Державний університет телекомунікацій
Київський національний університет імені Тараса Шевченка
Національний авіаційний університет
Військовий інститут телекомунікацій та інформатизації
Національний університет "Львівська політехніка"
Вінницький Національний університет
Національна академія оборони України
Академія Служби безпеки України
Інститут спеціального зв'язку та захисту інформації

Науково-технічна конференція
«Актуальні проблеми забезпечення інформаційної безпеки держави»

ЗБІРНИК
матеріалів науково-технічної конференції студентів, аспірантів, викладачів та науковців

18 грудня 2014 року

УДК 351.86:104.056

Актуальні проблеми забезпечення інформаційної безпеки держави:
Матеріали науково-технічної конференції студентів, аспірантів, викладачів та науковців: 18 грудня 2014 року. – Київ: Державний університет телекомунікацій, - 2014. – 132с.

Рекомендовано до друку рішенням Вченої ради
Навчально-наукового інституту захисту інформації
Державного університету телекомунікацій
(протокол № 5 від 23 грудня 2014 року)

к.п.н. Шевченко С.М., к.т.н., доцент Жданова Ю.Д.
Державний університет телекомунікацій

Основні аспекти технології ADSL як прогресивної технології передачі інформації

В доповіді обґрунтовано доцільність використання технології ADSL в сучасних системах передачі даних та встановлено актуальність використання кодування DMT на сучасному етапі розвитку технології.

ADSL – модемна технологія, що перетворює аналогові сигнали, які передаються за допомогою стандартної телефонної лінії, в цифрові сигнали (пакети даних), дозволяючи під час роботи здійснювати дзвінки. ADSL є технологією, яка дозволяє перетворити виту пару телефонних проводів у тракт високошвидкісної передачі даних. Саме це дозволяє здійснювати передачу текстової та графічної інформації, роботу з базами даних, передачу рухомого зображення та голосу, та інші додатки, використовуючи існуючу кабельну інфраструктуру, яка складається з мідних кабелів.

Технологія ADSL використовує метод розділення смуги пропускання мідної телефонної лінії на декілька частотних смуг. Це дає можливість одночасно передавати декілька сигналів по одній телефонній лінії.

Переваги ADSL перед іншими технологіями:

1. Висока швидкість отримання інформації (до 8 Мбіт/с).
2. Висока стабільність швидкості – кожен абонент має свою гарантовану смугу пропускання і ні з ким не розділяє її.
3. Надійний цілодобовий зв’язок.
4. Низька вартість робіт по переведенню звичайної аналогової телефонної лінії в ADSL.
5. Більш низькі вимоги до якості лінії зв’язку.
6. Низька вартість обслуговування лінії зв’язку, порівняно з вартістю обслуговування звичайної аналогової телефонної лінії.
7. Безпека даних, які передаються.

У пристроях технології ADSL існують 2 основних лінійні коди – це CAP (Carrierless Amplitude Phase) та DMT (Discrete Multi Tone), які відрізняються один від одного лише реалізацією. В технології ADSL використовується метод DMT, оскільки недоліком для застосування методу CAP є відсутність стандартизуючого документа, що визначає процедури, у відповідності з якими виконується перетворення сигналу. Вказаний метод лінійного кодування найбільш адаптований до умов лінії та забезпечує високу швидкість та надійність технології ADSL. Технологія DMT являє собою багатоканальний модем або пристрій, який працює за принципом частотного розділення каналів.

Наявність значних переваг технології ADSL, а саме висока швидкість та надійність передачі даних, легкість у впровадженні та застосуванні, низька вартість впровадження та обслуговування, а також наявність підґрунтя для вдосконалення та розвитку технології зумовлюють її популярність та активне втілення в життя.

Отже, на основі проведених досліджень можна зробити висновок про доцільність використання технології ADSL. Проведені дослідження дозволяють здійснювати подальший аналіз та вдосконалення технологій, особливо для безпеки країни, що є актуальним на сучасному етапі.

Левковець Г. С.
Державний університет телекомунікацій

Законодавчі аспекти управління інформаційною безпекою передачі закритої інформації по відкритим каналам

Нормативно-правовий захист інформації являється таким собі фундаментом побудови всієї інформаційної безпеки підприємства, організації, установи. В Україні основним Законом являється Конституція. В інформаційній сфері регламентуючими діяльність законами є:

- ЗАКОН УКРАЇНИ Про інформацію;
- ЗАКОН УКРАЇНИ Про державну таємницю;
- ЗАКОН УКРАЇНИ Про Державну службу спеціального зв’язку та захисту інформації України;
- ЗАКОН УКРАЇНИ Про телекомунікації;
- ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомунікаційних системах.

Взагалі, нормативно-правове забезпечення інформаційної сфери потребує суттєвого удосконалення. Одним з напрямків удосконалення системи інформаційного законодавства України може стати розроблення та ухвалення Інформаційного кодексу України, що дозволить розв'язати проблему подолання протиріч у законодавчих та нормативно-правових актах, забезпечити єдність та нефрагментованість нормативно-правового поля.

В інформаційній сфері, є його неконкретність, певна розмитість формулювань. Фактично відсутні визначення конкретних механізмів оприлюднення інформації, конкретних документів, що мають публікуватися. Не встановлюються терміни цієї діяльності, майже відсутні норми прямої дії щодо фінансового та кадрового забезпеченн

Довгаль А. В.
Державний університет телекомунікацій

Забезпечення інформаційної безпеки України

Під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави.

Інженерно-технічний захист - це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації.

За функціональним призначенням засоби інженерно-технічного захисту поділяються на такі групи:

• фізичні засоби, що включають різні об‘єкти і споруди, що перешкоджають фізичній проникненню (або доступу) зловмисників у місця захисту і до матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних дій. До фізичних засобів належать механічні, електромеханічні електронні, електронно-оптичні, радіо- та радіотехнічні та інші пристрої для заборона несанкціонованого доступу (входу виходу) пронесення (виносу) засобів і матеріалів та інших можливих видів злочинних дій;

• апаратні засоби. Сюди входять прилади, пристрої, пристосування та інші технічні рішення, використовувані в інтересах захисту інформації. У практиці діяльності підприємства знаходить широке застосування сама різна апаратура, починаючи з телефонного апарату до створених автоматизованих систем, що забезпечують виробничу діяльність. Основне завдання апаратних засобів - забезпечення стійкої захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності;

• програмні засоби, що охоплюють спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки (збирання, накопичення, зберігання, обробки і передачі) даних;

• криптографічні засоби - це спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по системам і мережам зв'язку, зберігається та обробляється на ЕОМ з використанням різноманітних методів шифрування.

Таким чином, система забезпечення інформаційної безпеки України включає в себе систему засобів, які забезпечують реалізацію державної політики в інформаційній сфері. Система таких засобів має працювати незалежно від внутрішньополітичної кон'юнктури в Україні та стану окремих елементів системи забезпечення інформаційної безпеки. Системним, інтегруючим чинником для діяльності цих засобів має бути спільна мета - забезпечення інформаційного суверенітету України.

к.в.н. Аносов А. О.
Державний університет телекомунікацій

МЕТОДИКИ АНАЛІЗУ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ

В доповіді показана актуальність теми дослідження, яка полягає у необхідності визначення захищеності інформаційно-телекомунікаційної системи (ІТС) центру сертифікації ключів (ЦСК), від несанкціонованого доступу. Зараз такі методики розробляються безпосередньо для аналізу вразливостей відповідного ІТС ЦСК, при цьому, кожен експерт, що працює в даній сфері, створює свої методики, що приводить до розбіжностей у підходах та зменшення ефективності оцінки вразливостей системи захисту ІТС ЦСК. Створення універсальної методики для аналізу вразливостей в ІТС ЦСК, що базується на міжнародних стандартах, дозволить вирішити питання критичності даної вразливості та терміновості її усунення. Новизна методики полягає у створені її на основі моделі загроз існуючих вразливостей ІТС ЦСК, що базуються на сімействі стандартів X.509 та дозволить структурувати можливі вразливості програмного забезпечення ІТС.

к.фіз-мат.н. Лукова-Чуйко Н.В.
КНУ ім.Т.Г. Шевченка

МЕТОДИ ОЦІНКИ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАСТОСУВАННЯ FUZZY-ТЕХНОЛОГІЙ

В доповіді запропоновано варіант застосування Fuzzy-технологій, що є реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ), які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використані теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу, задач з самих різних областей. Теорія нечітких мір, нечіткої логіки або FuzzyLogic- новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу - ведення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі.

к.т.н. Одіяненко О.В.
Державний університет телекомунікацій

ОБГРУНТУВАННЯ ВИБОРУ РАЦІОНАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ІНЦЕДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

В доповіді розглянуто методи вибору раціональної системи управляння інцидентами інформаційної безпеки та проведені приклади проблем управляння інцидентами ІБ, таких як: складнощі управляння інцидентами інформаційної безпеки, проблеми визначення інциденту, реєстрації інцидентів, усунення наслідків і причин інциденту, розслідування інциденту. Проведено відомі рішення цих проблем. Розглянуто основні стандарти які пов'язані із управлінням безпекою, у тому числі, міжнародний стандарт ISO 27001:2005 рекомендації його безпосередньо відносяться до процедур управляння інцидентами. Виходячи з цього, запропоновано дії щодо вибору системи управляння інцидентами інформаційної безпеки.

к.т.н., доцент Гулак Г.М.,к.т.н., доцент Жданова Ю.Д.
Державний університет телекомунікацій

КРИПТОГРАФИЧНО СТІЙКИ ГЕНЕРАТОРИ ПВЧ

Доповідь присвячена питанням генерації ключової інформації для симетрич- них криптосистем. Розглядаються особливості застосування та методика оцінки якості булевих функцій щодо побудови криптографічно стійких комбінуючих генераторів псевдовипадкових чисел. Як основні критерії щодо якості булевої функції використовуються критерії розповсюдження помилок, кореляційної імунності та лінійна складність комбінуючого генератора. Відповідні генератори ПВЧ доцільно використовувати для генерації первинної послідовності яка підлягає перешифруванню з метою отримання сеансових ключів, а також для побудови секретних параметрів криптопротоколів.

к.п.н. Шевченко С.М., Кисіль О.В.
Державний університет телекомунікацій

РОЗРОБКА КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ДОМАШНЬОЇ МЕРЕЖІ

В доповіді розглянуті особливості побудови та захисту домашніх мереж, у тому числі мереж типу "Розумний дім". Зроблено аналіз апаратних та програмних засобів захисту інформації, яка зберігаються на мережевих пристроях, та способів шифрування при її передачі. Розглядаються способи налаштування домашньої Wi-Fi мережі, тунелю довіреної VPN, обмеження доступу по MAC адресам, налаштуванню доступу до папок та встановленню мережевих екранів. Представлено методологію тестування на вразливості мережі за допомогою додаткового програмного забезпечення. Розроблені рекомендацій щодо створення комплексу засобів захисту домашніх мережах та налаштування його підсистем та засобів захисту.

к.т.н. Коршун Н.В., к.т.н. Одіяненко О.В.
Державний університет телекомунікацій

СЕРВІС ЧАСОВИХ МІТОК І АВТЕНТИФІКАЦІЯ ПОВІДОМЛЕНЬ

У доповіді розглядається випадок, за якого автентифікація повідомлення зводиться до автентифікаціїї його джерела. У зв'язку з цим, за стандартом X. 509 в інфрастуктурі відкритих ключів передбачено механізму міток часу. Мітка часу дозволяє визначити момент підписання повідомлення та перевірити легітимність ключової пари на відповідний момент. У більшості реалізацій цього сервісу для синхронізації момету пред'явлення повідомлення з еталоном використовують центр випуску міток часу (Time-Stamping Authority - TSA). Для одержання інформації про час TSA звертається до сервісу часу за захищеним протоколом. Поле (структура) даних мітки часу TSTinfo підписується приватним ключем TSA. У доповіді відмічено можливість побудови аналогічного сервісу для організації системи надання дозволів щодо моменту відправки або розшифрування повідомлень у корпоративних мережах.

к.п.н. Шевченко С.М., Березюк А.С.
Державний університет телекомунікацій

ЗАСТОСУВАННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ КЕРУВАННІ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У докладі розглянуто завдання підтримки прийняття рішень під час інцидетіві інформаційної безпеки (ІБ) в організаційно-технічних системах (ОТС), яке можна розглядати як частину більш загальної проблеми підтримки прийнятня управлінських рішень у кризових ситуаціях. У ході вирішення даного завдання визначено головні чинники,

критерії і показники автоматизованих процедур підтримки прийняття рішень щодо керування інцидентами ІБ. Організація процесу керування інцидентами ІБ без використання засобів автоматизації являє собою складне й трудомістке завдання. Розробку формалізованої методики підтримки прийняття рішень щодо керування інцидентами ІБ ускладнює ряд особливостей, про які йдеться мова в даній статті. Однак все ж таки можна визначити загальні принципи, якими зможе користуватися розробник такого класу ІСППР. Першим кроком у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація та включення до SLA (Service Level Agreement) визначень класів інцидентів. Пропонується постійно осучаснювати як закони, методики, так і відповідні інститути в галузі керування інформаційними технологіями та ІБ. Запропоновано функціональну схему ІСППР щодо керування інцидентами ІБ в ОТС. Дана схема цілком вписується в модель PDCA та процесний підхід, визначений у відповідних міжнародних стандартах ISO/IEC.

к.фіз-мат.н. Лукова-Чуйко Н.В.
КНУ ім.Т.Г. Шевченка

ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ДЛЯ ФОРМАЛІЗАЦІЇ ЗАДАЧІ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

В доповіді запропоновано методику обґрунтування сукупності показників оцінки рівня захищеності інформації на основі комплексних систем захисту (КСЗІ), що дозволяє всебічно оцінити функціонування КСЗІ взагалі, її окремих елементів і складових на різних ієрархічних рівнях та їх вклад у загальний рівень захищеності. Наукова новизна полягає у застосуванні теорії нечітких множин для формалізації задачі оцінки рівня захищеності інформації КСЗІ, визначенні показників захищеності інформації складних та простих складових КСЗІ з використанням різнорідної, у тому числі нечіткої, вхідної інформації, що дає можливість інтегральної оцінки рівня захищеності інформації КСЗІ на об'єктах інформаційної діяльності. Достовірність розробленої методики забезпечується коректною постановкою задачі дослідження, обґрунтованим вибором основних допущень й обмежень, використанням адекватного науково-методичного апарату оцінки рівня захищеності інформації КСЗІ, узгодженням і відповідністю теоретичних положень і практичних даних дослідження

к.т.н., доцент Гулак Г.М.,. к.в.н. Аносов А. О
Державний університет телекомунікацій

НАПРЯМКИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИЩЕНОСТІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

В докладі обґрунтовано важливість і актуальність питань захисту інформації. Причини такої підвищеної уваги до цієї проблеми цілком очевидні - від якості заходів захисту інформації безпосередньо залежить економічна безпека організації. Банківська інформація завжди була об'єктом пильної уваги всякого роду зловмисників. У системі забезпечення безпеки банку захист інформації відіграє найбільш важливу роль. Тому доцільно проводити дослідження уразливості, загроз і ризиків типової платіжної системи і оцінити рівень її захищеності, удосконалення системи, що є безумовно актуальним в наш час. Запропоновано впровадження та використання комплексу засобів захисту в системах електронного платежу для банківських організацій, які представляють собою інформаційні системи, побудовані на основі клієнт-серверної архітектурі. Сформульовані основні підходи до побудови типового комплексу засобів захисту системи електронного переказу у цілому та детально обгрунтована необхідність впровадження в систему електронного переказу банку цифрового електронного підпису.

Власенко В.О.
Державний університет телекомунікацій, Київ

МЕХАНИЗМЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ IEEE 802.11

В докладе рассмотрены различные программные й криптографические механизми защити беспроводных сетей стандарта IEEE 802.11. Разработаны критерии, а также обоснованы методи и средства комплексного обеспечения безопасности в системах беспроводной широкополосной связи. В результате анализа составлены рекомендации по использованию конкретньх механизмов информационной безопасности для построения и оптимизации комплексной системы защити информации в сетах стандарта IEEE 802.11.

Хлебалова М.В.
Державний університет телекомунікацій

Проблематика криптографічних методів захисту інформації з відкритим ключем

Для вирішення задач розподілу ключів та ЕЦП (електронно-цифрового підпису) були використані ідеї асиметричного перетворення і відкритого розподілу ключів Діффі і Хеллмана. В результаті була створення криптосистема з відкритими ключами, в якій використовується не один секретний ключ, а пара ключів: відкритий (public) і секретний (private) ключі. Секретний ключ, або закритий, відомий тільки одній взаємодіючій стороні. В типовій схемі шифрування даних з використанням відкритого ключа перший етап складається із обміну по несекретному каналі відкритими ключами, другий – реалізації шифрування повідомлень, на якому відправник зашифровує повідомлення відкритим ключем отримувача. Зашифрований файл може бути прочитаним тільки власником секретного ключа, тобто отримувачем. Схема розшифрування, що реалізується отримувачем повідомлення, використовує для цього закритий ключ отримувача.

Використання відкритих ключів в асиметричних криптографічних системах пов'язане з проблемами захисту інформації, що передається. Наприклад, з проблемою забезпечення достовірності відкритих ключів та їх власників. Можливість підробки або нав'язування невірного відкритого ключа може призвести до порушення обміну конфіденційної інформації, а в деяких випадках до повного або часткового розкриття інформації. Загальноприйнятим механізмом перевірки істинності відкритих ключів є механізм електронних сертифікатів, які видаються центром сертифікації. Так як ЦС є довіреною особою, то він не розглядається в якості порушника. С іншого боку, існування довіреної особи в рамках конфіденційного обміну інформації може розглядатися як додатковий об'єкт для атак порушника, бо контроль над ЦС дозволяє порушникові підроблювати та модифікувати інформацію, що передається.

ЕЦП забезпечує захист від модифікації інформації і дозволяє встановити власника сертифікату відкритого ключа. Даний сертифікат видається користувачу ЦС, котрий завіряє його своєю ЕПЦ. Іншим аспектом використання асиметричних ключів є можливість підтвердити авторство відправника зашифрованого повідомлення.

Л.В. Пригорницька,
Державний університет телекомунікацій

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Світові процеси глобалізації, впровадження новітніх інформаційних технологій, формування інформаційного суспільства посилюють важливість такої складової національної безпеки, як інформаційна безпека.

Безпека завжди відносна і має динамічний характер. У кожний конкретний відрізок часу стан захищеності може мати різний рівень, що визначається гостротою внутрішніх та зовнішніх загроз і характером реагування на них управлінського апарату відкритої соціальної системи.

Наприклад, одним з найважливіших завдань інформаційної діяльності будь-якої країни є формування і підтримання її позитивного іміджу (образу) у світовому інформаційному полі. З цього погляду процес формування позитивного іміджу України у світі оцінюють як неефективний. По-перше, загальний обсяг інформації про Україну та її зовнішню політику незна-чний, неадекватний її потенціалу. Крім того, в деяких секторах світового інформацій-ного простору, (окремих регіонах планети, верствах світової громадськості, ділових колах тощо) такої інформації взагалі немає.По-друге, навіть наявна інформація значною мірою є застаріла і тенденційна.

Водночас, аналіз сучасного стану та тенденцій розвитку вітчизняного інформаційного простору свідчить, що рівень інформаційної безпеки України, за окремими показниками, наближається до критично низької межі, за якою — втрата демократичних принципів і норм, повернення до авторитаризму, міжнародна ізоляція України. Таке становище спричинене негативним впливом, перш за все, внутрішніх політичних чинників.

Сьогодні в Україні за умов недосконалої інформатизації суспільства зволікання з її вирішенням призводить до величезних збитків. Воно зумовлене відсутністю досвіду розв'язання питання щодо створення сучасного інформаційного простору в Україні та системи його захисту.

Стеблинський О. А.
Державного університету телекомунікацій

Дослідження механізмів інформаційної безпеки в системах широкосмугового зв'язку Wimax і Wi-Fi

1.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 чіпами ASIC, які убудовані в пристрої бездротового зв'язку й управляють процесом передачі даних радіоканалом, запобігаючи:

a) спробам порушення конфіденційності;
b) порушенню цілісності даних;
c) порушенню автентичності джерела – споживача;
d) відмови в обслуговуванні. [1, 11]

2. Для захисту мереж 802.11 передбачений комплекс заходів безпеки передачі даних

На ранньому етапі використання Wi-Fi мереж таким був пароль SSID (Server Set ID) для доступу в локальну мережу, але з часом виявилось, що дана технологія не може забезпечити надійний захист

Головним же захистом довгий час було використання цифрових ключів шифрування потоків даних за допомогою функції Wired Equivalent Privacy (WEP). Самі ключі вдають із себе звичайні паролі з довжиною від 5 до 13 символів ASCII. Дані шифруються ключем з розрядністю від 40 до 104 бітів. Але це не цілий ключ, а тільки його статична складова. Для посилення захисту застосовується так званий вектор ініціалізації Initialization Vector (IV), який призначений для рандомізації додаткової частини ключа, що забезпечує різні варіації шифру для різних пакетів даних. Даний вектор є 24-бітовим. Таким чином, в результаті ми отримуємо загальне шифрування з розрядністю від 64 (40+24) до 128 (104+24) бітів, в результаті при шифруванні ми оперуємо і постійними, і випадково підібраними символами. [2, 433

3. В кінці 2003 року був упроваджений стандарт Wi-Fi Protected Access (WPA), який суміщає переваги динамічного оновлення ключів IEEE 802.1X з кодуванням протоколу інтеграції тимчасового ключа TKIP, протоколом розширеної аутентифікації (EAP) і технологією перевірки цілісності повідомлень MIC.

MIC — технологія перевірки цілісності повідомлень (Message Integrity Check).

Стандарт TKIP використовує автоматично підібрані 128-бітові ключі, які створюються непередбачуваним способом і загальне число варіацій яких досягає 500 мільярдів. Складна ієрархічна система алгоритму підбору ключів і динамічна їх заміна через кожних 10 кбайт (10 тис. переданих пакетів) роблять систему максимально захищеною. [2, 487]

4. Сьогодні бездротову мережу вважають захищеною, якщо в ній функціонують три основних складових системи безпеки: аутентифікація користувача, конфіденційність і цілісність передачі даних. Для отримання достатнього рівня безпеки необхідно:

1) шифрувати дані шляхом використання різних систем. Максимальний рівень безпеки забезпечить застосування VPN;
2) використовувати протокол 802.1X;
3) заборонити доступ до налаштувань точки доступу за допомогою бездротового підключення;
4) управляти доступом клієнтів по MAC-адресам;
5) заборонити трансляцію в ефір ідентифікатора SSID;
6) розташовувати антени якнайдалі від вікон, зовнішніх стін будівлі, а також обмежувати потужність радіовипромінювання;
7) використовувати максимально довгі ключі;
8) змінювати статичні ключі і паролі;
9) використовувати метод WEP-аутентификации "Shared Key" оскільки клієнтові для входу в мережу необхідно буде знати WEP-ключ;
10) користуватися складним паролем для доступу до налаштувань точки доступу;
11) по можливості не використовувати в бездротових мережах протокол TCP/IP для організації папок, файлів і принтерів загального доступу.
12) не вирішувати гостьовий доступ до ресурсів загального доступу, використовувати довгі складні паролі;
13) не використовувати в бездротовій мережі DHCP. Вручну розподілити статичні IP-адреса між легітимними клієнтами безпечніше. [3, 52]

Частокол М.М.
Державний університет телекомунікацій

Захист від дистанційного впровадження комп'ютерних вірусів за допомогою ВЧ-нав'язування

В наш час дистанційне впровадження комп'ютерних вірусів за допомогою ВЧ-нав'язування не є актуальною загрозою, проте в майбутньому зможе наносити суттєвий збиток державним і комерційним структурам. Ідея загрози нав'язування полягає у формуванні направленого спеціального електромагнітного імпульсу з метою примусового дистанційного запису вірусної програми у пам'ять електронно обчислювальної машини. При цьому в пам'яті ожлива активізація вірусного коду безпосередньо як у момент його нав'язування, так і у будь який інший момент вибраний зловмисником, в такому випадку шкідливий код буде записано на жорсткий диск ПК. Пропонується можливі способи захисту інформації, яка циркулює в електронно обчислювальних машин.

