і швидке їх поширення неминуче поєднують розвиток і реалізацію національних програм розробки та використання нових технологій з налагодженням та поглибленням міжнародного співробітництва. Сама природа процесів інформатизації економіки і суспільства носить інтернаціональний характер, тому що самостійне вирішення проблем

неминуче повинно спиратися на світовий досвід та враховувати його.
Література:

1. Стюарт Т. Інтелектуальний капітал. Нове джерело багатства організацій. "Нова постіндустріальна хвиля на заході". М., 2007, с.377.
2. Яценко О. До саміту - з національними ініціативами. "Урядовий кур'єр" від 9 грудня 2003 р., с.5.
3. Костіна О.В. Тенденції розвитку інформаційного суспільства: аналіз сучасних інформаційних і постіндустріальних концепцій / Електронний журнал "Знання. Розуміння. Уміння" 2009 № 4

Смутьська Вікторія Костянтинівна
Державний Університет Телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ШЛЯХИ ВДОСКОНАЛЕННЯ РЕГУЛЮВАННЯ ТА АКТИВІЗАЦІЇ ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери. Сталий розвиток інформаційно-телекомунікаційної інфраструктури є найважливішою передумовою для підвищення конкурентоспроможності економіки та інтеграції України у глобальне інформаційне суспільство, яке дозволяє розширити можливості людини отримувати доступ до національних та світових інформаційних ресурсів і також поліпшити умови та якість життя людини.

Протягом останніх років сфера телекомунікацій в Україні зберігає позитивну динаміку розвитку, незважаючи на кризові явища в економіці. Проте аналіз показників, що характеризує стан розвитку галузі у 2009 році та її інвестиційну забезпеченість свідчить про зменшення рівня доходів від надання окремих видів послуг та скорочення інвестиційних ресурсів, що спрямовуються у розвиток телекомунікаційних мереж.

Зниження обсягу інвестицій в 2009 році пояснюється, в першу чергу, впливом фінансово-економічної кризи на галузь, зменшенням власних інвестиційних коштів операторів, скороченням обсягів банківського кредитування.

Разом з тим, в Україні залишається невирішеною проблема телефонізації населення, особливо в сільській, гірській місцевостях та віддалених районах. Так на кінець 2009 року, за даними ВАТ «Укртелеком» в черзі на встановлення телефону перебувало 900 тис. осіб, в тому числі у сільській місцевості – 350 тис. осіб. Причинами такого значного незадоволеного попиту є обмеженість інвестиційних ресурсів у операторів через низьку рентабельність послуг міського та збитковість сільського телефонного зв'язку, відсутність фінансових механізмів інвестування розвитку загальнодоступних послуг та відшкодування збитків від їх надання.

Для розв'язання вищезазначених проблем та забезпечення прискореного розвитку телекомунікацій інвестиційна політика в державі повинна

проводитись з урахуванням напрямів, визначених Концепцією розвитку телекомунікацій в Україні, схваленої розпорядженням Кабінету Міністрів України

від

07.06.2006

№ 316-р – основним інструментом реалізації державної політики у сфері телекомунікацій:

- залучення фінансових та кредитних ресурсів національних і іноземних банків для реалізації пріоритетних інвестиційних програм і проектів;
- забезпечення економічної привабливості телекомунікаційних проектів та спрямування частини отриманого прибутку на розвиток телекомунікаційних мереж;
- стимулювання реалізації інвестиційних проектів, які здатні забезпечити строки окупності, валютні надходження та розв'язання проблем розвитку за рахунок самофінансування;
- створення сприятливих умов для залучення іноземних інвестицій в розвиток телекомунікацій для реалізації довгострокових проектів;
- спрямування іноземних кредитів на придбання новітніх технологій та телекомунікаційного обладнання, продукції і обладнання на конкурентних засадах.

Шляхи і способи розв'язання проблеми:

Для поліпшення інвестиційного клімату у галузі зв'язку та активізації залучення зовнішніх та внутрішніх інвестицій у створення сучасних телекомунікаційних мереж пропонується розробити наступні заходи щодо:

- впровадження радіотехнології мобільного зв'язку третього покоління 3G (UMTS) з метою розширення асортименту та підвищення якості надання послуг мобільного зв'язку шляхом проведення тендеру на отримання операторами ліцензії на користування радіочастотним ресурсом;
- розширення повноважень Національної комісії з питань регулювання зв'язку України в частині визначення та аналізу ринків телекомунікаційних послуг, у тому числі визначення операторів з істотною ринковою перевагою на цих ринках та покладання на них відповідних регуляторних зобов'язань з метою забезпечення ефективної конкуренції на ринку телекомунікацій;
- удосконалення тарифної політики у галузі зв'язку з метою забезпечення поступового збалансування тарифів на послуги зв'язку, що підлягають державному регулюванню, поступового уникнення перехресного субсидування одних послуг за рахунок інших;
- спрощення процедури доступу на ринок телекомунікацій шляхом переходу від ліцензування до реєстрації діяльності у сфері

телекомунікацій для покращення конкурентного середовища на ринку телекомунікацій;

- забезпечення гарантованого доступу до універсальних телекомунікаційних послуг на всій території України для задоволення потреб у цих послугах всіх верств населення, зокрема тих, які проживають у сільській, гірській місцевостях та віддалених районах шляхом створення Фонду універсальних телекомунікаційних послуг.

Висновки:

На сьогодні провідна роль у формуванні сприятливого інвестиційного клімату та активізації внутрішньої інвестиційної активності у сфері телекомунікацій належить і збережеться у майбутньому у Національній комісії з питань регулювання зв'язку України, на яку покладено згідно з законодавством повноваження щодо забезпечення зваженого ефективного регуляторного впливу на ринок телекомунікацій.

Смольська Вікторія Костянтинівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

РОЛЬ ТА ПРОБЛЕМИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Телекомунікації відіграють значну роль у соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

Важливою компонентою синтезу інтегрованих систем оперативного управління Міністерства надзвичайних ситуацій України (ІСОУ-МНСУ) є задача забезпечення надійного зв'язку. Здійснення заходів з запобігання надзвичайних ситуацій (НС), моніторингу та ліквідації вимагає надійного оперативного зв'язку для передавання команд і даних між органами управління МНС, цивільною обороною, органами влади, промисловими і транспортними та енергетичними компаніями, що залучаються до ліквідації загроз та місцями розташування об'єкта НС. Для забезпечення координації дій в цих ієрархічних структурах повинні використовуватись всі види зв'язку: комутовані телефонні лінії АТС, спеціальні виділені лінії і канали, урядові канали зв'язку і оповіщення, телетайпні, телеграфні і оптоволоконні лінії зв'язку, радіоканали та супутникові системи мобільного зв'язку, альтернативні системи зв'язку при руйнуванні кабельних магістралей, мобільні пункти передавання інформації та

зв'язку на основі короткохвильових, ультракороткохвильових систем радіозв'язку, супутникового радіозв'язку.

Об'єкти телекомунікаційної та управлінської структур характеризуються різноманітністю інформаційних потоків, які циркулюють між його елементами, що вимагає введення єдиних систем уніфікації і стандартизації представлення документів та протоколів обміну. Відповідно, основними цілями функціонування телекомунікаційних систем та зв'язку в інформаційній структурі підтримки прийняття рішень будуть: підвищення оперативності прийняття рішень та надання інформаційно-аналітичної підтримки на всіх рівнях управління, моніторингу та ліквідації НС, забезпечення посадових осіб і органів влади достовірною інформацією про НС, забезпечення сумісності інформації на всіх рівнях ієрархії управління за рахунок використання єдиних класифікаторів, стандартів, принципів побудови інформаційних структур і систем, оптимізація координації організаційної та інформаційної взаємодії функціональних систем МНС, оптимізація і автоматизація процесів збирання та комплексного оброблення даних, отриманих від системи моніторингу і переданих по каналах зв'язку, комп'ютерних і телекомунікаційних мережах, підвищення достовірності та повноти циркулюючої інформації за рахунок інтелектуального оброблення даних і засобів захисту каналів, забезпечення оперативних потоків даних визначеними маршрутами до центрів оперативного управління МНС, підтримка регулярного інформаційного обміну через мережі зв'язку і телекомунікаційні системи.

Відповідно до наведених завдань стратегічного рівня сформулюємо принципи побудови інформаційного забезпечення оперативних центрів МНС каналами передачі даних і радіомережами: оперативні центри управління створюються на основі інтеграції функціональних, інформаційних і програмно-апаратних засобів, інтеграція орієнтована на цільове використання потоків даних від різних джерел і на основі інтелектуального опрацювання даних формується в реальному часі об'єктивна оцінка НС та прогноз розвитку сценаріїв. Технологія збирання та накопичення даних передбачає автоматизацію вводу, алгоритмізацію та формалізацію, інформаційний обмін між структурними елементами по мережах і каналах зв'язку, передбачає автоматизацію передачі даних з врахуванням рівня доступу в інтегрованих структурах МНС. Інформаційною основою інтеграції потоків даних в межах центру управління НС-МНС є типові протоколи і елементи лексичного та лінгвістичного забезпечення і зі спільним регламентом інформаційного обміну, всі елементи інтегрованої системи ЦУНС-МНС мають можливість безпосереднього зв'язку з центром ОУ, що підвищує відповідно його інформованість щодо ходу моніторингу і ліквідації НС. Первинне оброблення даних ґрунтується на структуруванні та формалізації, кваліфікації блоків даних після їх інтелектуального оброблення.

Встановлено, що інформаційна сумісність передачі пакетів даних в комп'ютерних мережах та аналогової інформації в каналах зв'язку

забезпечується шляхом використання єдиного лінгвістичного забезпечення, лексичного і програмного, яке включає в себе уніфіковані інформаційні структури банків даних усіх рівнів системи, а також правил і протоколів передачі даних.

Смутьська Вікторія Костянтинівна
Державний Університет Телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ДИНАМІКА ТЕЛЕКОМУНІКАЦІЙНОГО РИНКУ УКРАЇНИ

Розвиток телекомунікацій у світі сьогодні характеризується подальшим розвитком конвергенції із сферою телебачення. Як відзначають експерти, така конвергенція з'являється у поєднанні телебачення, телефонії та послуг широкосмугового Інтернету у комплексній пропозиції для замовника. Україна не є винятком з світової тенденції. Останні роки в Україні відзначалися входженням так званих «Мобільний ТВ» на ринок - такий вид послуг пропонується провідним Оператори мобільного зв'язку України: Закрите акціонерне товариство «Київстар Дж.Ес.Ем.» (ТМ «Київстар», «Ace & Base», «DJUICE»), Закрите акціонерне товариство «Українське Мобільний зв'язок», Компанія з обмеженою відповідальністю «Астеліт» (ТМ «Life :»)). Цього року «Мобільний Інтернет» (відкритий міжнародний стандарт передачі даних «WAP», мережі GPRS тощо) зміцнив свої позиції на українському ринку.

Одна зі стратегічних для будь-якої країни галузей – галузь телекомунікацій – відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою для:

- промислової сфери
- сфери послуг і споживачів
- різних географічно розрізнених частин країни
- економічних центрів

Вже зараз неймовірно збільшені потоки інформації – телефонні розмови, факсимільна інформація, електронна пошта, масиви даних та телебачення – показують, якою мірою світ стає ще більш залежним від засобів телекомунікацій, які змінюють бізнес, стиль життя, суспільство в цілому.

Загальновідомим є той факт, що телекомунікації України значно відстають від телекомунікацій розвинутих країн як за обсягами, так і за рівнем технологій. Ринок телекомунікацій України – достатньо відкритий та лібералізований за останні 8 років.

Використання сучасного потенціалу телекомунікацій в Україні можна охарактеризувати за такими основними показниками:

- основні ресурси мереж фіксованого телефонного зв'язку (приблизно 60 відсотків) морально застаріли і фізично зношені;
- мережа ліній проводового та ефірного телерадіомовлення зношена приблизно на 90 відсотків, а близько 80 відсотків передавального обладнання є застарілим, що не дає можливості розвивати нові види послуг;

- значна частина персоналу, що працює на старому обладнанні, потребує перепідготовки для роботи в сучасних умовах та на сучасному обладнанні;
- сучасними можна вважати засоби мереж рухомого (мобільного) зв'язку, кабельного телебачення та комп'ютерного зв'язку (мережі Інтернет).
- Зробивши висновок, можна сказати, що у сфері телекомунікацій України існують такі проблеми:
- низький рівень забезпечення населення, підприємств, установ і організацій інтер-активними телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах); (248 *Актуальні проблеми міжнародних відносин. Випуск 88 (Частина I), 2010*)
- використання на стаціонарних телекомунікаційних мережах морально застарілого фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій негативно впливає на ефективність роботи операторів телекомунікацій;
- наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Токмина Тетяна Олександрівна

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Телекомунікаційній галузі належить особливе місце в економіці будь-якої держави. Обсяг інформації, що передається за допомогою інформаційно-телекомунікаційної інфраструктури, подвоюється у світі кожного року, що посилює значення телекомунікацій як на рівні компанії, так і в цілому у національній та світовій економіках. В даній темі проаналізовано роль телекомунікацій у розвитку економіки і у створенні належних умов життєдіяльності народу України.

На сьогоднішній день розвиток телекомунікацій є необхідною умовою для створення інфраструктури бізнесу, формування сприятливих умов для залучення інвестицій в країну, вирішення питань зайнятості населення, розвитку сучасних інформаційних технологій.

Враховуючи тенденцію збільшення попиту споживачів на нові види телекомунікаційних послуг, у світі відповідно змінюються і ринки надання цих послуг. Необхідність розвитку ринкових відносин викликає потребу у створенні сприятливих умов для суб'єктів господарювання шляхом регулювання їх діяльності в умовах лібералізації та конкуренції. Для таких масштабних реформ, направлених на реструктуризацію сфери телекомунікацій, як правило, вимагає створення незалежних регуляторних органів [1].

У світі відомі 3 основні моделі державного впливу на сферу телекомунікацій:

- функціонує тільки орган державного управління (орган виконавчої влади);
- функціонує тільки орган державного регулювання (державний колегіальний орган);
- одночасно функціонують органи державного управління та орган державного регулювання.

За оцінками дослідницької компанії ComnewsReserch незалежний телекомунікаційний регулятор діє в 150 державах. Це 80% від загальної кількості країн, які існують у світі. Цей показник є динамічним та швидко збільшується. Лише 2 країни за останні 6 років змінили статус регулятора у зворотному напрямку: з “незалежного” на “залежного”. Зокрема, у 2009 році Бахрейн та Грузія змінили статус “незалежності” у телекомунікаційного регулюючого органу. Причина: слабкий розвиток галузі. Однак, 7.03.2013р. у Грузії знову створена Національна комісія з комунікацій у якості незалежного телекомунікаційного регулятора. Наявність незалежного регулятора є одним із вимог функціонування телекомунікаційних ринків розвинених країн світу, наприклад, країн Євросоюзу. Наявність незалежного регулятора є вимогою Всесвітньоїторгової організації.

Саме формування незалежного регулятора на сьогодні є обов'язковим етапом реформування системи регулювання телекомунікаційної галузі практично у всіх країнах, а наявність такого регулятора — базовою характеристикою розвинутого телекомунікаційного ринку [2].

Як зазначалося раніше, у сфері телекомунікацій останніми десятиріччями відбувалися значні трансформації як в управлінні сферою, так і в її розвитку. Технологічний прорив у телекомунікаційних технологіях, лібералізація ринків призводять не тільки до розширення переліку телекомунікаційних послуг, у тому числі появи нових та перспективних, а й до збільшення попиту населення на такі послуги, при цьому найбільшим попитом користуються послуги безпроводового зв'язку, широкосмугового доступу. Стає зрозумілим, що при достатньо розвинених телекомунікаційних ринках вплив держави на

діяльність суб'єктів ринкових відносин шляхом створення сприятливих умов для провадження ними діяльності у сфері телекомунікацій є необхідним.

- Концепцію розвитку телекомунікацій в Україні визначено, що для прискореного розвитку телекомунікаційних мереж слід створити сприятливі умови для добросовісної конкуренції на ринку телекомунікаційних послуг, підвищити його інвестиційну привабливість, забезпечити прозорість відносин суб'єктів ринку телекомунікаційних послуг, консолідувати їх зусилля на розв'язання проблем розвитку телекомунікацій. Отже, значення телекомунікацій у повсякденному житті кожної людини та їх місце у розвитку суспільства потребують якісного державного регулювання сфери телекомунікацій[1].

Література:

1)Т.О. Корнієнко: Державне регулювання у сфері телекомунікацій : деякі термінологічні аспекти//

file:///C:/Users/User/Downloads/Unzap_2014_1_36.pdf ;

2)Державні регулятори у сфері телекомунікацій: напрямки розвитку та європейський досвід//

https://ukr.lb.ua/blog/roman_semenukha/317281_derzhavni_regulyatori_sferi.html.

Токмина Тетяна Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОСПРОМОЖНОСТІ

Одна зі стратегічних для будь-якої країни галузей – галузь телекомунікацій – відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою як промислової сфери, сфери послуг і споживачів, так і різних географічно розрізнених частин країни та економічних центрів. Стимулюючи людське спілкування за допомогою зв'язку, сучасні засоби телекомунікацій стають необхідною умовою для соціальної згуртованості та культурного розвитку всіх країн.

Загальновідомим є той факт, що телекомунікації України значно відстають від телекомунікацій розвинутих країн як за обсягами, так і за рівнем технологій. Ринок телекомунікацій України – достатньо відкритий та лібералізований за останні 8 років. Наведемо деякі цифри. Телефонна щільність у розвинутих країнах складає біля 60 телефонних номерів на 100 чоловік, тоді як в Україні – 20, а, наприклад, у Польщі, яка так само, як і Україна, вважається країною, що розвивається, – 24,6. Інтернетом у розвинутих країнах користуються 15-20% населення, в Україні – 1%, а у Польщі – близько 5%. Щодо мобільного зв'язку, то у розвинутих країнах – близько 30 телефонів на 100 чоловік, в Україні - 0,3, а у Польщі близько 7. По міжнародних та міжміських розмовах спостерігається відставання України від Польщі десь у 5 разів. Послуги зв'язку в рік на одну

особу у розвинутих країнах складають 254 дол., в Україні – 20,6, а у Польщі – 65,7. Загалом розвинуті країни вкладають у розвиток зв'язку до 20% від її доходу, країни, що розвиваються – близько 31%, слаборозвинені – 68,5%, тоді як в Україні – 18,1%, а у Польщі – 42,2%. Звідси й відповідні результати.

Взагалі, галузь телекомунікацій в Україні поділяється на два крупних сегменти: електрозв'язок та поштовий зв'язок. Одним з найдинамічніших за останні роки сегментів українського телекомунікаційного ринку є мобільний зв'язок. Причому як з точки зору зовнішніх впливів на галузь, так і з точки зору взаємовідношень між суб'єктами ринку. Але довготривала економічна криза та нестабільність вітчизняного законодавства суттєво пригальмувала розвиток українського ринку мобільного зв'язку [1].

Основними проблемами розвитку ринків телекомунікацій є:

- повільне впровадження на мережах рухомого (мобільного) зв'язку радіотехнологій третього та четвертого поколінь (3G, 4G) для забезпечення держави та її громадян усіма перевагами сучасних телекомунікаційних мереж та послуг;
- нерівномірність забезпечення споживачів (особливо у сільській, гірській місцевості і депресивних регіонах) телекомунікаційними послугами;
- затримка із впровадженням на мережах фіксованого та рухомого (мобільного) зв'язку послуги із перенесення абонентських номерів та неможливість забезпечити реалізацію права абонентів на вільний вибір постачальників послуг у повному обсязі;
- втрата значного сегменту ринку телекомунікацій України внаслідок тимчасової окупації Російською Федерацією території Автономної Республіки Крим та м. Севастополь, зменшення доходів українських операторів від надання телекомунікаційних послуг та надходжень до державного бюджету;
- невідповідність існуючих нормативно-правових та нормативно-технічних документів галузі сучасному стану та перспективам розвитку телекомунікаційної мережі загального користування (далі – ТМЗК) інформаційно-телекомунікаційних технологій та потребам ринку телекомунікацій України; [2]

Пропозицій до розв'язання проблеми, взагалі-то, може бути багато, але ми розглянемо саме такі, які є прийнятними для тих умов, що склалися на українському ринку телекомунікацій.

Тому, як вже зазначалося, дійсно необхідно по можливостях живити належних заходів щодо поступового розв'язання цих проблем.

Отже, на основі проведеного дослідження можна зробити висновок, що, незважаючи на динамічність розвитку галузі телекомунікацій, Україна у цій галузі на даний момент не може конкурувати не тільки з економічно розвиненими країнами, а й з країнами, що розвиваються. Звісно, найбільшою мірою це пояснюється станом економіки нашої держави в цілому, бо,

звісно, окрема галузь не може ефективно функціонувати, якщо загальна економічна ситуація в країні характеризується як незадовільна.

Але загалом слід відмітити, що, незважаючи на всі перешкоди та проблеми, Україна, хоч і повільно, але все ж таки просувається на шляху розвитку телекомунікацій, і залишається сподіватися, що ті заходи, які зараз проводять урядові та неурядові організації щодо розвитку галузі, дійсно сприятимуть підвищенню конкурентоспроможності нашої держави у сфері комунікацій.

Література:

- 1) Телекомунікаційна галузь України: проблеми і перспективи конкурентосдатності// <http://ua.textreferat.com/referat-9417-3.html> ;
- 2) Сучасний стан галузі телекомунікацій України// <http://kursak.net/referat-na-temu-suchasnij-stand-galuzi-telekomunikacij-ukra%D1%97ni/> .

Шорон Владислав Петрович

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ

Телекомунікаційна сфера в Україні стрімко розвивається, ринок знаходиться на стадії свого насичення, споживач стає все більш вибагливим, швидкість змін вражаюча.

Функціонуючи в умовах жорсткої конкуренції, що постійно загострюється, оператори телекомунікацій зіштовхуються з проблемою підвищення конкурентоспроможності своїх послуг та компанії в цілому.

Актуальність теми та приділення уваги конкурентоспроможності підприємства телекомунікаційної сфери зумовлені також тим, що цікавою рисою телекомунікаційного ринку є питання поширення нових технологій та сприйняття цих інновацій населенням. Адже сегментування ринку споживачів на різні категорії (новатори, ранні послідовники, рання більшість, пізня більшість та ретрогради) дає можливість сучасному націленому на стратегічний успіх та конкурентоспроможному підприємству побудувати такі тактичні плани та стратегічні розробки, які б враховували більшість можливих ризиків, опір змінам, ринкову кон'юнктуру та, що найважливіше, свої ключові фактори успіху, та дозволили б обійти конкурентів у завоюванні більшої долі ринку.

Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікацій. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

- забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання;

- впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень;

- дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неї вже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче забезпечення діяльності інвесторів та слабка державна підтримка цьому процесу.

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд.