До організаційних заходів можна віднести:
– збільшення радіусу контрольованої території навколо об'єкта електронно-обчислювальної техніки;
– навчання персоналу по знаходженню ознак впливу ВЧ-сигналів;
– здійснення контролю доступу до ліній зв'язку, терміналам, мережам електроживлення і іншим елементам мереж;
– розташування електронно-обчислювальної техніки в загублених приміщеннях.

До додаткових технічних мір відносять:
– створення і використання системи попередження про застосування «вірусної зброї» шляхом проведення постійного радіоконтролю на предмет виявлення сильних електромагнітних сигналів біля електронно обчислювальних машин;
– екранування персонального комп'ютера, з'єднання кабелів, іншого обладнання;
– установка фільтрів в ланцюгах електропостачання, управління і зв'язку.

Протидія можлива тільки спеціальними технічними засобами, які здатні не тільки вчасно виявити загрозу, але й протидіяти ним.

Підсумовуючи усе вище сказане слід сказати, що загрозі інформаційної безпеки при використанні ВЧ-нав'язування можливо протиставити відомі і відносно недорогі засоби захисту інформації

аспірант, Жебка В.В.
Державний університет телекомунікацій

До питання оптимізації системи управління мережею при наявності невизначених факторів

Дослідження та оптимізація телекомунікаційної мережі призводить до необхідності врахування двох факторів:

1. Наявність декількох критеріїв, які оцінюють якість функціонування системи.
2. Наявність завад, збурювань та іншого роду невизначеностей, про які відомі лише границі змін.

На етапі оптимізації системи управління мережею необхідно виконати багатокритеріальну оптимізацію мережі при наявності невизначених факторів. Тобто для оптимізації системи управління потрібно визначити не лише конкретні значення параметрів, які оптимізуються, а й вказати ті фактори, які залишаються невизначеними при оптимізації, але для яких відомі границі змін.

Причому, при такій оптимізації має бути можливість:

1. Визначити склад параметрів, які оптимізуються – вектор $x = (x_1,...,x_m) \in X$ (X – задана область їх змін).
2. Встановити склад невизначених факторів $y = (y_1,...,y_k)$, для яких відома лише область змін Y.
3. Виписати критерії $f_i(x,y)$, $i \in N$, які кількісно характеризують ефект, який досягається при фіксованому $x \in X$ і конкретному значенню $y \in Y$.

Задача оптимізації управління полягає у прийнятті найкращого рішення по управлінню мережею. Оптимізація полягає у знаходженні конкретного значення вектора $x \in X$, при якому досягаються можливо менші значення всіх компонентів вектор-функції виграшу $f(x,y) = (f_1(x,y),..., f_n(x,y))$, орієнтуючись при цьому на можливість реалізації будь-якого значення $y \in Y$. В даному випадку мається на увазі мінімізація функції $f_i(x,y)$, $i \in N$. Наявність невизначеного фактора y призводить до того, що неможливо однозначно визначити прийняття рішень.

До цього питання можна підходити з двох точок зору. По-перше, ми можемо розглянути питання прийняття рішення з точки зору теорії багатокритеріальних задач, враховуючи багатозначність критеріїв. По-друге, ми можемо розглянути питання з точки зору загальної теорії ігор, яка зумовлює наявність другого гравця, котрий вибором $y \in Y$ «максимально перешкоджає» діям першого гравця. В цьому випадку ми приходимо до антагоністичної гри з вектор-функцією виграшу.

Проведені дослідження дозволяють здійснювати подальше вдосконалення процесу оптимізації системи управління телекомунікаційною мережею в умовах невизначеності, що є особливо актуальним для забезпечення інформаційної безпеки держави на сучасному етапі.

к.т.н. Труш О.В., Годієнко Д.О., Онопрієнко М.А.
Державний університет телекомунікацій

ЦІЛІСНІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасні інформаційно-телекомунікаційні системи спеціального призначення є орієнтованими, в першу чергу, на обробку інформації з обмеженим доступом, яка є власністю держави. Відповідно до вимог законодавства для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації в таких ІТС повинна створюватися система захисту інформації (СЗІ), як невід'ємна їх складова. СЗІ являє собою складну організаційно-технічну, економічну й інформаційну систему, і, як правило, складається з організаційних та інженерних заходів, фізичних засобів захисту, комплексу технічного захисту інформації (ТЗІ) та комплексу засобів захисту від несанкціонованого доступу.

Метою технічного захисту інформації є запобігання витоку технічними каналами або порушення *цілісності інформації* з обмеженим доступом. Аналіз наукових праць та публікацій, присвячених забезпеченню ефективного захисту інформації свідчить про те, що підвищення безпеки інформації в ІТС СП можливе лише при *комплексному підході до аналізу можливих загроз й удосконалення засобів захисту від них*.

Загрозами будемо називати шляхи реалізацій дій, які вважаються небезпечними з погляду забезпечення захищеності інформації. Таким чином, загроза – це потенційно можливий несприятливий вплив на інформацію, що призводить до порушення конфіденційності, цілісності, доступності інформації, відмови в обслуговуванні тощо.

Оцінка ефективності функціонування СЗІ можлива на підставі аналізу узагальненої моделі її взаємодії з навколишнім середовищем. Причому узагальнена модель повинна відображати процес захисту інформації як взаємодію дестабілізуючих факторів і засобів захисту.

В даний час широко використовується узагальнена ймовірнісна модель процесу захисту інформації,

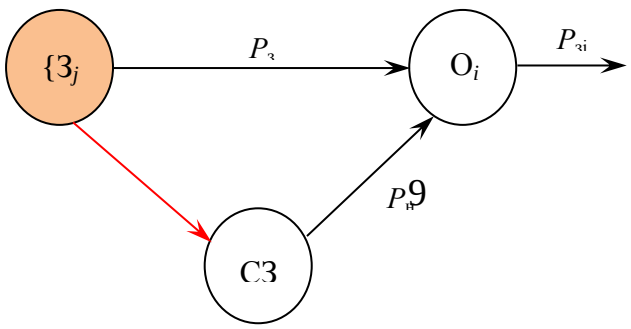


Рис. 1. Узагальнена модель процесу захисту

представлена на рис. 1. У відповідності до неї обробка інформації на об'єкті O_i здійснюється в умовах впливу на інформацію різних загроз $\{З_j\}$. Для забезпечення інформаційної безпеки об'єкту СЗІ повинна здійснювати нейтралізуючий вплив на дестабілізуючі фактори та загрози. Ймовірність ефективного захисту інформації від *j*-ї загрози $P_{зij}$ можна визначити наступним чином:

$$P_{зij} = 1 - P_{зj}(1 - P_{нj}),$$

де $P_{зj}$ – ймовірність впливу *j*-ї загрози на *i*-й об'єкт, $P_{нj}$ – ймовірність нейтралізації впливу *j*-ї загрози. Тоді загальну ефективність СЗІ $P_{сзі}$ (ймовірність захисту інформації від усіх можливих загроз *n*) запишемо, як

$$P_{сзі} = \prod_{j=1}^{n} P_{зij}.$$

Тому метою роботи є аналіз можливих загроз цілісності інформації в ІТС СП та визначення методів захисту від них. Цілісність забезпечується шляхом дотримання вимог політики безпеки по переміщенню інформації від відправника до отримувача. Під повнотою захисту при обміні, варто розуміти врахування багатьох можливих типів загроз, від яких забезпечується захист.

Серед способів захисту від порушень цілісності можна виділити наступні:

- введення надмірності в саму інформацію (використання коригувальних кодів);
- введення надмірності в процес обробки інформації (використання процедури аутентифікації);
- введення системної надмірності (підвищення живучості системи).

Загрози, які спрямовані на індивідуальні повідомлення, передані в ІТС. Типовим об'єктом нападу може служити інформаційний обмін між двома користувачами системи.

Застосовують наступні основні методи підвищення енергетичної і структурної прихованості системи передачі:

1. робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення необхідної якості зв'язку, використання радіосистем з адаптацією за потужністю випромінювання;
2. використання оптимальних способів приймання сигналів і пристроїв захисту (подавлення) від навмисних завад;
3. використання складних шумоподібних сигналів з великою базою. Такі сигнали, на відміну від простих, мають більш високу завадостійкість і прихованість, а отже і ефективність при забезпеченні цілісності переданої інформації;
4. використання частотно-адаптивних ліній зв'язку.

Таким чином, проведений аналіз дозволяє зробити наступні висновки.

В інформаційно-телекомунікаційних системах спеціального призначення основними загрозами канальній цілісності інформації є перехоплення, несанкціоноване відтворення інформації, маскування, маніпуляції даними та радіоелектронне подавлення.

Для захисту від порушень цілісності інформації необхідно застосовувати введення надмірності в саму інформацію, у процес її обробки, а також введення системної надмірності.

Поряд з криптографічними методами захисту інформації як один з основних напрямків забезпечення цілісності інформації в інформаційно-телекомунікаційних системах спеціального призначення заслуговує на увагу застосування методів підвищення прихованості зв'язку. Серед цих методів особливе місце займають шумоподібні сигнали, що дозволяють одночасно підвищити достовірність і прихованість передачі інформації. Застосування в інформаційно-телекомунікаційних системах спеціального призначення шумоподібних сигналів та інших методів забезпечення прихованості передачі сигналів дозволить підвищити рівень захищеності інформації від порушень цілісності та інших загроз.

ЛІТЕРАТУРА

1. *Закон України* „Про захист інформації в інформаційно-телекомунікаційних системах".

2. *Постанова КМ України* № 373 від 26.03.2006 „Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

3 *Антонюк А. Загрози інформації* і канали витоку / А. Антонюк, В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 2. – С. 42–46.

4. *Домарев В. В.* Безопасность информационных технологий. Системний поход / В. В. Домарев. – К.: ООО „ТИД" „ДС", 2004. – 992 с.

5. *Поповский В. В.* Защита информации в телекоммуникационных системах: Учебник/ В. В. Поповский, А. В. Персиков. – Х.: ООО „Компания СМИТ", 2006. – 238 с.

Доцент к.т.н. Лазаренко С.В.,
студентка групи СЗД-41 Цигак В.В.
Державний університет телекомунікацій

Проблеми виявлення атак на захищені об'єкти інформаційної діяльності за допомогою лазерних мікрофонів.

У цій статті проаналізовані атаки на захищенні об'єкти інформаційної діяльності з використанням лазерних мікрофонів та проблеми їх виявлення.

Актуальність теми: Атаки на об’єкти інформаційної діяльності з використанням лазерних мікрофонів це великий крок в світі інформаційного шпигунства. Лазерний промінь направлений на вікно є невидимим і його неможливо виявити без спеціальної апаратури та неможливо відстежити його джерело. Також, він дає змогу порушникам здійснювати несанкціонований доступ до інформації на відстані.

Основний матеріал. Лазерний мікрофон це - прилад прихованого спостереження, що використовує лазерний промінь для того, щоб фіксувати звукові коливання в віддалених об’єктах. Лазерний передавач, промінь якого знаходиться в інфрачервоному спектрі і невидимий неозброєним оком, необхідно направити на вікно приміщення,

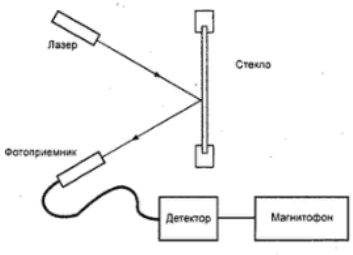


Рис. 1 в якому передбачається здійснення акустичного спостереження.

Частина випромінюваного лазерного променя відбивається віконним склом. Приймаючий вузол захоплює відбитий лазерний промінь і перетворює його в електричні сигнали, які, після їх фільтрації, посилюються і подаються в навушники і/або на звукозаписну апаратуру (рис.1).

Сучасне обладнання дозволяє зробити такий прилад самостійно в домашніх умовах.

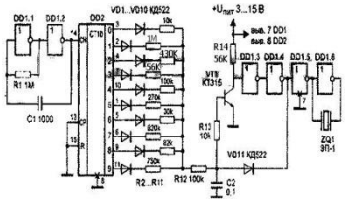
Для більш фінансованих злочинців такий прилад можливо купити в різних видах та комплектації.

Наприклад система розвідки SIPE LASER 3-DA SUPER може знімати інформацію з достатньою чутливістю на відстані до 450 м.

Лазерний мікрофон для акустичного спостереження модель AA79107, містить передавач та приймач в одному корпусі і може працювати від джерела живлення (батарейки) до 50 годин при вазі 1.6 кг., та може вести акустичне спостереження
до 250 м.

Такі прилади неможливо виявити неозброєним оком, тому для їх виявлення або боротьби з ними використовуються спеціальні пристрої.

Найпростішим методом боротьби з лазером є подавлювач лазерного мікрофона з вібрацією (рис. 2):
Також використовуються генератори шуму різних типів і характеристик.



Висновки: Використання апаратури захисту інформації в оптико-електронних каналах має перспективу внаслідок простоти і дешевизни відомих методів та способів захисту
Рис. 2 інформації.

Використання лазерних систем в технічному плані не має серйозних перешкод (крім вартості), і в найближчому майбутньому вони стануть звичайним засобом несанкціонованого отримання мовної інформації не тільки спецслужб.

Глєбова О.І., ст. викладач.
Державний університет телекомунікацій

СУЧАСНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Україна прагне до продуктивного міжнародного співробітництва в інформаційній сфері, враховуючи досвід найрозвинутіших країн (США, Канади, Японії, Німеччини, Франції, Англії). Йдеться про підтримання динамічної конкуренції, забезпечення відкритого доступу до інформаційно-телекомунікаційних систем та універсального доступу до інформаційних продуктів і послуг.

Водночас, аналіз сучасного стану та тенденцій розвитку вітчизняного інформаційного простору свідчить, що рівень інформаційної безпеки України, за окремими показниками, наближається до критично низької межі, за якою втрата демократичних принципів і норм, повернення до авторитаризму, міжнародна ізоляція України. Таке становище спричинене негативним впливом, перш за все, внутрішніх політичних чинників.

Забезпечення свободи слова, відкритість органів державної влади для громадського контролю є необхідними передумовами побудови в Україні громадянського суспільства, підвищення ролі засобів масової інформації, політичних партій, громадських організацій, які створюють надійну систему зворотних зв'язків між владою і громадянами.

Інформація є важливим і необхідним підґрунтям для інтенсивного розвитку економіки; сфери, в яких використовуються сучасні інформаційні технології, стають все більш прибутковими.

Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати: політичну й економічну роль окремих держав на світовій арені; поділ країн за інформаційною ознакою; процеси демократизації та подолання наслідків тоталітаризму в самій Україні. Це зумовлено наступними чинниками.

Лише наявність оперативної і достовірної інформації дає можливість органам державної влади приймати виважені та адекватні рішення; інформаційне забезпечення внутрішньої і зовнішньої політики держави створює передумови для її підтримки громадянами, сприяє формуванню об'єктивного іміджу України в світі.

Життєву важливість для суспільства і держави в сучасних умовах глобального інформаційного протистояння реалізації вимог статті 17 Конституції України, що забезпечення інформаційної безпеки відноситься до основних функцій держави і є справою всього Українського народу.

Відсутність ефективної державної політики з питань забезпечення інформаційної безпеки та потребу розвитку національної системи державних і недержавних суб'єктів забезпечення інформаційної безпеки, оптимізації їх завдань, функцій і повноважень.

Основою забезпечення інформаційної безпеки держави є :

– свобода збирання, зберігання, використання та поширення інформації, достовірність, повнота та неупередженість інформації;

– можливість задіяння в інтересах інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки;

– верховенство права;

– пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері;

– своєчасність і адекватність заходів захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці;

– обмеження доступу до інформації виключно на підставі закону;

– гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки;

– пріоритетність розвитку національних інформаційних технологій, ресурсів, продукції і послуг;

– гармонізація інформаційного законодавства з правовими актами Європейського Союзу та нормами міжнародного права.

В інформаційній сфері України вирізняються такі *життєво важливі інтереси:*

людини і громадянина:

– недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;

– забезпечення конституційних прав і свобод людини і громадянина на збирання, зберігання, використання та поширення інформації; права на спілкування мовою походження;

– захищеність від негативного інформаційно-психологічного впливу;

суспільства:

– інформаційне забезпечення суспільно-політичної стабільності, міжетнічної і міжконфесійної злагоди та розвитку громадянського суспільства;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу та громадян України усіх національностей;

держави:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав чи міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– інформаційно-інфраструктурне забезпечення економічного і науково-технологічного розвитку та формування позитивного іміджу України;

– інтеграція України у європейський та світовий інформаційний простір.

Манько О.О., Ніколов К.О., Скубак О.М.
Державний університет телекомунікацій, Україна

МОДЕЛЮВАННЯ ПЕРЕДАВАЛЬНИХ ХАРАКТЕРИСТИК САМОКЕРОВАНИХ ОБМЕЖУВАЧІВ ПОТУЖНОСТІ

Study of transfer characteristics of self-controlled power limiters

In this work the principles of modeling the transmission characteristics of passive protective device of microwaves range are considered. The devices are based on a self-controlled power limiter.

Вступ. На сучасному етапі розвитку безпровідних засобів зв'язку має місце інтенсивне освоєння НВЧ - діапазону електромагнітних коливань, пов'язане з ростом робочої частоти засобів до міліметрового діапазону довжин хвиль включно [1]. В цих діапазонах має місце застосування потужних стаціонарних імпульсних передавальних станцій. В зв'язку з цим виникає задача побудови ефективного захисного пристрою (ЗП), у функції якого входить обмеження вхідної потужності, що надходить на чутливі елементи. Основою для побудови такого пристрою може бути самокерований обмежувач потужності [2].

Однією з основних характеристик ЗП є передавальна характеристика –тобто залежність величини вихідної потужності від значення вхідної. Ця характеристика визначається параметрами керуючого вузла на *p*-*i*-*n*-діодах та діодної збірки (детекторного вузла), виконаного на діодах з бар'єром Шотткі (ДБШ). За вихідні дані для розробки математичної моделі ЗП в даній роботі взято вольтамперну характеристику (ВАХ) діодного вузла, виконаного на ДБШ, а також

експериментально отриману залежність внесеного загасання *p-i-n*-діодної збірки (керуючого вузла) від струму керування (рис. 1).

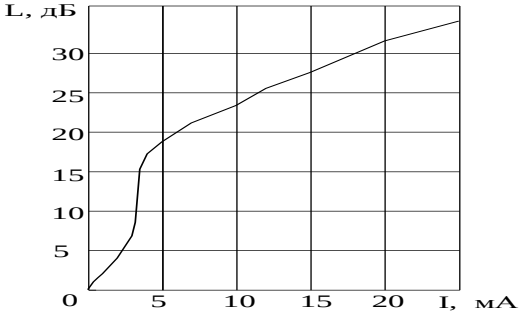


Рисунок 1. Залежність загасання *p-i-n*-діодної збірки від керуючого струму

Схемну побудову захисного пристрою було взято на основі конструкції, наведеної на рис. 2. Для *p-i-n*-діодної збірки (керуючого вузла) струм, випрямлений збіркою ДБШ (детекторним вузлом), буде керуючим струмом - $I_{кер}$. Протікаючи через *p-i-n*-діодну збірку, він буде визначати рівень загасання, яке вона вносить в тракт ЗП.

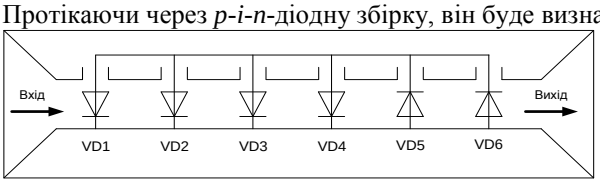


Рисунок 2. Схемна побудова захисного пристрою

Для побудови розрахункової моделі вольт-амперна характеристика ДБШ та залежність загасання *p-i-n*-діодної збірки від керуючого струму були апроксимовані кусочно-неперервними лінійними функціями. Для розрахунку передавальної характеристики необхідно перейти від вольт-амперної характеристики збірки ДБШ до ватт-амперної. В нашому випадку ця залежність буде мати вигляд:

$$I_{кер} = 1.376 \cdot P_{погл} - 1.003 , \qquad (1)$$

де $P_{погл}$ – НВЧ потужність, що подається на збірку ДБШ.

Алгоритм розрахунку полягає в наступному [3]:

- на першому кроці за величиною падаючої на вхід ЗП (вхідної) НВЧ-потужності $P_{вх}$ визначається прикладена до детекторної збірки потужність $P_{погл}$:

$P_{погл} = K_{зв} \cdot P_{вх}$, (2)

де $K_{зв}$ - коефіцієнт зв'язку збірки ДБШ з лінією, що визначає, яка частина падаючої НВЧ-потужності прикладається до детекторної збірки;

- з виразу (1) визначається струм детекторної збірки $I_{кер}$, що є керуючим струмом для керуючого вузла на *p-i-n*-діодах. За апроксимуючими виразами визначається загасання L, внесене керуючим вузлом. Падаюча на детекторний блок $P'_{вх}$ потужність у цьому випадку, з урахуванням L, буде визначатися , як

$$P'_{вх} = P_{вх} \cdot 10^{-0.1 \cdot L} ; \qquad (3)$$

- далі визначається $I'_{кер}$ і розрахунок повторюється доти, поки після виконання n-го циклу не виконається умова:

$$\left| I^{n}_{кер} - I^{n-1}_{кер} \right| \le \varepsilon , \qquad (4)$$

де ε - наперед задане додатне число, що визначає точність обчислення.

За аналогічним принципом був побудований алгоритм для моделювання роботи схеми з двома каскадами захисту, один з яких є попереднім каскадом з відгалужувачем (рис.3), і розрахованим на спрацьовування за великих рівнів вхідних потужностей, а другий – виконаний згідно з рис. 2.

Результати числового моделювання З використанням описаного вище алгоритму були проведені розрахунки характеристик ЗП для різних режимів його роботи при двох способах побудови: першого - коли ДБШ розташовані за збіркою з *p-i-n* діодів (рис.2), та комбінованого 2-х каскадного варіанта – з використанням попереднього каскаду ЗП з відгалужувачем [3] (рис.3). За вихідні дані для розрахунків були взяті вольтамперні характеристики конкретних типів ДБШ і експериментально отримані залежності ослаблення *p-i-n* аттенюаторів від керуючого струму. Аналіз отриманих характеристик ЗП, що являє собою конструкцію, виконану згідно з рис.2, з розташуванням ДБШ за *p-i-n* діодним атенюатором показує, що при рівні вхідного сигналу в межах від 0 до 0,1 Вт збільшення коефіцієнта зв'язку $K_{зв}$ до 0,2 дозволяє одержати ЗП з рівнем обмеження вхідного сигналу порядку 10-12 мВт.

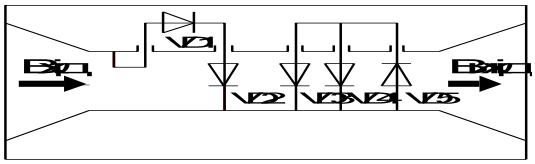


Рисунок 3. Електрична схема комбінованого 2-х каскадного обмежувача

Аналіз характеристик двокаскадного пристрою для різних значень $K_{зв1}$ (для VD5) і $K_{зв2}$ (для VD1) та зміні рівня вхідної потужності $P_{вх}$ в межах 0 - 1 Вт показує, що при малому значенні $K_{зв2}$ і рівнях вхідної потужності, що сягають 1Вт, перший каскад (VD1,VD2) практично не має впливу на хід характеристик, у той час як зі збільшенням $K_{зв2}$ відбувається спрацювання першого каскаду в розглянутому діапазоні вхідної потужності. У цьому випадку, після деякого наростання вихідної потужності $P_{вих}$ і стабілізації її значення відбувається різке зниження $P_{вих}$ при подальшому збільшенні вхідної, починаючи з деякого значення $P_{вх}$.

Різницю в поведінці передавальних характеристик можна пояснити тим, що в першому випадку, внаслідок малого значення $K_{зв}$, рівень вхідної потужності, що подається на VD1, виявляється недостатнім для його спрацювання. З урахуванням того, що ДБШ дуже критичні до значення потужності, що подається на них, двокаскадна схема краща у випадках підвищеного рівня вхідної потужності, коли спрацювання першого каскаду, з відносно малим коефіцієнтом зв'язку, охороняє ДБШ другого каскаду, з відносно великим коефіцієнтом зв'язку, від ушкодження.

Висновки Розроблено порівняно просту методику, що дозволяє проводити розрахунок передавальних характеристик досить складних багатокаскадних самокерованих обмежувачів потужності. Застосування запропонованих схем побудови захисних пристроїв дозволяє зберегти на потрібному рівні шумові характеристики НВЧ-приймачів, захищаючи змішувальні діоди від впливу потужних імпульсних завад. Результати цієї роботи дозволять підвищити надійність вхідних кіл НВЧ-приймачів РРЛ станцій надвисокочастотного діапазону, що працюють в умовах складної електромагнітної обстановки.

Література

1. Кременецька Я.А. Сучасні тенденції розвитку джерел міліметрового і субміліметрового діапазонів для перспективних систем зв’язку // Вісник ДУІКТ. – 2013. – №2. – С.94-97.

2. F. Jahan, M. Gaevski, J. Deng, R. Gaska, M. Shur, G. Simin. RF power limiter using capacitively-coupled contacts III-nitride varactor // Electronics Letters. – V.48. – Issue 23, 8 November 2012, p. 148-1481

3. Каток В.Б., Манько А.А., Соловьев Д.А. Численное моделирование характеристик самоуправляемого ограничителя мощности // Труды 10-й Международной крымской микроволновой конференции «СВЧ-техника и телекоммуникационные технологии» КрыМиКо 2000.- Севастополь: СГТУ (Украина) .- 2000.- С.156-157.

Руденко Є. В., Пеньков В. І.
Державного університету телекомунікацій , м. Київ

Дослідження методів та засобів захисту від НСД мереж стільникового зв'язку на основі стандарту GSM

GMS (англ. Global System for Mobile Communications, укр. Глобальна система мобільного зв'язку) — міжнародний стандарт для мобільного зв'язку другого покоління з розділенням каналів за принципом TDMA (Time Division Multiple Access). На сьогоднішній день GMS являється найбільш розповсюдженим стандартом, який використовується на території України. Стандарт був прийнятий в 1987 році, як Європейський стандарт цифрової мобільної технології другого покоління. GMS забезпечує людині більше можливостей для обміну інформацією, але разом з цим ця технологія може стати небезпечним інструментом для несанкціонованого отримання інформації сторонніми особами. Для забезпечення конфіденційності телефонних розмов, що здійснюються незахищеним GSM каналом, використовуються системи безпеки на основі шифрування даних. В країнах СНД для цього використовується друга версія алгоритму A5/2. Алгоритм заснований на регістрах зсуву з лінійної зворотним зв'язком певної довжини (19, 22, 23 біта). Початкові заповнення регістрів визначаються секретним і відкритим ключами. Відкритий ключ відомий і різний для кожного нового сеансу. При зв'язку двох абонентів шифрування здійснюється двічі, між абонентом і базовою станцією, станцією та абонентом. Але цього буває недостатньо. З швидким зростання потужностей обчислювальної техніки зловмиснику не складає зусиль для перехоплення та дешифрування сеансу розмови. Також широко використовується метод підміни базової станції(БС) для отримання несанкціонованого доступу до всіх сеансів зав’язків, які проходять у зоні покриття підмінної БС. Принцип дії більшості пристроїв для захисту передачі даних і голосу засновано на додатковому кодуванні або шифруванні даних. Одним з таких засобів є скремблери. Перевагою скремблерів є висока надійність захисту від будь-якого засобу прослуховування стільникових телефонів, у тому числі і від спеціального обладнання, встановленого у оператора. Недоліком є необхідність усім абонентам мати сумісні пристрої для приватної бесіди. Більш оригінальним способом захисту є ініціалізація сеансу зв’язку через канал даних GSM, з використання додаткового шифрування або кодування. Хоч технологія GSM вже застаріла та витісняється конкурентами з ринку мобільних послуг, при незначних доробках у пристроях абонентів можна досягти доволі високого рівня захисту від несанкціонованого доступу до інформації.

Список літератури:

1. A. Mehrotra. Cellular Radio: Analog and Digital Systems. Artech House, Boston-London. 1994. p.p. 460.

2. Ю.А. Громаков. Структура TDMA кадров и формирование сигналов в стандарте GSM. "Электросвязь". N 10. 1993. с. 9-12.
3. Вся правда о прослушивании мобильных телефонов:Спецвыпуск: Хакер, номер #059, стр. 059-052-1 (Електронный.ресурс) / Спосіб доступу: URL:http://www.xakep.ru/magazine/xs/059/052/1.asp

Хоботов Р.
Державного університету телекомунікацій , м. Київ

Дослідження методів та засобів управління ресурсами захисту інформації.

1. Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі
автоматизованої інформаційної системи підприємства. Управління доступомвключає наступні функції захисту:
• ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);-
• аутентифікацію (встановлення автентичності) об'єкту або суб'єкта по пред'явленому їм ідентифікатору;
• перевірку повноважень (перевірка відповідності дня тижня, часу доби,запрошуваних ресурсів і процедур встановленому регламенту);
• дозвіл і створення умов роботи в межах встановленого регламенту;
• реєстрацію (протоколювання) звернень до ресурсів, що захищаються;
• реагування (сигналізація, відключення, затримка робіт, відмова взапиті) при спробах несанкціонованих дій.
2. Засоби, призначені для захисту інформації. Ці засоби не призначенідля безпосередньої обробки, зберігання, накопичення і передачіінформації, що захищається, але що знаходяться в одному приміщенні зними.Діляться на:
a) пасивні – фізичні (інженерні) засоби, технічні засоби виявлення, ПС,
СЬКУД, ВН, прилади контролю радіоефіру, ліній зв'язку і т.п.;
b) активні – джерела безперебійного живлення, шумогенератори,
скремблери,пристрої відключення лінії зв'язку, програмно-апаратні засоби маскування інформації і ін.
3. Засоби, призначені для безпосередньої обробки, зберігання,
накопичення і передачі інформації, що захищається, виготовлені в
захищеному виконанні.
4. Засоби, призначені для контролю ефективності захисту інформації.
Пасивні засоби захисту акустичного і віброакустичного каналів
просочування мовної інформації.
Для запобігання просочування мовної інформації по акустичному і
віброакустичному каналам здійснюються заходи щодо виявлення каналів
витоку. В більшості випадків для несанкціонованого знімання інформації з
приміщення супротивник застосовує відповідні заставні пристрої.

Зварич Є. О.
Державного університету телекомунікацій , м. Київ

Технічні засоби захисту інформації

1. Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали й ін.
2. Захист від НСД може здійснюватися в різних складових інформаційної системи:
- прикладне й системне ПЗ;
- апаратна частина серверів і робочих станцій;
- комунікаційне устаткування й канали зв'язку;
- периметр інформаційної системи.
Для захисту інформації на рівні прикладного й системного ПЗ нами використовуються:
- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікации;
- системи аудита й моніторингу;
- системи антивірусного захисту.
Для захисту інформації на рівні апаратного забезпечення використовуються:
-апаратні ключі;
- системи сигналізації;

- засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мереженого захисту інформації:

- міжмережеві екрани (Firewall) — для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;
- системи виявлення вторгнень (IDS - Intrusion Detection System) — для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) — для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її дінамічного шифрування;
- засоби аналізу захищеності - для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

системи охоронної й пожежної сигналізації;

системи цифрового відеоспостереження;

системи контролю й керування доступом (СККД).

3. Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

4. З метою оцінки стану технічного захисту інформації, що обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, і підготовки обґрунтованих виводів для прийняття відповідних рішень звичайно проводиться експертиза в сфері технічного захисту інформації.

Література

1. Барсуков В.С. Безпека: технології, засоби, послуги / В.С. Борсуків. – М., 2001 – 496 с.
2. Ярочкин В.И. Інформаційна безпека. Підручник для студентів вузів / 3е изд. – М.: Академічний проект: Трікста, 2005. – 544 з.
3. Барсуков В.С. Сучасні технології безпеки / В.С. Борсуків, В.В. Водолазській. – М.: Нолідж, 2000. – 496 з., мул.

Кононський О.Д
Державний університет телекомунікацій

Цільові атаки та кібершпигунство

Вступ

Розвиток Інформаційних технології викликав появу нових умов, які використовуються кіберзлочинцями для скоєння цільових атак на національному, міжнародному і транснаціональному рівнях. Кіберзлочинці, об’єднуються в групи та використовують новітні технології для "відмивання" грошей, несанкціонованого доступу до інформації т. ін.

Актуальні приклади, цільових атак та кібершпигунства:

1. “Energetic Bear/crouching Yeti” (“енергетичний медвідь”) – група кіберзлочинців, причетна до декількох шкідливих атак класу APT (advanced persistent threat). Група почала активну діяльність на початку 2010 років. Інтереси кіберзлочинців поширюються, зокрема, на наступні сектори економіки: енергетика/машинобудування, промисловість, фармацевтичний сектор, будівництво, освіта, інформаційні технології. В ході атак група “Crouching Yeti” використовує кілька видів шкідливих програм, зокрема:

    - цільовий фішинг з використанням pdf-документів, зокрема, flash-експлоїт (Cve-2011-0611);
    - інсталятори з впровадженими в них троянськими програмами (призначені для операційних систем Windows: Havex, Sysmain, бекдор CLIEN, Karagany і пов'язані з ним засоби для крадіжки даних);
    - атаки типу watering hole із застосуванням різних відомих експлоїтів.

за допомогою яких вони проникають на ПК, крадуть конфіденційні дані, у тому числі інтелектуальну власність і іншу стратегічно важливу інформацію.

2. Epic Turla - ця група злочинців почала свої атаки з 2012 року, націлена на державні установи, посольства, військові, дослідницькі центри, освітні установи і фармацевтичні компанії. Для зараження кіберзлочинці використовують прийоми соціальної інженерії – зокрема:

- адресний фішинг (електронні листи, що відправляються при адресному фішингу, містять вкладені експлоїти нульового дня);
- атаки типа watering hole (з застосуванням Java-експлоїтів (Cve-2012-1723), експлоїтів для Adobe Flash, Internet Explorer).

Результати:

Способи ідентифікації кіберзлочинців:

1. Аналіз часових міток файлів шкідливих програм (час компіляції).
2. Дослідження мови написання програм.

Методи захисту:

1. Використання фаєрволів, антивірусів.
2. Використання ліцензійного ПЗ.
3. Розробка та впровадження галузевих, спеціалізованих засобів захисту(ПЗ).
4. Фільтрація пошти.
5. Використання перевірених каналів передачі данних.

Висновки:

1. рекомедується провести повноцінну розробку та прийняття Закону України "Про моніторинг телекомунікацій", проекту постанов, щодо проведення першочергових заходів, спрямованих на зниження рівня злочинної активності в мережі Інтернет, що регламентуватиме роботу постачальників Інтернет-послуг та їх клієнтів, провайдерів і операторів IP-телефонії, а саме: запровадити практику ідентифікації користувачів шляхом надання ідентифікаційного коду особи оператору зв'язку, при подачі письмової заяви про укладення договору на надання послуг;
2. проведення інвентаризації та сертифікації сайтів компаній і фірм, основною сферою діяльності яких є торгівля та надання послуг (у тому числі сайтів з азартних ігор, лотерей, аукціонів), які проводять розрахунки між продавцем та покупцем за допомогою засобів електронного зв'язку;

Список використаної літератури:

1. Проект закону “Про моніторинг телекомунікацій” № 4042 від 07.08.2008р. // ЛІГА: ЗАКОН
2. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине // Закон и жизнь. - 2010. - № 7.

Пеньков В. І., Руденко Є. В.,
Державного університету телекомунікацій , м. Київ

Методи і засоби протидії злоякісному , шпигунському і завідомо фальшивому ПЗ

Одна з найбільш актуальних проблем у сфері інформаційної безпеки в даний час є - проблема шкідливого програмного коду. Ще кілька років тому ситуація була досить простою - існували прикладні програми(включаючи операційну систему) і комп'ютерні віруси, тобто програми, здатні заражати інші програми шляхом впровадження в них свого машинного коду. Проте останнім часом з'явилась безліч програм, які не можна вважати вірусами, тому вони не мають здатність до розмноження. Для таких програм існує безліч категорій: Trojan, Backdoor, Trojan-Downloader, MalWare, SpyWare, Adware, Dialer ... Класифікація найчастіше досить спірна – виробники різного антивірусного ПЗ відносять одну і ту ж саму програму до різних категорій. Ці програми можуть здійснювати широке коло завдань, наприклад: запам'ятовувати натискання клавіш на клавіатурі, несанкціоновано і віддалено керувати комп'ютером, інсталювати на комп'ютер користувача додаткові програми, змінювати параметри операційної системи і перенаправляти активність браузерів. Шпигунське програмне забезпечення може потрапити на комп'ютер користувача в ході відвідування сайтів Інтернет або в результаті установки безкоштовних або умовно- безкоштовних програм.На сьогоднішній день основними заходами щодо запобігання зараження є: використання файрволів і проксі-сервери для блокування доступу до сайтів, відомим як розповсюджувач spyware, використання антивірусних програм з максимально «свіжими» вірусними базами, скачування програм тільки з довірених джерел, а також використання hosts - файлу, який перешкоджає можливості з'єднання комп'ютера з сайтами, відомим як розповсюджувачі spyware.

Список літератури

1. COMPUTER SECURITY AND CRYPTOGRAPHY ALAN G. KONHEIM ст 120
2. Компьютерные вирусы.Крис Касперски ст 202,348
3. Персональная защита от хакеров.Джерри Ли Форд ст 31,204
4. Теория и практика защиты программ.О.В.Казарин ст 16,306

Киричок Р.В.
Державний Університет Телекомунікацій

АТАКА НА ВІДМОВУ В ОБСЛУГОВУВАННІ: ТЕСТУВАННЯ НА СТІЙКІСТЬ СЕРВІСІВ

Відомо що, останнім часом все більшого поширення отримав цілий клас атак (DoS/DDoS), спрямованих на відмову в обслуговуванні. Успішна реалізація таких атак дозволяє блокувати доступ користувачів інформаційних систем до ресурсів різних серверів, що може вивести з робочого стану всю систему. І тому на сьогоднішній день все більше компаній звертається до спеціалістів з інформаційної безпеки не лише за тестуванням на проникнення, але і за перевіркою стійкості їх сервісів до атак на відмову в обслуговуванні, найчастіше - веб-сайтів. Розглянемо, як проводиться тестування на стійкість сервісів.
Для початку вибирається методика тестування і узгоджується із замовником. Вибір складається з:

- Атаки на канал (досягти максимальної пропускної спроможності);
- Атаки на мережеві сервіси (slow http, використання експлойтів для DDoS певних веб-серверів, атаки на SSL, інші техніки);
- Атака на application рівень (використання особливостей роботи цього додатка).

Узгоджується час, потужність, збирається скайп-чат в потрібний час і там вже узгоджуються всі дії.А тепер про кожну з методик:

Атака на канал. Завдання - забити канал сервера і привести до його недоступності для легітимних клієнтів. У реальності атакуючі використовують різні техніки - від реальних ботнетів до атак через публічні dns/ntp сервера.

Атаки на мережеві сервіси. Мета - покласти саме сам мережевий сервіс (веб-сервер, проксі, балансувальник, та інше) будь-яким способом.
Атака на application рівень. Завдання в тому, щоб знайти особливості роботи даного додатку і через них покласти сервер. Ніякі захисні технології, балансувальники, зовнішні сервіси не рятують від такого. Що я маю на увазі? Різні «важкі» запити, наприклад вибірка великих обсягів даних. По одному абсолютно легітимному запиту з пари десятків машин - і «приїхали». Природно, такі місця простіше знайти якщо тестування на DoS в рамках пентеста і є час вивчити додаток.

В основному, звичайно, все це спрямовано на атаку бекенд (пост обробка даних, база даних), але проблема в тому, що якогось універсального захисту від цього немає, і потрібні адміністратори/ програмісти/люди з безпеки на аналіз ситуації та її виправлення.

Таким чином, тестування на відмову в обслуговуванні може виявити неявні проблеми в архітектурі, від яких не врятуватися зовнішніми сервісами по захисту від DoS, cfg, новими правилами в iptables і т.п., саме тому варто приділяти належну увагу даному виду тестування.

Евгений Зобнин Журнал "Хакер", Устоять любой ценой. Методы борьбы с DoS/DDoS-атаками. — 2009.

Стребков – Саламатов
Державного університету телекомунікацій , м. Київ

Дослідження методів та засобів захисту системи електронних платежів.

1. Методи захисту платежів у мережі Internet

Слабким місцем мережної інфраструктури є незахищені канали зв'язку, де існує можливість появи неіснуючих платежів, перехоплення та несанкціонованого використання платіжних даних, інших проявів шахрайства та зловживань. Такі випадки траплялися в Internet. Існують два шляхи захисту передачі інформації: ізолювання мережі, яка використовується для обробки платежів, тобто використання приватних мереж, і шифрування даних.

Використання криптографічного захисту інформації при побудові політики безпеки платіжної системи значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися. Є дві групи криптографічних алгоритмів:
1) загальні:
- симетричні;
- асиметричні;
2) спеціальні.

Криптографічні алгоритми застосовують із метою:
- шифрування інформації;
- захисту даних і повідомлень (інформації) від модифікації або підробки.

Особливу увагу при вивченні теми потрібно приділити методам розподілу криптографічних ключів між учасниками платіжної системи, а саме методом:
- базово-сеансових ключів;
- відкритих ключів.

2. Апаратно-програмні засоби криптографічного захисту інформації в СБП забезпечують автентифікацію відправника та отримувача електронних банківських документів і службових повідомлень СБП, гарантують їх достовірність та цілісність, неможливість підроблення або викривлення документів у шифрованому вигляді й за наявності ЕЦП. Криптографічний захист інформації охоплює всі етапи оброблення електронних банківських документів з часу їх створення до зберігання в архівах банку. Використання різних криптографічних алгоритмів на різних етапах оброблення електронних банківських документів дає змогу забезпечити безперервний захист інформації в СБП. Криптографічний захист інформації гарантує цілісність та конфіденційність електронної банківської інформації, а також сувору автентифікацію учасників СЕП і їх фахівців, які здійснюють підготовку та оброблення електронних банківських документів.

Варто також звернути увагу на заходи захисту інформаційної безпеки. На протидію загрозам та з метою мінімізації можливих збитків користувачів і власників платіжної системи спрямовані чотири групи заходів:
1) правові;
2) морально-етичні;
3) адміністративні;
4) фізичні.

Для нормального функціонування платіжної системи повинні бути створені та введені в дію закони та підзаконні акти, які регламентують правила роботи з платіжною системою і платіжною інформацією, що обробляється, накопичується та зберігається в системі. У разі відсутності державних законів правила роботи платіжної системи повинні бути визначені нормативними документами власника платіжної системи й обов'язково виконуватись усіма учасниками системи.

ЛІТЕРАТУРА

1. "Інструкція про міжбанківський переказ грошей в Україні в національній валюті", затверджена Постановою Правління Національного банку України 17.03.2004 р. № ПО, зареєстрована в Міністерстві юстиції України 15.04.2004р. за №483/9082.
2. "Персональні ЕОМ в інженерній практиці", Т.З.Кренкель, А.Г.Коган, А.М.Тараторин, вид. Москва "Радіо і звязок", 1989р.
3. А.Н.Романов, Б.Е.Одинцов „Советующие информационные системы в экономике „ ЮНИТИ, Москва, 2000 г.
4. Алан Нейбауэр „Access 2000 для занятых», перевод с английского, Питер, 2001, - 288 с.

Курінний С.В, Сосюра А.О.
Державний Університет Телекомунікацій

ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ ЯК СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

Особливості рукописного підпису

Організаційне забезпечення електронного цифрового підпису (ЕЦП) здійснюється відповідно до законодавства держави, на території якої використовується такий засіб ЕЦП. Якщо такого законодавства немає, правове регулювання в галузі застосування засобів ЕЦП здійснюється на основі нормативних актів адміністративних органів.

У ст. 4 Закону "Про електронний цифровий підпис" зазначено, що електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами — суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Статтею 3 Закону № 852 визначено, що електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному в сертифікаті.

Власноручний підпис під документом віддавна вважається доказом того, що людина, яка підписала цей документ, ознайомилася з ним і згодна з його змістом. Тобто рукописний підпис є одним із засобів ідентифікації особи, в основу якого покладено гіпотезу про унікальність особистих біометричних параметрів людини. Чому ж підпис заслужив таку довіру? Основні причини такі:

Дійсність підпису можна перевірити (його наявність у документі дає змогу переконатися, чи справді він був підписаний людиною, що володіє правом ставити цей підпис);

Підпис не можна підробити (справжній підпис - доказ того, що саме та людина, якій він належить, поставила цей підпис під документом);

Підпис, що вже стоїть під одним документом, не може бути використаний ще раз для підписання іншого документа (підпис — невід'ємна частина документа і його не можна перенести в інший документ);

Підписаний документ не підлягає ніяким змінам;

Від підпису неможливо відректися (той, хто поставив підпис, не може згодом заявити, що він не підписував цей документ).

Насправді жодна з перерахованих властивостей підпису на всі 100 % не виконується. У нашому сучасному криміналізованому суспільстві підписи підробляють і копіюють, від них відрікаються, а в уже підписані документи вносять довільні зміни. Тобто застосування рукописного підпису не позбавлене недоліків:

- недостатній ступінь захисту (коли необхідна підвищена достовірність відомостей, що містяться у документі, використовують додаткові засоби захисту: наявність додаткових рукописних підписів, печатки юридичних осіб, засвідчення у нотаріуса, спеціальні бланки тощо);
- нерозривний фізичний зв'язок з матеріальним носієм (рукописний підпис можливий тільки на документах з матеріальною природою, тому особа, що підписує документ, має безпосередньо контактувати з матеріальним носієм цього документа);
- розбіжності між оригіналом та копіями, отриманими засобами копіювально-миожильної техніки (копії не мають тієї юридичної сили, яку має оригінал документа);
- ніяким чином не забезпечує аутентифікацію документа, тобто його цілісність і незмінність (без додаткових засобів захисту рукописний підпис не гарантує незмінності вмісту документа під час його збереження або транспортування).

Особливості електронного цифрового підпису

Застосування глобальних комунікацій в економічній діяльності та повсякденному житті зумовило появу принципово нового виду відносин, пов'язаних з обміном інформацією без використання паперових носіїв, тобто за допомогою електронних документів. Під електронним документом мають на увазі документ, в якому інформацію подано в електронній формі та який містить необхідні реквізити (у тому числі електронний цифровий підпис).

Електронний цифровий підпис (ЕЦП) є реквізитом електронного документа і призначений для його захисту від підробки. ЕЦП має не фізичну, а логічну природу. Під час побудови цифрового підпису замість звичайного зв'язку між печаткою або рукописним підписом та аркушем паперу простежується складна залежність між документом в електронному вигляді, секретним і загальнодоступним (відкритим) ключами, а також цифровим підписом. Складність підробки ЕЦП зумовлена дуже великим обсягом математичних обчислень.