Література:

1. Гранатуров В. М. Конкурентоспроможність телекомунікаційних компаній: проблеми теорії та практики управління: монографія/ В.М. Гранатуров, І.А. Кораблінова/ за наук. ред. проф. В.М. Гранатурова.-К: Кафедра, 2012.-320 с.

2. Латік В. Основні показники рівня життя населення // Праця і зарплата, 2005. - №10. - С.

3. Довгаль О.Г. Соціальні послуги , як елемент ринкової інфраструктури //Формування ринкових відносин в Україні, 2003. - № 7-8.

Мізин О.О.

*Державний університет телекомунікацій,
Навчально-науковий інститут
менеджменту та підприємництва
м. Київ*

СОЦІАЛЬНО-ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ

Докорінні економічні перетворення, що здійснюються в Україні, спрямовані на посилення економічних методів управління та формування умов для повноцінного функціонування ринкових відносин, одне з найактуальніших завдань економічної науки і практики полягає у вивченні суті, структури й методологічних принципів наявного господарського механізму управління, а також у його моделюванні й на цих засадах – подальшому вдосконаленні.

Пріоритетність цих напрямків зумовлюється тим, що на перших етапах соціально – економічних реформ у країні демонтаж попереднього господарського механізму відбувся випереджувальними темпами відносно формування нового; це призвело до відомих кризових явищ в економіці. І саме від успішної побудови механізму господарювання, адекватного сучасному стану продуктивних сил і виробничих відносин, значною мірою залежить перспективи розвитку як української економіки в цілому, так і окремих галузях.

Нині особливого значення набуває галузь зв'язку, справляючи величезний вплив на соціально – економічний розвиток суспільства, що переходить від індустріальної до інформаційної фази свого розвитку. Інформація дедалі більше стає повноправним учасником виробничих процесів і вирішальним чинником науково – технічного й соціального прогресу.

Розвиток соціально – економічних систем привів до того, що людина дістала можливості формування в новому соціумі. Вона стає соціально – активним, суспільним суб'єктом – особою зі своїм психологічним складом, дієздатністю і роллю в суспільстві. В цих умовах важливе місце в житті людини, в її соціальній діяльності займає зв'язок. Він (зв'язок) не лише перестає бути галуззю економіки країни в системі суспільного розподілу праці, організаційних і економічних відносин, але й є безпосередньо включеним в органіку людини. “Людина як особа сама створює і будує свої відносини, бере участь у соціальному спілкуванні, управляє процесами. Зв'язок створює і матеріальні умови цього управління. За допомогою засобів зв'язку людина здійснює комунікацію як у сфері виробництва так і в соціальних відносинах. При цьому природа зв'язку проявляється передусім у характері його послуг, тобто його предмета. Саме через предмет долається простір. Зв'язок поєднує людей для спілкування...”, яке є однією з найбільш важливих потреб людини.

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.

Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування

економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Доходи від надання послуг зв'язку за 2007 – 2009 рр. зросли на 6414,7 млн. грн. або на 16,1 %.

Економічна діяльність сфери телекомунікацій характеризується рівнем доходів. Значне зростання доходів відбулось від надання таких послуг як надання комп'ютерних послуг (на 1730,2 млн. грн. або на 106 %), послуг кабельного телебачення (на 543,3 млн. грн. або на 73,3 %), проводового мовлення (на 83,6 млн. грн. або на 76,3 %). Відбулось зростання доходів від надання послуг мобільного зв'язку на 3419,8 млн. грн. або на 13,6 %

Таким чином, можна визначити, що розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вжити ще більших заходів щодо сприяння розвитку саме цієї галузі. Недостатній розвиток телекомунікацій загрожує конкурентоздатності економіки України та перспективам її розвитку.

Література:

1. Крилюк О.І. Збірник тез IV Наукової конференції телекомунікацій Одеської національної академії зв'язку ім. О.С. Попова (ст. 154-156).
2. Звіт щодо діяльності НІРЗ та стану телекомунікацій в Україні.

Мізін О.О.

*Державний університет телекомунікацій,
Навчально-науковий інститут
менеджменту та підприємництва
м. Київ*

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ, ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ 5G

Розвиток інформаційних засобів і систем є в наш час одним із найважливіших факторів, що визначають темпи й досягнення науково-технічного прогресу. Жодна сфера людської діяльності вже не може розглядатися поза залежністю від засобів інформаційного обміну, значення яких неухильно зростає.

Цьому сприяє перехід до цифрових методів передачі повідомлень і цифрової обробки сигналів, застосування сигналів складної структури, а також різноманітних способів адаптації під час широкого використання мікропроцесорної техніки, що забезпечує інтеграцію засобів зв'язку і засобів обчислювальної техніки.

На цій основі створюються інтегральні цифрові мережі, в яких досягається не тільки повна інтеграція за видами зв'язку, але й інтеграція засобів передачі, обробки, комутації, керування і контролю. Кінцевою метою цього грандіозного процесу є створення єдиного інформаційного середовища, в основі якого лежить принцип мобільного доступу до всіх інформаційних ресурсів.

Прогнози провідних фахівців, працюючих в міжнародних проектах 5G [3, 4], показують, що домінуюче становище серед послуг, що надаються в

мережах 5G, будуть займати послуги передачі відео з високою якістю – HD-відео, а також 3D-відео. Звіти провідних операторів зв'язку, що використовують мережі 4G, показують, що в споживаному абонентами трафіку відеопослуги переважають і залишаться домінуючими в контенті мереж 5G. Так, зараз обсяг трафіку відеопослуг становить, за оцінками операторів [3], від 66 до 75% загального обсягу трафіку в мережах 4G, включаючи 34% – лише відео, а також 18% відеоспостереження (Video Surveillance).

Розвиток мереж 5G необхідно направити на створення ультращільних мереж (UDN) бездротового доступу з гетерогенною структурою сот радіусом не більше 50 метрів на основі нових видів сигнально-кодових конструкцій радіосигналів, які підвищують спектральну ефективність у порівнянні з мережами 4G і забезпечують передачу даних зі швидкостями більше 10 Гбіт/с. Для забезпечення таких швидкостей передачі даних в мережах 5G потрібно використовувати широкі смуги каналів як в лінії вниз (DL), так і в лінії вгору (UL) з безперервним спектром, шириною від 500 до 1000 МГц, що в 25-50 разів перевищує ширину каналів реалізованих в 4G. Виділення таких смуг для каналів 5G можливо тільки на верхній межі сантиметрового та в міліметровому діапазонах частот, що істотно скоротить зони покриття базових станцій 5G через зменшення радіуса сот до 50-100 м [1].

Складність швидкого переходу до 5G пов'язана з тим, що різні мережі будуються з використанням різних інформаційних технологій і відповідно різного програмного забезпечення, яке не сумісне поміж собою. Прискорити процес переходу можливо шляхом відокремлення функцій надання послуг від транспортних функцій та впровадження технологій, що забезпечать взаємодію різних мереж. Це дозволить створювати нові послуги та забезпечить високий рівень їх якості, а також дозволить вільно підключити нові служби.

Для прискорення переходу телекомунікаційних мереж до технології 5G, необхідно збільшувати пропускну здатність і гнучкість транспортних мереж і мереж доступу. При цьому головне значення тут відіграє середовище передачі та обрана технологія побудови фізичного рівня мережі. Для передачі інформації на фізичному рівні використовуються проводові та безпроводові середовища.

Впровадження концепції мобільних систем зв'язку четвертого покоління остаточно поставило крапку у визначенні напрямків подальшого розвитку мереж доступу.

Системи мобільного зв'язку четвертого покоління застосовують на фізичному рівні складні багаточастотні сигнали, основані на OFDM (OFDMA). При цьому ці системи вже поєднують у собі функції й переваги систем безпроводового доступу та стільникових систем зв'язку. Незважаючи на значні переваги та перспективи розвитку систем мобільного зв'язку четвертого покоління, вони не здатні повністю задовольнити всі вимоги мереж доступу 5G. Тому на сьогодні залишається актуальним питання проведення їх вдосконалення. Значне місце тут відводиться розробці нових підходів до побудови фізичного рівня, що, насамперед, визначається ефективністю обраних сигнально-кодових конструкцій.

Це можливо зробити під час використання перспективних сигнально-кодових конструкцій, побудованих на базі оптимальних багатопозиційних багаточастотних сигналів [2]. Використання цих конструкцій з ефективними методами завадостійкого кодування забезпечить високу достовірність передачі даних і дозволить підвищити частотну ефективність, збільшить гнучкість систем до потреб користувачів, а також посприє у вирішенні ряду завдань, що стоять перед мережами 5G. Для цього спочатку необхідно провести детальний аналіз технологій побудови фізичного рівня перспективних телекомунікаційних радіосистем, який і дозволить визначити напрямки подальших досліджень.

Література:

1. Ільченко М.Ю. Сучасні телекомунікаційні системи / М.Ю. Ільченко, С.О. Кравчук. – К.: Наук. думка, 2008. – 328 с.
2. . Ким А.В., Тихвинский В.О. Новый мобильный горизонт: итоги MWC-13 // Электросвязь, 2013. – №3.
3. Mobile and wireless communications Enablers for the 2020 Information Society. EU FP7 ICT-317669-METIS // www.metis2020.com/
4. Niri S.G. Towards 5G // LTE World Summit-2013.

Мізін О.О.

*Державний університет телекомунікацій,
Навчально-науковий інститут
менеджменту та підприємництва
м. Київ*

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

У сучасних умовах глобалізації інвестиційний розвиток держави є важливим чинником її загального розвитку. В умовах, коли економіка України відчуває значну нестачу інвестиційних ресурсів, питання розробки ефективної інвестиційної політики набуває особливої актуальності. При цьому значну увагу потрібно приділяти іноземним інвестиціям. Іноземний капітал (інвестиції) ефективно впливає на економічний розвиток господарства країн, які імпортують його. Перевагами таких грошових надходжень є те, що, по-перше, іноземні інвестиції – це додатковий капітал, залучений у країну для виробництва товарів і послуг, реалізації певних програм, а по-друге – це надходження в державу нових технологій та застосування нових методів управління. Крім того, іноземні інвестиції сприяють створенню в країні нових робочих місць, вирішенню нагальних соціальних проблем.

На даний час сфера телекомунікацій є однією з найважливіших складових інфраструктури в Україні. Відповідно інвестиційне забезпечення розвитку даної сфери є передумовою підвищення конкурентоспроможної 62 національної

економіки, що, у свою чергу, сприятиме входженню нашої країни у глобальний економічний простір.

На сучасному етапі широкосмугові технології стали не просто засобом передачі даних, а істотним чинником забезпечення сприятливих умов для розвитку системи державного управління, економіки, науки, освіти та культури, у тому числі надання адміністративних послуг.

Інвестиції в галузь зв'язку України дозволять вирішити такі існуючі проблеми, як: забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання; впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень; дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Інвестиції, у тому числі іноземні, є не лише механізмом розвитку, але й способом регулювання економіки шляхом переливання капіталу. На сучасному етапі розвитку ринку іноземні інвестиції виступають основним джерелом отримання новітніх конкурентоспроможних технологій. Залучення інвестицій – це необхідна умова розвитку всіх галузей економіки, особливо сфери телекомунікацій, що є інноваційною за своєю суттю. Інвестиційна діяльність операторів телекомунікацій сприятиме збільшенню обсягів послуг сфери телекомунікацій в Україні і підвищенню їх якості, а також розвитку та модернізації телекомунікаційної мережі. Разом з удосконаленням законодавства щодо іноземних інвестицій повинні розвиватися й інші чинники механізму залучення іноземних інвестицій. Необхідно забезпечити стабільність політичного середовища, вдосконалити та забезпечити стабільності: податкової, грошово-кредитної та митної політики; максимально спростити процедури, які регламентують взаємовідносини між державою і підприємцями в галузі залучення іноземних інвестицій; створити гарантії стабільності умов щодо довгострокового фінансування інвестиційних проєктів, здійснити вдосконалення системи захисту прав інвесторів; удосконалити роботу інститутів спільного інвестування; запровадити дієвість страхування інвестиційних ризиків.

Отже, створення сприятливих умов для залучення іноземного інвестування є найважливішою складовою серед тих економічних вимог, які покликані забезпечити реальні зміни в економічній структурі суспільства, надати поштовх усьому ланцюгу господарських взаємозв'язків цілісного процесу суспільного відтворення, спрямованого на розвиток економіки України.

Література:

1. Гилка У.Л. Особливості конкуренції на ринку послуг телекомунікацій: [Текст] / Гилка У.Л. // Наукові записки УНДІЗ. – 2009. – №3(11). – С. 95-103

2. Діденко Я.О. Удосконалення прямого іноземного інвестування: [Текст] / Діденко Я.О // Фінанси України. – 2004. – №12. – С. 96-105.
3. Підсумки роботи галузі: [Електронний ресурс]. – Режим доступу: <http://www.stc.gov.ua/uk/publish/article/63905>.

Трубій Іван Павлович

*Державний університет телекомунікацій
Навчально - науковий інститут менеджменту та підприємництва
м. Київ*

РОЛЬ І ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Телекомунікаційні послуги за останні роки зазнали значних змін, пов'язаних з активізацією розвитку інфокомунікаційних технологій, тим самим створюючи ситуацію, яка характеризується присутністю на ринку послуг зв'язку традиційних загальнодоступних послуг (фіксована міська та сільська телефонія) і нових послуг (мобільний зв'язок, Інтернет тощо).

Проте впровадження нових телекомунікаційних послуг та розвиток існуючих стикаються з низкою проблем. Це пов'язано з тим, що багато країн вступають в нову еру соціально-економічних відносин. Завдяки загальному руху соціально-економічних систем до інформаційного суспільства відбувається набуття та розвиток нових форм відносин в економічній, соціальній та політичній сферах. Суспільство неухильно рухається до такої інформаційної епохи, якій більша частина бізнесу та економіки постають в електронному вигляді та здійснюються у глобальній мережі Інтернет.

Також телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

У сфері телекомунікацій існують такі проблеми:

-низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;

-нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);

-використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;

-наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;

-неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;

-недостатній регуляторний вплив держави на ринок телекомунікацій;

-недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Література:

1. Орлов В.М. Проблеми та суперечності розвитку малого підприємства в телекомунікаційній сфері / В.М. Орлов, І.В. Яцкевич // Загальногалузовий науково-виробничий журнал Державної Адміністрації зв'язку та інформатизації України «Зв'язок». – 2007. – № 3(71). – С. 17-20.

2. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів] ; за заг. ред. В.М. Орлова. – О. : ОНАЗ ім. О.С. Попова, 2014. – 512 с.

3. Орлов В.Н. Экономические аспекты развития телекоммуникационных сетей сельских районов Украины / В.Н. Орлов, С.В. Зяблов, Г.А. Отливанская, И.В. Яцкевич // Загальногалузовий науково-виробничий журнал Державної Адміністрації зв'язку та інф.

Трубій Іван Павлович

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

СТРАТЕГІЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Стратегія розвитку телекомунікацій спрямована насамперед на розв'язання зазначених проблем, крім того, передбачає здійснення заходів для подальшого забезпечення розвитку телекомунікацій в Україні на базі телекомунікаційних мереж наступного покоління.

Розвиток телекомунікацій повинен здійснюватися за такими основними напрямками:

-прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень (радіотехнологій, волоконно-оптичних, пакетних технологій тощо);

-сприяння реалізації регуляторної політики у сфері телекомунікацій, спрямованої на об'єднання (консолідацію) можливостей суб'єктів ринку телекомунікацій з метою розв'язання основних проблем сфери, підвищення ефективності їх діяльності.

-удосконалення нормативно-правової бази у сфері телекомунікацій.

З урахуванням технологічних потреб в одночасному і гармонійному розвитку телекомунікаційних мереж, а також можливості випереджувального

використання в Україні сучасних і перспективних засобів телекомунікацій, основними напрямками розвитку телекомунікаційних мереж слід вважати:

- забезпечення розвитку випереджувальними темпами мультисервісних телекомунікаційних транспортних мереж для задоволення потреб споживачів телекомунікаційних послуг;

- збільшення ємності і пропускнуєї спроможності мереж доступу до транспортних телекомунікаційних мереж з використанням перспективних технологічних рішень, у тому числі радіотехнологій;

- прискорення розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах з використанням найбільш ефективних технологій;

- приведення системи нумерації телекомунікаційних мереж у відповідність з європейськими стандартами;

- розвиток та оптимізація всіх елементів телекомунікаційної інфраструктури українського сегмента Інтернет (у тому числі із системою транзиту Інтернет-трафіку) з метою забезпечення розвитку Інтернет в Україні;

- створення технічної можливості вибору постачальників телекомунікаційних та інформаційних послуг в телекомунікаційних мережах;

- створення технічних можливостей для розвитку розподілених інформаційно-довідкових служб та служб екстреного виклику, в тому числі служби допомоги (112) із забезпеченням доступу до цих служб абонентів мобільного зв'язку;

- створення науково-технічної та нормативно-правової бази для розширення національної багатооператорської мережі на основі мультисервісних телекомунікаційних транспортних мереж;

- прискорене запровадження радіотехнологій рухомого (мобільного) зв'язку та використання систем абонентського радіодоступу;

- створення національної системи супутникового зв'язку;

- модернізація та розвиток спеціальних телекомунікаційних мереж для задоволення потреб національної безпеки та оборони держави – мереж Державної системи урядового зв'язку, національної системи конфіденційного зв'язку, спеціальної позаміської мережі зв'язку, мереж Воєнної організації держави;

- створення рівних умов для доступу споживачів до національної мережі обміну Інтернет-трафіком.

Література:

1. Закон України «Про Телекомунікації». – К. : Державне видав-ничо-інформаційне агентство «Зв'язок», 2003. – 58 с

2. Орлов В.Н. Реализация общедоступных телекоммуникационных услуг в сельских районах Украины: выбор вариантов / В.Н. Орлов, С.В. Зяблов, Ю.І Зяблова, Г.А. Отливанская // Загальногалузевий науково-виробничий журнал Державної Адміністрації зв'язку та інформатизації України «Зв'язок». – 2006. – № 3(63). – С. 27-30.

3. Кузьминов А.В. Проблемы и противоречия в управлении электросвязью региона и пути их разрешения / А.В. Кузьминов // Спеціалізований випуск матеріалів конференції

Трубій Іван Павлович

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОЗДАТНОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ ГАЛУЗІ В УКРАЇНІ

Одним з найдинамічніших за останні роки сегментів українського телекомунікаційного ринку є мобільний зв'язок. Причому як з точки зору зовнішніх впливів на галузь, так і з точки зору взаємовідношень між суб'єктами ринку. Але довготривала економічна криза та нестабільність вітчизняного законодавства суттєво пригальмувала розвиток українського ринку мобільного зв'язку. Однак, як і інших галузей економіки. Більш того, мобільний зв'язок, як один з найприбутковіших напрямів діяльності, потрапив під пильну увагу контролюючих, інспектуючих та інших подібних “експроприуючих” органів. За останні роки спостерігалися спроби накласти як на суб'єктів ринку, так і на його споживачів різного роду додаткові збори, податки, акцизи і т.д. Це аж ніяк не сприяє розвитку галузі. Але все ж таки на сьогоднішній день можна сказати, що український ринок мобільного зв'язку поступово набуває цивілізованих рис, незважаючи на активну боротьбу (а, можливо, і завдяки їй) п'яти мобільних операторів зв'язку (UMC, KyivStar GSM, DCC, Wellcom, Golden Telecom GSM) за невелику частину платоспроможної клієнтури.

Також порівняно динамічною сферою українських телекомунікацій можна назвати Інтернет. Загальна кількість користувачів Інтернетом в Україні на початок 1999 року становила приблизно 100-120 тис. У відношенні до загальної кількості користувачів у світі вона складає менше 0,1% або, точніше, 0,065%. Але в середньому за кожні шість місяців кількість користувачів збільшується в 1,67 рази, що вище середніх темпів зростання у світі в цілому. Зараз мають місце такі прогностичні коефіцієнти росту кількості українських користувачів Інтернетом: 2002 р. – 1,5; 2003 р. – 1,5; 2004 р. – 1,4; 2005 р. – 1,4. Необхідно зазначити, що скільки існує та розвивається вітчизняний сегмент Інтернету, впадає в око один не дуже приємний факт – складається враження, що “існує та розвивається” він тільки у Києві. В інші регіони протягнуто лише невеличкі джерела виділених каналів від крупних київських провайдерів. Але не слід забувати, що перші виділені канали, наприклад, з'явилися не в Києві, а в Харкові, що помітна частина найкращих інформаційних ресурсів України знаходиться не тільки у Києві, але й в Одесі, Донецьку, Дніпропетровську.

Щодо сегмента електров'язку, то рівень телефонізації в Україні на сьогодні у два рази нижчий, ніж у країнах Центральної та Західної Європи. Із загальної кількості діючих у телефонній мережі АТС 21,1% належать

електронним та квазіелектронним, решта – морально застарілим аналоговим. Щільність телефонного зв'язку, як вже зазначалося, становить близько 20,1 телефонів на 100 осіб. Кількість основних телефонних номерів складає в Україні близько 9 млн., з яких 86,6% встановлено у міських телефонних мережах, 13,4% – у сільських. Подальша телефонізація населених пунктів з низьким показником кількості телефонних номерів через низьку платоспроможність у таких регіонах триває повільно – в цілому по країні показники телефонізації зростають за рахунок, знову ж таки, Києва та інших великих міст.

Взагалі, характерною особливістю української телекомунікаційної галузі є значне відставання за часом по застосуванню нових технологій між Києвом та іншими регіонами країни. Наприклад, мобільний зв'язок у Харкові з'явився через 2-3 роки після його появи у Києві, а в деяких великих містах з населенням в 25 і більше тис. людей він відсутній і досі. Мобільним зв'язком покрито усього біля 25% території України.

Слід зазначити також, що ринок телекомунікацій в Україні характеризується високим рівнем монополізму. “Укртелеком”, “Утел”, УМС, “Укрпошта” – їх сумарна частка у структурі даних послуг становить 90 %. Як вважає Інтернет Асоціація України, зараз практично всі недержавні учасники телекомунікаційного ринку у тій чи іншій мірі потерпають від монопольного становища ВАТ “Укртелком”.

Для світового телекомунікаційного ринку характерні процеси інтеграції та глобалізації, тому що в цілому світовий ринок стає все більш інтегрованим. А Україна, нажаль, часто не може налагодити роумінг у масштабах країни. Україна повинна мати стратегічних партнерів. Ці партнери повинні бути у Європі, Америці, Азії. Бажаним для України є входження до одного з глобальних об'єднань.

Проблемою розвитку телекомунікацій в Україні також є наявність близько 70% аналогових АТС від їхньої загальної кількості. На модернізацію вітчизняних комунікацій потрібно близько 19 млрд. дол. В Україні капітальні інвестиції в розвиток телекомунікацій складають лише 0,3% ВВП. Для порівняння, у Німеччині – 4,8%, у Франції – 3,1%.