ЕЦП може мати цілком "буквений" вигляд, але частіше він поданий у вигляді послідовності довільних символів. Цифровий підпис може зберігатися разом з документом, наприклад, стояти на його початку, в кінці або в окремому файлі (природно, що в останньому випадку, перевіряючи підпис, необхідно мати у своєму розпорядженні як сам документ, так і файл, що містить підпис).

Електронний цифровий підпис — це засіб, що дає змогу на основі використання криптографічних методів визначити авторство і дійсність документа. При цьому електронний цифровий підпис має такі переваги:

- дематеріалізація документів (незалежність ЕЦП від носія дає можливість використовувати його в електронному документообігу й установлювати договірні взаємовідносини без безпосереднього контакту між фізичними або юридичними особами);
- рівнозначність копій (логічна природа ЕЦП дає змогу не розрізняти копії одного документа та зробити їх рівнозначними);
- додаткова функціональність: в основі механізму ЕЦП лежить криптографія, тому ЕЦП є не тільки засобом ідентифікації, а й засобом аутентифікації документа (в електронний документ, підписаний ЕЦП, не можна внести зміни, не порушивши підпису);
- автоматизація (створення, застосування, засвідчення та перевірка ЕЦП виконується із застосуванням програмних та апаратних засобів обчислювальної техніки, тому добре автоматизується);
- порівнянність захисних властивостей (об'єктивна оцінка сертифікованих програмних та апаратних засобів обчислювальної техніки, призначених для створення ЕЦП (далі — засобів ЕЦП), базується на чіткому математичному аналізі, а не на гіпотезі про унікальність біометричних параметрів людини);
- масштабованість (виходячи з оцінки захисних властивостей ЕЦП, у цивільному документообігу можна використовувати найпростіші засоби ЕЦП, у службовому — сертифіковані для секретної інформації — спеціальні засоби ЕЦП).

Усі наведені властивості ЕЦП широко використовуються в електронній комерції. Однак у використанні ЕЦП є й недоліки. Хоча електронний документообіг з електронним підписом сприяє підвищенню продуктивності праці, але виводить механізм підпису з-під контролю звичайними методами (візуальними) та може створювати ілюзію благополуччя. Тому для використання ЕЦП необхідне спеціальне технічне, організаційне та правове забезпечення.

Онопрієнко М.А. Гордієнко Д.О.
Державний університет телекомунікацій

Кібернетичний тероризм та кібершпигунство на території України

Сучасний світ сприймає інформацію на одному рівні з енергетичними та матеріальними ресурсами і розглядає як важливий чинник якісних змін у житті суспільства. Побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного соціально–економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З іншого, – сучасні інформаційні технології, перетворює інформаційні системи урядового, оборонного, виробничого, кредитно – банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кібернетичних загроз об'єкти. І тут національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечується кіберпростором інформаційного середовища.

Метою даної роботи є висвітлення основних проблем, щодо підходів формування державної політики у сфері забезпечення кібернетичної безпеки України, правового забезпечення системи кібернетичної безпеки та визначення напрямів їх *вирішення для ефективної* ***протидії*** *проти* ***кібертероризму*** *та* ***кібершпигунства*****.**

Україна послідовно виходить з того, що кіберпростір є відкритим простором – відкритим до інновацій, вільного розповсюдження інформації, ідей та обміну думками. Низка вітчизняних підприємств, порушення роботи яких може становити загрозу життю та здоров'ю громадян, може стати потенційною ціллю для здійснення терористичних актів, в тому числі – із застосування сучасних інформаційних технологій. Не меншою загрозою є вчинення протиправних дій на шкоду третім країнам, що здійснюються із використанням вітчизняної інформаційної інфраструктури, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп хакерів-активістів(*організація хактивістів «Anonymous» блокує роботу сайтів урядів в знак підтримки народних рухів*), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

Воєнна сфера зазнає чи не найдраматичніших змін внаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформує свої потенціали у сфері оборони в напрямі посилення кібернетичних можливостей ведення бойових дій та захисту від аналогічних дій з боку супротивника, оскільки все актуальнішими стають нові типи загроз. З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема, створення ЄАСУ ЗС України, оборонний потенціал нашої держави стає більш чутливим до кібернетичних загроз. Впровадження провідними країнами сучасних кібернетичних озброєнь перетворює кіберпростір на окрему, поряд з традиційними «Земля», «Повітря», «Море», «Космос», сферу ведення бойових дій, а у найближчому майбутньому, рівень обороноздатності країни буде визначатись у т.ч. наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатність протистояти кібернетичним загрозам в сфері оборони.

Таким чином, проведений аналіз кібернетичного простору дозволяє зробити наступні висновки.

Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків в ключових сферах життєдіяльності, а саме приведенню української національної системи інформаційної безпеки у відповідність зі світовими стандартами у даній сфері, що мають особливе значення для забезпечення кібернетичної безпеки України. З метою вдосконалення вітчизняного нормативно-правового поля та у зв'язку з створенням Національної системи кібернетичної безпеки, необхідно внесення наступних змін до Законів України:

- Про основи національної безпеки *щодо визначення кібернетичної безпеки самостійною сферою національної безпеки, загроз, основних напрямів державної політики*;
- Про оборону України *щодо підготовки Збройних Сил України до відбиття агресії в кіберпросторі*;
- Про боротьбу з тероризмом *щодо боротьби з кібернетичним тероризмом*;
- Про Державну службу спеціального зв'язку та захисту інформації України *щодо уточнення компетенції та повноважень у зв'язку зі створенням Національної системи кібернетичної безпеки*.

ЛІТЕРАТУРА

1. Указ Президента України „Про Стратегію національної безпеки України" від 12 лютого 2007 року № 105/20..
2. Проект Закону про внесення змін до Закону України "Про захист суспільної моралі" (щодо захисту інформаційного простору) 04.06.2013 - Верховна Рада України. – *http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=47240&pf35401=264705*
3. Тероризм і національна безпека. – *http://marchuk.kiev.ua/ua/94p.html*.

Вовк В.О.
Державний Університет Телекомунікацій,м.Київ

Безпека IP-телефонії: максимальний захист корпоративних IP-мереж.

Універсального засобу безпеки IP-телефонії не існує як такого, але рішення цього завдання має стати складовою частиною загальної стратегії безпеки. Технологія VoIP - це додаток, що працює в IP-мережі, де мають бути реалізовані належні методи захисту, тобто потрібно чітко розуміти, чим вища безпека мережі в цілому, тим важче буде зловмисникові організувати підслуховування, атаку типу «відмова в обслуговуванні» (DoS), «зламати» ОС або додаток системи VoIP. Найбільш поширеними загрозами, до яких схильні IP-мережі, можна назвати:

- реєстрацію чужого терміналу, що дозволяє робити дзвінки за чужий рахунок;
- підміну абонента;
- внесення змін до голосового чи сигнального трафіку;
- зниження якості голосового трафіку;
- перенаправлення голосового або сигнального трафіку;
- перехоплення голосового або сигнального трафіку;
- підробка голосових повідомлень;
- завершення сеансу зв'язку;
- відмова в обслуговуванні;
- віддалений несанкціонований доступ до компонентів інфраструктури IP-телефонії;
- несанкціоноване оновлення програмного забезпечення на IP-телефоні (наприклад, з метою впровадження троянської або шпигунської програми);
- злому білінгової системи (для операторської телефонії).

І це далеко не весь перелік можливих проблем, пов'язаних з використанням IP-телефонії. Значить при всіх перевагах IP-телефонії потрібно відразу розглядати питання організації системи захисту своїх мереж, що дозволить повною мірою використовувати вигоди від переходу до технологій VoIP. Архітектура IP-телефонії включає кілька основних структурних елементів, кожен з яких може бути підданий атаці зловмисників. Тому потрібне застосування комплексного підходу при реалізації завдання щодо забезпечення максимального рівня безпеки корпоративної телефонії.

У якості «першої лінії оборони»: системи виявлення та запобігання атак, принцип дії яких полягає в розмежуванні доступу до інфраструктури IP-телефонії та здійсненні регулярного моніторингу системи. Також рекомендується використання стандартних антивірусів і міжмережевих екранів. Використання цих технологій надає можливості для:

- фільтрації трафіку управління установкою IP-телефонних з'єднань;
- передачі трафіку управління через NAT і мережеві тунелі;
- TCP-перехоплення, яке забезпечує перевірку закриття TCP-сесій, що дозволяє захищатися від ряду атак типу відмови в обслуговуванні (DoS).

«Друга лінія оборони» - захист шляхом використання протоколів шифрування та організації заходів забезпечення безпеки щодо використання пристроїв системи IP-мережі (починаючи від сервера до самих IP-телефонів).Саме спеціалізована конфігурація політик безпеки IP-системи, прав авторизації і доступу внутрішніх абонентів, встановлення обмежень на робочий функціонал системи послужать однією з найбільш ефективних ініціатив щодо оптимізації рівня безпеки та роботи корпоративної IP-системи. Ризики, пов'язані із загрозою несанкціонованого вторгнення зловмисника в систему адміністрування IP-телефонією,також можуть бути практично зведені до нуля. Оскільки сама інфраструктура IP-телефонії є достатньо розгалуженою системою, то управління конфігурацією IP-телефонів і взаємодія їх з сервером управління повинно здійснюватися по захищеному від несанкціонованого доступу каналу, що дозволяє запобігти будь-які спроби прочитання або модифікації команд. Для захисту каналу управління можуть використовуватися різні протоколи - IPSec, SSL, TLS.

IP-телефонія і використання системи VoIP є цілком безпечними. Відповідаючи потребам і вимогам сучасного бізнесу, при грамотному підході до налаштування системи та її конфігурації з позиції мережевого захисту - VoIP істотно підвищує рівень конкурентоспроможності компанії, сприяє раціоналізації використання ресурсів та підвищенню мобільності і продуктивності співробітників. При цьому потрібно пам'ятати - максимально ефективними заходи безпеки можуть бути тоді, коли вони покривають всі рівні мережевої інфраструктури.

Важливо пам'ятати, що атаки з боку зловмисників (прослуховування , фальсифікація абонента, неавторизоване проникнення в систему, перехоплення інформації, перевантаження ліній) застосовані як для традиційної, так і для IP-телефонії. Питання полягає в тому, що виявлення, локалізація і запобігання загрозам в системі IP-телефонії – задача доволі простіша і завдає менше витрат. При цьому, витрати на IP-телефонію істотно нижчі, ніж на аналогову. Безпека IP-телефонних рішень у зв'язку з їх зростаючою популярністю і попитом є вирішальним фактором при побудові телекомунікаційної IP-інфраструктури і саме тому потребує особливої уваги.

В. Ю. Однорог, О.В. Богомоленко
Державний університет телекомунікацій

ВИКОРИСТАННЯ СМАРТ-КАРТ ЯК ЗАСОБІВ АУТЕНТИФІКАЦІЇ

Вступ. Проблема аутентифікації користувачів при доступі до інформаційних ресурсів все ще є досить актуальною. Зараз існує декілька способів аутентифікації, серед них використання логіну та паролю, ідентифікація по біометричним параметрам та, власне, використання смарт-карт. Смарт-карта надає зручний спосіб аутентифікації користувачів.

Постановка задачі. Для дослідження маємо USB-ключ (рис. 1)

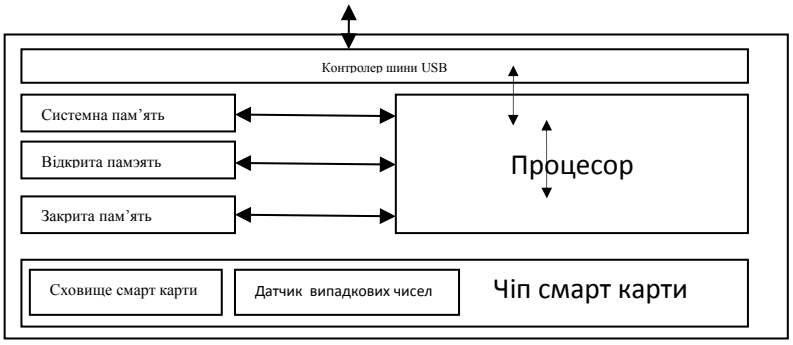


Рис. 1 Схема USB-ключа.

Необхідно дізнатись, як добре захищений закритий ключ та за що відповідає чіп смарт-карти [1].

Мета дослідження. Визначення переваг та недоліків при аутентифікації з використанням смарт-карт.

Результати досліджень і висновки. Смарт-карта має декілька розділів пам'яті. В системній містяться дані, що необхідні для перевірки вводимих паролів, у відкритій містяться дані, які можна прочитати без PIN-кода, закрита пам'ять містить дані, доступ до яких можливий тільки по PIN-коду. Чіп смарт-карти зберігає закриті ключі у сховищі, зчитати ці дані неможливо, генерує ключову пару, реалізує симетричні алгоритми шифрування, алгоритми хешування та асиметричні алгоритми.

До переваг можна віднести зручність в зберіганні та експлуатації, стійкість до зовнішніх впливів, а також невисоку вартість. Несанкціоновано зчитати дані зі смарт-карти можливо лише маючи безпосередній доступ до неї.

Тож смарт-карти це зручний засіб автентифікації, що дозволяє суттєво полегшити розробку, введення та експлуатацію системи контроля доступу на заданому об'єкті.

Список використаної літератури:

1. *И. М. Голдовский* Банковские микропроцессорные карты. — М.: «Альпина Паблишер», 2010. — 694 с.

А.А. Корченко
Национальный авиационный университет

Формирование эвристических правил для систем обнаружения вторжений

Современная теоретическая и практическая база, которая используется для обнаружения атак в компьютерных сетях, имеет определенные ограничения по идентификации новых и несигнатурных типов кибератак. С этой целью разработана базовая модель параметров, универсальная модель эталонов и модель эвристических правил (ЭП), которая за счет множества эталонных параметров, логико-лингвистических связок и лингвистических идентификаторов позволяет формализовать процесс формирования множеств ЭП для выявления аномального состояния. Разработан метод выявления аномалий, который за счет указанных моделей и сформированных текущих параметров, позволяет строить средства обнаружения несигнатурных и новых типов кибератак. На основе этого метода предложено новое структурное решение системы выявления аномального состояния в компьютерных сетях. Она состоит из подсистем первичной обработки, формирования нечетких эталонов и формирования ЭП, а также модулей нечеткой арифметики, логического вывода и визуализации. Это решение используется для совершенствования систем сетевой безопасности, которое основывается на реализации указанного метода обнаружения аномалий и ориентировано на осуществление контроля активности в определенной среде окружения.

Для поддержки функционирования указанной системы актуальным является разработка соответствующего средства, обеспечивающего эффективную работу подсистемы формирования ЭП. В связи с этим, целью данной работы является создание алгоритмического обеспечения и нового структурного решения, которое может использоваться на практике для расширения функциональных возможностей современных систем обнаружения вторжений. Достижение поставленной цели будет основываться на методе выявления аномалий порожденных кибератаками, на основе которого предлагается новое структурное решение соответствующей системы формирования ЭП, ориентированной на построение решающих правил, направленных на проверку истинности взаимосвязей эталонных и текущих параметров для оценивания сетевой активности.

Система содержит: регистр эталонов (РЭ); блок коммутации (БК), служащий для формирования потоков $\underset{\sim}{t}_i$, поступающих на блок формирования логико-лингвистических связок (БФЛЛС); БФЛЛС, предназначенный для логического преобразования эталонных T_{ij}^{ef}; блок ранжирования (БР), осуществляющий формирование коэффициента важности; блок инициализации правил (БИП), формирующий матрицы $LI(i,r_r)$ и $LC(i,r_r)$; базу правил (БП),

служащей для хранения в соответствующих секторах данных (СД$_i$, $i=\overline{1,d}$) наборов правил ER_{i_i} $(i=\overline{1,n})$; регистры текущих значений (РТЗ) и лингвистических идентификаторов (РЛИ), предназначенные соответственно для хранения в процессе всех вычислений значений $\tilde{t}$ и LI_i $(i=\overline{1,d})$; регистр правил (РП), предназначенный для приема и хранения подмножеств правил ER_i. Система работает согласно построенному алгоритму.

Например, каждому ER_{ij} соответствует эвристическое выражение (правило), т.е. формируются связки $ER_{11}=LC_{11} \to LI(1,1)$, $ER_{12}=LC_{12} \to LI(1,2)$, $ER_{13}=LC_{13} \to LI(1,3)$, $ER_{14}=LC_{14} \to LI(1,4)$, $ER_{15}=LC_{15} \to LI(1,5)$, которые интерпретируются одним из сообщений – Н, БНВ, БВН, В, П и соответственно отображаются текстовыми значениями «Низкий», «Больше низкий чем высокий», «Больше высокий чем низкий», «Высокий» и «Предельный». Далее например, посредством сформированных матриц инициализации для AT$_i$ и P$_j$ (при $i=1$ и $j=\overline{1,2}$) и наборов ЭП, направленных на выявление $AT_1=SN$ (т.е. SN – «Сканирование портов») (при P$_1$=КВК – «Количество виртуальных каналов» и P$_2$=ВВК – «Возраст виртуального канала»), определяются для $\boldsymbol{ER_1}$ значения $ER_{11}...ER_{15}$ т.е.:

$\boldsymbol{ER_1}=\{ ER_{11}=(\tilde{t}_{ВВК} \cong \tilde{M}^e \wedge \tilde{t}_{КВК} \cong QM^e) \to Н$, $ER_{12}=(\tilde{t}_{ВВК} \cong \tilde{M}^e \wedge \tilde{t}_{КВК} \cong M^e) \to БНВ$, $ER_{13}=(\tilde{t}_{ВВК} \cong \tilde{M}^e \wedge \tilde{t}_{КВК} \cong \tilde{C}^e) \to БВН$,

$ER_{14}=(\tilde{t}_{ВВК} \cong \tilde{M}^e \wedge \tilde{t}_{КВК} \cong \tilde{Б}^e) \to В$, $ER_{15}=(\tilde{t}_{ВВК} \cong \tilde{M}^e \wedge \tilde{t}_{КВК} \cong QБ^e) \to П \}$.

Тогда этим значениям будут соответствовать следующие наборы решающих правил: ER$_{11}$ = «Если $\tilde{t}_{ВВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{ВВК}$ и $\tilde{t}_{КВК}$ наиболее близко к QM^e, входящего в $\tilde{T}^e_{КВК}$, то уровень аномального состояния, порожденного *SN* будет НИЗКИЙ»; ER$_{12}$ = «Если $\tilde{t}_{ВВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{ВВК}$ и $\tilde{t}_{КВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{КВК}$, то уровень аномального состояния, порожденного *SN* будет БОЛЬШЕ НИЗКИЙ, ЧЕМ ВЫСОКИЙ»; ER$_{13}$ = «Если $\tilde{t}_{ВВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{ВВК}$ и $\tilde{t}_{КВК}$ наиболее близко к $\tilde{C}^e$, входящего в $\tilde{T}^e_{КВК}$, то уровень аномального состояния, порожденного *SN* будет БОЛЬШЕ ВЫСОКИЙ, ЧЕМ НИЗКИЙ»; ER$_{14}$ = «Если $\tilde{t}_{ВВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{ВВК}$ и $\tilde{t}_{КВК}$ наиболее близко к $\tilde{Б}^e$, входящего в $\tilde{T}^e_{КВК}$, то уровень аномального состояния, порожденного *SN* будет ВЫСОКИЙ»; ER$_{15}$ = «Если $\tilde{t}_{ВВК}$ наиболее близко к $\tilde{M}^e$, входящего в $\tilde{T}^e_{ВВК}$ и $\tilde{t}_{КВК}$ наиболее близко к $QБ^e$, входящего в $\tilde{T}^e_{КВК}$, то уровень аномального состояния, порожденного *SN* будет ПРЕДЕЛЬНЫЙ». Также, для группы правил $\boldsymbol{ER_1}$, ориентированных на идентификацию $AT_1=SN$ можно получить графическое отображение нечетких опорных двумерных областей (Н, БНВ, БВН, В, П), характеризующих возможные уровни аномального состояния относительно ЛП **КВК** и **ВВК**. Имея эталоны, а также вычислив текущие значения параметров, можно с помощью ЭП определить уровень аномального состояния в компьютерных системах, идентификатором которого будет одна из полученных опорных областей.

Предложенное новое структурное решение системы формирования ЭП для оценивания сетевой активности может быть реализовано программно или программно-аппаратно и использоваться для формирования решающих правил, направленных на проверку истинности взаимосвязей эталонных и текущих параметров для оценивания сетевой активности в среде окружения, а также применяться в качестве основы при построении систем обнаружения вторжений.

Цигак В. В.
Державний університет телекомунікацій м. Київ

СИСТЕМИ КОНТРОЛЮ І КЕРУВАННЯ ДОСТУПОМ

Система контролю і управління доступом (СКУД) – це сукупність програмно-апаратних технічних засобів безпеки, що забезпечують обмеження та реєстрацію входу-виходу об'єктів – людей чи транспорту на заданій території через «точки проходу»: двері, ворота, КПП.

Сучасні системи контролю доступу здатні вирішувати три основні завдання:

- організація контролю переміщення персоналу-правильна організація праці,тобто кожному користувачу досить видати один ключ для його ідентифікації системою охорони об'єкта, а також виключити можливість довільного проходження співробітників;

- організація обліку - створення системи обліку робочого часу (на основі аналізу часу приходу / відходу співробітника з території підприємства або робочого місця), а також контроль місця знаходження співробітника на об'єкті з точністю до зони доступу;

- організація охорони підприємства - інтеграція СКД з системою охоронно-пожежної сигналізації для комплексного вирішення завдань безпеки. Забезпечення реакції охоронної складової системи на спроби несанкціонованого доступу, злому дверей і т.д. Можливість автоматичної постановки / зняття з охорони

приміщень за фактом проходу в зону доступу співробітника. Надання вільного доступу в разі виникнення пожежі.

Існує декілька режимів роботи СКУД.

Стандартний режим проходу - у кожної точки доступу на підприємстві, що підлягає контролю, встановлюється контролер доступу і зчитувальні пристрої. Для того щоб співробітники мали можливість проходу через точки доступу, кожному з них видається унікальний ідентифікатор користувача, також в якості ідентифікатора може виступати біометрична інформація.

Заборона повторного проходу (правило antipassback) - використовується для того, щоб одним ідентифікатором не можна було скористатися повторно для входу в яку-небудь зону доступу, попередньо не вийшовши з неї.

Доступ за правилом двох (або більше) осіб, що мають узгоджені рівні доступу – застосовується для контролю доступу в зони доступу з підвищеними вимогами безпеки. При піднесенні першого ідентифікатора контролер доступу переходить в режим очікування другого ідентифікатора. Якщо пред'явлений після цього ключ має неузгоджений рівень доступу, то контролер заборонить прохід. Якщо ж рівень доступу буде узгоджений, доступ буде наданий .

Закритий режим доступу - у цьому випадку заборонені всі види доступу через керовану точку. Прилад може бути переведений в цей режим централізованою командою. Режим може бути використаний для тимчасового блокування службою безпеки доступу в певні приміщення об'єкта.

Відкритий режим доступу - через керовану точку проводиться вільний прохід без пред'явлення ідентифікаторів. У режимі «Доступ відкритий» контролер постійно видає відкритий вплив на відповідне реле (реле даного напрямку або безперервно включено, або безперервно виключено).

В залежності від розміру та виду об’єкту, який має бути забезпечений системою контролю і управління доступом розрізняють: автономні системи контролю доступу,автономні системи контролю доступу зі збором даних,мережеві та прохідні системи контролю доступу.

В наш час найбільш ефективними є системи створені на комбінації бездротових електронних замків та циліндрів з онлайн контролерами СКУД. Розподіл інтелекту системи між електронним замком/циліндром та ключем-картою дозволяє ефективно управляти системою без прокладки кабелів і перетворює систему електронних замків у повноцінну мережеву СКУД з багатьма функціями. Саме такі передові технології дозволяють вирішувати найскладніші та нестандартні задачі в рамках єдиної, гнучкої та універсальної системи контролю та управління доступом в приміщеннях будь якого типу,розміру та призначення.

В.С. Наконечний, Н.В. Цьопа
Державний університет телекомунікацій

МЕТОДИ ВИМІРУ РАДІОЛОКАЦІЙНИХ ОЗНАК ОБ’ЄКТІВ СПОСТЕРЕЖЕННЯ

Одним з найважливіших напрямів сучасної радіолокації є пошук методів здобуття якнайповнішої інформації, що міститься в радіолокаційних сигналах і перешкодах. Радіолокаційне розпізнавання (РЛР) є частиною даного напряму і передбачає вимір радіолокаційних характеристик (РЛХ) різних об'єктів, вибір найбільш інформативних, стійких ознак і ухвалення рішення щодо приналежності цих об'єктів до певного типу [1]. Розробка систем РЛР пов'язана з вирішенням ряду проблем, основними з яких є складання словника ознак і вибір найбільш ефективного алгоритму розпізнавання, здатного з високою ймовірністю правильного розпізнавання (ЙПР) класифікувати до якого типу відноситься виміряна від об'єкту дослідження інформація [2].

При одноетапному ухваленні рішення щодо типу об’єкта спостереження, алгоритми його розпізнавання відрізняються мірою обліку статистики вимірюваних ознак і перешкод. Найбільше значення ЙПР забезпечують параметричні і непараметричні байєсовські алгоритми. Складність технічної реалізації таких алгоритмів полягає у відсутності відомостей про закони розподілу вимірюваних ознак і перешкод, а також параметри цих законів. Серед одноетапних непараметричних алгоритмів найбільші ЙПР забезпечують евристичні алгоритми обчислення відстаней, зокрема алгоритм Махалонобіса [2]. Недоліком таких алгоритмів є необхідність пошуку мінімуму і зниження шумів округлення. В зв'язку з цим викликають значний інтерес евристичні алгоритми оцінки сумарної потужності ознак розпізнавання, що співпадають з ознаками еталону. До таких алгоритмів можна віднести алгоритм Кейпона та теплового шуму, ефективність яких залежить від точності виміру інформативних ознак розпізнавання [3].

Для виміру простору ознак розпізнавання найбільш зручним інструментом є радіолокація, яка по ефективності в більшості випадків перевершує відео або інфрачервоні методи виміру характеристик досліджуваних об'єктів. Радіолокаційний дальнісний портрет (РЛДП) об’єкта вважається найбільш інформативною його ознакою тому, що містить інформацію про довжину і характерні риси об'єкта (кількість максимумів, мінімумів на РЛДП та відстань між ними). Такі РЛДП можуть бути виміряні, або ж отримані, також і з використанням методів математичного чи фізичного моделювання. Основними недоліками при математичному моделюванні є обмежена точність уявлення поверхні імітаційних моделей, складність і неоднозначність рішення електродинамічної задачі взаємодії імітаційних моделей з площинною електромагнітною хвилею зондуючих сигналів, особливо в разі рухомих моделей.

При фізичному моделюванні досліджувані процеси або об'єкти відтворюються із збереженням їх фізичної природи (натурне моделювання) або з використанням подібних фізичних явищ (масштабне моделювання). Натурне моделювання процесу виміру РЛДП вимагає створення коштовних макетів РЛС, що опромінюють об'єкти. Для виміру РЛДП об'єктів під різними ракурсами необхідний або обліт їх навколо радіолокаційних станцій (РЛС) або переміщення макету РЛС навколо об'єкту, розташованого на землі. У першому випадку процес виміру РЛДП буде

достатньо коштовним, а в другому - практично не вирішується задача придушення заважаючих віддзеркалень від землі і місцевих предметів.

При масштабному моделюванні дослідження проводяться на фізичних моделях, що володіють фізичною подібністю. Прикладом дослідження процесів поширення радіохвиль може служити використання безлунових камер надвисоких частот (НВЧ) - електродинамічне моделювання, яке є основним і точним методом виміру ознак макетів об’єктів спостереження, їх РЛДП. При виконанні вимог електродинамічної подібності в виміряних результатах враховуються нелінійності трактів проходження сигналу і ефекти його перевідбиття, вклад яких практично неможливо оцінити іншими зазначеними методами.

Таким чином, при створенні систем розпізнавання, які працюють в реальному масштабі часу важливими залишаються питання виміру ознак розпізнавання об'єктів спостереження. Приведений аналіз методів виміру радіолокаційних ознак об’єктів спостереження показує, що таке вимірювання, при умовах обмеженого фінансування, можливо проводити з використанням безлунових камер НВЧ. Крім того важливим етапом розробки систем розпізнавання залишається вибір інформативних, стійких ознак і вибір ефективного алгоритму розпізнавання, що працює при обмеженому об'ємі навчальної вибірки в реальному часі.

Яскравими представниками таких алгоритмів є відомі в цифровому спектральному аналізі алгоритми Кейпона та теплового шуму, які можуть бути застосовані і на етапі порівняння вектора виміряних від об'єкту ознак з еталонами, що зберігаються в банку еталонних ознак системи розпізнавання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Небабин В.Г. Методы и техника радиолокационного распознавания / В.Г. Небабин, В.В. Сергеев. - М.: Радио и связь, 1984. - 154 с.

2. В.С. Наконечний. Исследование возможности измерений радиолокационных дальностных портретов воздушных целей при использовании современных методов цифрового спектрального анализа / Н.В. Мордвицев, В.С. Наконечний, К.В. Садовый // Контрольно-измерительные приборы и автоматика. – Х.:ФТИ, 2005. - Вып. май/июнь. - С. 43 – 47.

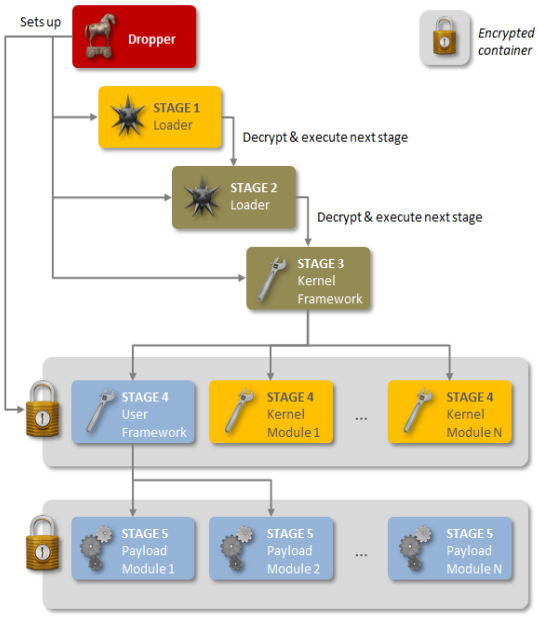
3. Марпл.-мл. С.Л. Цифровой спектральный анализ и его приложения: пер. с англ. / С.Л. Марпл.-мл. - М.: Мир, 1990. - 584 с.

О.В. Богомоленко, А.С. Старжинський.
Державний університет телекомунікацій

ДОСЛІДЖЕННЯ ТРОЯНСЬКОЇ ПРОГРАМИ REGIN

Мета. Розглянути троянську програму під назвою Regin. Провести аналіз дослідницьких звітів Symantecі Лабораторії Касперського. Визначити основні напрямки і принципи роботи Regin.

Вступ. За даними звіту Symantec, троянський кінь Regin приховано працює з 2008 року і є дуже серйозною розробкою, яка максимально налаштовується, надаючисвоїм власникам віддалений доступ, а також спостерігати за мережевим трафіком. Основною його метою є шпигунство, а основними об'єктами атаки стали оператори зв'язку, через які це шпигунство і здійснювалося.



Структура троянської програми Regin

Постановка задачі. Regin – багаторівнева програма, в якій кожен рівень замаскований і зашифрований, крім першого етапу. Запуск першого породжує ланцюгову реакцію з розшифровкою кожного наступного. Тільки після «складання» всіх п'яти рівнів можливо проаналізувати функціональність програми. Тому виявити її не вдавалося так довго.

Regin, атакує лише найважливіші цілі з обмеженого списку категорій: телекомунікаційні компанії, органи державної влади, фінансові та наукові установи, міжнародні політичні організації і вчені, що беруть участь в математичних і криптографічних дослідженнях.

Програма складається з близько 50 модулів, у кожного з яких своя задача. Далі приведено декілька з цих модулів.Модуль RAT дозволяє своїм власникам як отримати віддалений доступ, так і робити скріншоти або ж спостерігати за мережевим трафіком. Присутній модуль, що використовується при зараженні інфраструктури GSM-зв'язку і виявлений в мережі одного з великих операторів зв'язку. Його основною функцією є запис всієї активності певних базових станцій стільникового зв'язку, модуль веде журнал, де зберігаються всі введені команди для базових станцій виробництва Ericsson. Також присутній модуль для моніторингу трафіку веб-сервера Microsoft IIS.

Механізм управління та контролю Regin вкрай складний і заснований на комунікаційних вузлах, встановлюваних зловмисниками в мережі жертви. Зловред зв'язується з іншими машинами мережі, використовуючи різні протоколи, відповідно до налаштувань конфігураційного файлу. Межові машини мережі працюють в якості маршрутизатора, пов'язуючи заражені машини жертв із зовнішніми серверами управління і контролю.

Результати аналізу досліджень і висновки.

Таким чином, є два основних напрямки роботи Regin: збір інформації та забезпечення проведення атак інших типів. На даний момент ця проблема залишається актуальною, так як виявити цю програму в системі вкрай важко. Виходячи зі складності та вартості розробки Regin, дослідники «Лабораторії Касперського» уклали, що ця операція повинна мати підтримку державного рівня а також й те, що це серйозна розробка, на яку пішли місяці або навіть роки. При цьому вдалося знайти вкрай малий об'єм метаданих, що ускладнює визначення того, яка країна стоїть за цією атакою.

Список використаної літератури

1. Kaspersky Lab Report, Version 1.0 - 24 November 2014.
2. Symantec Security Response, Version 1.0 – November 24, 2014.

Корченко О.Г., д.т.н., проф.
Національний авіаційний університет
Дрейс Ю.О., к.т.н.
Житомирський військовий інститут ім. С.П. Корольова ДУТ

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Донедавна функції захисту персональних даних виконувала Державна служба України з питань захисту персональних даних (ДСЗПД), але після факту несанкціонованого втручання в роботу інформаційних систем (ІС) Міністерства юстиції України, що призвело до припинення функціонування 12 Державних та Єдиних реєстрів інформаційної мережі через блокування інформації і порушення встановленого порядку її маршрутизації, цю службу було скомпрометовано щодо належного і гарантованого захисту окремих державних інформаційних ресурсів (ДІР). Це стосується саме тих ДІР, які містять дані про фізичних осіб, що обробляються без їх згоди в інтересах національної безпеки, економічного добробуту та прав людини, тобто, *персональних даних* (ПД) розпорядником яких є держава.

Як наслідок, у 2013 році після внесення змін до Закону України «Про захист персональних даних» контроль за додержанням законодавства про захист ПД покладено на Уповноваженого Верховної Ради України з прав людини та суди, а забезпечувати захист ПД від випадкової втрати або знищення, незаконної обробки чи доступу до цих ПД зобов’язано володільців, розпорядників ПД та третіх осіб. Зокрема, в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках ПД має бути створений структурний підрозділ або визначена відповідальна особа, яка організовує роботу, пов’язану із захистом ПД при їх обробці. Як факт остаточного усунення уповноваженого державного органу з питань захисту ПД вказує й прийнята Постанова Кабінету Міністрів України (КМУ) № 442 від 10.09.2014 року «Про оптимізацію системи центральних органів виконавчої влади» за якою ДСЗПД ліквідовано.

Однак відомо, що ПД, крім знеособлених, за режимом доступу є інформацією з обмеженим доступом (ІзОД), а саме – *конфіденційною інформацією* (КІ). Тому держава, як розпорядник ПД якому (в інтересах національної безпеки) надано право обробляти ці дані від імені володільця, повинна не тільки визначати склад цих ПД, мету і процедуру їх обробки, але й забезпечувати захист такої КІ у власних ІС.

На попередження й нейтралізацію існуючих наразі потенційних і реальних загроз національній безпеці в інформаційній сфері, згідно рішення Ради національної безпеки і оборони України від 28.04.2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», Державну службу спеціального зв’язку та захисту інформації України разом зі Службою безпеки України зобов’язано: 1) розробити та подати на затвердження КМУ заходи щодо посилення захисту ДІР від протиправного втручання; 2) ужити додаткових заходів щодо захисту ІзОД (насамперед ПД, що належать до КІ) під час її обробки в ІС.

Тептя І.І, Білобородов М.Ю.
Державний університет телекомунікацій

Стенографічний метода передачі даних, що використувую службові сигнали мережевого протоколу OSPF

Мета. Розглянути службові пакети, що використовуються у роботі протокола мережевого рівня моделі OSI — OSPF та визначити можливості передачі даних за домогою таких пакетів.

Вступ. OSPF - протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology) і використовує для знаходження найкоротшого шляху алгоритм Дейкстри.

Постановка задачі. OSPF використовує 5 типів пакетів службових:
Hello - використовується для виявлення сусідів і побудови відносин сусідства з ними.
Database Description (DBD) - перевіряє синхронізацію бази даних між маршрутизаторами
Link-State Request (LSR) - запитує певні записи про стан каналів від маршрутизатора до маршрутизатора.
Link-State Update (LSU) - відправляє певні записи про стан каналів у відповідь на запит.
Link-State Acknowledgment (LSAck) - підтверджує отримання інших типів пакетів.

При певному налаштуванні апаратного і програмного забезпечення маршрутизаторів можливо здійснивати передачу невеликих текстових файлів, скриваючи сам факт такої передачі від зловмисників. Пакети мають довжину 32 біта, але використовувати у кожному пакеті можна не більше 8. Навіть якщо у мережі не відбувається передача жодних даних, за допомогою службових пакетів можливо передати інформацію, тому що обмін службовими пакетами відбувається завжди, тобто для скриття факту самої передачі не потрібний “фоновий шум” у вигляді передачі даних по запиту користувача.

Результати аналізу досліджень і висновки.

Таким чином, такий спосіб передачі даних може використовуватись в мережах, лінії передачі яких можуть піддаватися перехвату та зняттю інформації. Для повного налаштування передачі інформації таким чином потрібний дуже глибокий аналіз роботи самих маршрутизаторів та їх переналаштування на програмному та апаратному рівні.

Список використаної літератури

1. Пузиренко, Олександр (2006). «Комп’ютерна стеганографія. Теорія і практика»
2. http://xgu.ru/wiki/ospf

Ярош В., Ільницька М.
Державний університет телекомунікацій

Технології захисту інформації у віртуальних приватних мережах

Мережа Internet є загальновживаною та загальнодоступною. Вона побудована на принципах відкритих систем. Інформація передається по загальнодоступних каналах, тому потенційно можливе порушення конфіденційності, цілісності та доступності інформації.

Забезпечення безпечної передачі даних через мережу Інтернет зараз
становить одну з найважливіших проблем. Кількість мережевих атак постійно зростає, вони якісно змінюються, тому пошук надійної системи захисту інформації завжди актуальний. На сьогоднішній день широкого розповсюдження набули мультисервісні мережі. Вони представляють собою мережі нового покоління, основною особливістю яких є передача різних типів інформації (інтернет, передача даних, відео, аудіо, телефонія) по одній мережі (наприклад волоконно-оптичній), завдяки чому досягається універсальний доступ до мережі, надається різноманітний спектр послуг, від розважальних до навчальних. Для передачі важливої конфіденційної інформації існує можливість створення мереж за допомогою технології VPN (Virtual Private Network) - "віртуальна приватна мережа". Суть цієї технології в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організовується зашифрований канал, що забезпечує високий рівень захисту каналу інформації. У загальному випадку VPN - це об'єднання локальних мереж або окремих комп'ютерів, підключених до мережі загального користування, в єдину віртуальну мережу, що забезпечує конфіденційність і цілісність переданої інформації. Використання технології VPN доцільно для захисту корпоративної мережі від дії вірусів, зловмисників, а також від інших загроз, які є результатом помилок в конфігурації або адмініструванні мережі.

Можна виділити три основні технології захисту інформації що перетворюють корпоративну мережу, побудовану на базі мережі загального користування, у захищену віртуальну приватну мережу:

- шифрування;
- аутентифікація;
- контроль доступу.

Тільки реалізація всіх цих трьох властивостей дозволяє захистити інформаційні ресурси корпорації та фізично незахищені канали зв'язку від несанкціонованого доступу та витоку інформації .

Всі продукти для створення VPN можна умовно розділити на дві категорії: програмні і апаратні. Програмне рішення для VPN - це, як правило, готовий додаток, що встановлюється на підключеному до мережі окремому комп'ютері. Розгортати апаратно VPN, безумовно легше. Для цього необхідно підключити мережеве обладнання (комутатори, концентратори, маршрутизатори), які підтримують VPN протоколи.

Отже, застосування програмно-реалізованих технологій VPN дозволяє

ефективно забезпечити швидку та безпечну передачу конфіденційної інформації через мережу Інтернет. Перевагою технології VPN є те, що
організація віддаленого доступу робиться не через виділені канали зв'язку, а через Інтернет, що набагато дешевше й легше. Недолік технології VPN в тому, що засоби її побудови не є повноцінними для виявлення та блокування атак.

І.Е. Похабова, д.т.н., проф. Беркман Любов Наумівна
Державний університет телекомунікацій

Особливості векторного синтезу систем управління програмно-конфігурованої мережі

Згідно з прогнозами, при підвищенні якості та збільшенні обсягу наданих послуг кількість управляючої інформації в СУ стрімко зростає. Внаслідок цього СУ може поглинути основну мережу.

СУ адекватно поняттю - "велика система". Останнє характеризується кількома специфічними ознаками. Це, насамперед, багатомірність розмаїття структури; багатозв'язність елементів (взаємозв'язок підсистем на одному рівні та між різними рівнями ієрархії); різнорідність бази елементів; багатократність зміни складу і стану (змінність структури, зв'язків і складу системи); багатокритеріальність; багатоплановість.

Система управління (СУ) сучасними телекомунікаційними мережами має такі характерні ознаки:

- великі розміри;
- складність;
- розвинуті функціональні можливості;
- конкурентноспроможність;
- жорстку вимогливість до забезпечення захисту інформації;
- високу чутливість до помилок.

Загальна постановка задачі векторного синтезу зводиться до системи управління. Кожна система характеризується вектором показників якості: $K=(k_1, k_2, \ldots, k_m)$. У m-мірному просторі R_m показників якості $k_1, \ldots, k_m$ кожній СУ відповідає єдине визначене значення вектора і навпаки, кожному вектору K відповідає єдина цілком визначена система. У просторі R_m всім строго допустимим значенням вектора K відповідає множина точок (множина строго допустима, що задовольняє цим обмеженням). Вид цієї множини визначається сукупністю умов і обмежень, які накладаються на синтезовану систему та її показники якості.

Задача векторного синтезу зводиться до того, щоб з множини строго допустимих точок вибрати таку точку (систему), яка має найкраще значення вектора K. При цьому передбачається, що поняття "найкращого вектора K" уточнюється, виходячи з умови задачі.

Крушець А.О.
Державний університет телекомунікацій

НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО КОМП'ЮТЕРА ЗА ДОПОМОГОЮ ЛЕГАЛЬНОГО ПЗ

Як вже відомо, що головним ворогом хакерів (в даному випадку цим терміном позначаються ті, хто займається створенням / розповсюдженням шкідливих програм) є антивіруси, які з тим або іншим ступенем успішності виявляють їх вироби і видаляють. Одним із способів запобігання виявленню їх незаконної діяльності і використовуваних для цього утиліт є спроба «змусити» легальне ПЗ служити їхнім цілям.

Останнім часом найбільшу популярність серед хакерської спільноти здобула програма Remote Manipulator System (RMS) виробництва російської компанії Tekton IT.

Головні функції даної програми:

1. Можливість прихованої установки і роботи;
2. Зв'язок через сервер, а не до IP безпосередньо;
3. Можливість управління великою кількістю комп'ютерів;
4. ПЗ легально та має ЕЦП;
5. Файли самої програми детектуються невеликою кількістю антивірусів.

Коротко про технологічну суть роботи RMS:

1. На комп'ютер «жертви» в прихованому режимі встановлюються файли RMS, причому іноді навіть за допомогою офіційного installer, хоча частіше «вручну» - скрипт кладе файли в потрібну папку і запускає їх «тиху» реєстрацію або реєструє їх сам;
2. Господарю на пошту приходить ID і пароль;
3. У ботнеті зловмисника з'являється +1.

Реалізується це у вигляді SFX-архіву з bat-файлом, який все зробить або у вигляді NSIS - installer.

Було проведено дослідження на детектування різними антивірусами в наступних номінаціях:

1. детектування файлу rutserv.exe з різних версій RMS.
2. детектування файлу з під іншого білдера (він завжди однаковий, а cfg різний);
3. детектування bat-файлів для установки RMS в систему - взято їх з різних статей з самостійної збірки даного «шкідника» і кілька з форумів, де навпаки намагаються позбутися цієї загрози.

Antivirus	rutserv.exe	second builder	bat-files
Avast	-	+	+
DrWeb	+/-	+	+
ESET-NOD32	+	-	+/-
Kaspersky	+	+	+

Таким чином, з представленої таблиці видно, що не кожна антивірусна програма здатна впоратися з даним видом загроз (несанкціонованого доступу). Тобто, мається на увазі, що в якості троянів можна використовувати цілком легальні і безумовно потрібні програми для адміністрування, адже RMS - це не єдина програма, їх дуже багато.

Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. (2004 г.)

Крушець А.О., Сорокін Д.І.
Державний університет телекомунікацій

СТІЙКІСТЬ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ – ЗА ГОЛОСОМ

Що ж насправді є аргументом стійкості систем аутентифікації по голосу?

Звичайно ж, якщо мова йде про біометричну аутентифікацію не суттєво знижуючи або підвищуючи стійкість системи в порівнянні з парольним захистом.

Очевидно, що доводитися повинна саме стійкість методів, а не їх нестійкість. Також, як доводиться стійкість шифру перед його використанням (хоча доводиться вона саме спробами злому і статистичним аналізом). У разі помилкового прийняття нестійких методів можуть постраждати десятки або навіть сотні мільйонів людей.

Саме тому далі буде розглянуто основні докази стійкості біометричної аутентифікації:

1. Повинно бути показано, що поєднання розпізнавальних параметрів голосу важко відтворити спільно з обманом системи розпізнавання мови (одноразової кодової фрази).

2. На базі накопиченої з кількох мільйонів записів, що належать сотням тисяч осіб, повинна бути запущена система аутентифікації, яка розподілить всі записи згідно з їх власниками.

3. Система повинна виключати те, що зловмисник збере в режимі реального часу кодову фразу з доступних йому записів голосу, враховуючи можливість того, що зловмиснику доступні записи будь-яких часто вживаних слів, букв і їх поєднань.

4. Наявність багатофакторної біометричної ідентифікації для ускладнення роботи зловмисника.

5. Відсутність віддаленої біометричної ідентифікації, а використання багатофакторної біометричної ідентифікації лише для розблокування захищеного від крадіжки інформації електронного ключа, за допомогою якого виконується криптографічна аутентифікація на сервері.

Взагалі системи віддаленої біометричної аутентифікації можуть бути стійкими до віддаленого використання, проте ця стійкість, швидше за все, буде значно нижче стійкості традиційного парольного захисту (так як зразки голосу можна вкрасти не лише з пристрою, а пароль - тільки з пристрою, на якому він вводиться).

Проте найкраще, коли системи віддаленої аутентифікації будуть комбінованими. А саме, використовувати пристрої, що активізуються за допомогою біометрії, але здійснюють аутентифікацію за допомогою криптографічних методів. Таким чином, біометричний захист, фактично, переходить з віддаленої в локальну систему. У такому випадку, зловмисникові доведеться фізично красти пристрій, що підвищує надійність аутентифікації і робить її більш стійкою, ніж однофакторний парольний захист.