Отже, як бачимо, стан галузі телекомунікацій України особливо не вражає, але оскільки, як було зазначено раніше, розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вживати усіх можливих заходів щодо сприяння такому розвитку, зокрема, аби підвищити конкурентоспроможність України в цій галузі.

Література:

1. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – М. : Инфра-М, 1996. – 493 с.
2. Гранатуров В.М. Управление услугами зв'язку [Текст] : навч. посіб / В.М. Гранатуров, І.В. Литовченко. – К. : Освіта України, 2010. – 254 с.
3. Орлов В.М. Стратегічне управління розвитком телекомунікаційної сфери регіону // В.М. Орлов, С.В. Зяблов, О.В. Орлова // Економічні науки. Серія «Регіональна економіка» : збірник наукових праць. – Вип. 3(9), ч. 2. – Луцьк. – 2006. – С. 108-115.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційного обслуговування, переробки величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, який грає роль підсилювача інтелектуальних можливостей людини і суспільства в цілому, а комунікаційні засоби, які використовують комп'ютери, служать для зв'язку і передачі інформації.

Поява і розвиток комп'ютерів - це необхідна складова процесу інформатизації суспільства.

Сучасні інформаційні технології увібрали в себе лавиноподібні досягнення електроніки, а також математики, філософії, психології та економіки. Утворений в результаті життєздатний гібрид ознаменував революційний стрибок в історії інформаційних технологій, яка налічує сотні тисяч років.

Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки. Тому без інформаційних технологій, так само як без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати не може.

Застосування відкритих інформаційних систем, розрахованих на використання всього масиву інформації, доступною в момент суспільству у певному його сфері, дозволяє вдосконалити механізми управління громадською пристроєм, сприяє гуманізації та демократизації суспільства, підвищує добробут його членів. Процеси, які у через відкриття інформаційною суспільства, сприяють як прискоренню науково-технічного прогресу, інтелектуалізації всіх видів людської діяльності, а й створенню якісно нової інформаційного середовища соціуму, які забезпечують розвиток творчий потенціал індивіда.

За аналогією і для інформаційної технології повинно бути щось подібне. Такими технічними засобами виробництва інформації будуть апаратне, програмне і математичне забезпечення цього процесу. З їхньою допомогою відбувається переробка первинної інформації в інформацію нової якості. Виділимо окремо з цих засобів програмні продукти і назовемо їх інструментарієм, а для більшої чіткості можна його конкретизувати, назвавши програмним інструментарієм інформаційної технології.

Необхідно розуміти, що освоєння інформаційної технології і подальше її використання повинні бути зведені до того, щоб було потрібно спочатку добре оволодіти набором елементарних операцій, кількість яких обмежена. З цієї обмеженої кількості елементарних операцій у різних комбінаціях складається дія, а з дій, також у різних комбінаціях, складаються операції, що визначають той або інший технологічний етап. Сукупність технологічних етапів утворює технологічний процес (технологію). Він може починатися з будь-якого рівня і не включати, наприклад, етапи або операції, а складатися тільки з дій. Для реалізації

етапів технологічного процесу можуть використовуватися різні програмні середовища.

У наш час людство переживає науково-технічну революцію, в якості матеріальної основи якої служить електронно-обчислювальна техніка. На базі цієї техніки з'являється новий вид технологій - інформаційні.

Під інформаційними технологіями розуміється переробка інформації на базі комп'ютерних обчислювальних систем.

Таким чином, інформаційні технології міцно увійшли в наше життя. Вони відкрили нові можливості для роботи і відпочинку, дозволили багато в чому полегшити працю людини.

До них відносяться процеси, де «вихідним матеріалом» і «продукцією» (виходом) є інформація. Зрозуміло, що перероблялася інформація пов'язана з певними матеріальними носіями і, отже, ці процеси включають також переробку речовини і переробку енергії. Але останнє не має істотного значення для інформаційних технологій. Головну роль тут відіграє інформація, а не її носій.

В якості основного засобу автоматизації інформаційно-управлінської діяльності сьогодні виступають персональні ЕОМ. Застосування ЕОМ стало буденною справою, хоча ще зовсім недавно робоче місце, обладнане комп'ютером, було великою рідкістю. Свою роботу в конторі службовець здійснює через реалізацію різних інформаційних процесів, тобто процесів отримання, реєстрації, накопичення, перетворення, генерації, відображення і передачі інформації.

Найбільш ефективно ПЕОМ використовуються в поєднанні з різноманітними засобами зв'язку (комунікації). Сучасні засоби комунікації, розроблені для персональних комп'ютерів, надають у розпорядження користувачів на додаток до широких можливостей ПЕОМ як таких можливості доступу в ЕОМ вищого класу, підключення їх в локальні обчислювальні мережі. Останнє особливо важливо для контор, тому що забезпечує перехід від автоматизації індивідуальної роботи службовців до розподіленої обробки даних в умовах взаємопов'язаних АРМ (автоматизованих робочих місць).

Щоб сукупність АРМ могла функціонувати як єдина система, необхідно забезпечити автоматичний обмін даними між ними (використання відеотермінала).

ПЕОМ шляхом кабельного з'єднання утворюють мережу (глобальна, локальна) - групу комп'ютерів, з'єднаних між собою засобами зв'язку для спільного використання ресурсів та надання користувачам додаткових послуг.

Найпоширенішою глобальною мережею є мережа Інтернет. Численні прогнози говорять про те, що вже до початку наступного століття Інтернет не тільки перетворить стали вже звичними персональні комп'ютери в щось принципово інше, але і змінить тим самим образ життя більшості населення Землі.

Сучасне суспільство навряд чи можна уявити без інформаційних технологій. Перспективи розвитку обчислювальної техніки сьогодні складно уявити навіть фахівцям. Проте, ясно, що в майбутньому нас чекає щось

грандіозне. І якщо темпи розвитку інформаційних технологій не скоротяться, (а в цьому немає ніяких сумнівів), то це відбудеться дуже скоро, головне, направити розвиток цього потужного знаряддя в потрібне русло.

Література:

1. <http://it-tehnolog.com/statti/suchasni-informatsiyni-tehnologiyi>
2. http://bukvar.su/informatika_programmirovanie/169612-Sovremennye-informacionnye-tehnologii.html
3. <http://referatbank.com.ua/referat2.php?id=4491>

Сафін Катерина Олексіївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ

Інтернет (від англ. Internet), міжмережся — всесвітня система взаємополучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів. Інтернет також називають мережею мереж. Інтернет складається з мільйонів локальних і глобальних приватних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою з використанням різноманітних дротових, оптичних і бездротових технологій.

Інтернет становить фізичну основу для розміщення величезної кількості інформаційних ресурсів і послуг, таких як взаємопов'язані гіпертекстові документи Всесвітньої павутини (World Wide Web — WWW) та електронна пошта. Мережа побудована на використанні протоколу IP і маршрутизації пакетів даних. В наш час Інтернет відіграє важливе значення у створенні інформаційного простору глобального суспільства, слугує фізичною основою доступу до веб-сайтів і багатьох систем (протоколів) передачі даних.

У 1990-ті роки мережа, відома вже як Internet, зазнала найбільших змін і почала охоплювати справді глобальні простори, розповсюджуючись по всьому світу і надаючи користувачам все нові види інформаційних джерел і послуг. Відпала необхідність нагляду за розвитком і використанням мережі з боку Агентства перспективних наукових проєктів США. За перспективний розвиток і підтримку Internet взялася група організацій, таких, як US National Science Foundation - Національне наукове товариство США. Але навіть після цих, здавалося б, принципових перетворень, здатних докорінно змінити саму суть мережі, основні, базові елементи, закладені як технічні та організаційні основи при створенні мережі ARPAnet, залишилися без змін.

INTERNET надає такі основні види послуг:

1. e-mail — електронна пошта;
2. групи новин;
3. списки поштової розсилки;
4. доступ до файлів віддалених комп'ютерів;
5. сеанси зв'язку з іншими комп'ютерами, під'єднаними до INTERNET;

6. пошук інформації в базі даних в оперативному режимі;
7. спілкування з іншими користувачами шляхом використання сервісу Internet Relay Chart;
8. доступ до інформаційної системи World Wide Web (WWW).

З додаткових послуг можна виділити наступні:

- ⑩ широка передача MultiMedia;
- ⑩ RadioInternet;
- ⑩ розмовний конференційний зв'язок;
- ⑩ безпечні угоди;
- ⑩ відеоконференційний зв'язок;
- ⑩ безпроводне з'єднання.

Сучасний Інтернет має також дуже багато соціальних та культурних граней. Він є універсальним середовищем для спілкування, розваг та навчання. Так, за результатами дослідження Оксфордського університету підлітки, які мали доступ до Інтернету, отримували вищі оцінки за тих, хто не мав доступу до інтернету.

За допомогою Інтернету стало можливо робити покупки та оплачувати послуги. Для багатьох людей Інтернет — це спосіб заробітку. А в цілому Інтернет — це віддзеркалення сучасного суспільства та світосприйняття.

Одним з проявів субкультури Інтернету є День безпечного інтернету, що відзначається щорічно з 2004 року другого вівторка лютого.

Із зростанням популярності Інтернету стали проявлятися і негативні сторони його застосування. Зокрема, дехто настільки захоплюється віртуальним простором, що проводить за комп'ютером до 18 годин на добу. Таку залежність багато хто порівнює з тютюнопалінням чи наркоманією. Визначення інтернет-залежності звучить так: «Це наполегливе бажання вийти в Інтернет, перебуваючи off-line, і нездатність вийти з Інтернету, знаходячись on-line». Згідно з даними різноманітних досліджень, сьогодні інтернет-залежними є близько 10 % користувачів у всьому світі. Фахівці вже розробили методики позбавлення від цієї залежності.

За останніми даними український ринок Інтернету щороку зростає на 37-43%, а європейський - на 29-33%, але бум у Європі вже частково пройшов, а у нас він лише ще наближається, тому за цим показником наша держава займає одне з перших місць у світі і це подає надію на те, що Інтернет буде досить активно розвиватися в Україні.

Чинниками, які на сьогодні стримують розвиток українського сегмента мережі Internet, є відносно висока вартість оренди каналів зв'язку і незначні фінансові можливості більшості провайдерів послуг. Не останню негативну роль у цьому відіграє також низька платоспроможність більшості як наявних, так і потенційних користувачів. Аналіз інтенсивності графіка через зовнішні канали доступу до міжнародних ресурсів Internet свідчить, що вхідний трафік у 3-4 рази інтенсивніший за вихідний. Це означає, що внутрішні користувачі з зарубіжних

інформаційних ресурсів отримують набагато більше інформації, ніж зарубіжні користувачі намагаються знайти у нас. Інформатизація фінансової та грошової системи, державного фінансово-економічного контролю є одним з пріоритетних напрямів державної політики. У структурі Міністерства фінансів України діє автоматизована багаторівнева система фінансових розрахунків, де впроваджено автоматизовані робочі місця на рівні центрального апарату, в Автономній Республіці Крим та на обласному рівні. Для інформаційного забезпечення ефективності роботи податкової системи у Державній податковій адміністрації використовується ряд централізованих інформаційних систем, зокрема, для належного забезпечення обліку платників податків - як юридичних, так і фізичних осіб, урахування пільг певних категорій населення та інше. Для забезпечення обміну інформацією між базами даних Державної податкової адміністрації та Держмитслужби діє автоматизована міжвідомча інформаційна система. Державні органи вважають, що насамперед потрібно вкладати кошти в модернізацію вже існуючої інфраструктури, в забезпечення доступу до мережі всім бажаючим, а потім уже в підтримку робіт над новим поколінням технологій і служб. Однак, ураховуючи зарубіжний досвід розвитку Internet, необхідно діяти навпаки.

Якісний і прийнятний за ціною доступ до Internet - зараз одна з насущних вимог українського користувача. Із збільшенням кількості споживачів послуг Internet в Україні дуже гостро встало питання про розвиток високошвидкісних мереж доступу, що відповідають потребам і можливостям українців. Але крім рівня життя потенційних споживачів мережевих сервісів, на розвиток Internet в країні впливає телефонна щільність, якість ліній зв'язку, почасова оплата за користування ними, взаємини між провайдерами і телекомунікаційними операторами і т.д.

Український ринок Internet, реагуючи на швидке зростання користувачів, повторює світові тенденції розвитку глобальної мережі і просувається по шляху збільшення, інтеграції і здешевлення сервісів. Розвивається інфраструктура мережі, ростуть модемні пули провайдерів (їх сьогодні налічується приблизно більше 20 тис. ліній), розширюються їх канали, а також збільшується кількість контент-проектів. Розробляється спеціалізована нормативна база, без якої в Україні неможливий розвиток електронної комерції, а також реалізація ідеї електронного державного самоврядування.

Література:

1. Вікіпедія - "Інтернет" - [Електронний ресурс] - <https://uk.wikipedia.org/wiki/Інтернет>
2. "Проблеми та перспективи розвитку мережі Інтернет в Україні" - [Електронний ресурс] - <https://bibliofond.ru/view.aspx?id=588135>
3. Вікіпедія - "Інтернет в Україні" - [Електронний ресурс] - http://www.gpedia.com/uk/gpedia/Інтернет_в_Україні
4. "Історія розвитку мережі Internet" - [Електронний ресурс] - http://pidruchniki.com/13560615/ekonomika/istoriya_rozvitku_merezhi_internet

СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ ПРОБЛЕМЫ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИЙ

Сейчас ситуация в отрасли телекоммуникаций в мире определяется несколькими ключевыми факторами: быстрым ростом сегмента мобильных телекоммуникаций, взрывным развитием Интернета, практически остановившимся ростом доходов операторов традиционных услуг связи, снижением цен и усилением конкуренции, а также активным развитием процессов либерализации и приватизации.

Сохраняются и значительные региональные различия, почти полностью объясняющиеся различием экономического положения регионов, а также в некоторых случаях сопротивлением реформам, направленным на повышение уровня конкуренции. В Африке, большей части Азии и некоторых частях Латинской Америки на душу населения приходится менее 10 телефонов. В беднейших странах к Интернету подключено <менее одного человека> на 10 тыс. населения, в то время как в наиболее развитых странах Интернетом охвачено уже более 20% населения.

Однако Китай, Индия, страны Восточной Европы и большинство латиноамериканских стран сейчас демонстрируют впечатляющие темпы роста. В результате принятия Соглашения Всемирной торговой организации (ВТО) об основных телекоммуникационных услугах (1997 г.) 69 стран, на которые приходится более 90% мирового рынка телекоммуникационных услуг, согласились уйти от жестких двусторонних соглашений и либерализовать свои рынки, что резко повысило уровень конкуренции между операторами, способствует улучшению качества услуг, снижению цен и росту масштабов рынков.

Существенное влияние на развитие мирового телекоммуникационного рынка оказало и открытие национальных рынков странами ЕС с 1 января 1998 г., а также либерализация крупнейшего в Азиатско-Тихоокеанском регионе рынка Японии.

Либерализация телекоммуникационных рынков крупнейших стран ожидалась уже давно. Усиление конкуренции приводит к падению цен на телекоммуникационные услуги, позволяя бизнесу все активнее использовать их в своей деятельности. В будущем эта тенденция еще более усилится.

Однако не следует считать, что операторы страдают от вынужденного снижения цен. Наоборот, в отрасли телекоммуникаций наблюдается настоящий бум. Несмотря на падение цен, общий рост прибыли поставщиков телекоммуникационных услуг в последние годы примерно в два раза превышает рост мировой экономики

Стоит выделить основные три проблемы которые на данный момент влияют на развитие телекоммуникаций. Первая проблема – операторы не всегда способны оперативно и эффективно создать бизнес-модель, адаптированную к новому формату услуги или сервиса.

Вторая проблема – неспособность оператора, действующего в условиях постоянной ценовой войны с конкурентами, достаточно быстро переориентироваться с голоса на трафик данных. Создать нового рода услуги по передаче данных, адаптировать имеющиеся услуги и извлечь дополнительную прибыль.

Следующая проблема, о которой хочется упомянуть, присуща всей российской экономике, независимо от отрасли. Это жёсткая организационная структура операторов и неспособность к гибкости и ускорению принятий решений и реализации. Низкая эффективность на всех уровнях. Низкий уровень компетенции производственного персонала.

Отсутствие наработанных аналитических программ, способных монетизировать неструктурированные огромные массивы информации, полученной в результате изучения клиентуры. В локальном масштабе программы, позволяющие анализировать данные, есть у каждого оператора, но о результатах мы почти ничего не знаем.

Неуверенность в готовности инвестировать в новые технологии, которые меняются достаточно часто. На смену 3G пришёл стандарт 4G. К 2020 году появится технология 5G со скоростью около 10 000 Мбит/с. И насколько быстро можно будет возратить инвестиции в строительство новой инфраструктуры и при этом получить прибыль, сказать сложно. Во многом неуверенность основывается на следующем риске – в отрасли имеет место быть большое регулирующее государственное влияние. На уровне госрегулирования риски становятся глобальными для бизнеса.

Література:

1. «Телекоммуникации и связь: проблемы и решения» - [Электронный ресурс]: <https://www.to-inform.ru/index.php/arkhiv/item/перспективы-и-проблемы-развития-телекоммуникационной-отрасли>
2. «Рынок телекоммуникаций – глобальные тенденции» - [Электронный ресурс]: <http://old.rcb.ru/archive/articles.asp?id=1325>

*Пилипей Анастасія Святославівна
Державний університет телекомунікацій
Навчально – науковий інститут менеджменту та підприємництва
м. Київ*

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове)

передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

У сфері телекомунікацій існують такі проблеми:

- низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);
- використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;
- наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Стратегія розвитку телекомунікацій спрямована насамперед на розв'язання зазначених проблем, крім того, передбачає здійснення заходів для подальшого забезпечення розвитку телекомунікацій в Україні на базі телекомунікаційних мереж наступного покоління

Розвиток телекомунікацій повинен здійснюватися за такими основними напрямками:

- *прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень (радіотехнологій, волоконно-оптичних, пакетних технологій тощо);*
- *сприяння реалізації регуляторної політики у сфері телекомунікацій, спрямованої на об'єднання (консолідацію) можливостей суб'єктів ринку телекомунікацій з метою розв'язання основних проблем сфери, підвищення ефективності їх діяльності.*
- *удосконалення нормативно-правової бази у сфері телекомунікацій.*

Прискорений розвиток телекомунікацій є одним із основних чинників, що впливатиме на розбудову національної економіки та масове впровадження інформаційних технологій, побудову в Україні інформаційного суспільства, на процес інтеграції України в ЄС та у світову економіку, а також збільшення надходжень до державного бюджету.

Для реалізації завдань Концепції необхідна державна підтримка розвитку телекомунікацій за такими напрямками:

- залучення вітчизняних наукових установ та окремих науковців до визначення принципів державної політики у сфері телекомунікацій, спрямування їх діяльності на вирішення системних питань, що впливають на розвиток телекомунікацій;
- розвиток науково-технічної та регуляторної політики у зазначеній сфері шляхом прискореного розроблення рекомендацій, нормативних документів і регламентів, організації пошукових і науково-дослідних робіт з оптимального використання наявних ресурсів (фінансових, трудових, матеріальних, частотних, номерних, адресних тощо) з метою підвищення ефективності діяльності суб'єктів ринку телекомунікацій;
- сприяння залученню зовнішніх та внутрішніх інвестицій для розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах;
- залучення вітчизняних наукових установ та окремих науковців до визначення принципів державної політики у сфері телекомунікацій, спрямування їх діяльності на вирішення системних питань, що впливають на розвиток телекомунікацій;
- розвиток науково-технічної та регуляторної політики у зазначеній сфері шляхом прискореного розроблення рекомендацій, нормативних документів і регламентів, організації пошукових і науково-дослідних робіт з оптимального використання наявних ресурсів (фінансових, трудових, матеріальних, частотних, номерних, адресних тощо) з метою підвищення ефективності діяльності суб'єктів ринку телекомунікацій;
- сприяння залученню зовнішніх та внутрішніх інвестицій для розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах;

Висновок:

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.

Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації

в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.

Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Полєха Анна Сергіївна

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва

м. Київ

ВПЛИВ ІТ СИСТЕМ НА ЕКОНОМІКУ УКРАЇНИ

Вітчизняна індустрія програмної продукції є найбільш мобільним сектором економіки, який, при цьому, не потребує для свого розвитку таких значних фінансових і матеріальних вкладень, як металургія, машинобудування, хімічна промисловість чи інші галузі.

За три останні роки вклад ІТ в економіку України суттєво зріс: з 0,8% в 2012 році до 3%, які очікуються в 2015 році.

Це дозволяє прогнозувати, що в майбутньому вплив ІТ буде тільки збільшуватись і в економіці, і в суспільстві в цілому .

ІТ-галузь має потужний потенціал, представлений висококваліфікованими кадрами, які здатні розробляти унікальні програмні продукти, що не мають аналогів у світі й користуються значним попитом провідних компаній. Саме розвиток ІТ-галузі, як інноваційної сфери економіки з високою доданою вартістю, дасть змогу в стислий термін збільшити ВВП країни, забезпечити стабільні валютні надходження до української економіки.

Розглянемо автоматизовані інформаційні системи, які сприятимуть розвитку сучасного бізнесу, що дозволить переконатися у важливості використання ІС в економіці:

- системи для ведення бухгалтерського обліку;
- міжнародні системи взаємодії;
- користувацькі інтернет-системи, що містять інформацію про діяльність організації;
- системи безпеки та захисту інформації;

- ERP системи (EnterpriseResourcePlanning, планування ресурсів підприємства)

Останнім часом все частіше і частіше використовується словосполучення як «ERP-система».

Не кожна особа може дати точне визначення таким системам і сказати, яку мету переслідують підприємства, не шкодуючи десятків, сотень, а іноді навіть мільйонів доларів, на установку даного програмного забезпечення.

Цінність і суть роботи ERP-системи полягає в тому, що вона має необхідну інформацію про поточний стан справ на підприємстві для прийняття оперативних рішень.

«Компанія приймає рішення про те, що і коли потрібно зробити, на яких умовах відвантажити замовнику, яка сировина та в яких обсягах буде потрібно для цього закупити, які фінансові кошти для цього знадобляться.

В основі цього лежить інформація про поточний стан бізнесу: про фінанси, товари та матеріали, незавершене виробництво, завантаженні потужності.

Ця інформація формується в процесі роботи підрозділів (відділів постачання, збуту, виробництва, маркетингу), результати якої «зберігаються» у вигляді транзакцій в системі та служать основою для аналізу ситуації і прийняття рішень в процесі управління ресурсами».

Говорячи про ERP-системі, варто мати на увазі «оперативність» і «цілісність» - це і є основною причиною, яка змушує керівників підприємств купувати дане ПО, мати можливість своєчасно «поглянути» на будь-який бізнес-процес

Також можна виділити ще кілька критеріїв, які є пріоритетними при виборі ERP-системи. В першу чергу це функціональні можливості і масштаби підприємства, на яке орієнтоване рішення. «Коробкові» варіанти можуть елементарно не відповідати конкретним потребам і завданням. Також велику роль відіграє і вартість проекту впровадження такого роду системи. У вартість можуть входити не лише програмне забезпечення, але і вартість послуги, ліцензії, спеціальне обладнання, а також навчання персоналу. Крім того, на ціну впливає, яка програмна платформа використовується.

Проблема контролю над діяльністю та бізнес-процесами не оминула і Україну. Але активно намагатися вирішувати дану проблему в нашій країні стали тільки останнє десятиліття. Крім того, усе загострюється ще й тим, що багато програм у своїй діяльності експлуатують безліч продуктів різних виробників. Ситуація почала змінюватися з 2000 року в гонці за лідерство багато керівників не боялися вкладати кошти в ІТ-інфраструктуру і розвивати продуктивність своїх підприємств.

В Україні на даний час присутні всі складові для успішного розвитку галузі інформаційних технологій: високий рівень забезпеченості

висококваліфікованими ІТ-фахівцями, підтримка зі сторони країн - світових лідерів, наявність політичної волі й бажання до прогресивних змін в економіці (й ІТ-галузі, зокрема) зі сторони уряду країни.

Щоб забезпечити динамічний розвиток ІТ-галузі, необхідно: розширити та покращити підготовку ІТ-спеціалістів; посилити боротьбу з порушенням авторських прав та кіберзлочинністю; інформувати потенційних інвесторів про привабливість українського ІТ-ринку в спеціалізованих іноземних виданнях та на Інтернет-сайтах; прийняти ряд законодавчих актів, які б забезпечували ефективну систему податкових стимулів для працюючих в ІТ-галузі; забезпечити розвиток ІТ-інфраструктури (насамперед - створення ІТ-парків); розвивати сферу надання адміністративних послуг населенню в електронному вигляді; впроваджувати інформаційні технології в усіх галузях. Успішна реалізація цих заходів сприятиме розвитку і зростанню не лише інформаційної індустрії, а й економіки України в цілому.

Криза 2014-2015 рр. може змусити ІТ-ринок просісти на 10%, але завдяки аутсорсинговій моделі роботи українські компанії продовжують бути прибутковими навіть під час економічної нестабільності - саме тому даний сектор вважається одним з ключових в країні. Найбільші угоди в ІТ-секторі за минулий рік укладалися непомітно для ринку, адже в більшості випадків їх фінансували діючі акціонери. ModnaKasta, Megogo, all.biz, Slando і Aukro отримали семизначні інвестиції на прискорення зростання своїх проєктів. В цілому, розмір венчурних інвестицій, включаючи нові угоди і до інвестиції, за підсумками 2014 року склали \$ 50 млн. Гравці цього ринку відзначають спад активності з боку інвесторів, але впевнені, що це тимчасове явище. Багато локальних інвесторів взяли паузу і чекають розвитку ситуації щодо переоцінки структури ризиків.

Світові технологічні тренди сьогоdnішнього дня - мобільні пристрої, управління ними і загальна віртуалізація.

Смартфони стають центром домашніх екосистем - в наступні п'ять років буде активно розвиватися напрямок "розумних" будинків.

Зростаючий попит на енергоресурси в сьогоdnішньому світі призводить до зростання їх вартості. Це, в свою чергу, змушує світ впроваджувати енергозберігаючі технології. У даний час все більшу кількість користувачів вимагає інтерактивності навколо себе. За даними дослідження EricssonConsumerLab, в найближчі три роки споживачі хочуть побачити вдвічі більше додатків для онлайн-шопінгу, відвідування ресторанів і місць дозвілля, догляду за дітьми або літніми людьми, а також комунікації з урядовим сегментом

Розвиток бізнесу будь-якого масштабу безпосередньо залежить від взаємодії людини з інформаційними системами, оскільки саме рівень інформатизації підприємства підвищує його конкурентоспроможність й успішність. Отже, застосування ІТ в бізнесі призводить до більшого прибутку галузі. Надання рекомендацій щодо впровадження певних кроків до розширення ІТ-ринку дозволять розвиватися та зростати інформаційній індустрії та економіки України в цілому. Інформаційна автоматизація сьогоdnі відіграє таку

ж роль, як «промислова революція» на початку 19 століття в Англії, тому проведений аналіз різновидів інформаційних систем дозволить встановити певний їх вплив на сучасний бізнес та визначити ефективність цих систем, а саме мати чітке уявлення про матеріальні вигоди й втрати від їх придбання та використання в бізнес-процесах.

Подальші дослідження доцільно продовжувати в пошуку напрямів та створенні сприятливих умов росту ІТ-індустрії, розробці з Міністерством Фінансів та Комітетом Верховної Ради поступової оптимізації прийнятних умов оподаткування ІТ-індустрії, залученню та розвитку кваліфікованих ІТ-фахівців за рахунок створення екосистем для розвитку не тільки аутсорсингових компаній, а і стартапів, e-commerce ініціатив. У системі освіти варто налагодити взаємодію між ВУЗами та бізнесом, обмін досвідом зі світовими університетами з підготовки ІТ-фахівців, підтримати освітні ІТ-стартапи. Необхідна подальша популяризація професії програміста (ІТ-фахівця), адже попит на таких фахівців зростає.

Мирошниченко Наталія Володимирівна

Державний університет телекомунікацій

Навчально – науковий інститут менеджменту та підприємництва.

м. Київ

ПРО СХВАЛЕННЯ КОНЦЕПЦІЇ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

1. Загальні положення

Концепція розвитку телекомунікацій в Україні відповідно до Закону України "Про телекомунікації" (1280-15) визначає основні засади і напрями подальшого розвитку телекомунікаційних мереж загального користування (далі - телекомунікаційні мережі) в ринкових умовах і спрямована на досягнення стратегічних інтересів та конкурентоспроможності України на міжнародному ринку. { Абзац перший розділу 1 із змінами, внесеними згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }

Концепція є інструментом реалізації державної політики у сфері телекомунікацій щодо координації діяльності державних органів та підприємств, установ і організацій, пов'язаної з розвитком телекомунікаційних мереж в Україні. Положення цієї Концепції також повинні враховуватися органами виконавчої влади під час розроблення та затвердження концептуальних і програмних документів з питань розвитку спеціальних, відомчих або корпоративних телекомунікаційних мереж.

Концепція визначає проблеми розвитку телекомунікацій, стратегію і основні шляхи їх розв'язання, а також принципи забезпечення комплексного розвитку телекомунікацій. Для реалізації завдань Концепції передбачається залучити ресурси мереж загального користування різних форм власності,

забезпечити взаємодію цих мереж з урахуванням потреб національної безпеки та оборони держави, захист інформації та безпеки критичних елементів мереж, а також управління всіма мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Стратегія розвитку телекомунікаційних мереж повинна базуватися на використанні новітніх технологій, які відповідають міжнародним стандартам, враховувати необхідність технологічної взаємодії всіх мереж при наданні телекомунікаційних послуг, забезпечити підвищення ефективності їх функціонування.

2. Роль і проблеми розвитку телекомунікацій

Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи підтримку розвитку економіки держави та соціальної сфери. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери. { Абзац перший розділу 2 із змінами, внесеними згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }

У сфері телекомунікацій існують такі проблеми:

1. низький рівень забезпечення населення, підприємств, установ і організацій широкосмуговими телекомунікаційними послугами; { Абзац третій розділу 2 із змінами, внесеними згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }
2. нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);
3. використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;
4. наявність великої кількості операторів телекомунікацій, що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій; {Абзац шостий розділу 2 із змінами, внесеними згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }
5. неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
6. недостатній регуляторний вплив держави на ринок телекомунікацій;

7. недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій;
8. низький рівень координації органами виконавчої влади діяльності з розвитку мереж загального користування; { Розділ 2 доповнено абзацом згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }
9. недосконалість нормативної бази з питань провадження інвестиційної діяльності; { Розділ 2 доповнено абзацом згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }
10. невідповідність системи нумерації телефонної мережі загального користування міжнародним та європейським вимогам; { Розділ 2 доповнено абзацом згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }
11. обмеженість вибору альтернативних мереж операторів телекомунікацій. { Розділ 2 доповнено абзацом згідно з Розпорядженням КМ N 1612-р (1612-2008-р) від 27.12.2008 }

Література:

1) КАБІНЕТ МІНІСТРІВ УКРАЇНИ

Р О З П О Р Я Д Ж Е Н Н Я

від 7 червня 2006 р. N 316-р

Київ

Про схвалення Концепції розвитку

телекомунікацій в Україні

{ Із змінами, внесеними згідно з Розпорядженням КМ

N 1612-р (1612-2008-р) від 27.12.2008 }

Картамишева Олена Володимирівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ

ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ

Сьогодні стає загальновизнаним той факт, що засоби телекомунікацій знаходяться на етапі перетворення, який охопив системи і мережі електрозв'язку та інформаційні послуги, які вони надають.

Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікацій. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як

наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

- забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання;
- впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень;
- дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Виконання таких завдань ставить нові вимоги по кадровому забезпеченню та науково-технічному розвитку галузі. Перед закладами освіти постає задача підготовки, перепідготовки та підвищення кваліфікації фахівців для галузі телекомунікацій, де освітянський рівень працівників галузі, сформований ще 10-20 років тому, не відповідає зростанню технологічної бази та новітніх засобів телекомунікацій.

Особливо гостро проблема підготовки фахівців стоїть для підгалузі поштового зв'язку. Підготовкою спеціалістів для поштового зв'язку не займається жодна установа вищої освіти в Україні. Серед керівних та інженерно-технічних робітників підгалузі поштового зв'язку дуже низька доля фахівців з вищою освітою з поштового зв'язку (менше 3 %).

Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неї вже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче забезпечення діяльності інвесторів та слабка державна підтримка цього процесу.

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд. Основою для інвестування вітчизняного та іноземного капіталу і кредитів мають стати продумане планування та тісна співпраця учасників галузі. Але відкриття ринку послуг іноземним компаніям у розвинених країнах допускається тільки за мірою достатнього його насичення послугами, що надаються національними операторами. Такий підхід дозволяє підвищити конкурентоспроможність національних операторів, підготувати їх до умов відкритого ринку та уникнути зайняття домінуючих позицій іноземними операторами.

Нині ринок інформаційних і телекомунікаційних технологій - один з найбільш прибуткових секторів економіки України, що динамічно розвивається.

Проте досягнутий рівень телефонізації досить низький у порівнянні з показниками розвинених країн.

Література:

- 1. Латік В. Основні показники рівня життя населення // Праця і зарплата, 2005. - №10.
- 2. Довгаль О.Г. Соціальні послуги , як елемент ринкової інфраструктури //Формування ринкових відносин в Україні, 2003. - № 7-8

***Картамишева Олена Володимирівна**
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ*

ВПЛИВ РОЗШИРЕННЯ ЄВРОПЕЙСЬКОГО СОЮЗУ НА РОЗВИТОК УКРАЇНСЬКИХ ТЕЛЕКОМУНІКАЦІЙ

Розширення Європейського Союзу (ЄС) створює якісно нову ситуацію на шляху подальшого технічного, економічного та соціального розвитку України. Границі України стають границями з ЄС. Прямо і нагально постає завдання повноправного входження України до цього Союзу. Як наслідок, уже сьогодні починається підготовчий період до вступу України до ЄС. З точки зору українських телекомунікаційних систем також починається підготовчий період до їх функціонування в телекомунікаційному середовищі країн-членів ЄС, створення якого є одним з найважливіших національних завдань бо в ХХІ сторіччі сама інформація стає стратегічним ресурсом.

Прийнятий Верховною Радою України Закон “Про телекомунікації”, 299 переважна більшість положень якого відповідає чинному європейському законодавству, відкриває широкі перспективи розвитку вітчизняної телекомунікаційної сфери в її русі до інтеграції телекомунікацій держав Європейської спільноти. Телекомунікації України, як і інших країнах, виконують три основні функції: а) надання важливих послуг індивідуального споживання (міжперсональне телеспілкування, інформаційне самозабезпечення, самоосвіта, відпочинок, розваги, тощо); б) складання частини виробничої інфраструктури (бізнес-зв’язки, реклама, брокераж, просторово-рознесені виробничі процеси, тощо); в) участь у вдосконаленні соціальної організації суспільства (електронне врядування, осередки громадянського суспільства, екстренна та медична допомога, тощо).

Підготовча ситуація невідпорно потребуватиме швидкого вдосконалення сфери українських телекомунікацій в частині усіх зазначених функцій. Однак причини вдосконалення кожної із них будуть свої. Функція індивідуального споживання послуг зв’язку повинна бути піднята до рівня аналогічного споживання в країнах-членах ЄС. Без цього громадяни України не зможуть себе відчувати рівними з громадянами інших країн ЄС як у спілкуванні, так і в організації персональної інформаційно- комунікаційної сфери. Недостатній

рівень споживання послуг зв'язку, особливо їх сучасних видів – мобільного та Інтернет, можуть бути істотною складовою невдоволення населення від вступу до ЄС. Лишати основну масу українських громадян з недорозвиненою системою стаціонарного телефонного зв'язку і з початковим рівнем забезпечення мобільним зв'язком і Інтернет – це означає лишати їх права на сучасні загальнодоступні види зв'язку, права, вже реалізованого в країнах ЄС. Функція українських телекомунікацій, як складової виробничої інфраструктури, повинна розвиватися випереджаючими економіку України темпами з тим, щоб створювати максимально сприятливі умови швидкого зростання економіки і добробуту українських громадян перед вступом до ЄС. Без наближення рівня життя українських громадян до рівня, хоча б, нових членів ЄС не уникнути масового невдоволення вступом до ЄС, посилення міграційних процесів і соціальної напруги в українському суспільстві. Відомо, що розвиток інформаційно-комунікаційної сфери країни слугує каталізатором її промислового і економічного розвитку.

Цю обставину слід сповна використати у даній підготовчій ситуації. Функція вдосконалення суспільної організації також повинна розвиватися у підготовчому періоді якнайшвидше, оскільки ЄС вимагає від країн-членів більш прозорості, демократичної і соціально спрямованої організації суспільства. Це є однією з основних вимог до країн-кандидатів у члени ЄС. 300 Таким чином, високі вимоги до основних державотворчих функцій українських телекомунікацій перед вступом до ЄС та низький їх сьогодиншній рівень розвитку ставить на порядок денний необхідність розробки і прийняття стратегії швидкого кількісного розвитку (у 3-10 разів на протязі 10-15 років) базових видів зв'язку українських телекомунікацій.

Картамишева Олена Володимирівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ

РОЗВИТОК МЕРЕЖІ ІНТЕРНЕТ ТА ОНЛАЙН-РЕСУРСІВ В УКРАЇНІ ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Актуальність проблеми. Нові інформаційно-комунікаційні технології спричинили революційні зміни у сфері медіа, хоча безпрецедентні можливості, що вони відкривають перед людством, тільки починають використовуватись. Сьогодні найбільш перспективною технологічною платформою для подальшого розвитку інфраструктур масової інформації та комунікації – як на глобальному, так і на локальному рівнях – вважається саме Інтернет і пов'язані з ним нові види медіа-сервісів. Уже сьогодні всесвітня мережа є інтегральною складовою більшості аспектів людського життя, але завдяки розповсюдженню та

вдосконаленню ІКТ її вплив на глобальний політичний, економічний, гуманітарний розвиток продовжує швидко зростати.

Водночас, за самою своєю природою та архітектурою „всесвітня павутина” є структурою, функціонування і розвиток якої дуже складно спрогнозувати, а тим більше – скерувати. Втілена на сьогодні модель Інтернет являє собою принципово „горизонтальну”, децентралізовану і неієрархічну структуру, позбавлену якогось єдиного осередку контролю та керування.

Аналіз проблеми. Особливості Інтернет приблизно з середини 90-х рр. минулого століття (коли він почав набувати масштабів глобального феномену) неодноразово спонукали представників фінансово-промислових кіл та уряди деяких країн підіймати питання про підвищення рівня його керованості, зміну архітектури, введення обмежень тощо. У 1999 р. зафіксовані перші спроби застосування цензури в Інтернет. У низці країн (Саудівська Аравія, Іран, Єгипет, Китай, деякі пострадянські держави) на офіційному рівні обмежується доступ населення до Інтернет, передбачені жорсткі покарання, застосовується технічне блокування певних серверів і сайтів політичного, релігійного, розважального характеру. У США та Західній Європі також усвідомлюють загрози, пов'язані з безконтрольним поширенням інформації у всесвітній мережі, але намагаються контролювати інформаційні обміни в Інтернеті дозовано, з одного боку обмежуючи явища, небезпечні для суспільства, економіки, приватної власності та державних інститутів, а з іншого – охороняючи невід'ємні (у даному разі – інформаційні) права особистості.

Загалом, у сучасному світі поки що вдається дотримуватись проголошеного ще у 80-х рр. минулого століття принципу „Інтернет нікому не належить”. На сьогодні існує низка міжнародних координаційних та/або консультативних органів, що опікуються питаннями глобального розвитку Інтернет, проте жоден з них не позиціонує себе як центральна інституція з директивно-керівними повноваженнями. Зокрема, на III Форумі з керування Інтернет (IGF – Internet Governance Forum), що відбувся у грудні 2008 р. у м. Хайдерабаді (Індія), серед іншого, обговорювались питання охоплення доступом до Інтернет „наступного мільярда” населення земної кулі та боротьби з кіберзлочинністю.

Водночас, варто підкреслити, що в структурі всесвітньої мережі все ж існують вагомні технологічні та адміністративні передумови для її монополізації. Наприклад, один зі „стовпів” Інтернету, всесвітня служба DNS (Domain Name System – Система доменних імен) функціонує на основі 13 машин, т. зв. „кореневих серверів”, пов'язаних з кількома тисячами проміжних серверів-реле по всій земній кулі. Десять з цих машин, включаючи головний сервер „А”, що контролює розподіл доменів в залежності від географічної зони (наприклад, .fr для Франції, .de для Німеччини, .ua для України) та/або від сектору діяльності (.com, .net, .org, .aero тощо), знаходяться на території США. Весь світовий ансамбль доменних імен перебуває під наглядом та управлінням ICANN (Internet Corporation for Assigned Names and Numbers – Інтернет-корпорація з призначення імен та номерів), яка була створена у 1998 р. за контрактом з Департаментом

Торгівлі США. Але кореневий сервер „А” залишається під безпосереднім контролем цього департаменту. І в принципі адміністратор DNS має технічну можливість „редагувати” контент всесвітньої мережі. Утім, на сьогодні це лише теоретично припустима можливість.

Згідно з результатами дослідження, проведеного компанією ComScore, у грудні 2008 р., нині світова Інтернет-аудиторія складає приблизно 1,07 млрд осіб.

За кількістю користувачів Інтернет на першому місці знаходиться Китай (179 млн осіб), на другому місці – США з більш ніж 163-мільонною Інтернет-аудиторією, на третьому – Японія (60 млн осіб). Росія посіла 8-е місце – близько 29 млн користувачів.

На Європу припадає 28 % світової Інтернет-аудиторії – насамперед завдяки Німеччині (3,7 %), Сполученому Королівству (3,6 %), Франції (3,4 %) та Італії (2,1 %). Активні користувачі складають в цих країнах у середньому від 40 % до 60 % всього населення, але це не найвищі показники. Серед країн ЄС найбільшою популярністю Інтернет користується в Нідерландах, де зі 100 осіб близько 90 є користувачами. У Норвегії цей показник складає 85 на 100, у Швеції – 80 на 100, у Бельгії – 70 на 100. Найменше у Євросоюзі охоплення населення мережею Інтернет має Греція – 20 на 100.

Що ж до України, то вона досі зберігає один з найнижчих в Європі показників доступу населення до Інтернет – нині він складає 17,8 користувачів на 100 жителів. З іншого боку, наявною є висока динаміка інформатизації країни і зростання вітчизняної Інтернет-аудиторії: наприкінці 2007 р. названа пропорція складала 12 користувачів всесвітньої мережі на 100 мешканців, у 2006 р. – 9 на 100*.

За результатами дослідження агентства Gemius – лідера онлайн-вимірювань у регіоні Центрально-Східної Європи – абсолютна кількість української Інтернет-аудиторії у 2008 р. склала 7,1 млн користувачів (real users) у віці 16 років і більше. Це на 1,7 млн користувачів, або на 30 % більше, ніж у попередньому році.

Ключовими чинниками зростання чисельності вітчизняної Інтернет-аудиторії є досить інтенсивна інформатизація країни – розбудова телекомунікаційних мереж, швидке впровадження ІКТ на тлі підвищення (принаймні до четвертого кварталу минулого року) платоспроможності населення. Сегмент послуг комп’ютерного зв’язку, зокрема надання доступу до Інтернет, є найбільш динамічним на вітчизняному ринку зв’язку. Лише у 2008 р. доходи від послуг комп’ютерного зв’язку зросли в 1,5 разу, у тому числі від надання доступу до Інтернет – на 148 %.

Одним з пріоритетних напрямків розвитку телекомунікаційних мереж залишається будівництво сучасних волоконно-оптичних ліній зв’язку з впровадженням технологій CWDM та DWDM*, розвиток мережі широкопasmового доступу, в тому числі бездротового за технологіями Wi-Fi та WiMAX. Зростає аудиторія абонентів широкопasmового доступу до мережі Інтернет: на кінець 2008 р. цей показник складав близько

1,2 млн користувачів. Рівень проникнення широкосмугового доступу перевищив 8 % від загальної кількості сімей в Україні.

Торік операторами зв'язку усіх форм власності збудовано та введено в експлуатацію понад 2,5 тис. км волоконно-оптичних ліній зв'язку, з них 2,1 тис. км – ВАТ "Укртелеком". Таким чином, у цій сфері також зберігається позитивна динаміка, хоча варто підкреслити, що наведені цифри є значно меншими за показники 2007 (5,7 тис. км) та 2006 (близько 4 тис. км) років.

Разом з цим, уже багато років дуже нерівномірним залишається розподіл користувачів Інтернет по регіонах. Торік позицію абсолютного лідера, як і раніше, продовжував займати Київ – 58 % загальної чисельності користувачів. Далі, у порядку зменшення частки користувачів, ідуть Одеса, Дніпропетровськ, Донецьк, Харків, Львів, Крим та Запоріжжя (їх сумарна частка складає 31 %). На решту ж регіонів припадає лише 11 %. Далі, якщо у розвинених країнах зазвичай немає суттєвої різниці між охопленням населення Інтернет-сервісами у місті й на селі, то в Україні в сільській місцевості мешкають лише 10 % від загальної кількості користувачів. Щоправда, у 2008 р. ці диспропорції дещо пом'якшилися активністю регіональних користувачів – за обсягом трафіку і часу перебування в мережі вони в середньому майже наздогнали столичних.