Анализ биометрических интеллектуальных методов аутентификации и идентификации личности по от печаткам пальцев и по голосу для защиты от несанкционированного доступа/ П. А. Филоненко, Е. И. Барсуков, Е. А. Винокурова(2012 г.)

СорокінД.І.
Державний університет телекомунікацій

ВАГОМІ ДІРИ В ЗАХИСТІ ВЕБ-САЙТІВ ВІД CSRF-АТАК

На сьогоднішній день у сфері забезпечення безпеки веб-сайтів та програм виникла достатньо бентежна ситуація: з одного боку, деякі розробники приділяють особливу увагу безпеці, з іншого, вони геть забувають про деякі види атак і не вважають помилки, що дозволяють виконати дані атаки, уразливими. До такої категорії можна віднести CSRF (CrossSiteRequestForgery). Ця атака дозволяє виробляти різні дії на уразливому сайті від імені авторизованого користувача.

Якщо підходити формально, то CSRF є атакою, а не вразливістю, як і XSS. Уразливістю є неправильна обробка вхідних даних, а CSRF це використовує.

Надалі буде розглянуто основні типові помилки, які найчастіше допускаються при забезпеченні безпеки веб-сайтів:

- Повністю відсутній захист від CSRF;

- Захищені не всі запити (На багатьох сайтах, де реалізований який-небудь захист від CSRF, можна знайти вразливі запити.Ви повинні захищати абсолютно всі запити, які змінюють що-небудь на сайті. Додавши токен в форму зміни адреси електронної пошти, зловмисник не зможе заволодіти аккаунтом вашого користувача, змінивши від його

імені пошту, а потім і пароль. От тільки така міра марна, якщо можна просто відправити запит на переказ грошей з акаунта жертви на гаманець атакуючого, минаючи даний захист);

- Використання для захисту від CSRF чого-небудь, крім токенів;
- Відсутність перевірки анти-CSRF токена при обробці запиту;
- Часткова перевірка анти-CSRF токена (Наприклад, один із сайтів використовував токени виду «Ім'я_користувача. Поточний_час. Довге_випадкове_число». При цьому перевірялося тільки відповідність імені користувача в токені і логіна того, від чийого імені було відправлено запит. Це трохи ускладнює атаку, але не робить її неможливою);
- Можливість використовувати один токен для різних користувачів;
- Недостатня довжина точена (токен повинен бути настільки довгим, щоб зловмисник витратив на його підбір як мінімум стільки ж часу, скільки і на підбір пароля користувача);
- Передбачувані токени;
- Відсутність токенів в адмін-панелі або системі для співробітників тех.підтримки;
- Передача токенов у відкритому вигляді, особливо в GET-запитах.

Наявність цих помилок навіть на великих і серйозних сайтах показує, що проблема захисту від CSRF-атак стоїть досить гостро. Безумовно, цей список не є вичерпним. Однак якщо ви перевірите свої сайти на наявність проблем і виправите їх, то значно підвищите захищеність проекту.

Скембрей Д., Шема М. "Секреты хакеров. Безопасность Web-приложений" – 2003.

Фомін О. О.
Державний університет телекомунікацій

БЕЗПЕКА МЕРЕЖЕВОГО ЦЕНТРУ ОБРОБКИ ДАНИХ

У корпоративних центрах обробки даних містяться ресурси, додатки та інформація, які часто стають метою мережевих атак зловмисників. Кінцеві пристрої, наприклад, сервери центрів обробки даних, є "ласим шматочком" для зловмисника і тому потребують надійного захисту. Атаки проти груп серверів можуть призвести до порушення працездатності додатків електронної комерції та додатків типу B2B, а також до крадіжки конфіденційної інформації або інформації, що представляє для організації особливу цінність. Для того щоб знизити ймовірність катастрофічних наслідків, організаціям необхідно забезпечити надійний захист як локальних мереж, так і мереж зберігання даних (SAN).

Розуміння механізмів проведення мережевих атак двох найбільш поширених типів дозволяє краще оцінити, наскільки рішення інформационной безопастности для центрів обробки даних пом'якшують наслідки таких атак або запобігають їх здійснення.

Розглядаються атаки двох типів: крадіжка даних і поширення Інтернет- черв'яків. Атаки першого типу спрямовані на крадіжку інформації; метою атак другого типу є блокування нормальної роботи додатків, тому їх можна класифікувати як атаки типу "відмова в обслуговуванні" (DoS).

До заходив захисту можна Віднести:

- Розмежування доступу і сегментація доступу
- Безпека протоколів стека TCP / IP
- Аутентифікація, питання цілісності і конфіденційності
- данни х при взаємодії клієнтів і серверів
- Аналіз трафіку, виявлення і запобігання вторгненнї
- Забезпечення безпеки мережевих пристроїв
- Доступ до структурі комутації і цільовим пристроям
- Безпека протоколів SAN
- Безпека доступу до сховищу з використанням протоколу ip
- Цілісність і конфіденційність даних
- Доступ до механізмам мережевого управління

Для запобігання несанкціонованого доступу необхідно забезпечити захист керуючих інтерфейсів мережевих пристроїв: зловмисник, що володіє доступом до консолі мережевого пристрою, може легко змінити конфігурацію мережі і створити "люк", що дозволяє обійти систему безпеки..

Иванчук В.И.
Государственный университет телекомуникаций

Методика проектирования системы информационной безопасности в ИТ

Быстрое развитие и повсеместное проникновение информационных технологий в самые различные сферы деловой деятельности привело к тому, что информация в настоящее время имеет вполне определенную стоимость. В связи с этим выросла вероятность утечки защищаемой информации, что привело к необходимости применения защитных мер для предотвращения ее утечек.

Меняется среда ведения бизнеса: мобильность, совместная работа, виртуализация и вычислительные облака становятся причинами появления новых угроз. За последние несколько лет одним из приоритетов в области бизнеса стало: обеспечение бесперебойности деятельности, снижение рисков и повышение защищенности.

Информационная безопасность (далее ИБ) – это длительный и сложный процесс, состоящий из множества элементов. Малейшая уязвимость и несогласованность (например, со службой ИТ) в любом из них приводит к ослаблению всей системы. Поэтому к ИБ нужен комплексный подход.

Основными задачами системы ИБ являются обеспечение конфиденциальности, целостности и доступности информации.

Крайне важно при решении данных задач добиваться экономической эффективности ИБ. Необходимо оценивать стоимость защищаемой информации, ущерб от инцидентов, эффективность проектов по ИБ.

Объектом исследования работы являлась система ИБ крупного ИТ-холдинга.

Цель работы – разработка централизованного подхода к обеспечению и управлению ИБ в крупной ИТ-компании с распределенной филиальной сетью, на основе практического внедрения.

Для достижения поставленной цели в работе решались следующие задачи: исследование вопросов управления ИБ; проведение аудита ИБ; создание организационно-распорядительных документов по ИБ; формирование портфеля проектов ИБ, направленных на достижение приемлемого уровня защищенности с экономическим обоснованием инвестиций в безопасность.

При построении или модернизации системы обеспечения ИБ необходимо руководствоваться едиными принципами и подходами. В противном случае конечным результатом станет разрозненный набор технических средств и документов, который нельзя будет назвать «системой» и эффективность которого будет невысока. Соответственно, сделанные компанией инвестиции не дадут ожидаемого эффекта.

Стартом проекта стал проведенный внешней организацией анализ угроз и уязвимостей (GAP-анализ) и технический анализ (тесты на проникновение) применяемых механизмов обеспечения ИБ в ИТ. В ходе выполнения аудита использовались передовые методики и стандарты, такие как Open Source Security Testing Methodology Manual, Standards for Information Systems Auditing , Web Application Security Consortium , Open Web Application Security Project.

По результату проведенного аудита была разработана Концепция обеспечения ИБ. Определены основные цели, задачи и требования, а также общая стратегия построения системы ИБ, составлен перечень важных информационных ресурсов.

Следующим этапом построения системы ИБ было ее проектирование, включая систему управления ИБ. При выборе поставщиков продуктов для комплексной системы ИБ, был проанализирован рынок основных производителей решений в области ИБ. Остановились на тех, кто входит в консорциум Open Platform for Security, объединяющий более 300 производителей, продукты которых можно интегрировать в «единый организм»

После проведения тестирования спроектированной системы ИБ, приступили к ее внедрению. Работы по внедрению включали выполнение следующих основных задач: поставка, инсталляция и настройка компонентов ИБ, приемо-сдаточные испытания, обучение пользователей и ввод системы ИБ в промышленную эксплуатацию.

Для эффективной дальнейшей эксплуатации системы необходимо обеспечить ее поддержку и сопровождение, собственными силами компании или силами привлекаемых специалистов.

В результате проекта в ИТ-холдинге были разработаны и внедрены:

- базовые процессы поддержки ИБ на основе рекомендаций ITIL и Cobit;
- политика ИБ;
- частные политики ИБ;
- план восстановления ИТ после сбоя;
- проекты, направленные на достижение приемлемого уровня обеспечения ИБ;
- регламенты, процедуры, внутренние технические стандарты.

В качестве критических факторов успеха построения системы ИБ необходимо рассматривать следующее: политика ИБ организации, принципы обеспечения ИБ, поддержка высшего руководства в вопросах безопасности, анализ и управления рисками, распространение разъяснений по политике ИБ среди сотрудников и контрагентов, сбалансированная система измерения эффективности и совершенствования системы ИБ.

Подводя итог, можно сказать, что система ИБ – это именно система, требующая понимания, планирования и адекватных затрат для нормального и успешного функционирования. Успех растущего бизнеса, обеспечивается тщательным планированием, особенно в вопросах безопасности.

Кузьмич Олег Юрійович
Державного університету телекомунікацій , м. Київ

Дослідження кіберзлочинності, пов'язаною з ризиком НСД до ІзОД

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, інформації, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від "робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксіватиї і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців.

Далі буде розглянуто основні види кіберзлочинності та способи протидії:

- **Фішинг** - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти,інтернет-магазинів.

  Протидія: Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується «антифішинг».
- **Смішінг** - вид фішингу через SMS. Шахраї відправляють жертві SMS-повідомлення, що містить посилання на фішинговий вебсайт і мотивуюче повідомлення увійти на цей сайт.

  Протидія: Треба бути обережними і пам'ятати, що інформацію про раптове отриманні призу у розіграші / лотереї / акції, в яких ви не виявляли бажання брати участь, надсилають різного роду шахраї і фішери. І хочуть вони зовсім не обдарувати вас, а роздобути тим чи іншим способом ваші гроші.
- **Кіберсквоти́нг** - протизаконна діяльність, що полягає у реєстрації, використанні та пропонуванні до продажу доменного імені із несумлінним наміром отримати прибуток від паразитування на гудвілі або торговельній марці, яка належить іншій особі. Після несумлінної реєстрації, несумлінний реєстрант (*кіберсквотер*) зазвичай пропонує продати доменне ім'я законному власнику знака за значно вищою ціною.

  Протидія: Вводити URL-адресу вручну і переконатися в тому, що він набраний без помилок; Не відкривати підозрілі повідомлення електронної пошти і не проходити по посиланнях в них; Усунути уразливості в ОС і додатках; Встановити антивірусне програмне забезпечення для захисту від інтернет-загроз і своєчасно оновлювати його.
- **Ата́ка «злий двійни́к»** - різновид фішинга, вживана в бездротових комп'ютерних мережах. Атакуючий створює копію бездротової точки доступу, що знаходиться в радіусі прийому користувача, тим самим підміняє оригінальну точку доступу двійником, до якого підключається користувач, відкриваючи зловмисникові можливість доступу до конфіденційної інформації.

  Протидія: Уважність. Найчастіше можливо виявити підміну логін-сторінок через недостатньо точного копіювання оригіналу атакуючим. Слід звертати увагу на дрібниці, такі, як анімації на сторінці, присутність на сторінці всіх картинок, відповідність версій сторінки, наприклад, для мобільних пристроїв чи ні; Використовувати віртуальну приватну мережу при підключенні до відкритих бездротових мереж. У цьому випадку мережевий трафік на шляху від клієнта до VPN-сервера зашифрований. Атакуючий не зможе отримати з каналу зв'язку інформацію про дії клієнта і підмінити оригінальні сайти фішинговими двійниками; Стежити за повідомленнями браузера про порушення шифрування або невідповідних сертифікатах безпеки. При спробі підміни сайту, що використовує шифрування каналу зв'язку на рівні протоколу (протоколи SSL / TLS / HTTPS), браузер може видати помилку.
- **Спам** - масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів. Також вважаються спамом освідчення в коханні на електронну пошту, в чатах, соціальних мережах тощо.

  Протидія: **Використання капчі** (капча - графічний малюнок із зображенням цифр/символів); **блокування спамерів по ір-адресі; блокування спам-роботів за допомогою параметра REFERER**(адреса попередньої сторінки-джерела звідки виконаний перехід); **блокування/видалення спама за допомогою фільтра тексту на спам-слова.**
- **DOS\DDOS Атака (Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні)** - напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними до користувачів, для яких комп'ютерна система була призначена.

Також, способами захисту від кіберзлочинності можуть бути: отримання чіткої інформації про особу або підприємства, використання електронних сертифікатів, ЕЦП, безпечних протоколів передачі даних; прийняття відповідних законодавчих актів тощо.

Боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Одним за таких кроків є підписання у листопади 2001р. Радою Європи, а також США, Канадою та Японією «Міжнародної конвенції про кіберзлочинність». Але оскільки кіберзлочинність частково належить до внутрішньої компетенції кожної держави окрема, то необхідним є паралельне напрацювання і національного законодавства, яке буде спрямоване на боротьбу з комп'ютерними злочинами.

Таким чином, кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

Список літератури

- Кіберзлочинність можна зупинити тільки разом.-// Україна:бізнес-ревю №5-6 від 11.02.2013.
- Комп'ютерна злочинність - К.: Атіка, 2002
- Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004.
- Разработка европейского законодательства по борьбе с киберпреступностью. // Уголовное право. 2005. № 1.

Фузік К. М.
Державний університет телекомунікацій

Зниження впливу побічних електромагнітних випромінювань на комунікаційне обладнання

Побічні електромагнітні випромінювання, що генеруються електромагнітними пристроями, обумовлені протіканням диференціальних і синфазних струмів.

Випромінювання, викликане синфазними струмами, обумовлено виникненням спадань напруги в пристрої, що створює синфазну напругу щодо землі.

У процесі функціонування засобів обчислювальної техніки в конструктивних елементах та кабельних з'єднаннях циркулюють електричні струми інформативних сигналів, у результаті чого формуються електромагнітні поля, рівні яких можуть бути достатніми для приймання сигналів і здобування інформації за допомогою спеціальної апаратури.

Канали витоку інформаціє можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території (КТ). Інформативні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами КТ.

Класифікація електричних каналів витоку інформації:

- Паразитні зв'язки і наводки
- Паразитні ємнісні зв'язки
- Паразитні індуктивні зв'язки
- Паразитні електромагнітні зв'язки
- Паразитні електромеханічні зв'язки
- Паразитні зворотні зв'язки через джерела живлення
- Витік інформації по ланцюгах заземлення

Для зменшення рівня побічних електромагнітних випромінювань застосовують спеціальні засоби захисту інформації: екранування, фільтрацію, заземлення, електромагнітне зашумлення.

Високочастотні поля екранують феромагнітними матеріалами, або високопровідними немагнітними матеріалами. Але, такі матеріали є досить дорогими, тому екранування є дорогим рішенням. Останнім часом з'явилися композиційні матеріали, які можуть бути ефективним і досить дешевим розв'язком цієї проблеми.

Свередюк К.А.
Державний університет телекомунікацій

АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодення характеризується інтенсивним впровадженням інформаційних технологій в усі сфери діяльності. Особливо широко інформаційні технології застосовуються в державних органах влади, кредитних організаціях (банки, біржі, фонди), у великих системоутворюючих організаціях (нафтові, газові, енергетичні компанії, в торгівельних та інших). Важко знайти організацію, в якій в тій чи іншій мірі не використовувалися б засоби інформатизації.

Водночас значно почастішали несанкціоновані дії на інформаційні системи як з боку злоумисників, конкурентів, так і співробітників фірм. Саме тому більшість організацій направляють значні кошти на забезпечення певного рівня інформаційної безпеки. Вимоги інформаційної безпеки повинні бути спрямовані на забезпечення оптимального режиму функціонування інформаційної системи в цілому. В свою чергу побудова будь-якої системи інформаційної безпеки має починатися з аналізу ризиків інформаційної безпеки.

Згідно з ISO 31000:2009, оцінка ризику - це загальний процес ідентифікації ризику, його аналізу та визначення.

Таким чином, при проведенні повного аналізу ризиків інформаційної безпеки необхідно:

- Визначити цінність ресурсів;
- Додати до стандартного набору список загроз, актуальних для досліджуваної інформаційної системи;
- Оцінити ймовірність загроз;
- Визначити вразливість ресурсів;
- Запропонувати рішення, що забезпечує необхідний рівень інформаційної безпеки.

В першу чергу аналіз ризиків рекомендується проводити у випадках:

- Оновлення інформаційної системи або істотних змін в її структурі;
- Переходу на нові інформаційні технології побудови комп'ютерних інформаційних систем;
- Організації нових підключень в компанії (наприклад, підключення локальної мережі філіалу до мережі головного офісу);
- Підключення до глобальних мереж (в першу чергу до Internet);
- Змін у стратегії і тактиці ведення бізнесу (наприклад, при відкритті електронного магазину);
- Перевірки ефективності корпоративної системи захисту інформації.

Також слід наголосити, що аналіз ризиків інформаційної безпеки є обов'язковим етапом як в рамках побудови комплексних систем захисту інформації (п. 6.1.3 НД ТЗІ 3.7-003-05) так і в рамках побудови систем управління інформаційної безпеки для банківської сфери та для підприємства іншого виду діяльності (вимоги п. 6.1.2 ISO/IEC 27001: 2013, п. 4.2.1 ISO/IEC 27001: 2005, п. 4.2.1 СОУ Н НБУ 65.1 СУІБ 1.0:2010).

Аналіз ризиків можна підрозділити на два взаємно доповнюючі один одного види: якісний і кількісний. Якісний аналіз має на меті визначити (ідентифікувати) чинники, області та види ризиків. Кількісний аналіз ризиків повинен надати можливість чисельно визначити розміри окремих ризиків і ризику підприємства в цілому.

Підсумкові результати якісного аналізу ризику, в свою чергу, слугують вихідною інформацією для проведення кількісного аналізу.

Підхід на основі аналізу інформаційних ризиків підприємства є найбільш значущим для забезпечення інформаційної безпеки. Однак при використанні в організації комплексної, налагодженої системи забезпечення інформаційної безпеки аналіз інформаційних ризиків застосуємо як один з методів вимірювання ефективності захисту інформації.

При цьому слід зазначити що, результат аналізу повинен бути зіставний та відтворюваний, та незалежити від досвіду та кваліфікації фахівця який цей аналіз проводив.

Гнатченко А. В.
Державний університет телекомунікацій

Дослідження методів забезпечення безпеки електронних документів

Поняття «електронного документу» та його особливості.

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Останнім часом, у зв'язку з бурхливим розвитком комп'ютерної техніки і комп'ютерних мереж загального доступу, виникла можливість перенесення частини діяльності господарюючих суб'єктів і державних органів управління в так званий "кіберпростір", під яким варто розуміти циркуляцію вмісту локальних і глобальних мереж, об'єднаних Інтернетом.

Електронний документ - це зафіксована інформація у виді електронних даних, включаючи обов'язкові реквізити документа відповідно до Положення про документальне забезпечення записів затвердженим Міністерством фінансів України.

Поняття "електронний документ" є полісемічним за своєю сутністю. Це пов'язано з тим, що на відміну від документа в традиційному розумінні ЕД нерозривно пов'язаний з програмно-апаратними засобами ЕОТ, за допомогою якої він створюється, підписується, передається та зберігається.

Основні засоби захисту електронних документів

Елемент організаційного захисту є стержнем, який зв'язує в одну систему всі інші елементи. Центральною проблемою при розробці методів організаційного захисту інформації є формування дозвільної (обмежувальної) систем і доступу персоналу до конфіденційних відомостей, документів і баз даних. Важливо чітко і однозначно встановити: хто, кого, до яких, відомостей, коли, на який період і як допускає.

Дозвільна система доступу вирішує наступні задачі: забезпечення співробітників всіма необхідними для роботи документами і інформацією; обмеження кола осіб, які допускаються до конфіденційних документів; виключення несанкціонованого ознайомлення з документу Ієрархічна послідовність доступу реалізується по принципу "чим вища

цінність конфіденційних відомостей, тим менша чисельність співробітників можуть їх знати". У відповідності з цією послідовністю визначається необхідний ступінь посилення захисних мір, структура рубежів (ешелонів) захисту інформації.

Доступ співробітника до конфіденційних відомостей, який здійснюється у відповідності з дозвільною системою, називається санкціонованим. Дозвіл (санкція) на доступ до цих відомостей завжди є строго персоніфікованим і видається керівником в письмовому вигляді: наказом, що затверджує схему посадового чи іменного доступу до інформації, резолюцією на документі, списком-дозволом в карточці видачі справи або на обложці справи ознайомлення з документом.

Дозвільна система доступу вирішує наступні задачі: забезпечення співробітників всіма необхідними для роботи документами і інформацією; обмеження кола осіб, які допускаються до конфіденційних документів; виключення несанкціонованого ознайомлення з документу Ієрархічна послідовність доступу реалізується по принципу "чим вища цінність конфіденційних відомостей, тим менша чисельність співробітників можуть їх знати". У відповідності з цією послідовністю визначається необхідний ступінь посилення захисних мір, структура рубежів (ешелонів) захисту інформації.

Особливості забезпечення безпеки при роботі з електронними документами

Робота з електронними конфіденційними документами дозволяється тільки при наявності у фірмі сертифікованої системи захисту комп'ютера і локальної мережі.

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

При зберіганні електронних документів обов'язкове додержання таких вимог:
1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;
2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;
3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Вимоги щодо надійності комунікаційних і документаційних систем

Конфіденційність. Ця вимога передбачає захищеність документа від ознайомлення з ним сторонніх осіб - перш за все, під час пересилання. Механізм протидії — кодування електронних документів перед їхнім пересиланням адресату або на сервер для зберігання. Хоча ця технологія передбачає різні ступені захисту, звичайно використовують один алгоритм кодування – той, що забезпечує захист найважливіших документів. Гарантування конфіденційності значною мірою залежить від надійності призначеного для кодування ПЗ і комп'ютерного обладнання, електронних ключів тощо.

Цілісність. Відповідно до цієї вимоги, дані та інформація повинні надійти до зазначеного адресата неушкодженими і без змін . Незалежно від природи несанкціонованих змін запропоновано два механізми протидії: електронний підпис, коди аутентифікації повідомлення (Message Authentication Codes, MAC). За їхньою допомогою на основі даних, що захищаються, можна утворювати кодовані додатки, що містять відомості про оригінальний документ та у разі його зміни засвідчать цей факт, проте не дадуть змоги ні визначити зміни, які відбулися, ні відновити документ.

Ідентифікація. Ця вимога передбачає ідентифікацію даних і комуніканта.
1. Ідентифікація даних покликана підтвердити, що документ складено або відправлено саме потрібною особою. 2. Ідентифікація комуніканта підтверджує, що партнер у комунікативному акті — дійсно особа, чиї реквізити наведено. Механізми ідентифікації — перевірка електронного підпису і MAC.