Триває повільне, але стабільне зростання *національного сегменту Інтернет*, за яким серед користувачів та медіа-експертів вже міцно закріпилася назва „Уанет” (від доменних присвоєнь .ua і .net, що можна перекласти як „українська мережа” – UAnet). У 2008 р. кількість українських веб-сайтів сягнула 41,5 тис. (для порівняння: наприкінці 2007 р. – 40,3 тис., у 2006 р. – 36,0 тис.), кількість реальних хостів у національному домені мережі Інтернет – 215,5 тис. (у 2007 році – 200,5 тис.), кількість діючих доменів в українському сегменті мережі Інтернет – 89,2 тис.

Найбільшими ресурсами українського сегменту Інтернет нині є Meta.ua, Bigmir.net, Korrespondent.net, Marketgid.com, I.ua, Liga.net, Pravda.com.ua, Online.ua, сайти групи Обоз, Unian.net та інші.

Традиційно приналежність ресурсу до того чи іншого національного сегменту визначають за двома базовими критеріями: національний домен (наприклад – .ru, .de, .fr, .ua) та мова. Останній критерій для Уанету підходить лише частково через мовнокультурну амбівалентність нашого суспільства, практично всі громадяни якого вільно володіють російською, зате далеко не всі – українською. Саме через це чимало вітчизняних онлайн-ресурсів є повністю російськомовними, деякі репрезентують механічну суміш української та російської, треті існують у двомовному (подекуди – з англійською – тримовному) варіанті. При цьому майже завжди йдеться про орієнтацією не на зовнішню, неукраїнську аудиторію, а саме на вітчизняного користувача. У такій ситуації природним конкурентом Уанету стає російській сегмент вебу – Рунет, який, будучи значно розвиненішим й насиченішим інформаційно, донині легко перебирає на себе більшу частину української аудиторії.

Змальоване становище почало поступово виправлятися лише приблизно після 2006 р., – в основному за рахунок збільшення в Уанеті специфічно

українського контенту, але без помітного зростання питомої ваги української мови.

За одностайною думкою фахівців, Уанет у своєму розвитку на декілька років відстає не лише від світових лідерів, але й від найближчих сусідів (Росія, Польща, країни Балтії). Відставання це спостерігається, насамперед, за такими напрямками:

- відсоток користувачів в населенні країни;
- обсяг, частотність оновлення, якість контенту, питома вага контенту власного виробництва;
- сектор інтерактивного Інтернет Web 2.0 (форуми, блоги, соціальні мережі, аукціони, Вікіпедія тощо), що розглядається експертами як найперспективніший вектор розвитку всесвітньої мережі на найближче десятиліття;
- сервіси Уанету творять фрагментарне, недостатньо структуроване інформаційне поле з багатьма „лакунами”, значну частину інформації доводиться шукати поза межами національного сегмента;
- нормативно-правова неврегульованість галузі, відсутність перевіреного практикою і прийнятого спільнотою кодексу корпоративної етики;
- обсяг ринку Інтернет-комерції та онлайн-реклами.

Загалом, український сегмент Інтернет, наслідуючи алгоритми розвитку інших країн регіону, у найближчі 3-5 років буде, очевидно, планомірно рухатись у напрямку подолання вищезначених проблем. Водночас, немає вагомих підстав очікувати його „проривного”, випереджаючого розвитку, який необхідний, зокрема, для успішної конкуренції з Рунетом.

У поточному році додатковим стимулом для його розвитку, однак, може стати сприятлива кон'юнктура для ринку онлайн-реклами. Сьогодні обсяг цього ринку, за різними оцінками, складає від 18 до 22 млн дол., і можна досить впевнено прогнозувати його зростання щонайменше на 20-40 % завдяки, зокрема, таким чинникам: а) швидке зростання аудиторії; б) наявність значної кількості дешевих рекламних площ на тлі зростання розцінок в інших різновидах медіа; в) широкі можливості варіювання рекламних стратегій, форм подачі інформації, вибору „нішових” аудиторій.

Висновки та пропозиції

Ступінь інтегрованості країни у глобальний веб-простір можна визначити за трьома тісно пов'язаними між собою показниками:

- а) щільність й технологічна досконалість телекомунікаційних мереж;
- б) кількість Інтернет-аудиторії;
- в) питома вага та рейтинг національного сегменту у всесвітній мережі.

Україна поки що помітно відстає від більшості розвинених країн за всіма цими показниками. Однак спостерігається достатньо висока динаміка їх зростання протягом 2006-2008 рр., причому вагомим підстав очікувати

кардинального зламу даної тенденції у середньостроковій перспективі, навіть з урахуванням впливу світової кризи, немає.

Так, не дивлячись на кризові явища, у 2009 р. найімовірніше *триватиме активний розвиток ринку телекомунікацій* і насамперед – комп'ютерного зв'язку, широкосмугового доступу в Інтернет з використанням технологій CWDM та DWDM, а також підготовки до масового впровадження 3G у стандарті UMTS (широкосмугового мобільного Інтернет). До такого прогнозу спонукають три чинники: 1) значні невикористані можливості українського ринку; 2) наявність сильних гравців, в принципі здатних працювати в загальнонаціональному масштабі – „Укртелеком”, „Воля-Кабель”, „Київстар”, „МТС-Україна”, „Телесистеми України”, „Інтертелеком” та інших; 3) швидка окупність впровадження названих технологій, особливо DWDM.

Можна також констатувати, що *розвиток телекомунікацій в Україні відбувається в загалом оптимальному на сьогоднішній день напрямку – поступового впровадження інноваційних технологій*, зокрема мереж останнього покоління, розрахованих на чимдалі глибшу конвергенцію інформаційних, мультимедійних, комп'ютерних форматів та сервісів.

Позитивна динаміка на ринку телекомунікацій природним чином сприятиме *подальшому зростанню вітчизняної Інтернет-аудиторії*. Малоімовірно, що кризові явища і пов'язане з ними зниження платоспроможності населення суттєво сповільнять цей процес, оскільки: а) буде збільшуватись відсоток територій та населення, охоплених телекомунікаційними мережами нового покоління при збереженні відносно стабільних тарифів на підключення й обслуговування; б) за своєю вартістю Інтернет-послуги в Україні нині є цілком доступними для широких верств населення – у 2008 р. майже половина вітчизняної веб-аудиторії складалася з людей з низьким рівнем доходів (до 3000 грн.) при тому, що 83 % українських користувачів мали домашнє підключення до Інтернет.

Національний сегмент Інтернет (Уанет) за більшістю основних показників (див. стор. 6) децю відстає від інших держав регіону, демонструючи при цьому багато в чому аналогічні напрямки та алгоритми розвитку. У середньостроковій перспективі немає вагомих підстав очікувати його випереджаючого зростання, що необхідне, зокрема, для успішної конкуренції з Рунетом. Таким чином, найімовірнішим сценарієм є стабільний розвиток зі збереженням відставання.

Основне завдання держави на даній стадії розвитку мережі Інтернет та її національного сегменту в Україні вбачається у подальшому розвитку та оптимізації відповідної нормативно-правової бази за такими напрямками: а) регулювання „онлайнових” секторів економіки (торгівля, надання фінансових і банківських послуг, реклама тощо); б) впровадження електронного документообігу, здійснення експортно-імпортних операцій, сертифікаційних процедур з використанням електронного цифрового підпису; в) оптимізація порядку державної реєстрації та звітності суб'єктів підприємницької діяльності, які діють в Інтернет; г) захист авторських прав в Інтернет.

У зв'язку з двома останніми пунктами окремої уваги заслуговує питання засобів масової інформації у всесвітній мережі. Сьогодні серед вітчизняних фахівців нині немає єдиної думки щодо необхідності державної реєстрації Інтернет-видань національного сегменту. Треба, однак, підкреслити, що чітке законодавче визначення поняття „онлайн-ЗМІ” та його юридично-правового статусу, є ефективним важелем вирішення таких проблем як порушення авторських прав, неоподатковані доходи від реклами, недостовірна інформація, матеріали, що зачіпають честь та гідність людини, поширення порнографії, кіберзлочинність тощо.

Гукасян Анна Суренівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ

СУЧАСНИЙ СТАН СИСТЕМ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

Розвиток телекомунікацій в Україні відбувається за такими на-прямками:

- *створення локальних мереж установ на основі стандартного об-ладнання;*
- *створення спеціалізованих телекомунікаційних систем загаль-ного чи відомчого призначення;*
- *створення вузлів/шлюзів для виходу на глобальні міжнародні мережі.*

Національне агентство з питань інформатизації здійснює експерти-зу проєктів державних, галузевих інформаційних, інформаційно-обчислювальних мереж і систем та програмно-технічних комплексів. На жаль, діючі зараз в Україні телефонні мережі зв'язку далеко не повною мірою відповідають сучасним вимогам. Основа системи зв'язку України — первинна мережа загального користування (ПМЗК) поки що є в основному аналоговою.

Використовуване обладнання здебільшого застаріле. Щоправда, вже проводиться робота з модернізації первинної та вторинних мереж зв'язку в напрямку їх переведення на цифрові системи передачі. Реконструються існуючі, споруджуються нові магістральні, територіальні та місцеві мере-жі зв'язку. У 1996 р. було завершено цифровізацію міжміського зв'язку Укра-їни: в усіх обласних центрах встановлено цифрові АТС. Всього змон-товано 26 цифрових міжміських АТС; 24 з них належать СП Утел, а дві підпорядковано Укртелекому.

У багатьох містах України впроваджено цифрову мережу з інтег-рацією послуг (ISDN), яка дозволяє здійснювати високошвидкісний доступ до інформаційних ресурсів світу. Зараз усі обласні центри та багато великих міст охоплені системою мобільного зв'язку. До того ж в Україні розширюється мережа пакетної комутації «Укрпак», яку використовує понад 1270 абонентів, забезпечується їх-ня взаємодія з мережею Internet. Київське метро разом із Endru створює мережу на волоконно-оптичному кабелі.

Ряд банків мають вихід на SVIFT. Є вихід на мережі: FidoNet, EARN, ClassNetUkraine (німецька мережа) та ін. В Україні функціонує понад 100 провайдерів (22 з них у Києві, найбільші: Адамант, Global Ukraine, Infocom, Укртелеком), які на-дають послуги доступу до Internet як по комутованих каналах зв'язку, так і по виділених, на основі Frame Relay, ISDN, супутни-кових каналів та ін. Деякі провайдери висунули концепцію побудови єдиної інформаційної мережі в Україні. Позаяк декілька десятків провайдерів ма-ють свої відокремлені канали, пропонується об'єднати зусилля і створити національну backbone. За підтримки закордонних організацій і фірм здійснюється низка проектів. Зокрема, представництво ООН в Україні створює виходи на Internet для наукових і навчальних закладів на некомерційній ос-нові. Міжнародний науковий фонд працює над створенням академі-чної некомерційної мережі наукових організацій (вузли мережі в Академмістечку, на проспекті Науки, в Теремках, КПІ).

*Гукасян Анна Суренівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ*

ТЕЛЕКОМУНІКАЦІЙНА ГАЛУЗЬ УКРАЇНИ, ПРОБЛЕМИ І ПЕРСПЕКТИВИ КОНКУРЕНТОЗДАТНОСТІ

Одна зі стратегічних для будь-якої країни галузей – галузь телекомунікацій – відіграє величезну роль у збалансованому розвитку глобальної та регіональної економіки. Вона є з'єднувальною ланкою як промислової сфери, сфери послуг і споживачів, так і різних географічно розрізнених частин країни та економічних центрів. Стимулюючи людське спілкування за допомогою зв'язку, сучасні засоби телекомунікацій стають необхідною умовою для соціальної згуртованості та культурного розвитку всіх країн.

Вже зараз неймовірно збільшені потоки інформації – телефонні розмови, факсимільна інформація, електронна пошта, масиви даних та телебачення – показують, якою мірою світ стає ще більш залежним від засобів телекомунікацій, які змінюють бізнес, стиль життя, суспільство вцілому. Так, діти в Сінгапурі застосовують пейджинг або стільниковий телефон для підтримання зв'язків з батьками, а аборигени Австралії продають свій живопис, використовуючи можливості відеоконференції, бразильські банки пропонують свої послуги в мережі Інтернет, а французькі домогосподарки радяться з телефонними компаніями у справі вибору слюсаря. Як бачимо, комунікаційні послуги стирають кордони між культурами, мовами та часом.

У багатьох країнах світу сектор послуг у наш час вже дає близько половини їх валового національного продукту, і ця тенденція не обмежується лише економічно розвинутими державами. В таких різних країнах, як наприклад Сінгапур, Гонконг або Угорщина, сектор послуг забезпечує до 60% економічної

активності країни. Навіть у найменш розвинутих країнах частка сектору послуг (43%) перевищує частку сільськогосподарського сектору (37%) або промислового (20%). При цьому вже на початку 90-х років світова частка сфери послуг в економіці становила в середньому близько 60%, а вже протягом наступних років від 70 до 80% економіки розвинутих країн знаходяться під значним впливом інформаційних технологій.

Отже, наприкінці ХХ ст. – початку ХХІ ст. світ перебуває в стані інформаційної революції, вплив якої можна порівняти з впливом індустріальної революції минулого століття. Є всі підстави вважати, що обробка інформації – одна з найвагоміших складових економічної активності. Тому можна стверджувати, що розвиток телекомунікацій як важлива складова інформатизації суспільства та забезпечення населення високоякісними послугами зв'язку є одним з найважливіших напрямів національного та економічного розвитку будь-якої держави, і, зокрема, України.

У даній роботі спробуємо дослідити реальний стан галузі телекомунікацій в Україні, позитивні та негативні фактори, що визначають розвиток українських телекомунікацій, проблеми такого розвитку, а також пропозиції та заходи, спрямовані на подолання проблем, для того, щоб оцінити конкурентоспроможність України у цій галузі.

2. Постановка проблеми

Загальновідомим є той факт, що телекомунікації України значно відстають від телекомунікацій розвинутих країн як за обсягами, так і за рівнем технологій. Ринок телекомунікацій України – достатньо відкритий та лібералізований за останні 8 років. Наведемо деякі цифри. Телефонна щільність у розвинутих країнах складає біля 60 телефонних номерів на 100 чоловік, тоді як в Україні – 20, а, наприклад, у Польщі, яка так само, як і Україна, вважається країною, що розвивається, – 24,6. Інтернетом у розвинутих країнах користуються 15-20% населення, в Україні – 1%, а у Польщі – близько 5%. Щодо мобільного зв'язку, то у розвинутих країнах – близько 30 телефонів на 100 чоловік, в Україні - 0,3, а у Польщі близько 7. По міжнародних та міжміських розмовах спостерігається відставання України від Польщі десь у 5 разів. Послуги зв'язку в рік на одну особу у розвинутих країнах складають 254 дол., в Україні – 20,6, а у Польщі – 65,7. Загалом розвинуті країни вкладають у розвиток зв'язку до 20% від її доходу, країни, що розвиваються – близько 31%, слаборозвинені – 68,5%, тоді як в Україні - 18,1%, а у Польщі – 42,2%. Звідси й відповідні результати.

Взагалі, галузь телекомунікацій в Україні поділяється на два крупних сегменти: електрозв'язок та поштовий зв'язок. Електрозв'язок має два основні напрями: наземний (фіксований чи дротовий) та радіозв'язок. До першої групи, як правило, включають телефонний, телефонний міський, телефонний сільський, телефонний міжміський, телефонний міжнародний зв'язок. Сюди ж можна віднести Інтернет (хоча зараз Інтернет переміщується й у радіозв'язок). До другої групи належать супутниковий, стільниковий, пейджинговий, транкінговий зв'язок.

3. Аналіз проблеми

Одним з найдинамічніших за останні роки сегментів українського телекомунікаційного ринку є мобільний зв'язок. Причому як з точки зору зовнішніх впливів на галузь, так і з точки зору взаємовідношень між суб'єктами ринку. Але довготривала економічна криза та нестабільність вітчизняного законодавства суттєво пригальмувала розвиток українського ринку мобільного зв'язку. Однак, як і інших галузей економіки. Більш того, мобільний зв'язок, як один з найприбутковіших напрямів діяльності, потрапив під пильну увагу контролюючих, інспектуючих та інших подібних “експроприуючих” органів. За останні роки спостерігалися спроби накласти як на суб'єктів ринку, так і на його споживачів різного роду додаткові збори, податки, акцизи і т.д. Це аж ніяк не сприяє розвитку галузі. Але все ж таки на сьогоднішній день можна сказати, що український ринок мобільного зв'язку поступово набуває цивілізованих рис, незважаючи на активну боротьбу (а, можливо, і завдяки їй) п'яти мобільних операторів зв'язку (UMC, KyivStar GSM, DCC, Wellcom, Golden Telecom GSM) за невелику частину платоспроможної клієнттури.

Також порівняно динамічною сферою українських телекомунікацій можна назвати Інтернет. Загальна кількість користувачів Інтернетом в Україні на початок 1999 року становила приблизно 100-120 тис. У відношенні до загальної кількості користувачів у світі вона складає менше 0,1% або, точніше, 0,065%. Але в середньому за кожні шість місяців кількість користувачів збільшується в 1,67 рази, що вище середніх темпів зростання у світі в цілому. Зараз мають місце такі прогностичні коефіцієнти росту кількості українських користувачів Інтернетом: 2002 р. – 1,5; 2003 р. – 1,5; 2004 р. – 1,4; 2005 р. – 1,4. Необхідно зазначити, що скільки існує та розвивається вітчизняний сегмент Інтернету, впадає в око один не дуже приємний факт – складається враження, що “існує та розвивається” він тільки у Києві. В інші регіони протягнуто лише невеличкі джерела виділених каналів від крупних київських провайдерів. Але не слід забувати, що перші виділені канали, наприклад, з'явилися не в Києві, а в Харкові, що помітна частина найкращих інформаційних ресурсів України знаходиться не тільки у Києві, але й в Одесі, Донецьку, Дніпропетровську.

Щодо сегмента електровз'язку, то рівень телефонізації в Україні на сьогодні у два рази нижчий, ніж у країнах Центральної та Західної Європи. Із загальної кількості діючих у телефонній мережі АТС 21,1% належать електронним та квазіелектронним, решта – морально застарілим аналоговим. Щільність телефонного зв'язку, як вже зазначалося, становить близько 20,1 телефонів на 100 осіб. Кількість основних телефонних номерів складає в Україні близько 9 млн., з яких 86,6% встановлено у міських телефонних мережах, 13,4% - у сільських. Подальша телефонізація населених пунктів з низьким показником кількості телефонних номерів через низьку платоспроможність у таких регіонах триває повільно – в цілому по країні показники телефонізації зростають за рахунок, знову ж таки, Києва та інших великих міст.

Взагалі, характерною особливістю української телекомунікаційної галузі є значне відставання за часом по застосуванню нових технологій між Києвом та іншими регіонами країни. Наприклад, мобільний зв'язок у Харкові з'явився

через 2-3 роки після його появи у Києві, а в деяких великих містах з населенням в 25 і більше тис. людей він відсутній і досі. Мобільним зв'язком покрито усього біля 25% території України.

Слід зазначити також, що ринок телекомунікацій в Україні характеризується високим рівнем монополізму. “Укртелеком”, “Утел”, УМС, “Укрпошта” – їх сумарна частка у структурі даних послуг становить 90 %. Як вважає Інтернет Асоціація України, зараз практично всі недержавні учасники телекомунікаційного ринку у тій чи іншій мірі потерпають від монопольного становища ВАТ “Укртелком”.

Для світового телекомунікаційного ринку характерні процеси інтеграції та глобалізації, тому що в цілому світовий ринок стає все більш інтегрованим. А Україна, нажаль, часто не може налагодити роумінг у масштабах країни. Україна повинна мати стратегічних партнерів. Ці партнери повинні бути у Європі, Америці, Азії. Бажаним для України є входження до одного з глобальних об'єднань.

Проблемою розвитку телекомунікацій в Україні також є наявність близько 70% аналогових АТС від їхньої загальної кількості. На модернізацію вітчизняних комунікацій потрібно близько 19 млрд. дол. В Україні капітальні інвестиції в розвиток телекомунікацій складають лише 0,3% ВВП. Для порівняння, у Німеччині – 4,8%, у Франції – 3,1%.

Отже, як бачимо, стан галузі телекомунікацій України особливо не вражає, але оскільки, як було зазначено раніше, розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вживати усіх можливих заходів щодо сприяння такому розвитку, зокрема, аби підвищити конкурентоспроможність України в цій галузі.

Пропозиції до розв'язання проблеми

Пропозицій до розв'язання проблеми, взагалі-то, може бути багато, але ми розглянемо саме такі, які є прийнятними для тих умов, що склалися на українському ринку телекомунікацій. Це такі пропозиції:

Підвищити технологічний рівень галузі.

Усунути монополію на ринку.

Створити належне законодавче підґрунтя функціонування галузі.

Підвищити рівень телефонізації по всій території країни.

Створити сприятливий інвестиційний клімат для залучення іноземних інвестицій у галузь.

Виділяти належні кошти на наукові дослідження всередині галузі.

5. Обґрунтування пропозицій та вибір альтернатив

На мою думку, щоб галузь телекомунікацій України дійсно вийшла на належний рівень конкурентоспроможності, необхідно втілювати в життя усі вищезазначені пропозиції у комплексі. А як це буде відбуватися, залежить вже, насамперед, від політики держави, а також, від діяльності тих організацій, які мають безпосереднє відношення до галузі.

Щодо технологічного розвитку галузі, то, взагалі, можна запропонувати дві альтернативи розвитку. Перша: застосовувати більш дешеві, але й більш застарілі технології – виграш у кількості, програш в якості. Друга: брати більш дорогі, але й сучасніші технології. Значно виграємо у якості, але програємо у кількості. Необхідний розумний компроміс. Тут важливим є мистецтво регулюючого органу, його бачення і передбачення.

На жаль, до теперішнього часу в Україні не існує оптимальної нормативної бази, котра б регулювала відносини у сфері телекомунікацій та інформаційних технологій, а, як відомо, без належного законодавчого підґрунтя жодна галузь економіки не може ефективно функціонувати та розвиватися. Отже, основним завданням уряду на сьогодні є створення такої законодавчої бази, яка б сприяла розвитку галузі.

Дуже важливою є роль науки. Зараз вона щодо телекомунікацій, на жаль, у катастрофічному стані. Зв'язок державі виділяє приблизно 50 млн.грн. щороку на науку, програма в цьому році складена на 8,9 млн.грн., видали грошей усього на три угоди. На Заході, наприклад, на науку виділяється близько 2-2,5%, а в Японії – 4%, бо телекомунікації – наукомістка галузь.

6. Здійснення пропозицій урядовими та неурядовими організаціями

Розглянемо для початку заходи щодо розвитку телекомунікацій, здійснювані урядом країни та іншими урядовими організаціями.

Протягом 1999 – 2001 років Верховною Радою України було розглянуто та ухвалено такі важливі закони, як “Про особливості приватизації ВАТ «Укртелеком»”, “Про поштовий зв'язок”, “Про радіочастотний ресурс”. Ціла низка подібних законів роками перебувала в парламенті на розгляді, але Держкомзв'язку України спромігся забезпечити успішне їх затвердження. Також Держкомітет розробив законопроекти “Про телекомунікації”, “Про електронний цифровий підпис”, “Про електронний документ”.

Найважливішим, звісно, є проект закону “Про телекомунікації”, який повинен стати своєрідною “конституцією” у сфері телекомунікацій та інформаційних технологій. Готуючи такий важливий закон, спеціалісти Держкомзв'язку провели цілу низку “круглих столів” та обговорень, врахували думки зарубіжних та вітчизняних експертів, потенціальних та діючих інвесторів, спеціалістів міжнародних фінансових організацій і т.п. Нещодавно проект закону було подано на розгляд до Верховної Ради. Він пропонує законодавчим шляхом врегулювати питання ведення діяльності у сфері телекомунікацій в країні, ліцензування телекомунікаційної діяльності та визначити права та обов'язки операторів зв'язку.

Щодо ліцензування, то тут слід зазначити, що, за думкою експертів Держкомзв'язку, одним з найбільш дієвих важелів регулювання є саме ліцензування підприємницької діяльності операторів з врахуванням особливостей сфери діяльності. Закон України “Про ліцензування деяких видів господарської діяльності”, який вступив у силу з вересня минулого року, не враховує особливостей діяльності у галузі зв'язку і навіть прямо забороняє враховувати їх в інших законах. Вивчення міжнародного досвіду з законодавчого

регулювання діяльності у сфері зв'язку (законів про телекомунікації Німеччини, Франції, Польщі, Росії та ін.) засвідчує, що політика ліцензування у сфері зв'язку законодавчо визначається окремими законами про регулювання саме в цій досить специфічній галузі. Тому лише підтримка та ухвалення законопроекту “Про телекомунікації”, який передбачає особливості ліцензування діяльності у сфері зв'язку, можуть розв'язати проблему.

Щодо дій неурядових організацій у напрямку розвитку галузі телекомунікацій, слід відмітити особливий внесок у цей розвиток найбільшого в Україні оператора з надання послуг зв'язку ВАТ “Укртелеком”. Для успішного розвитку будь-яких систем зв'язку необхідно забезпечити створення потужної транспортної системи на основі оптико-волоконних ліній, які повинні доповнюватися радіорелейними та супутниковими лініями. Без її формування, в тому числі на рівні зони (області) та на рівні найбільших міст, неможливо ефективно розвивати інші мережі зв'язку. Над створенням саме такої системи і працює зараз “Укртелеком”.

В останні роки “Укртелеком” вже здійснив перші кроки щодо побудови транспортної мережі, заснованої на технологіях ATM, Frame Relay та IP. На базі цієї мережі багатофункціонального використання вже будується корпоративна мережа, мережа Інтернет та мережа Frame Relay “Укртелекому”. Ця мережа допоможе “Укртелекому” перевести надання послуг зв'язку на принципово новий технологічний рівень без погіршення якості та розширити можливості впровадження широкого переліку послуг у перспективі.

Для подальшого успішного просування у напрямку підвищення технологічного рівня у галузі телекомунікацій необхідно також вирішити низку складних питань, що стосуються шляхів забезпечення взаємодії існуючих мереж у вітчизняних телекомунікаціях. Тут явно виділяються декілька основних проблем. Щодо технічного аспекту їх розв'язання, то Укртелеком, поряд з іншими організаціями та установами, спрямовує зусилля на здійснення таких заходів:

- розробка і стандартизація нових універсальних протоколів, сумісних зі світовими стандартами, із врахуванням питання взаємодії з існуючою аналого-цифровою мережею електрозв'язку;
- вирішення ряду принципових мережових питань, таких як нумерація на мультисервісних мережах, сигналізація в них для різноманітних служб, забезпечення динамічного керування всіма ресурсами мережі;
- розробка та реалізація інтерфейсів мереж нового типу з традиційними мережами та службами електрозв'язку;
- розробка і масове впровадження сучасних недорогих методів доведення сигналів різноманітних служб електрозв'язку до багатофункціональних кінцевих терміналів користувачів з урахуванням географічних та демографічних особливостей країни.

Необхідні ресурси та умови

Якщо проаналізувати необхідні умови для подальшого успішного розвитку телекомунікацій, то можна прийти до висновку, що такі умови взагалі-то наявні на теренах нашої держави. Це:

1. Досить висока ємність ринку – 49 млн. чоловік.

2. Низький рівень телекомунікацій – отже, досить низьке насичення ринку телекомунікаційних послуг.

3. Транзитне положення країни на основних комунікаціях з Європи в Азію, висока інтенсивність зовнішніх товарних, фінансових, транспортних, людських потоків.

4. Високий рівень освіченості населення: за кількістю осіб з вищою освітою на 1000 мешканців України – серед перших 20 країн світу.

- Високий рівень урбанізації – більше 70% населення України мешкає у містах, та значне розкидання великих міських центрів та агломератів по території країни.
- Культурна та споживча орієнтація значної частини населення на європейські стандарти та умови життя внаслідок високої інтенсивності культурного, міграційного та господарського обміну з країнами Західної Європи, де рівень телекомунікацій значно вищий, ніж в Україні.
- Досить високий рівень розвитку організацій та установ сфер громадського життя та тих галузей, які є найбільш інтенсивними споживачами телекомунікаційних послуг, в першу чергу, фінансової сфери та сфери державного правління. Однак їх гіпертрофоване розширення, особливо останньої, в Україні різко контрастує із занепадом в інших сферах громадської діяльності, особливо в науці та виробництві.

Однак розвиток телекомунікацій в Україні суттєво гальмується, що у свою чергу гальмує розвиток інших перспективних галузей економіки. Основним негативним фактором є дуже низький рівень життя населення. Рівень грошових доходів приблизно 50% населення України достатній лише для задоволення елементарних потреб. Існує і подальша тенденція зниження рівня та якості життя, що є основною причиною відмови населення від цілого спектра телекомунікаційних послуг з причини їх відносної дороговизни для бідної категорії громадян. Собівартість введення одного телефонного номера у сільській місцевості складає понад 1000 дол., тобто телефонізація сільської місцевості є збитковою, оскільки трафік сільських абонентів через їхнє, зазвичай, дуже низьке матеріальне становище невисокий.

Висновки

Отже, на основі проведеного дослідження можна зробити висновок, що, незважаючи на динамічність розвитку галузі телекомунікацій, Україна у цій галузі на даний момент не може конкурувати не тільки з економічно розвиненими країнами, а й з країнами, що розвиваються. Звісно, найбільшою мірою це пояснюється станом економіки нашої держави в цілому, бо, звісно, окрема галузь не може ефективно функціонувати, якщо загальна економічна ситуація в країні характеризується як незадовільна. Але загалом слід відмітити, що, незважаючи на всі перешкоди та проблеми, Україна, хоч і повільно, але все

ж таки просувається на шляху розвитку телекомунікацій, і залишається сподіватися, що ті заходи, які зараз проводять урядові та неурядові організації щодо розвитку галузі, дійсно сприятимуть підвищенню конкурентоспроможності нашої держави у сфері комунікацій.

Література:

1. В.Цхведиани. Телекоммуникации Украины – перспективы развития и основные проблемы // Фондовый рынок. - №16. – 2000.
2. Н. Васильєва. Основні тенденції розвитку ринку інформаційних технологій та комунікацій // Економіст. - №10. – 2000.
3. С.О.Довгий. Стан та проблеми розвитку телекомунікаційної мережі України // Наука та наукознавство. - №3. – 2000.
4. KM-inform IT magazine (про українські телекомунікації) //www.km-inform.com.ua/communication/communication.shtml?4
5. О состоянии телекоммуникационного рынка Украины //www.cdmaua.com/russian/telecom.shtml
6. О. Шевчук. О телекоммуникациях Украины //www.fas.com.ua/14_06_00/brams.html
7. Ю.Соловйов, консультант "Телесистеми України" о рынке телекоммуникаций Украины //www.niss.gov.ua/iso/Table/Litvin1/03.htm

***Гукасян Анна Суренівна**
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ*

РОЗВИТОК ІНФОРМАЦІЙНИХ СИСТЕМ В МЕДИЧНИХ ЗАКЛАДАХ

В умовах прискореного науково-технічного прогресу особливої актуальності набуває подальше впровадження інформаційних технологій в різні сфери медицини. Останнім часом накопичено позитивний досвід застосування інформаційних технологій в управлінні охороною здоров'я, комп'ютерній діагностиці (в тому числі телемедичній діагностиці), в медичній освіті та науці.

За роки незалежності в державі проведена значна робота з формування теоретичних основ та практичного застосування в охороні здоров'я новітніх комп'ютерних технологій. Розроблена і успішно втілюється у життя Концепція державної політики інформатизації охорони здоров'я в Україні, Державною політикою інформатизації охорони здоров'я передбачено заходи, спрямовані на ліквідацію відставання у цій сфері від передових світових держав і прискорення входження в інформаційний простір міжнародного співтовариства з метою підняти на сучасний рівень системи практичної медицини, медичної освіти, науки.

Реалізація цієї політики здійснюється в декількох основних напрямках:
розроблення нормативно-правової бази інформатизації охорони здоров'я;
удосконалення її організаційного та кадрового забезпечення; формування відповідної технічної бази та засобів інформатизації; залучення громадських організацій до інформатизації галузі.

Перший з цих напрямів вже достатньо розвинений. Він ґрунтується на 5 законах України, указах Президента України, постановах Кабінету Міністрів України, наказах Міністерства охорони здоров'я

Основою подальшої інформатизації охорони здоров'я є створення єдиного медичного інформаційного простору України. Процес його формування базується не новітніх інформаційних, телекомунікаційних технологіях та медичних інформаційно-аналітичних системах. До його складу включаються галузеві та регіональні бази даних, системи медико-статистичного аналізу інформації.

Створення такого інформаційного середовища сприяло забезпеченню процесу управління охороною здоров'я своєчасною та достовірною інформацією.

Провідну роль в інформатизації охорони здоров'я України відіграють громадські організації. Найбільша й найстаріша з них — Українська асоціація "Комп'ютерна, медицина" (УАКМ) — сьогодні об'єднує близьке 80 установ та організацій (науково-дослідних установи, вищі медичні навчальні заклади наукові товариства, науково-виробничі об'єднання) і понад 1500 індивідуальних членів.

Завдяки тому, що УАКМ є національним членом Міжнародної Асоціації медичної інформатики (ІМІА) та Європейсько-Федерації медичної інформатики (ЕРМІ), українські фахівці беруть участь у роботі міжнародних робочих груп з опрацювання міжнародних проектів у галузі медичної інформатики та телемедицини. У складі УАКМ працює вчена рада, до якої входить понад 60 фахівців, у тому числі й відомі зарубіжні експерти — спеціалісти з різних напрямів медичної науки, які мають великий досвід створення медичних інформаційних технологій.

За угодою з Європейською комісією з телемедицини на базі кафедри клінічної Інформатики та інформаційних технологій в управлінні охороною здоров'я Харківської медичної академії післядипломної освіти (ХМАПО) створено і функціонує з 1997 р. Український сервер Європейської обсерваторії з телемедицини (ЕНТО), який входить до всесвітньої мережі серверів на національних мовах. До цієї мережі також входять Франція, Швеція, Португалія, Фінляндія, Греція, Іспанія, Аргентина.

Усе це дає змогу розвивати процес інформатизації системи охорони здоров'я на сучасному рівні, інтегрувати систему охорони здоров'я України у світовий інформаційний простір.

Як відомо, суттєвий внесок у зменшення втрат здоров'я активної частини населення забезпечують такі форми медичного обслуговування, як первинна медико-санітарна допомога, швидка медична допомога, реанімація, акушерство тощо. Тому інформатизація цих служб розглядається як стратегічний пріоритетний напрям побудови єдиного медичного інформаційного простору, спрямований на поліпшення роботи системи лікувально-профілактичної допомоги.

Література:

1. Підаєв А.В., Возіанов О.Ф., Москаленко В.Ф., Пономаренко В.М. та інші Панорама охорони здоров'я України – К.: Здоров'я, 2003. – 396 с.
2. Підаєв А.В., Пономаренко В.М., Вороненко Ю.В. Інформаційні технології в системі охорони здоров'я. – К.: Здоров'я, 2003 – 335 с.
3. Крамаренко В.І. Менеджмент: Навчальний посібник. – К.: ЦУМ, 2000. – 248 с.
4. Хміль Ф.І. Основи менеджменту: Підручник – К.: Академвидав, 2003. – 608 с.

Васильєва Юлія Іванівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ

ГОСПІТАЛЬНІ ІНФОРМАЦІЙНІ СИСТЕМИ (ГІС)

Проведений аналіз інформаційних потреб лікарів показує, що впровадження електронних засобів збору, накопичення та опрацювання інформації про пацієнтів дозволяє ефективно опрацьовувати великі обсяги даних без втручання людини.

Одним із напрямів побудови медичних інформаційних систем є госпітальні інформаційні системи (ГІС). Ними оснащуються різні медичні заклади та їх підрозділи. До складу таких систем входять автоматизована реєстратура, формалізовані амбулаторні карти прикріпленого контингенту, облік і аналіз відвідуваності, захворюваності, профілактичних оглядів, диспансеризації, тимчасової непрацездатності, щеплень, флюорографічних досліджень, планування й облік роботи лікарів, формування всієї звітної-статистичної документації про діяльність поліклініки і її підрозділів.

ГІС забезпечують управління персоналом, фінансами, матеріально-технічними ресурсами, зокрема медикаментами, медичними інструментами та апаратурою. Якщо розглядати єдиний медичний простір з позиції пацієнта, то його основу становить електронна історія хвороби як важлива складова ГІС. Лікар зможе одержувати оперативний доступ до необхідної медичної інформації за наявності електронної історії хвороби або за допомогою індивідуальної електронної медичної картки пацієнта незалежно від того, де перебуває пацієнт, в який медичний заклад він звернувся або був госпіталізований (державний або приватний).

Широке впровадження ГІС у систему охорони здоров'я України має велике значення для ефективного управління лікувально-профілактичним закладом, підвищення рівня якості й об'єктивності діагностики.

У складі ГІС функціонують комп'ютерні діагностичні системи (комп'ютерна електрокардіографія; електрокардіографія високого рівня розв'язування; комп'ютерні електроенцефалографія, реоенцефалографія, пневмографія; системи оброблення рентген та ЯМР-зображень тощо).

Широкий набір функціонально орієнтованих прикладних програм ГІС дозволяє створювати різноманітні інформаційно-обчислювальні мережі,

орієнтовані на рішення всього спектра задач організації управління лікувальним і лікувально-профілактичним процесом у різних медичних закладах — лікарнях, поліклініках, диспансерах, медсанчастинах тощо.

Набуло поширення у закладах охорони здоров'я використання комп'ютерної техніки для опрацювання фінансової документації. При цьому скорочується термін виконання фінансових операцій і зменшується число помилок.

Електронна історія хвороби забезпечує оперативний облік витрат, пов'язаних із діагностичними та лікувальними процедурами, використанням медикаментів і матеріалів, оплатою послуг медичного персоналу тощо, що має ключове значення для впровадження страхової медицини.

Українські вчені активно розробляють ГІС, які забезпечуватимуть оперативне одержання даних про фактичні витрати в лікувальних закладах.

Розвиток обчислювальної техніки і, зокрема, поява величезних можливостей запам'ятовування і збереження впорядкованих даних стали могутнім поштовхом до розвитку реєстрів і баз даних медичного призначення. Вивчення світового досвіду щодо створення таких реєстрів є суттєвим підґрунтям для формування на сучасному рівні програми в галузі охорони здоров'я нашої держави. Так, наприклад, у США розроблена й успішно функціонує база даних із соціальної роботи, що містить дані про соціальний і клінічний статус пацієнтів. У цій базі реалізовано вискоєфективний метод доступу до даних, що дозволяє ефективно й оперативно одержувати інформацію про пацієнта. Для аналізу даних використовується адекватне спеціальне програмне забезпечення для планування епідеміологічних досліджень. Розроблено методику побудови інтегральних систем на основі об'єктно-орієнтованого підходу, що доцільно використовувати в охороні здоров'я і для вивчення впливу навколишнього середовища на здоров'я населення.

У пострадянському просторі однією з найважливіших проблем є формування й оптимальне використання даних про ліквідаторів Чорнобильської аварії та потерпілих у ній. Наявність баз даних з великим обсягом інформації, що переробляється, вимагає використання автоматизованих інформаційних систем оцінки здоров'я й інформаційного супроводу необхідного обсягу лікувально-оздоровчих заходів для забруднених радіонуклідами районів. Дані, які заносяться в комп'ютер, приведені до єдиної стандартної форми, що не тільки полегшує їх опрацювання, а й уможливорює використання їх в інших інформаційних системах.

У Росії створений і функціонує спеціальний Чорнобильський реєстр, використання якого переслідує дві цілі:

- спостереження за медичними наслідками і щорічна аналітична оцінка виявлених ефектів, формування рекомендацій з диспансеризації населення;
- радіаційно-епідеміологічний аналіз нових даних про стан здоров'я осіб з груп ризику.

Цей реєстр містить дані про понад 500 тис. осіб, які постраждали внаслідок аварії на ЧАЕС, і більше ніж у п'ять разів перевищує Японський реєстр, що діє у зв'язку з бомбардуваннями Хіросіми і Нагасакі.

Україна, яка найбільше постраждала від, Чорнобильської катастрофи, має найстаріший і найоб'ємніший реєстр. Він налічує інформацію про понад 1 млн. ліквідаторів та осіб, які постраждали внаслідок Чорнобильської аварії. Однак нині виникають проблеми щодо експлуатації цього реєстру, пов'язані з необхідністю застосування сучасних технологій побудови і ведення баз даних.

Одним із могутніх сучасних інструментів проведення медико-соціальних і медико-екологічних досліджень є географічні інформаційні системи (ГЕІС). Кожна країна, маючи мережу моніторингування здоров'я населення, демографічних характеристик, екологічних, економічних і соціальних параметрів, проводить детальний аналіз захворюваності та смертності населення залежно від шкідливих чинників середовища. Медичні географічні системи дозволяють включати просторовий і часовий аналіз параметрів середовища як чинник, який впливає на здоров'я населення і демографічну ситуацію. Відтак виникає чимало питань, спрямованих на розроблення комплексної системи моделювання і прогнозування показників здоров'я і використання їх у формуванні географічних систем.

ГЕІС, що функціонують на Європейському рівні, переслідують дві мети:

- географічне моніторингування середовища і нагляд за здоров'ям;
- оцінка ризику для здоров'я і розроблення рекомендацій з управління відомими небезпечними чинниками середовища. Зокрема, ГЕІС, що об'єднує інформацію з 32 європейських країн ВООЗ, містить дані про забруднення повітря і здоров'я 43 % міського населення. Це сприяє визначенню "гарячих точок" у середовищі та здоров'ї і є основою для обґрунтування національних та міжнародних дій.

Проте роль медичних ГЕІС у виявленні несприятливих географічних чинників середовища не слід переоцінювати. Використання картографічного методу дослідження генофонду і захворюваності населення в Росії показало, що географічні зміни генофонду лише незначною мірою відбивають природну неоднорідність середовища. Саме генофонд виступає як домінуючий чинник в етіології багатьох відомих хвороб.

В Україні активно розробляються медичні ГЕІС різного призначення. Особливу роль ці системи можуть зіграти в процесі управління галуззю та регіонами, надаючи управлінцям інформацію про території, які потребують посиленої уваги. Одним із напрямів використання медичних географічних систем є вивчення стану здоров'я населення України. Нині інтенсивне розвивається опорна зона інформатизації охорони здоров'я в Харківському регіоні. З ініціативи Міністерства охорони здоров'я України та за підтримки Харківської обласної державної адміністрації розпочав роботу перший в Україні Харківський обласний медичний інформаційно-аналітичний центр (www.oblzdraw.ic.kharkov.ua) в якому вже функціонує географічна система медичного призначення.

На відміну від традиційних центрів статистики завдання цього центру значно ширші. Вони полягають у створенні регіональної компоненти галузевої медичної комп'ютерної мережі, створенні та наповненні спеціалізованих регіональних баз даних, організації телемедичних консультативних центрів, упровадженні сучасних комп'ютерних методів функціональної діагностики в лікувальних закладах тощо.

Література:

1. Підаєв А.В., Возіанов О.Ф., Москаленко В.Ф., Пономаренко В.М. та інші Панорама охорони здоров'я України – К.: Здоров'я, 2003. – 396 с.
2. Підаєв А.В., Пономаренко В.М., Вороненко Ю.В. Інформаційні технології в системі охорони здоров'я. – К.: Здоров'я, 2003 – 335 с.
3. Крамаренко В.І. Менеджмент: Навчальний посібник. – К.: ЦУМ, 2000. – 248 с.
4. Хміль Ф.І. Основи менеджменту: Підручник – К.: Академвидав, 2003. – 608 с.

Васильєва Юлія Іванівна
Державний Університет Телекомунікацій
Науково-навчальний інститут менеджменту та підприємництва
м.Київ

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОХОРОНІ ЗДОРОВ'Я УКРАЇНИ

Для поліпшення керованості станом здоров'я населення та управління охороною здоров'я сьогодні передусім необхідно впровадити таку основну групу інформаційних систем:

- систем, які забезпечують інформаційну підтримку процесів управління службою охорони здоров'я регіону (області, міста, району), медичним закладом;
- систем, які забезпечують інформаційний супровід заходів, спрямованих на профілактику захворювань та діагностично-лікувальні процеси щодо конкретної особи.
- реалізація цих стратегічних планів можлива за умови розв'язання таких конкретних завдань:
- реалізація галузевої програми інформатизації охорони здоров'я з урахуванням реалій та стратегії соціально-економічного розвитку країни, основних напрямів розвитку інформатизації в державі;

Поява доступної інформації дозволить вирішувати питання координації політики різних відомств у галузі охорони здоров'я, суттєво підвищувати інформованість лікарів щодо новітніх ефективних медичних технологій, радикально впливати на швидкість отримання та якість даних про стан здоров'я пацієнта, методи лікування, забезпечувати медичні заходи профілактичного і просвітницького характеру. Саме таке інформаційне середовище створить необхідні передумови для подальшого реформування системи охорони здоров'я, покращення стану здоров'я

населення та підвищення ефективності лікувально-діагностичного процесу і профілактичних заходів.

Література:

1. Підаєв А.В., Возіанов О.Ф., Москаленко В.Ф., Пономаренко В.М. та інші Панорама охорони здоров'я України – К.: Здоров'я, 2003. – 396 с.
2. Підаєв А.В., Пономаренко В.М., Вороненко Ю.В. Інформаційні технології в системі охорони здоров'я. – К.: Здоров'я, 2003 –335 с.
3. Крамаренко В.І. Менеджмент: Навчальний посібник. – К.: ЦУМ, 2000. – 248 с.
4. Хміль Ф.І. Основи менеджменту: Підручник – К.: Академвидав, 2003. – 608 с.