Найпоширеніші нині технології захисту електронних документів — кодування та електронний підпис - стикаються з проблемою їхнього практичного застосування при архівації документів: алгоритми у зв'язку з розвитком цифрових технологій мають дуже обмежений «термін надійності» — значно коротший, ніж строк зберігання документів в архіві, і підлягають регулярній перевірці на розкодування та постійній модернізації

Федюк Б.С.
Державний університет телекомунікацій

Дослідження методів та засобів захисту системи електронних платежів

Хоча електронні гроші порівняно недавно увійшли в наше життя, розвиток цього ринку здійснюється доволі стрімко. В Україні станом на 2014 рік, громадяни мають доступ до різних видів електронних платіжних інструментів. Частина з них створена резидентами України та працює тільки з гривнею, інші представлені компаніями – резидентами інших країн, які оперують іншими валютами, проте також є доступними для використання громадянами України. На разі, для ринку України актуальним є питання щодо формування сучасної, чіткої й прозорої регуляторної бази, заснованої на кращому міжнарод-ному досвіді, із дотримуванням балансу між захистом прав споживачів, державним наглядом за функціонуванням електронних платіжних інструментів, систем електронних грошей і забезпечення їх захисту.

В таких системах використовується різноманітні модифікації уже існуючих асиметричних алгоритмів шифрування та ЕЦП.ЕЦП забезпечує захист від модифікації інформації і дозволяє встановити власника сертифікату відкритого ключа. Даний сертифікат видається користувачу ЦС, котрий завіряє його своєю ЕПЦ. Іншим аспектом використання асиметричних ключів є можливість підтвердження авторства відправника повідомлення. Також обов'язковим елементом є можливість анонімних покупок яка забезпечується «сліпим підписом».

Глущенко В.В.
Державний Університет Телекомунікацій, м.Київ

Класифікація загроз інформаційній безпеці

Під політичними факторами загроз інформаційній безпеці розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері[14, с. 16-17].
- Ієрархічна класифікація загроз інформаційній безпеці.

Глобальні фактори загроз інформаційній безпеці:

- недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;
- діяльність іноземних розвідувальних та спеціальних служб;
- діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
- злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

- використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
- невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
- відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
- недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
- розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
- зростання злочинності в інформаційній сфері;

- використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
- відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

- перехоплення електронних випромінювань;
- застосування підслуховуючих пристроїв або закладок;
- дистанційне фотографування;
- розкрадання носіїв інформації та промислових відходів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне приєднання до апаратури та ліній зв'язку;
- упровадження та використання комп'ютерних вірусів і т. ін.[14, с. 25-27].

Дмитренко Віталій Анатолійович
Державний Університет Телекомунікацій, м.Київ

Технічні засоби захисту акустичної інформації

Акустичне маскування ефективно використовується для захисту мовної інформації від витоку по всіх каналах інформаційних сигналів.

При використанні засобів акустичного захисту виникає дискомфорт, тому актуальними є пристрої, що створюють перешкоду тільки при розмові, в інший же час пристрій «мовчить». Для захисту мовної інформації використовують активні і пасивні методи захисту.

До пасивних методів захисту відносять створення перешкод, наприклад екранування приладів, звукоізоляція приміщення, використання акустичних екранів та звукопоглинальних матеріалів.

Активні методи захисту мовної інформації повинні забезпечувати зменшення співвідношення сигнал/шум за рахунок збільшення рівня шуму.

Найбільш ефективним методом протидії несанкціонованому отриманню мовної інформації є перешкода звукозапису переговорів або її ретрансляції з приміщення шляхом створення шумової акустичної або віброакустичної завади, що забезпечує маскування інформативного сигналу. Співвідношення величини шумового сигналу/величина інформативного сигналу, повинне забезпечувати надійне маскування інформативного сигналу або зниження його розбірливості до допустимих меж.

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкта розвідки, технічного засоби розвідки (ТЗР), за допомогою якого видобувається інформація про цей об'єкт, і фізичного середовища, в якій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання за допомогою ТЗР розвідувальної інформації про об'єкт.

У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, і для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони. Мініатюрні мікрофони об'єднуються (або з'єднуються) з портативними пристроями звукозаписними (диктофонами) або спеціальними мініатюрними передавачами. Автономні пристрої, конструкційно об'єднують мініатюрні мікрофони і передавачі, називають заставними пристроями перехоплення мовної інформації, або просто акустичними закладками. Перехоплена заставними пристроями мовна інформація може передаватися по радіоканалу, оптичному каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму, сполучних лініях допоміжних технічних засобів і систем (ВТЗС), стороннім провідникам (трубах водопостачання і каналізації, металоконструкцій і т. п.). Причому для передачі інформації по трубах і металоконструкцій можуть використовуватися не тільки електромагнітні, але і механічні ультразвукові коливання.

Огірчак В.О.
Державний Університет Телекомунікацій, м.Київ

Інциденти інформаційної безпеки, пов’язані з роботою персоналу та їх розслідування.

Жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

Кількість потенційних каналів витоку інформації достатньо велика. Найбільш поширені з них відносяться до категорії ненавмисного розкриття інформації співробітниками організації з причин непоінформованості або недисциплінованості. Відсутність уявлень щодо правил роботи з конфіденційними документами, невміння визначити, які документи є конфіденційними, та звичайна неуважність при роботі з інформацією – все це може призвести до виникнення події або інциденту інформаційної безпеки.

Розглянемо декілька визначень понять події та інциденту ІБ:

1. Згідно з [1] під подією інформаційної безпеки (ПІБ) розуміється стан системи, сервісу або мережі, котрий свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки, тоді як інцидент інформаційної безпеки (ІІБ) – це одна або серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути, як матеріальними(вартість інформації, експлуатаційні витрати і т.д.) так і нематеріальними(репутація організації, зміна морально-психологічного клімату і т.д.) .

2. В [2] подія інформаційної безпеки – це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки. Інцидент інформаційної безпеки відповідно до [2] – це одинична подія або ряд небажаних та непередбачених подій інформаційної безпеки, із-за яких велика ймовірність розкриття конфіденційної бізнес-інформації.

Як приклад, інцидентами інформаційної безпеки, що сталися з вини співробітників можуть бути:

- порушення конфіденційності та цілісності цінної інформації;
- незаконний моніторинг інформаційних систем;
- знищення інформації;
- компрометація інформаційної системи (наприклад, розголошення пароля користувача);
- відмова в обслуговувані сервісів, засобів обробки інформації, обладнання;
- пошкодження електричних мереж;
- Неавторизоване використання системи для зберігання особистих даних;
- та інші порушення вимог до інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації).

Для того, щоб захистити організацію від витоку конфіденційної інформації через її співробітників, треба:

- контролювати доступ співробітників до закритої документації і до баз данних, кожен співробітник незалежно від свого службового положення повинен володіти лише тією інформацією, яка йому потрібна для роботи;
- періодично продивлятися данні та визначати ступінь їх секретності;
- зберігати важливу інформацію у вогнестійких сейфах, оснащених кодовим замком. Необхідно організовувати систему класифікації з обмеженим доступом різних категорій співробітників, які пройшли спеціальну перевірку;
- встановити на всіх ПК антивірусні програми та регулярно їх обновлювати;
- упорядкувати використання співробітниками копіювальної техніки;
- встановити апарат для знищення непотрібних документів(включаючи використаний копіювальний папір);
- встановити персональну відповідальність співробітників за збереження конфіденційної інформації з чіткою градацією мір дисциплінарного та морального впливу за її витік.

В загальному випадку, ознаки інциденту поділяються на дві основні категорії, повідомлення про те, що інцидент відбувається в даний момент і повідомлення про те, що інцидент, можливо, станеться в недалекому майбутньому.

Для опису процедури управління інцидентами безпеки використовується класична модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга – модель ПРПД(Плануй(Plan) — Роби(Do) — Перевіряй(Check) — Дій(Act) – модель PDCA).

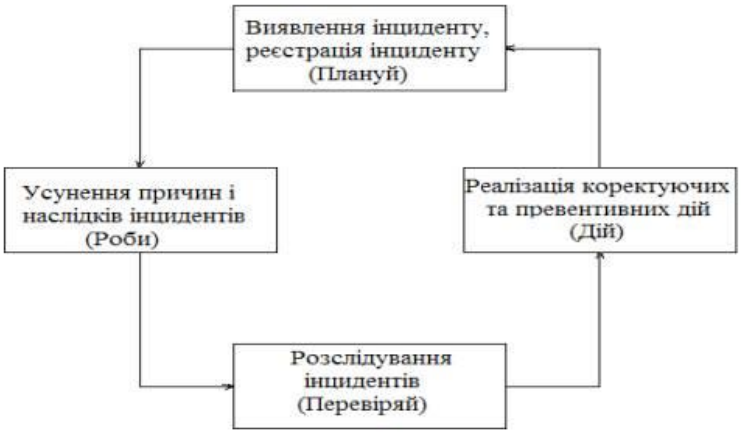


Рис. 1 – Модель управління інцидентами ПРПД.

Одним із етапів управління інцидентами ІБ є їх розслідування.

Процес розслідування може бути розділений на два етапи: збір даних та їх криміналістичний аналіз.

Аналіз зібраних даних включає аналіз файлів протоколів роботи, конфігураційних файлів, історії Інтернет-провідників (включаючи cookies), повідомлень електронної пошти і прикріплених файлів, інстальованих додатків, графічних файлів і іншого. Необхідно провести аналіз ПЗ, пошук за ключовими словами, перевірити дату і час інциденту.

Криміналістичний аналіз може також включати пошук видалених файлів і областей, втрачених кластерів, вільного місця, а також аналіз відновлених даних із зруйнованих носіїв (наприклад, по залишковій намагніченості).

Інформація, зібрана в ході виконання першого етапу розслідування, надалі використовується для вироблення стратегії реагування на інцидент. На етапі аналізу, власне, і визначається, хто, що, як, коли, де і чому були залучені в інцидент.

При розслідуванні інциденту збір даних може бути виконаний з допомогою програмного забезпечення "Disk Duplicate". Воно дозволяє зробити точні копії жорстких дисків ("сектор в сектор") автоматизованих робочих місць користувачів (співробітників компанії) і серверів. Для аналізу отриманих даних можуть використовуватися спеціальні засоби емуляції робочих машин користувачів, наприклад "VMware Virtual Machine". Аналіз просторів жорстких дисків може проводитися з використанням спеціалізованого програмного продукту "Encase Enterprise Edition" або експертних засобів компанії Vogon International. Ці два продукти - ключові в світі при проведенні розслідування інцидентів ІБ. У ряді випадків для виявлення слідів комп'ютерних інцидентів можуть бути використані всілякі програмно-апаратні комплекси для "прослухування" локальній мережі компанії (часто використовується продукт Ettercap - мережевий сніффер).

На етапі розслідування інцидентів важливу роль відіграють: ведення журналів реєстрації подій, чітке розділення повноважень користувачів, відповідальність за виконані дії — важливі докази того, хто брав участь в інциденті і які дії він виконував.

Типовою практикою є ведення журналу розслідування інциденту, який не має стандартної форми і розроблюється командою реагування.

Ключовими позиціями подібних журналів є:

- статус розслідування, який є на даний момент;
- опис інциденту;
- дії, проведенні командою реагування в процесі обробки ІІБ;
- перелік свідоцтв(з обов’язковою вказівкою джерел), зібраних в процесі обробки інциденту;
- коментарі учасників розслідування інциденту;
- опис послідуючих дій.

Для підвищення ефективності розслідування інцидентів інформаційної безпеки в організації повинен буди інженер з інформаційної безпеки, що буде:

- розробляти політики безпеки (ПБ) з детально опрацьованими документами, які регламентують діяльність персоналу всіх рівнів з чітко вказаною відповідальністю в межах покладених обов’язків;
- розробляти посадові інструкції, правила, регламенти з чітко визначеними правами та обов’язками персоналу, пов’язані з текучими бізнес-процесами, що дозволяють добре прогнозувати наслідки та розробити надійні превентивні дії для запобігання повторення таких інцидентів.

В організації повинен бути розроблений відповідний дисциплінарний процес, що проводиться у відношенні до порушників безпеки і передбачує розслідування наслідків інцидентів та прийняття адекватних мір впливу на них.

При визначені міри запобігання виникненню інцидентів ІБ, інженеру з інформаційної безпеки або юристу, необхідно орієнтуватися на положення дійсного законодавства України. Відносини між робітником та роботодавцем та відповідальність за порушення інформаційної безпеки організації регулюються Кримінальним Кодексом, Адміністративним Кодексом та Кодексом Законів про Працю:

1. За шкоду, заподіяну підприємству, установі, організації при виконанні трудових обов'язків, працівники, з вини яких заподіяно шкоду, несуть матеріальну відповідальність у розмірі прямої дійсної шкоди, але не більше свого середнього місячного заробітку.

2. Умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності, - караються штрафом від двохсот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк до п’яти років, або позбавленням волі на строк до трьох років.

3. Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

4. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах(комп’ютерах), автоматизованих системах, комп’ютерних мережах, або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи ;

5. Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, - тягне за собою накладання штрафу від п’яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої.

На жаль, про розслідування інцидентів в компаніях часто просто забувають. Як тільки наслідки інциденту усунені, і бізнес-процеси відновлені, подальші дії з розслідування інциденту і здійснення коректуючих заходів не виконуються.

Думан М.О.
Державний Університет Телекомунікацій

ОЦІНКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ

Інформаційна безпека (ІБ) в даний час стає одним з найважливіших аспектів загальної економічної безпеки діяльності сучасної організації, характеризуючи стан захищеності її бізнес-середовища. Захист інформації являє собою особливу діяльність щодо запобігання витоку інформації, несанкціонованих змін її потоків та інших впливів, які негативно впливають на стабільну роботу організації та пов'язаних з нею економічних агентів (клієнтів, постачальників обладнання, інвесторів, держави та ін.). У цьому зв'язку своєчасна, оперативна і коректна оцінка ризиків зниження або повної втрати ІБ сьогодні є актуальною проблемою в діяльності будь-якої організації. У сучасних публікаціях, які зачіпають питання ІБ, виділяється 4 типи джерел загроз впливають на інформаційну безпеку:

• природні;
• техногенні;
• людські навмисні;
• людські ненавмисні.

Враховуючи суттєву різнотипність зазначених джерел, розробка методик та алгоритмів оцінки ризику зниження або повної втрати ІБ - досить трудомістка і значуще завдання для будь-якої інформаційної системи, що вимагає виконання низки умов. По-перше, необхідна побудова гнучких моделей інформаційної системи, описувати її комплексно, з урахуванням програмних, апаратних ресурсів, внутрішніх і зовнішніх загроз і вразливостей, здатних налаштовуватися відповідно до особливостей конкретної організації. По-друге, з урахуванням значної кількості факторів ризику, математична модель оцінки ІБ повинна допускати розробку ефективних чисельних алгоритмів обробки інформації в моделях. По-третє, має бути гранично прозора методика оцінки ризиків, щоб власник інформації міг адекватно оцінити застосовність і ефективність методики до конкретної інформаційної системи. Для оцінки ризиків ІБ важливо виділити і проаналізувати, по-можливості, все або, принаймні, основні загрози та вразливості, через які можлива реалізація загроз, і які діють на інформаційну систему в сенсі відмов або зниження її працездатності. На сьогоднішній день існує ряд методик оцінки ризиків інформаційної безпеки, до основних з яких можна віднести наступні:
1) Метод оцінки ризиків, заснований на побудові моделі загроз і вразливостей;
2) Метод оцінки ризиків, заснований на побудові моделі інформаційних потоків.

Перша методика заснована на використанні переважно експертної та статистичної інформації про погрози і вразливості. Для оцінки ризиків в інформаційній системі організації визначається захищеність кожного цінного ресурсу за допомогою оцінки ймовірностей реалізації загроз, що діють на конкретний ресурс організації (наприклад, вірогідність збоїв в роботі системи ІБ у зв'язку з низькою кваліфікацією співробітників, відсутністю або старінням програмного або апаратного забезпечення і т. п.), а також вразливостей, через які дані загрози можуть бути реалізовані. Зазначена оцінка ймовірностей дозволяє поділяти загрози та вразливості за ступенем ризиковості. Так як ризики ІБ тісно пов'язані із застосуванням сучасних інформаційних технологій, що визначають ефективність діяльності організації в її інноваційному аспекті, то їх можна віднести до різновиду інноваційних ризиків. Визначаючи інноваційний ризик як «імовірність втрат внаслідок неправильно поставленої або недосягнутої стратегічної мети», при характеристиці ризиків відмови працездатності системи доцільно використовувати такий показник, як рівень витрат (в матеріальному або вартісному виразі) на відновлення працездатності системи. Виходячи з експертно певних даних про ризики, уразливість і витрати по кожному з ресурсів, можна побудувати модель загроз і вразливостей, актуальних для інформаційної системи організації, і провести аналіз функціонування інформаційної системи з погляду мінімізації ризиків відмови або зниження працездатності системи і, отже, максимізації її ефективності за критерієм ІБ. Наведемо нижче коротку характеристику етапів алгоритму за рішенням описаної задачі. На першому етапі виділяються найбільш важливі для організації напрями діяльності, які визначають (з точки зору її керівництва) рівень інформаційної безпеки. На другому етапі, за виділеними напрямками діяльності організації, на основі оцінки експертами ймовірності реалізації загрози ІБ, розраховується значимість кожної загрози, а також оцінюється рівень витрат у вартісному вираженні на відновлення працездатності системи. Далі розраховується сумарний ризик відмови працездатності системи як сума ризиків по кожному з напрямків. Результатом рішення описаної задачі будемо вважати розподіл фінансового ресурсу по виділених напрямках діяльності організації, мінімізуючого ризики відмови працездатності системи за критерієм ІБ. У висновку відзначимо, що багато підприємств малого та середнього бізнесу, перебуваючи в інформаційному середовищі, не звертають увагу на різного роду погрози, яким схильна їх інформаційна система, тим самим піддаючи себе ризику фінансових втрат. Саме тому необхідно розробляти моделі аналізу ризиків ІБ, а також створювати алгоритми та методи їх аналізу з метою створення систем підтримки прийняття рішень з управління ІБ організації.

Література:

1. Бармен Скотт «Розробка правил інформаційної безпеки»

2. Галицький А.В., Рябко С.Д., Шаньгина В.Ф. «Захист інформації в мережі – аналіз технологій і синтез рішень»
3.

Салюк М.
Державний університет телекомунікацій

Впровадження системи управління захистом інформації електронних платіжних систем.

Електронні платіжні системи (англ. Electronic Payment Systems) –призначені для здійснення платіжних операцій з використанням мережі Інтернет. За допомогою платіжної системи можна здійснювати розрахунок за товари та послуги різних проектів і сервісів . Наприклад, оплачувати мобільний зв'язок, комунальні послуги, кабельне або супутникове телебачення, послугиІнтернет-провайдерів, а також різноманітні покупки в Інтернет-магазинах .Платіжними засобами в електронних платіжних системах виступають електронні (цифрові) гроші , вони є аналогом готівки і, при потребі, миттєво передаються з одного електронного гаманця на інший. Всі електронні платіжні системи за способом доступу до електронного рахунку можна розділити на дві групи : системи, що мають веб-інтерфейс для керування електронним гаманцем; системи, що вимагають встановлення додаткового програмного забезпечення для керування електронним гаманцем.

Зростання з кожним роком кількості використання платіжних систем неминуче, оскільки вони мають дуже важливі та незаперечні переваги, такі як:

● доступність – будь-який користувач має можливість безкоштовно відкрити
власний електронний рахунок;

● простота використання – для відкриття та використання електронного рахунку не потрібно яких-небудь спеціальних знань, всі наступні дії інтуїтивно зрозумілі;

● мобільність – незалежно від місця свого знаходження користувач може
здійснювати зі своїм рахунком будь-які фінансові операції;

● оперативність – переказ коштів з рахунку на рахунок відбувається протягомдекількох секунд;

● безпека – передача інформації ведеться з використанням SSL1 протоколу з кодовим ключем 128 біт або іншими криптографічними алгоритмами.

Щоб стати учасником і користуватися послугами будь-якої платіжної системи потрібно пройти процес реєстрації й відкрити в ній електронний рахунок у вигляді електронного гаманця . Електронний гаманець зберігає інформацію про суму коштів на рахунку користувача в тій чи іншій платіжній системі. Для того, щоб мати можливість виконання розрахункових операцій, необхідно ввести гроші в платіжну систему, інакше кажучи, поповнити електронний рахунок. Це можна зробити за допомогою банку, поштового переказу, платіжного термінала або іншим зручним способом залежно від використовуваної платіжної системи. При потребі, електронні гроші завжди можна вивести із сис теми та обміняти їх на готівку .

Електронні платіжні системи дають змогу максимально спростити фінансові операції між покупцем і продавцем. Також вони сприяють розвитку електронної комерції , оскільки дають змогу здійснити операцію майже миттєво. Єдиним недоліком і головною перешкодою для більш стрімкого розвитку електронних платіжних систем як і раніше є недовіра багатьох користувачів до електронних грошей. Однак варто відзначити, що безпека елек-тронних платежів з часом значно підвищується і зловмисникам усе важче отримати доступ до чужого електронного або банківського рахунку. Багато в чому безпека рахунків цілком залежить від самого власника, які халатно ставляться до конфіденційності власної інформації.

1. Автоматизовані банківські системи та їх структура. [Електронний ресурс]. – Доступний
з http://ru.osvita.ua/vnz/reports/bank/20377/
2. Голдовский И.М. Безопасность платежей в Интернете / И.М. Голдовский. – СПб. : ИД"Питер", 2001. – 240 с.
3.Електронні платіжні системи Інтернету. [Електронний ресурс]. – Доступний з http://www.blogs.biz.ua/blog.php?user=judin&note=189

Салюк М.
Державний університет телекомунікацій

Загрози, пов'язані з використанням систем електронних платежів

Розглянемо можливі загрози руйнуючих дій зловмисника по відношенню до даної системи. Для цього розглянемо основні об'єкти нападу зловмисника. Головним об'єктом нападу зловмисника є фінансові кошти, точніше їх електронні заступники (сурогати) - платіжні доручення, циркулюючі в платіжній системі. По відношенню до даних засобів зловмисник може переслідувати наступні цілі:

1. Викрадення фінансових коштів.
2. Впровадження фальшивих фінансових коштів (порушення фінансового балансу системи).
3. Порушення працездатності системи (технічна загроза).

Зазначені об'єкти і цілі нападу носять абстрактний характер і не дозволяють провести аналіз та розробку необхідних заходів захисту інформації, тому в таблиці наводиться конкретизація об'єктів і цілей руйнуючих дій зловмисника.

З даної таблиці випливають базові вимоги, яким повинна задовольняти будь-яка система електронних платежів через Інтернет:
По-перше, система повинна забезпечувати захист даних платіжних доручень від несанкціонованого зміни і модифікації.
По-друге, система не повинна збільшувати можливості зловмисника з організації атак на комп'ютер клієнта.
По-третє, система повинна забезпечувати захист даних, розташованих на сервері від несанкціонованого читання і модифікації.
По-четверте, система повинна забезпечувати або підтримувати систему захисту локальної мережі банку від впливу з глобальної мережі.
У ході розробки конкретних систем захисту інформації електронних платежів, дана модель і вимоги повинні бути подолані подальшої деталізації. Тим не менш, для поточного викладу подібна деталізація не потрібна.

Модель можливих руйнуючих дій зловмисника Таблиця1

Об'єкт впливу	Мета впливу	Можливі механізми реалізації впливу.
HTML-сторінки на web-сервері банку	Підміна з метою отримання інформації, яка вноситься до платіжне доручення клієнтом.	Атака на сервер і підміна сторінок на сервері. Підміна сторінок в трафіку. Атака на комп'ютер клієнта і підміна сторінок у клієнта
Клієнтські інформаційні сторінки на сервері	Отримання інформації про платежі клієнта (ів)	Атака на сервер. Атака на трафік. Атака на комп'ютер клієнта.
Дані платіжного доручення, що вносяться клієнтом у форму	Отримання інформації, яка вноситься до платіжне доручення клієнтом.	Атака на комп'ютер клієнта (віруси і т.д.). Атака на дані доручення при його пересилання по трафіку. Атака на сервер.
Приватна інформація клієнта, розташована на комп'ютері клієнта і не відноситься до системи електронних платежів	Отримання конфіденційної інформації клієнта. Модифікація інформації клієнта. Виведення з ладу комп'ютера клієнта.	Весь комплекс відомих атак на комп'ютер, підключений до мережі Інтернет. Додаткові атаки, які з'являються в результаті використання межанізмів платіжної системи.
Інформація процесингового центру банку.	Розкриття і модифікація інформації процесингового центру та локальної мережі банку.	Атака на локальну мережу, підключену до Інтернет.