Селіна Дар'я Юріївна

Державний Університет Телекомунікацій

*Науково-навчальний інститут менеджменту та підприємництва
м.Київ*

НЕДОСТАТНІЙ РЕГУЛЯРНИЙ ВПЛИВ ДЕРЖАВИ НА РИНОК ТЕЛЕКОМУНІКАЦІЙ

Телекомунікації в Україні — є найсучаснішим, різноманітним і швидко зростаючим сектором економіки України. Державне регулювання у сфері телекомунікацій в Україні здійснює державний колегіальний орган НКРЗІ (з листопада 2011 року).

Український ринок телекомунікаційних послуг характеризується стійкістю ринкових позицій ключових операторів, стабільним попитом на послуги, а також високою конкуренцією в сегменті суміжних продуктів. Згідно з даними в 2011 році зростання ринку телекомунікацій склав 6% і перевищив зростання економіки в цілому.

Основні тенденції ринку телекомунікацій в Україні: зростання числа споживачів в сегменті послуг широкосмугового доступу в Інтернет на 25,9% в 2011 році, що обумовлено підвищенням активності операторів і впровадженням нових телекомунікаційних технологій; збільшення доходів операторів мобільного зв'язку обумовлено, перш за все, зростанням обсягів надання послуг широкосмугового доступу в інтернет, а також надання додаткових сервісів; скорочення доходів від надання послуг фіксованого міжміського та міжнародного в зв'язку з розвитком конкуренції з боку мобільного зв'язку і ринку інтернет телекомунікацій; розширення абонентської бази шляхом просування різноманітних пакетів послуг і тарифних планів.

Однією з ключових умов економічного зростання країни є подальший розвиток інформаційнокомунікаційних технологій (ІКТ). Міжнародний досвід говорить про їх вагомий вплив на ринки, організації, конкурентні стратегії, інновації, фінансові та інші послуги, працевлаштування, освіту, регіональний розвиток тощо. Тобто вони стосуються практично всіх сторін діяльності людини та функціонування суспільства. Крім того, телекомунікації – один з ключових секторів економіки України, оскільки майже 20% усього обсягу наданих у країні послуг реалізуються у процесі діяльності її операторів і провайдерів. За 2011 р. доходи від надання послуг у цій сфері збільшилися на 6% і дорівнювали 46,2

млрд. грн. Лідером протягом останніх років є мобільний зв'язок, питома вага якого в загальному обсягу телекомунікаційних послуг у 2011 р. становила 67,1%.

Аналіз тенденцій розвитку телекомунікаційної сфери свідчить про те, що існує низка чинників, які і в подальшому можуть негативно позначатися на темпах зростання цього важливого сектору господарського комплексу країни. Підґрунтям для таких висновків слугують декілька обставин.

По-перше, це уповільнення темпів зростання доходів від найбільш високо технологічних сегментів телекомунікаційного ринку – мобільного та широко смугового (комп'ютерного) зв'язку, спільна частка яких у загальних доходах від надання телекомунікаційних послуг, за підсумками 2011 р., становила 79,3%. Досягнутий в Україні рівень щільності мобільного зв'язку, який перебуває на рівні розвинутих країн (де мобільних телефонів значно більше, ніж населення), дозволяє зробити висновок про певне насичення ринку стільникового зв'язку та подальше зменшення темпів зростання цього сегмента ринку, який сьогодні визначає обсяги й динаміку доходів від надання послуг зв'язку в Україні. Уповільнення зростання доходів стосується також послуг широкосмугового доступу до мережі Інтернет, який є найбільш динамічним і конкурентним сегментом ринку телекомунікацій. Доходи від цих послуг у 2009 р. (порівняно з 2008 р.) виросли на 39,2%, у 2010 р. (порівняно з 2009 р.) – на 26,1%, у 2011 р. (порівняно з 2010 р.) – лише на 12,1%³. Крім того, подальшій динаміці в цьому сегменті ринку телекомунікаційних послуг заважає відносно низька забезпеченість населення персональними комп'ютерами. Рівень платоспроможності значної частки населення України не дозволяє в найближчій перспективі з оптимізмом дивитися на суттєве його підвищення і, як наслідок, на відчутний вплив комп'ютерного зв'язку на темпи зростання доходів у телекомунікаційній сфері.

По-друге, це тенденція до постійного зменшення доходу телекомунікаційних операторів у розрахунку на одного абонента мобільного та широкосмугового (комп'ютерного) зв'язку. Так, за 2003–2011 рр. він знизився з 841,5 до 557,5 грн. Це пов'язано з підвищенням рівня конкуренції (і, як наслідок, зі зниженням тарифів для користувачів послуг), зміною структури споживачів за рахунок скорочення частки корпоративних абонентів і збільшення загальної кількості користувачів шляхом залучення менш заможних верств населення. Про зниження за значеного доходу операторів свідчить те, що споживачів у 2011 р. (порівняно з 2010 р.) стало більше на 25,9%, а доходів – лише на 12,1%.

Таким чином, існуюча тенденція в телекомунікаційній сфері характеризується гальмуванням темпів її розвитку, що загрожує можливою стагнацією цієї важливої інфраструктурної складової економіки України. Тому є потреба в розробці та реалізації ефективних заходів, спрямованих на усунення або зниження негативних наслідків тих тенденцій, які заважають цій сфері.

Література:

1. «Державне регулювання розвитку телекомунікаційної сфери України» - [Електронний ресурс] - http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/EkUk_2012_10_5.pdf

***Григоренко Олександр Олександрович**
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ*

ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ В УКРАЇНІ

На сьогодні питанням розвитку сфери телекомунікацій приділяється особлива увага як з боку державних органів так і приватного сектору. У зв'язку з цим на перший план виходять питання здійснення ефективного управління сферою телекомунікацій для забезпечення сучасних умов та темпів розбудови як окремих складових так і інформаційного суспільства в цілому.

У сфері телекомунікацій основним законодавчим актом, який регламентує, в тому числі і питання державного управління та їх напрями, є Закон України «Про телекомунікації». Положеннями даного Закону визначено, що ухвалення державної політики та законодавче забезпечення державного управління і регулювання у сфері телекомунікацій здійснює Верховна Рада України. А державне управління у сфері телекомунікацій здійснюють Кабінет Міністрів України та центральний орган виконавчої влади в галузі зв'язку. Крім того, положеннями даного Закону визначено повноваження КМУ та центрального органу виконавчої влади в галузі зв'язку (далі - ЦОВЗ).

До основних повноважень ЦОВЗ слід віднести наступні:

- розробка пропозицій щодо державної політики у сфері телекомунікацій і реалізація її у межах своїх повноважень;
- впровадження технічної політики у сфері надання телекомунікаційних послуг, стандартизації, підтвердження відповідності технічних засобів телекомунікацій;
- розробка прогнозів розвитку телекомунікаційних мереж та послуг;
- організація наукового забезпечення функціонування і розвитку сфери телекомунікацій;
- інформування суб'єктів ринку телекомунікацій про політику та стратегію розвитку телекомунікаційних мереж загального користування.

Крім того, розвиток та вдосконалення телекомунікаційних мереж загального користування України здійснюється відповідно до Концепції розвитку телекомунікацій України. Також даним законом визначено головну мету даної Концепції, яка полягає в гармонійному та динамічному розвитку телекомунікаційних мереж на всій території країни, насамперед у регіонах з недостатнім рівнем насиченості місцевих мереж загального користування.

З одного боку сфера телекомунікацій показує позитивну динаміку розвитку та доходів. З іншого боку розвиваються тільки ті сегменти сфери телекомунікацій, які комерційно вигідні операторам та провайдерам телекомунікацій. Тобто рівномірного розвитку телекомунікацій по всій території країни не відбувається. Тому залишається значна частина населення, яка не може їх отримати.

Аналіз статистичних даних вказує на низькі темпи росту доходів операторів телекомунікацій, що може бути пояснено декількома основними причинами, а саме. По-перше, активний розвиток мереж припинився і оператори не розвивають свої мережі в бік малонаселених територій із низької прибутковості мереж в зазначених регіонах. По-друге, населення досягло піку необхідного об'єму для нього телекомунікаційних послуг існуючої якості. По-третє, оператори телекомунікацій з різних причин не в змозі розширити перелік послуг, що надаються або суттєво підвищити якість надання існуючих телекомунікаційних послуг. По-четверте, державна тарифна політика на загальнодоступні послуги направлена на підвищення тарифів при різкому зниженні тарифів операторів телекомунікацій на інші телекомунікаційні послуги, що призводить до міграції населення між мережами. Деякі з зазначених причин мають своє коріння в недосконалості державного регулювання усунення яких і повинно стати пріоритетним напрямком удосконалення державної політики у сфері телекомунікацій.

За останні роки не вдалося досягти такого рівня організації виконавчої влади, коли б її суб'єкти створили функціонально достатню та структурно несуперечливу систему. Враховуючи вищевказане пропонуємо шляхи вдосконалення за напрямками:

- по інституційним змінам (повернення до виділення окремого органу державного управління (наприклад – Державної служби зв'язку) підвищить ефективність здійснення управлінських заходів в сфері телекомунікацій; це дасть можливість здійснювати моніторинг та управління всього спектру питань і напрямів в сфері телекомунікацій).
- по законодавчій та нормативній базі (необхідно внести певні корективи відносно розширення інструментарію здійснення державного управління).
- ресурсна база (матеріально-технічна, фінансова, людські ресурси: участь держави та приватного сектору в забезпеченні необхідною ресурсною базою у вирішенні проблемних питань в сфері телекомунікацій, а також для можливості розбудови телекомунікаційної сфери, як складової інформаційно-комунікаційних технологій)
- галузева наука (необхідно зберегти існуючі наукові та науково-дослідні установ).

Література:

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : закон України від 09.01.2007 № 537-V / Відомості Верховної Ради України від 23.03.2007 - 2007 р., № 12, стор. 511, стаття 102.
2. Сайт НКРЗІ. [Електронний ресурс]. - Режим доступу: <http://www.nkrz.gov.ua/uk/1360082595>.

3. Про телекомунікації : закон України від 18.11.2003 № 1280-IV / Відомості Верховної Ради України від 19.03.2004 - 2004 р., № 12, стаття 155.
4. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Указ Президента України від 30 червня 2011 року № 717/2011 / Офіційний вісник Президента України від 19.07.2011 -2011 р., № 21, стор. 4, стаття 878.

Григоренко Олександр Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

ЕЛЕКТРОННИЙ БІЗНЕС

У даній роботі ми розглянемо: Електронний бізнес. Стрімкий розвиток електронного обміну даними та глобальної мережі Інтернет радикально змінюють способи здійснення зовнішніх торгових операцій. Компаніям електронний простір пропонує новий

- інструмент маркетингу та середовище для ведення бізнесу, засіб
- зниження витрат на комунікації з клієнтами. Останні, в свою чергу,
- отримали нове інформаційне джерело про товари та послуги, нові шляхи
- задоволення своїх потреб, а також новий ефективний засіб комунікації,
- як з виробниками, так і між собою.

Електронний бізнес – це вид економічної діяльності компаній через комп'ютерні мережі, зокрема, Internet, з метою отримання прибутку. Це електронна економічна діяльність.

Електронний бізнес ґрунтується на таких важливих технологіях:

- мережні технології;
- корпоративні;
- Інтернет-технології;
- виробничі ІТ;
- система підтримки ухвалення рішень.

Література:

1. Федішин І.Б. Електронний бізнес та електронна комерція (опорний конспект лекцій для магістрів спеціальності 8.18010012 «Управління інноваційною діяльністю») / І.Б. Федішин. – Тернопіль, ТНТУ імені Івана Пулюя, 2016. – 155 с.
2. Електронна комерція, Платіжні системи - Пиріг С.О. Бібліотека українських підручників
3. «Видавництво «Центр учбової літератури» Київ – 2012

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-ПОСЛУГ У СІЛЬСЬКІЙ МІСЦЕВОСТІ

Теперішнє суспільство як ніколи розуміє важливість побудови сучасного інформаційного суспільства, де в кожного громадянина буде доступ до світових інформаційних ресурсів. Саме в стратегії сталого розвитку «Україна -2020» зазначено, що головною ціллю подальшого розвитку держави є її вихід на першорядні позиції у світі через здійснення ряду реформ, направлених на підвищення ефективності діяльності всіх секторів економіки та соціальної політики держави в напрямку євроінтеграції.

Головним показником який визначає рівень розвитку Інтернет-послуг в країні є рівень доступності жителів всіх населених пунктів до сучасних телекомунікаційних послуг. Ці послуги в сучасному суспільстві є надзвичайно важливими для виконання функцій державного управління, а також потреб підприємств, організацій та населення.

Надання доступних та якісних послуг зв'язку у сільській місцевості має важливе значення, бо саме телекомунікації є одним з основних чинників життєзабезпечення населення. Сільські райони в Україні потребують швидкого розвитку телекомунікаційних мереж, бо деякі села ще досі знаходяться фактично відрізнаними від зовнішнього світу. Лише 26 % мешканців сільської місцевості мають постійний доступ до мережі Інтернет. Подальший розвиток телекомунікаційної сфери на селі стримується за рахунок цілої низки проблем, які пов'язані з кризовим становищем економіки, складними політичними умовами, зниження обсягу зовнішнього і внутрішнього фінансування та доходів верств населення.

Велику кількість робіт вітчизняних авторів, а саме: П.П. Воробієнка, В.М. Орлова, В.М. Гранатурова, Г.А. Отливанської, С.В. Зяблова присвячено дослідженню проблем формування послуг зв'язку. Але питання по визначенню соціально-економічної ефективності впровадження Інтернет-послуг в сільській місцевості, привертають увагу незначної кількості вчених, тому дослідження є дещо фрагментарними. На даний час існують проблеми, які потребують подальшого розгляду. До них можна віднести:

- проблема цифрового розриву, яка пов'язана з нерівномірним розподілом сучасних технологій по території України;
- недоліки тарифної політики операторів, що пропонують свої послуги в селах. Ціни в селах на послуги можуть бути вищими ніж у містах більше чим в 4 рази;
- недосконалість законодавчої та нормативно-правової бази в сфері телекомунікацій, більшість законодавчих документів не відповідають стану теперішньої ринкової економіки, так і державної політики;
- недостатність кількості висококваліфікованих фахівців які можуть компетентно працювати з обладнанням та зменшення їхньої кількості у зв'язку

з постійною еміграцією. Це все спричиняє зменшення кількості інновацій, науково-дослідних та дослідно- конструкторських робіт;

- нестабільну економічну і політичну ситуацію в країні, що сприяє збільшенню рівня інфляції та безробіття, зменшенню споживання послуг зв'язку [1].

Судячи з вищенаведених проблем можна сказати, що операторам може бути не рентабельно розвивати сільський зв'язок з новітніми телекомунікаційними послугами, а тим більш його модернізувати. З точки зору всього суспільства розвивати телекомунікаційні послуги вкрай необхідно, тим більше що Україна підписала Туніську Декларацію та заявила про необхідність ліквідації цифрового розриву для побудови інформаційного суспільства. Якщо враховувати інтегральний соціально- економічний ефект [2; 3], то впровадження сучасних телекомунікаційних послуг з необхідною якістю може бути рентабельним навіть для оператора з урахуванням окремих пільг для нього від місцевої влади. Отже обов'язковою умовою розвитку соціальної інфраструктури села є оновлення і розширення мереж телекомунікацій. Якісний телефонний зв'язок у сфері матеріального виробництва сприяє економії часу, дозволяє поліпшити використання сільськогосподарської техніки та оперативне маневрування нею з урахуванням погодних умов, зменшити її простої і прискорити ремонт, забезпечити своєчасні постачання та заготівлі сільськогосподарської продукції.

Література:

1. Економіка телекомунікацій [Текст] : навч. посіб. [для студентів вищих навчальних закладів] ; за заг. ред. В.М. Орлова. – О. : ОНАЗ ім. О.С. Попова, 2014. – 512 с.
2. Кузнєцова О.В. Соціальна ефективність підприємства: сутність та визначення / О.В. Кузнєцова // Науковий вісник Одеського національного економічного університету. – Науки: економіка, політологія, історія. – 2015. – № 1(221). – С. 53-67.
3. Кузнєцова О.В. Щодо сутності економічної ефективності / О.В. Кузнєцова // Розвиток методів управління та господарювання на транспорті : зб. наук. праць. – Вип. 4(49). – Одеса : ОНМУ, 2014. – С. 178-189.

Козій Катерина Андріївна

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

РЕГУЛЮВАННЯ РИНКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ: МІЖНАРОДНИЙ ДОСВІД

Розглянуто роль телекомунікацій в забезпеченні економічного зростання держав на сучасному етапі постіндустріального розвитку. Досліджено міжнародний досвід формування регуляторної політики щодо телекомунікаційної галузі. Обґрунтовано пропозиції оптимізації заходів державного впливу на ринок телекомунікаційних послуг України.

Глобалізація економічного життя та зростаюча роль технологічних інновацій суттєво підвищили роль інформації як одного з ключових факторів забезпечення конкурентоспроможності в сучасній економіці. Телекомунікації стали

інтегральною частиною бізнесу та забезпечують внутрішні та міжнародні потоки інформації в процесі прийняття ділових рішень. Обсяг інформації, що передається завдяки інформаційно-телекомунікаційній структурі, подвоюється кожні 2-3 роки, що посилює значення телекомунікацій як на рівні компаній, так і в цілому в економіці світу, що в свою чергу підсилює процеси глобалізації.

Розвиток нових технологій вніс істотні корективи в хід розвитку людства. Лідерство країни на міжнародній арені останнім часом починає усе більшою мірою визначатися вже не тільки наявністю природних ресурсів, рівнем розвитку сільського господарства і промисловості, а й якісними і кількісними показниками сконцентрованих у її національній економіці інформаційних потоків.

Інформаційні ресурси країни, регіону, організації сьогодні є стратегічними і мають не менше значення, ніж запаси сировини, енергії, копалин та інших ресурсів. Інформація в сучасному суспільстві являє собою найважливіший фактор економічного зростання. Отже, сучасний етап розвитку економічних систем, стан яких прийнято називати «ною економікою», неможливо розглядати без телекомунікаційного сектору, що є основним знаряддям управління інформаційними потоками сучасного суспільства й основою економіки в її сучасному розумінні.

Об'єктивні процеси розвитку економічної системи призвели до того, що останнім часом в Україні приділяється все більше уваги сектору телекомунікацій, що сьогодні є основою нової економіки на Заході й одним із найперспективніших і швидко зростаючих сегментів вітчизняної економіки.

Розвиток сучасних економічних систем має місце в умовах постійної активізації процесів глобалізації. Масштаб, характер, структура, якісні і кількісні параметри включення національних економічних систем у ці процеси сьогодні вже асоціюються з об'єктивними показниками розвитку сучасних держав, ключовими детермінантами їхнього майбутнього.

З урахуванням виняткової ролі інформації у визначенні перспектив розвитку держави, очевидно є потреба в ефективному регулюванні сфери інформаційно-телекомунікаційного сектору країни задля його подальшого розвитку та зростання. Особливо важливою є ситуація для України.

Дослідженню проблем регулювання інноваційного розвитку в національних економіках як в Україні, так і за кордоном, присвячене широке коло робіт В.Андрійчука, М.Гонака, Б.Данілішина, М.Долішнього, Ю.Макогона, Е.Саведбева, О.Чмир, М. Чумаченка., І.Дюмулена, В. Шумілова. Серед іноземних авторів особливої уваги заслуговують роботи таких авторів як Дж. Д. Браун, К. Чанг, П. Коухи, Д. Джерадін, Д. Лафф, К. Кoenіг, А. Ньюманн, К. Жанг.

Разом з тим, у більшості випадків розглянуті дослідження не фокусують увагу на особливостях секторального регулювання ринку України на прикладі телекомунікаційної галузі. Значною мірою це викликано новизною проблематики, покладеної в основу даної статті. З кожним роком, починаючи з кінця XX століття, інформаційно-комунікаційна складова національних

економік кардинально змінюється, - збільшуючись, вона набуває суттєвішої значущості та впливу у всебічному розвитку держави.

Слід також зазначити виняткову *актуальність* дослідження питань, пов'язаних з процесами регулювання ринку телекомунікацій і тісно пов'язаної з цим проблематики інформаційного наповнення сучасного соціуму.

Сказане вище свідчить про актуальність дослідження питань регулювання національного та міжнародного ринків телекомунікацій, так і розробки рекомендацій практичного плану, спрямованих на забезпечення прискореного зростання ринку телекомунікаційних послуг України, дослідивши методи регулювання іноземних ринків телекомунікацій.

Мета та задачі дослідження. Метою статті є дослідження міжнародного досвіду в регулюванні ринків телекомунікаційних послуг, а також розробка на цій основі практичних рекомендацій зі створення моделі регулювання даного ринку для України.

Досягнення поставленої мети здійснювалось через постановку і вирішення наступних завдань:

- визначити особливості моделей регулювання ринків телекомунікаційних послуг в розвинутих країнах та тих, що розвиваються;
- провести аналіз переваг та недоліків в регулюванні ринків телекомунікацій в країнах з різним рівнем економічного розвитку;
- визначити особливості регулювання вітчизняного ринку телекомунікацій та надати рекомендації щодо подолання неефективних заходів регулювання в Україні.

Основна частина: В процесі економічного розвитку активне використання телекомунікаційних технологій забезпечує перехід до так званого інформаційного суспільства, коли інформація стає найважливішим економічним ресурсом. Тому активний розвиток телекомунікацій сьогодні являється необхідною умовою економічного прогресу та досягнення розвитку постіндустріального суспільства в країнах з перехідною економікою. На сьогодні у більшості країн телекомунікації розвиваються випереджаючими темпами відносно економіки в цілому, частково вирівнюючи коливання ВВП та збільшуючись скоріше за стадії сукупного розвитку багатьох країн.

Кінець XX – початок XXI ст. став часом стрімких технологічних змін в телекомунікаційній галузі. Виробники та оператори запропонували користувачам безліч нових послуг та устроїв. Більшість технологічних інновацій виявились задіяними населенням, корпораціями та державами. Таким чином, неймовірний технологічний прорив з боку пропозиції відповідав стрімкому зростанню попиту на традиційні та нові послуги, що дозволило ринку телекомунікаційних послуг зрости в декілька разів за останні 15 років, збільшивши свою частку як в ВВП в цілому, так і в послугах. Слід зазначити, що основна частина приросту попиту на телекомунікаційні послуги була забезпечена населенням.

Важливу роль у розвитку інформаційно-комунікаційних технологіях (ІКТ) відіграє регулювання галузі. Перш за все, стрімкий розвиток технологій стирає

межі між телекомунікаціями та інформаційними технологіями (ІТ), у зв'язку з чим сьогодні ці 2 галузі все частіше розглядаються та регулюються як одна єдина. Технологічний розвиток ІКТ вимушує постійно коректувати діюче регулятивне середовище, формує новітні підходи до створення найкращих умов розвитку галузі в контексті постійних технологічних інновацій.

Література:

1. Мировой рынок телекоммуникаций: современные тенденции, стратегии и перспективы развития [Текст]: монография / О.Б. Аникин. – М.: ГУУ, 2009. – 170 с.
2. Держкомстат України [Електронний ресурс]. – Режим доступу: <http://www.ukrstat.gov.ua>
3. European Business Association [Електронний ресурс]. – Режим доступу: http://af.attachmail.ru/cgi-bin/readmsg/eba_fta_position_paper_ukr.txt?rid=3002490474&&id=12773133200000000948;0;1&mode=attachment&channel=
4. Гава Ю. Роль сучасних технологій в економіці// Економіст. – 2006. - №6. – с.61 – 63

Козій Катерина Андріївна

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

АКТУАЛІЗАЦІЯ МЕХАНІЗМІВ СПРИЯННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Сучасний світ стрімко розвивається в телекомунікаційній галузі і створюються нові системи управління засновані на інтелектуальних технологіях, які використовують способи подання знань для побудови соціально-економічного розвитку телекомунікацій. Необхідним є детальний аналіз ринку телекомунікаційних послуг з метою визначення позицій підприємств, виявлення проблем функціонування та розроблення заходів їх подолання. Проблеми які виникають під час піднесення на більший високий щабель розвитку галузі телекомунікацій характеризуються високою невизначеністю і динамікою бізнес-середовища, існуванням великої кількості взаємозв'язків і залежностей між учасниками телекомунікаційного ринку і т. д., що зумовлює враховувати різні фактори впливу під час прийняття рішень.

Активний розвиток ринкових відносин у телекомунікаційній галузі зумовлює необхідність розроблення нових підходів до управління підприємствами. При цьому значна увага приділяється стратегічному аспекту управління, який включає формування, реалізацію та аналіз стратегії на підприємствах цієї галузі.

Враховуючи особливості телекомунікаційної галузі телекомунікаційне середовище потрібно визначити, як сукупність структур та об'єктів, які беруть участь в інформаційно-комунікаційному процесі в суспільстві. Воно повинно адекватно відповідати потребам споживачів, сприяти раціональній організації й забезпечувати ефективне управління інформаційними потоками для задоволення потреб населення, суб'єктів господарювання і суспільства в цілому.

Останнім часом прослідковується тенденція залежності об'ємів виробництва від потужності інформаційно-телекомунікаційних технологій. Так, однієї із найважливіших проблем соціально-економічного розвитку телекомунікацій на сьогоднішній час є неефективне управління, контроль

діяльності підприємств та система правил взаємовідносин між зацікавленими особами. Зміни мають відбутися для того, щоб забезпечити повну зайнятість населення та повний обсяг виробництва шляхом абсолютного економічного та соціального зростання діяльності підприємств у сфері інформатизації та телекомунікації.

Розвиток підприємств телекомунікаційної галузі має розглядатися, як система суспільних зв'язків, яка дозволить розвивати відносини на новому рівні взаємодії і сформувати для телекомунікаційної компанії сприятливіше середовище ведення бізнесу.

Однією із причин невисокого місця України в телекомунікаційній галузі є нерівномірність доступу до телекомунікаційних послуг в регіонах, що підтверджують результати аналізу стану розвитку інформаційно-комунікаційної інфраструктури та впровадження послуг телекомунікацій в різні сфери життєдіяльності регіонів.

Таким чином, на даний час виникла необхідність запровадження механізмів сприяння підвищенню рівня використання телекомунікацій в країні та актуалізації завдань суттєвого підвищення дієвої координації зусиль держави щодо розробки та реалізації стратегії розвитку цієї галузі.

Сьогодні можемо констатувати, що телекомунікації є матеріально-технологічною основою виникнення та розвитку інформаційного суспільства, що обумовлює значимість соціально-економічного розвитку об'єктивного нормативно-правового упорядкування цієї сфери.

Література:

1. Гриценко А. Методологічні основи модернізації України / А.Гриценко // Економіка України. – 2011. – № 2. – С. 4 - 12.
2. Інноваційні підходи до регіонального розвитку в Україні / С.О. Біла, Я.А. Жаліло, В.І. Жук та ін. К.: НІСД, 2011. – 47 с.
3. Маркетингова інформація: підручник / Є.В. Крикавський, О.В. Дейнега, І.О. Дейнега. — Львів: Видавництво Львівської політехніки, 2014. – 416 с.
4. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене) / Довгий С.О., Воробієнко П.П., Гуляєв К.Д. – К.: «Азімут-Україна». – 2013. – 608 с.

Шарій Тимофій Олегович

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ В УКРАЇНІ

Сфера телекомунікацій є однією з важливих складових інфраструктури національної економіки. У сучасних умовах господарювання забезпечення сталого розвитку телекомунікацій є найважливішою передумовою у розбудові конкурентоспроможної ринкової економіки та інтеграції України у глобальне інформаційне суспільство.

Економічні перетворення, що здійснюються в Україні, спрямовані на посилення економічних методів управління та формування умов для повноцінного функціонування ринкових відносин, одне з найактуальніших завдань економічної науки і практики полягає у вивченні суті, структури й методологічних принципів наявного господарського механізму управління, а також у його моделюванні й на цих засадах – подальшому вдосконаленні.

Нині особливого значення набуває галузь зв'язку, справляючи величезний вплив на соціально – економічний розвиток суспільства, що переходить від індустріальної до інформаційної фази свого розвитку. Інформація дедалі більше стає повноправним учасником виробничих процесів і вирішальним чинником науково – технічного й соціального прогресу.

Розвиток соціально – економічних систем привів до того, що людина дістала можливості формування в новому соціумі. Вона стає соціально – активним, суспільним суб'єктом – особою зі своїм психологічним складом, дієздатністю і роллю в суспільстві. В цих умовах важливе місце в житті людини, в її соціальній діяльності займає зв'язок. Він (зв'язок) не лише перестає бути галуззю економіки країни в системі суспільного розподілу праці, організаційних і економічних відносин, але й є безпосередньо включеним в органіку людини.

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.

Однак, розвиток телекомунікаційної сфери стримується за рахунок низки проблем, які виникають унаслідок науково-технічного прогресу, кризового становища економіки, зниження обсягу інвестування та доходів верств населення тощо. Термін «проблема» нині набув широкого поширення як у практичній, так і в науковій діяльності. Згідно із [1], проблема – це складне питання, розв'язання якого має важливе практичне або теоретичне значення, але цьому розв'язанню перешкоджає відсутність загальноприйнятих методів. У широкому сенсі проблема розглядається як складне теоретичне або практичне питання, яке вимагає вивчення, дозволу. У науці під проблемою розуміється суперечлива ситуація, що виступає як протилежні позиції в поясненні будь-яких явищ, об'єктів і потребує адекватної теорії її вирішення. Під проблемою також розглядається наявність істотної розбіжності між бажаним і фактичним станом системи, як концентроване вираження протиріч, що виникають у процесі суспільного розвитку, форму їх проявлення у господарській діяльності для соціально-економічних проблем.

Як перше, так і наступні розуміння «проблеми» не суперечать один одному і відображають головні сутнісні сторони: складність і протиріччя. В умовах телекомунікаційної сфери необхідно виділити виробничий, науково-технічний, організаційно економічний, соціальний та екологічний аспекти протиріч, які і формують відповідні проблеми. У зв'язку з цим слід розуміти поняття проблеми як концентроване вираження виробничих, науково-технічних, економічних та

соціальних протиріч, що носять складний характер і вимагають свого вирішення [2].

Проведення розбудови телекомунікаційної сфери не може бути здійснено без аналізу проблем і протиріч накопичених і знов виникаючих в старих системах управління. Тому стає таке завдання як створити таку систему управління, яка буде підготовлена до вирішення наявних проблем і протиріч. У роботі не представляється можливим розкрити весь перелік питань, пов'язаних з вирішенням усіх наявних проблем у сфері телекомунікацій. Для аналізу розглянемо лише деякий перелік протиріч, наявних в області задоволення послуг зв'язку, які носять різний характер. До них можна віднести: - проблему цифрового розриву, яка пов'язана з недостатньо рівномірним розповсюдженням сучасних технологій; - недоліки тарифної політики, у зв'язку з чим виникають проблеми зі взаєморозрахунками між телекомунікаційними підприємствами та споживачами послуг зв'язку, що спричиняє конфлікти, а, як наслідок, підвищуються тарифи на телекомунікаційні послуги. Крім того, існує проблема із забезпеченістю населення універсальними послугами зв'язку; - фізичний та моральний знос обладнання, що спричиняє погіршення якості послуг зв'язку; - недосконалість стратегії розвитку телекомунікаційної сфери, тобто відсутність єдиної збалансованої стратегії розвитку та планування у телекомунікаційній сфері; - недосконалість нормативно-правової та законодавчої бази, немає узгодженості між нормативно- правовим документами, крім того більшість законодавчих документів не відповідають стану як ринкової економіки, так і державної політики; - складність отримання та використання обчислювальних ресурсів за рахунок їхньої нерозвиненості; - недостатність кількості висококваліфікованих фахівців та зменшення їхньої кількості у зв'язку з постійною еміграцією, що сприяє зменшенню кількості інноваційних, науково-дослідних та дослідно- конструкторських робіт; - відсутність механізму підтримки вітчизняного виробника, що спричиняє неможливість забезпечити себе продукцією власного виробництва; - нестабільну економічну і політичну ситуацію в країні, що сприяє збільшенню рівня інфляції та безробіття, зменшенню споживання послуг зв'язку [3].

Найважливішою передумовою є розв'язання соціально економічних проблем щодо вирівнювання рівнів розвитку телекомунікацій у міській та сільській місцевості.

Таким чином, можна визначити, що розвиток телекомунікацій має величезну роль у загальному економічному розвитку країни, то як урядовим, так і неурядовим організаціям необхідно вжити ще більших заходів щодо сприяння розвитку саме цієї галузі. Недостатній розвиток телекомунікацій загрожує конкурентоздатності економіки України та перспективам її розвитку.

Література:

1. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – М. : Инфра-М, 1996. – 493 с.
2. Кузьминов А.В. Проблемы и противоречия в управлении электросвязью региона и пути их разрешения / А.В. Кузьминов // Спеціалізований випуск матеріалів конференції «Проблеми управління та економічного розвитку підприємств зв'язку – Економіка'99» : збірник наукових праць. – О. : УДАЗ ім. О.С. Попова, 1999. – 98 с.

Шарій Тимофей Олегович
Государственный университет телекоммуникаций
Научно-учебный институт менеджмента и предпринимательства
г. Киев

ПЕРСПЕКТИВЫ РАЗВИТИЯ УКРАИНСКИХ ИТ- ПРЕДПРИЯТИЙ

Америка открывает для себя украинский ИТ-бизнес. Так можно сформулировать главные результаты бизнес-форума SeattleTechDays, который организовал ИТ-комитет Европейской Бизнес Ассоциации (ЕВА). В ходе мероприятия своим опытом, достижениями и прогнозами относительно развития ИТ-сектора поделились топ-менеджеры AOL, GlobalLogic, Google, KPMG, Luxoft, Microsoft, SigmaSoftware, Ciklum и ряда других компаний.

ИТ-сектор в Украине — одна из самых динамично развивающихся сфер бизнеса. Темпы его роста превышают показатели других отраслей экономики. В 2012 году вклад ИТ в экономику страны был на уровне доли в 0,8% от общего объема ВВП. В 2015 году показатель достиг уровня в 3% ВВП. При этом ожидается устойчивый рост этого сектора и в будущем. ИТ сейчас занимает третье место по вкладу в ВВП страны после металлургии и агросектора и конкурирует с экспортом химических материалов — такие данные озвучила Елена Минич, директор департамента инноваций и интеллектуальной собственности Министерства экономического развития и торговли Украины. По ее словам, ежегодно ИТ-сектор в стране растет на 25%, а за последние 10 лет он вырос в 10 раз.

Основной продукт украинского ИТ-сектора — это разработка программного обеспечения на заказ. Согласно опросам топ-менеджеров ведущих ИТ-компаний Украины, рост экспортной ИТ-индустрии составил 9% по результатам 2015 года. Основной риск, который видят партнеры из-за рубежа, — политическая и экономическая нестабильность из-за событий на востоке страны.

По оценкам ведущих ИТ-ассоциаций, в том числе и ИТ-комитета ЕВА, объем услуг, предоставленных украинскими разработчиками зарубежным компаниям, достиг в 2015 году \$2,3 млрд.

"ИТ-индустрия Украины может быть конкурентоспособной во многих сегментах и нишах одновременно в контексте глобального роста хай-тек, идет ли речь о создании продуктов либо о предоставлении сервисов. Важно выдерживать проверенную формулу — предоставлять лучший товар — качественный и инновационный. Украина может его создать благодаря своему основному конкурентному преимуществу — человеческому капиталу, квалифицированным ИТ-специалистам, способным вести творческую деятельность и создавать

инновации, двигать новую экономику вперед", — поясняет Владимир Бек, Глава ИТ-комитета ЕВА.

По словам Виталия Нужного, управляющего директора по Восточной Европе компании LuxoftUkraine, при благоприятных условиях для развития отрасли до 2020 года можно ожидать трехкратный рост ИТ-отрасли в Украине — до \$7 млрд. К 2020 году доля ИТ-сектора в ВВП страны может достигнуть 5,7%. Количество рабочих мест только в ИТ-секторе до 2020 года может составить 180 тыс. человек, при этом более 400 тыс. рабочих мест будут созданы в других секторах экономики. По данным ассоциации NASSCOM, объединяющей более тысячи ИТ-компаний Индии, один новый ИТ-специалист создает до четырех дополнительных рабочих мест в смежных отраслях. Это соотношение работает и для Украины.

Украина — один из лидеров в списке стран, наиболее привлекательных в мире для заказа разработки программного обеспечения. По результатам 2015 года Украина заняла 24-е место в глобальном рейтинге самых привлекательных стран для разработки ИТ-решений (GlobalServicesLocationIndex). У нашей страны есть целый ряд преимуществ для развития индустрии по разработке программного обеспечения на экспорт.

Основными заказчиками услуг украинских ИТ-компаний являются компании из США и Европы. Основными конкурентами Украинской ИТ-индустрии является Польша и Румыния. Поэтому в последнее время ИТ-отрасль Украины очень озабочена вопросом формирования своего имиджа за границей.

Одной из успешных инициатив по популяризации бренда Украины как флагмана ИТ-аутсорсинга и одного из европейских и мировых ИТ-центров стал бизнес-форум SeattleTechDays. Целью мероприятия, организованного Европейской Бизнес Ассоциацией в городе Сиэтл (США) 25 августа 2016 года, стало более тесное знакомство американского и мирового бизнес-сообщества с Украиной и украинским ИТ-сектором.

Выбор места можно объяснить тем, что Сиэтл готовится стать второй Кремниевой Долиной. В этом регионе активно открывают офисы крупнейшие ИТ-компании, в том числе Amazon, Boeing, Costco, Expedia, Microsoft, T-mobile. За первый квартал 2016 года ВВП штата Вашингтон, в котором расположен Сиэтл, вырос почти на 4%, при этом рост в 1% был достигнут за счет ИТ-сектора — такие данные на форуме SeattleTechDays озвучил Джозеф Вильямс, руководитель департамента экономики штата Вашингтон, США.

Благодаря таким мероприятиям у украинского ИТ-бизнеса есть возможность продемонстрировать свои компетенции, познакомиться с потенциальными заказчиками и бизнес-партнерами.

"Такие мероприятия по продвижению бренда Украины за рубежом, как SeattleTechDays, являются одним из инструментов, с помощью которых мы имеем возможность привлекать в страну еще более масштабные и более интересные проекты. Это мотивирует людей работать в Украине и создавать интеллектуальный продукт не выезжая из страны", — говорит Владимир Бек.

На SeattleTechDays много говорили о потенциале Украины как технологического центра Восточной Европы. Несмотря на ряд сложностей (макроэкономическая нестабильность, отсутствие системы фискальной поддержки, отток специалистов из страны), рост ИТ-рынка в ближайшие годы не вызывает сомнений.

Ежегодно Украина готовит около 15 тысяч ИТ-специалистов. Мощный образовательный потенциал государства обеспечивается выпускниками, обладающими уникальными знаниями и узкой специализацией. "Если к этому добавить низкую стоимость жизни и ведения бизнеса в Восточной Европе, можно получить набор выгод для американских компаний, которые будут заинтересованы передавать разработку высокотехнологичных проектов в Украину", — так на SeattleTechDays оценил потенциал Украины Патрик Коркоран, директор по внешним связям и работе с аналитиками компании Luxoft.

Брэд Белл, генеральный менеджер по облачным технологиям и инфраструктуре в Microsoft, считает, что одним из преимуществ Украины должно стать наличие лидеров, которые смогут управлять глобальными командами, члены которых работают в разных часовых поясах: "ИТ-компании должны уметь привлекать специалистов из разных географических регионов. Но если люди не привыкли работать удаленно, они вряд ли смогут в полной мере выразить себя в современной среде, им трудно будет быть продуктивными. Для меня, например, не имеет значения, где вы живете. До тех пор, пока у нас есть контракт и отлаженная система взаимодействия, позволяющая добиться результата".

Література:

1. Искусство управления ИТ-проектами, 2-е изд. Автор: С. Беркун

2. ИТ-инфраструктура Автор: Олейник А.И., Сизов А.В.

3. 10 мифов об ИТ-секторе Украины. Автор: Всеволод Некрасов

Шарій Тимофій Олегович

Державний університет телекомунікацій

Навчально-науковий інститут менеджменту та підприємництва

м. Київ

РОЗВИТОК СУЧАСНИХ ПОСЛУГ

Найбільша частина в обсязі послуг припадає на телефонний зв'язок, яким охоплено близько 13,1 млн. абонентів. Телефонна щільність зараз становить близько 26,4 телефони на 100 мешканців, що перевищує середні показники країн з аналогічним економічним рівнем, однак в 3 рази менша, ніж в розвинутих країнах. Загальні результати розвитку галузі телекомунікацій незалежної України можна охарактеризувати таким чином[7]: -з'явився і досяг насичення на рівні 55,3 млн. активованих SIM-карт новий вид телекомунікацій – рухомий (мобільний)

радіозв'язок; -з'явився і в останні роки почав швидко розвиватися новий вид телекомунікаційних послуг – доступ до інформаційно-комунікаційних послуг Інтернету; кількість швидкісних підключень до Інтернету досягла 2,1 млн, а кількість користувачів Інтернету біля –10,5 млн. -кількість абонентів мережі фіксованого телефонного зв'язку зросла у 1,8 разу – до 13,1 млн; -міжміський і міжнародний трафік зріс майже у 17 разів (до 11,1 млрд телефонних переговорів на рік [7]).

Для об'єктивної оцінки стану розвитку інфокомунікацій(ІКТ) в Україні використовуємо методи,що застосовують міжнародні організації(ITU,WEF) і методики їх оцінок. Це індекси NRI [12] та IDI [11] Визнаним в світі є метод рейтингу окремих країн за значеннями узагальненого показника (індексу). Зміна цього індексу у часі та зміна місця країни у переліку країн за значенням індексу, і є оцінкою успіхів окремої країни. Питома вага показників галузі телекомунікацій в індексі IDI(ІCT Development Indeks) становить біля 70%.Він введений ITU,охоплює 11 показників і дозволяє оцінити прогрес ІКТ. Оцінка розвитку різних країн світу за індексом NRI(Networked Readiness Indeks) ведеться з 2002 року. У першому звіті WEF(Всесвітній економічний форум), в якому була застосована методика NRI, за 2002-2003 роки було зібрано і проаналізовано показники розвитку ІКТ-сфери 82-х країн світу.

Для України тоді індекс NRI склав 2,98 і вона тоді зайняла 70-те місце у рейтингу за значенням NRI. Перше місце у цьому рейтингу посіла Фінляндія з NRI=5,92. У звіті WEF за 2006-2007 роки ІКТ-сферу України оцінено вже значенням NRI=3,46 і вона зайняла 75 місце з 122-х країн світу. Перше місце діталось Данії з NRI=5,71. У останньому звіті WEF за 2008-2009 роки 283 Україна отримала оцінку NRI=3,88 і зайняла 62-ге місце у рейтингу серед 134 країни світу.

Перше місце зайняла Данія з NRI=5,85 [7]. Ціновий кошик ІКТ.Фахівцями ITU показники цінової доступності ІКТ- послуг спеціально не були включені як складові до індексу IDI, оскільки цінова доступність ІКТ є дуже важливою оцінкою ІКТ-сфери і, крім того, більш складною у оцінюванні характеристикою. Тому для неї в звіті [26] введено спеціальний вимірюваний показник цінової доступності ІКТ-послуг – “ціновий кошик ІКТ” (ЦК_ІКТ).

В цьому показнику комбіновано враховано тарифи на послуги фіксованої та мобільної телефонії і послуги фіксованого швидкісного підключення до Інтернету (ШПІ). Значний розвиток отримали радіотехнології, особливо в частині цифрового мобільного зв'язку. Системою мобільного зв'язку охоплено територію, де проживає близько 95% населення України. Початок будівництва мереж мобільного зв'язку третього та четвертого поколінь і початок перебудови центральних частин ТТМ за принципами NGN, які спостерігаються в Україні означає початок ери NGN в телекомунікаційній галузі. Варто зауважити, що високі техніко-економічні характеристики сучасних засобів телекомунікацій та нездорова конкуренція призвели до масового неефективного будівництва паралельних телекомунікаційних мереж.

Потужним зовнішнім фактором впливу на розвиток телекомунікацій України є використання зарубіжного досвіду масового впровадження новітніх засобів телекомунікацій та пов'язане з цим зменшення витрат на будівництво і розвиток телекомунікаційних мереж України. Оператори телекомунікацій України, відстаючи на 4-5 років відносно операторів розвинутих країн, впроваджують на мережах засоби, що вже пройшли масову комерційну апробацію в розвинутих країнах. Відставання України з впровадження нових засобів телекомунікацій добре видно при порівнянні ходу розвитку сучасних видів зв'язку (мобільного та швидкісного доступу до Інтернету) для розвинутих європейських країн і України (рис.3).[7].

Наукове видання

«СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЙ»

Збірник матеріалів

V Міжнародної науково-технічної конференції студентства та молоді

Київ, 07 грудня 2017 року

Редагування: Бондаренко Є.О.

Відповідальні за випуск: Бондаренко Є.О.

Подано до друку 06.12.17

Формат 60x84. Папір друкарський. Гарнітура «Time New Roman».

Державний університет телекомунікацій
вул. Солом'янська, 7, м. Київ, 03110, Україна



Контакти

dut.edu.ua

lsd.dut.edu.ua