1.Гайкович Ю.В, Першин А.С. Безпека електронних банківських систем. - М: Єдина Європа, 2004 р .
2.Титоренко Г.А. та ін Комп'ютеризація банківської діяльності. - М: Финстатинформ, 2007 р .
3. Дьомін В.С. та ін Автоматизовані банківські системи. - М: Менатеп-Інформ, 2007 р .

Поліщук К.А.
Державний університет телекомунікацій

Процесний підхід до управління інформаційною безпекою

У результаті інтенсивного використання інформаційних технологій практично в усіх сферах діяльності задачі управління сучасною організацією та її Інформаційною безпекою з кожним днем стають все складнішими.

Все частіше перед спеціалістами інформаційної безпеки ставиться задача не просто впровадити засоби або систему захисту,а й побудувати систему управління інформаційною безпекою.

Правильна побудова, впровадження,функціонування, контроль,вчасне коригування, підтримка і поліпшення системи управління інформаціною безпекою (далі-СУІБ)є важливою задачею керівника.

Згідно ISO 27001, система управління інформаційною безпекою (СУІБ) - це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки». Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

У разі прийняття рішення про створення СУІБ слід чітко розуміти, що це не разовий захід, а постійна робота, оскільки ефективність процедур системи управління може з плином часу знижуватися.

Всі процедури процесного підходу до управління повинні послідовно проходити наступні чотири етапи: планування, впровадження, моніторинг та аналіз, вдосконалення. Кожен етап характеризується виконанням різних процедур.

Етапи функціонування можна описати так:

1. Планування процедур СУІБ:
 - рішення про створення системи управління керівництвом компанії;
 - вибір області дії системи;
 - інвентаризація та категоріювання інформаційних активів;
 - оцінка рівня захищеності інформаційної системи (ІС) - визначення вразливостей і загроз ІБ;
 - аналіз інформаційних ризиків;
 - розробка Положення про застосовність;
 - вибір заходів щодо зниження інформаційних ризиків;
 - розробка бази нормативних документів з ІБ.
2. Впровадження процедур СУІБ:
 - впровадження заходів щодо зниження інформаційних ризиків;
 - визначення методів оцінки ефективності впроваджених заходів;
 - підвищення кваліфікації співробітників компанії в області ІБ;
 - впровадження системи управління інцидентами ІБ.
3. Моніторинг та аналіз процедур СУІБ:
 - регулярні перевірки ефективності процедур системи управління;
 - регулярний перегляд результатів аналізу інформаційних ризиків;
 - реєстрація записів системи управління з метою оцінки її ефективності.
4. Удосконалення СУІБ:
 - виконання коригувальних і превентивних дій;
 - забезпечення ефективності вжитих заходів вдосконалення СУІБ.

Варто зупинитися докладніше на деяких процедурах СУІБ, які, як правило, викликають найбільші складності.

При виборі області дії СУІБ поширюється на всю ІС компанії. Проте впровадження системи управління - досить складний процес, тому, як правило,компанії вибирають один з критичних бізнес-процесів або автоматизованих систем і впроваджують процедури системи управління, а потім поширюють їх на інші процеси компанії.

Можна відзначити,що в рамках області дії СУІБ потрібно визначити наступні активи:

- інформаційні ресурси;
- засоби зберігання та обробки інформації;
- програмне забезпечення;
- користувачі ІС;
- допоміжні сервіси та системи життєзабезпечення.

Рівень необхідної захищеності залежить від ступеня критичності інформації для компанії - навіщо витрачати на захист інформації $ 100, якщо сама інформація коштує $ 10? Оцінку критичності інформації проводять, як правило, за трьома критеріями - конфіденційності, цілісності та доступності, тобто для кожної інформації потрібно визначити збиток,який понесе компанія при її розголошенні, модифікації або неможливості отримати до неї доступ.

Після проведення аналізу ризиків, вибору та впровадження контрзаходів, необхідно оцінити ефективність процедур. Як правило, ефективність впроваджених засобів захисту визначається за допомогою повторного аналізу ризиків. Необхідно зрозуміти, наскільки дійсно знизився ризик.

Враховуючи, що заходами зниження ризиків можуть бути не тільки окремі програмні або апаратні рішення (скажімо, антивірус), але і різні заходи (напр. регулярне резервне копіювання інформації). Щоб оцінити ефективність таких заходів необхідно знати,чи виконуються необхідні дії відповідно до вказівок і який внесок у забезпечення безпеки вони вносять.

Ясно, що готовність системи управління до сертифікації визначається індивідуально для кожної компанії, але, як правило, якщо не пройдений хоча б одне коло PDCA-моделі, про сертифікацію говорити рано. для успішного проходження сертифікації аудиторів сертифікаційних органів необхідно надати всі документи системи управління безпекою, а також докази того, що процедури виконуються точно відповідно з документами. Таким чином, до моменту сертифікації слід накопичити деяку кількість записів, які доводять ефективну роботу СУІБ.

Крім того, аудитори будуть самостійно виконувати перевірку співробітників компанії і налаштувань інформаційних ресурсів, тобто все, що декларується в документах і відображається в записах, повинно бути дійсно виконано.

Розглянувши основні етапи створення СУІБ,можна сказати , що цей підхід закладений в міжнародних стандартах на системи управління, в тому числі і ISO / IEC 27001 досить складний і тривалий. Зусилля, витрачені на створення системи управління інформаційною безпекою, дозволять організації вийти на новий вищий рівень.

ЛІТЕРАТУРА:

1. В.А. Трайнёв, А.А. Федулов «Информационная безопасность» ИТК Дашков и К, 2005. – 336 с.
2. СимоновС.В.«Управление информационными рисками. Экономически оправданная безопасность» ДМК Пресс, 2004. – 384
3. Система управления информационной безопасностью в соответствии с ISO/IEC 27001

Чередніченко О.О.
Державний університет телекомунікацій

Аудит інформаційної безпеки організації та систем

Аудит інформаційної безпеки - це системний процес одержання об'єктивних якісних и кількісних оцінок поточного стану безпеки організації або інформаційної системи. В Україні, аудит інформаційної безпеки організацій та інформаційних систем, проводиться на відповідність таким вимогам:

- Нормативних документів у галузі технічного захисту інформації (НД ТЗІ).
- ISO\IEC 27001:2005.
- PCI DSS.

На даний час, за умов стрімкого розвитку інформаційних технологій виникає необхідність захищеності інформаційних ресурсів організацій та підприємств для боротьби із зовнішнім і внутрішнім загрозами. З метою посилення інформаційної безпеки та утримання її на належному рівні, пропонується проведення аудиту. Процес аудиту повинен проходити в декілька етапів:

1. Вивчення поточного стану ІБ в організації.
2. Порівняння цих результатів відповідно до стандартів та аналогічним об’єктам дослідження.
3. Розробка рекомендацій для організації, що стосуються посилення інформаційної безпеки
4. Оформлення та подання результатів.

Зараз, в Україні, ефективність проведення аудиту в сфері інформаційної безпеки не є дуже великою і вистачає різних проблем, але все ж прогрес відбувається. Я вважаю, що аудит здатний стати реальним засобом ліквідації різного типу загроз в сфері ІБ.

І.Г. Зотова, Д.С. Берестов,
Центр воєнно-стратегічних досліджень
Національного університету оборони України
ім.. І.Черняховського, Київ

ВПРОВАДЖЕННЯ СЕРЕДОВИЩА АУТЕНТИФІКАЦІЇ.

Інтенсивний розвиток і поглинання суспільства інформаційними технологіями вимагає створення надійної системи віддаленого підключення користувачів до інформаційних ресурсів за допомогою відкритих каналів зв'язку. Важливу роль у рішенні цього завдання відіграє будівництво інфраструктури відкритих ключів, створення, впровадження, безпечне та надійне функціонування систем ідентифікації та аутентифікації, які використовуються як для перевірки існування входу в систему користувача так і для уникнення відмови в обслуговуванні зареєстрованого користувача. В доповіді розглядаються основні протоколи аутентифікації та їх можливості для побудови надійного середовища довіри між суб’єктами відносин в інформаційно-телекомунікаційній системі.

к.т.н., с.н.с. Голобородько М.Ю.
Центр воєнно-стратегічних досліджень
Національного університету оборони України
ім.. І.Черняховського, Київ

НФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ

На сьогодні найбільш надійні способи аутентифікації, захисту даних при їх обробці, зберіганні і передачі по телекомунікаційних каналах засновані на шифруванні інформації і, відповідно, на технологіях управління ключами шифрування (у разі застосування систем з так званими асиметричними алгоритмами шифрування принциповим є забезпечення обміну відкритими ключами користувачів системи), впровадження яких можливо на основі єдиної

розподіленої системи створення, зберігання та розповсюдження цифрових сертифікатів відкритих ключів користувачів - інфраструктури відкритих ключів - *PKI* (англ. - *Public Key Infrastructure*).

В даній доповіді розглядається побудова архітектури інфраструктури відкритих ключів і необхідні компоненти - учасники процесу вироблення довірених відкритих ключів.

Гвоздев А.Д.

Обоснование необходимости инноваций в сфере информационной безопасности

Инновации в сфере информационной безопасности – конечный продукт вложений трудовых, материальных и иных ресурсов в разработку, производство и внедрение новых продуктов в области информационной безопасности с целью повышения ее эффективности и получения прибыли.

Сущность инновационного процесса

Инновационный процесс представляет собой совокупность взаимосвязанных действий, ограниченных сроками, исполнителями и ресурсами, направленных на достижение поставленных целей и задач. Инновационный процесс в области информационной безопасности состоит из последовательности исследовательских, административных, производственных, технологических и коммерческих мероприятий, приводящих к инновациям. К таким мероприятиям можно отнести научные исследования, направленные на создание нового продукта, поиск квалифицированного персонала для проведения этих исследований, прогнозирование результатов деятельности, поиск источников финансирования исследований и производства, также тестирование и внедрение созданных продуктов, обеспечивающих защиту данных.

Возможность рисков

В настоящее время выполнение работ, связанных с разработкой и применением инноваций в сфере информационной безопасности, сопряжено с достаточно большой вероятностью получения неудовлетворительных результатов, возникает риск потерь при вложении ресурсов на проведение исследований и производство новых продуктов и услуг. Это обусловлено тем, что они могут не найти ожидаемого спроса на рынке и не оправдать ожиданий как своих создателей, так и конечных потребителей. Чаще всего инновационный риск возникает при внедрении менее затратного для производителя метода производства товара или услуги по сравнению с уже использующимся методом, при создании нового продукта с использованием старого оборудования и неподготовленного персонала, или при производстве с помощью новой техники и технологий, которые еще недостаточно изучены. Также успешность и последующая экономическая эффективность внедрения нововведений зависит от системы управления в каждой конкретной организации. Необходимо совершенствовать менеджмент инноваций и повышать его уровень, что является важным и необходимым условием успешного управления бизнесом. В соответствии с общепризнанным подходом к инновациям, любое нововведение в области информационной безопасности должно быть рассмотрено как бизнес-проект, т.е. с четким выявлением целей проекта, возможных рисков, способов и точек контроля, и его стратегии. Проведение анализа наиболее «уязвимых» мест проекта и грамотное управление сопутствующими рисками может нивелировать вероятность неудачи в инновационной деятельности. Как правило, успешность такого анализа обуславливается опытом и профессионализмом лиц, проводящих анализ, поскольку универсальный метод решения данной задачи отсутствует по причине наличия индивидуальных особенностей в каждом конкретном случае. Также необходимо повышать инновационную грамотность посредством обучения, использования консалтинговых услуг в таких сферах, как управление проектами и рисками, бизнес-планирование. Все эти меры значительно повышают шансы на успех инновационного проекта.

Необходимость применения инноваций

В условиях современной рыночной экономики инновации в информационной безопасности являются условием сохранения конкурентоспособности и развития направления деятельности в области информационной безопасности. Активность организации в сфере инноваций является одним из основных условий его успешного функционирования в будущем и расширения сферы деятельности. Так, в последние годы инновационная активность среди производителей продуктов и услуг в области информационной безопасности заметно увеличилась. Внедрение инноваций в сфере информационной безопасности становится самым эффективным способом повышения конкурентоспособности производимых продуктов и услуг, повышения темпов развития технологий, и, как следствие, увеличения доходов организаций-производителей. Не менее важным аспектом является актуальность нововведений, которая влияет на успешность их внедрения и реализации, что также положительно сказывается на финансовом состоянии и успешности фирм-производителей продукции в сфере информационной безопасности.

Использованная литература

1) Медынский В. Г. Инновационный менеджмент: Учебник. — М.: ИНФРА-М, 2008. — С. 168-173.
2) Дурович А. П. Основы маркетинга: Учебное пособие. — М.: Новое знание, 2004. — С. 24-30.
3) ru.wikipedia.org

Майстренко М.К
Державний університет телекомунікацій

Основні методи дій кіберзлочинців в банківській сфері

На відміну від звичайного злочинця, який діє в реальному світі, кіберзлочинець не вдається до традиційної зброї - ножа чи пістолета. Його арсенал - інформаційна зброя, всі інструменти, що використовуються для проникнення в мережі, зламу і модифікації програмного забезпечення, несанкціонованого одержання інформації або блокування роботи комп'ютерних систем. До зброї кіберзлочинця можна додати: комп'ютерні віруси, програмні закладки, різноманітні види атак, що дозволяють отримати несанкціонований доступ до комп'ютерної системи.

Поговоримо про банківські платіжні картки. Як діють кіберзлочинці? Їхні зусилля спрямовані, в основному, на викрадення даних пластикових карт з тим, щоб виготовити дублікати і таким чином зняти чужі гроші з карткового рахунку, або впровадити в систему шкідливе програмне забезпечення, яке дозволить зловмисникам розпоряджатися чужим рахунком, що трапляється значно рідше.

Давайте спробуємо розібратися, де ці слабкі ланки, щоб розуміти, де нас може підстерігати небезпека.

Механізм функціонування системи електронних грошових розрахунків індивідуальних клієнтів, заснований на застосуванні пластикових карток, включає в себе операції, що здійснюються за допомогою банкоматів, електронних систем розрахунків населення в торговельних організаціях, систем банківського обслуговування приватних осіб вдома і на робочому місці, і деякі інші.

Основні методи дій кіберзлочинців такі:

- *Скімінг* - установка спеціальних пристосувань, що зчитують дані карток на банкоматах або POS-терміналах (або замість POS-терміналів) в торгових точках. Якщо ви бачите на банкоматі якусь дивну накладку - не користуйтеся ним. Це може бути скімінговий пристрій. Благо, зараз банкоматів більш ніж достатньо. Одне з правил платіжних систем каже - не випускайте свою картку з поля зору. Якщо Ви розраховуєтеся карткою в ресторані, то офіціант зобов`язаний підійти до столика зі спеціальним POS-терміналом, а не забирати картку кудись. Якщо офіціант забрав картку, то він може пропустити її через скімінговий пристрій. Не дозволяйте цього.
- *Фішинг* - спроби виманити дані про картку через розсилку власникам карток електронних листів з проханням надати відповідну інформацію (типу: ви виграли приз чи в лотерею, отримали спадок і т.д., дайте дані про свій картковий рахунок, куди можна перерахувати гроші) або через відкриття «лівих» сайтів, де пропонується заповнити реквізити своєї картки для отримання чого-небудь. Якщо картодержатель ведеться на таку пропозицію, то шахраї списують його гроші з рахунку. Не вірте подібним пропозиціям, особливо якщо ви не купували лотерейного квитка. Іноді шахраї дзвонять, представляються працівниками банку, намагаючись вивідати ПІН-код під якимось приводом. Пам`ятайте - ніхто не має права знати ваш ПІН-код, окрім вас.
- *Використання шкідливого програмного забезпечення* - більше стосується систем дистанційного обслуговування і управління рахунком типу «клієнт-банк» (СДО) і до карткових рахунків відноситься у меншій мірі. Впровадження подібного ПО відбувається через електронну пошту або інтернет, що категорично заборонено правилами використання СДН - не можна користуватися електронною поштою та інтернетом з комп`ютера, на якому встановлена система «клієнт-банк». Шкідливий вірус, може блокувати комп`ютер користувача, генерувати ключі і паролі, зробити списання коштів з рахунку клієнта на рахунок зловмисників з подальшим переведенням у готівку.
- *Злом банківських карткових систем або систем передачі даних процесингових центрів* з метою розкрадання карткових даних - зустрічається вкрай рідко через надзвичайну складність і постійного вдосконалення систем захисту. На жаль, картодержатель може впливати на цей процес тільки своїм відходом з скомпроментірованного банку. Але банки дуже дорожать своєю репутацією, тому крім постійного вдосконалення систем інформаційної безпеки, часто також використовують різні страхові програми, системи відшкодування викрадених коштів у рамках програм лояльності клієнтів і т.д.
- *Інші способи компрометації платіжних інструментів* - все, що не потрапило в перші три пункти.

Міщенко М.В.
Державний університет телекомунікацій

КІБЕРЗЛОЧИННІСТЬ: ЗМІСТ ТА МЕТОДИ БОРОТЬБИ

У статті розкривається зміст поняття кіберзлочинність, її схеми та способи боротьби з нею.

Національна економіка та інфраструктура будь-якої країни сьогодні тісно пов’язані з сучасними комп’ютерними технологіями. Як і будь-який прогресивний винахід Інтернет та Інтернет-послуги містять у собі ряд небезпек, а саме нову особливу форму злочинства - «кіберзлочинність». Виникає небезпека несанкціонованого втручання в приватне життя громадян, шахрайство, розповсюдження вірусів, злому паролів, крадіжки кредитних карток та розповсюдження протизаконної інформації. Все це свідчить про актуальність вивчення поняття кіберзлочинності та способів боротьби з нею.

Питанням кіберзлочинності займаються такі зарубіжні та українські вчені як: Волчинская Е., Баурин Ю.М., Дашян М.С., Дешамп С., Кохутов М.М., Марков А.С., Юрасов А.В. та ін.

Метою статті є вивчення змісту поняття кіберзлочинність, її схем, негативних наслідків та способів боротьби з нею.

«Комп'ютерна злочинність» - це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [1, с.387]. Кіберзлочинність - це поняття, яке охоплює, на нашу думку, комп'ютерну злочинність (де комп'ютер - предмет злочину, а інформаційна безпека - об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо.

Нині виділяють такі види кіберзлочинності: шахрайство з пластиковими картками; несправжні Інтернет-аукціони; шахрайство з банківськими кредитами; пошук та використання «проривів» (похибок) в програмах; розсипка листів (спам); азартні ігри в онлайн середовищі; викуп та реєстрація доменних імен (кіберсквоттинг); крадіжка послуг (фоунфрейкинг, «staff fraud»); створення вірусів; крадіжкаінформаціїта особистих даних; викладення у електронних ЗМІ неправдивих новин та ін.

Окрім створення фіктивних електронних магазинів, інвестиційних банків, туристичних агентств, які збирають інформацію про кредитні картки та отримують гроші за неіснуючі товари та послуги, злочинці використовують ряд схем кіберзлочинності. Серед них найбільш розповсюджені такі:

Схеми шахрайства з кредитними картками. Найпростіший вид - Інтернет- кардинг - крадіжка коштів з пластикових карток в Інтернеті. Варіанти шахрайства трансакцій:

покупець - введення номеру чужої картки; створення картки-двійника; отримання та використання товарів або послуг у формі інформації (книжки, компакт диски та інше) та відмова від їх оплати;

продавець - збільшення суми платежу; запам'ятовування отриманого номеру картки та використання його для своїх покупок; відмова від угоди;

банк - підробка трансакцій;

зловмисники, які не беруть безпосередньої участі в угоді - несанкціонований збір інформації про користувача; генерація (зазвичай програмна) існуючого номеру пластикової картки; перехоплення даних платника при передачі, а також «злом» комп'ютерних систем продавця або банку, використання цих даних для маніпуляції з рахунками тощо.

Найбільш розповсюдженим видом злочинів, із-за недосконалості існуючих платіжних систем, є шахрайство з пластиковими картками.

- несправжні інтернет-аукціони.
- схема покупки за найменшою ціною. Шахрайство з банківськими кредитами. Схема «Повітряного змія».
- пошук та використання «розривів» (похибок) в програмах.
- піраміди та листи по ланиржку.
- викуп та реєстрація доменних імен.
- крадіжка послуг.
- викладення у електронних ЗМІ неправдивих новин.

Сьогодні кіберзлочинність має широке розповсюдження та наявність багатьох схем застосування. У зв'язку з цим виникає необхідність застосування певних заходів щодо попередження можливих негативних наслідків розповсюдження кіберзлочинності.

Способами захисту від кіберзлочинності можуть бути: отримання чіткої інформації про особу або підприємства (для перевірки репутації американських сайтів можна відвідати Інтернет- сторінку організації із захисту прав споживачів Better Business Bureau); використання електронних сертифікатів, ЕЦП, безпечних протоколів передачі даних; не надання продавцям реквізитів пластикових карт та паспортних даних; використання кредитних карток (в цьому випадку можливо здійснити чарджбек - процедуру опротестування трансакції); прийняття відповідних законодавчих актів тощо.

Боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Але оскільки кіберзлочинність частково належить до внутрішньої компетенції кожної держави окремо, то необхідним є паралельне напрацювання і національного законодавства, яке буде спрямоване на боротьбу з комп'ютерними злочинами.

Література:

1. Дашян М.С. Право информационных магистралей. - М, 2007. - 288 с.
2. В. Голубев. Стратегия и тактика борьбы с киберпреступностью в странах СНГ. - http://www.crime-research.ru/articles/golubeviune/
3. Голубев В.А. Интервью: Компьютерная преступность - угрозы и прогнозы. - http://www.crime-research.ru/interviews/golubev_interv06/

Мужанова Т.М, к.держ.упр.,доцент
Державний університет телекомунікацій

Кадровий аспект забезпечення інформаційної безпеки держави

Сьогодні, в умовах формування інформаційного суспільства та поступального розвитку інформаційної сфери, основним фактором могутності держави стає володіння найсучаснішими інформаційними технологіями, мережами і засобами, що дозволяють ефективно обробляти, зберігати, передавати, поширювати і, що має особливе значення, захищати інформацію. Володіння державою таким потенціалом, а також функціонування надійної загальнодержавної системи забезпечення інформаційної безпеки (ЗІБ) є передумовою нарощування економічної, військової та безпекової міцності держави, здатності бути конкурентоздатним гравцем на міжнародній арені.

З огляду на зростаючу роль людського фактора у всіх сферах суспільного буття і державного управління необхідним є розгляд персоналу як системоутворюючого елементу системи ЗІБ держави. Особливе значення цього фактора викликане багатьма обставинами.

Незважаючи на те, що вітчизняне законодавство загалом регулює питання розвитку інформаційної сфери держави [5], інформаційної безпеки держави [4,6], діяльності державних органів, які мають повноваження у сфері ЗІБ держави [1-3], (рис.1), потребує удосконалення та приведення до міжнародних стандартів нормативне забезпечення кадрових питань у сфері інформаційної безпеки та впровадження механізмів реалізації правових норм діючого законодавства. Так, на нашу думку, необхідно законодавчо визначити види правопорушень в інформаційній сфері (як у технічному, так і психологічному аспектах), врегулювати питання несанкціонованих дій з використанням мережі Інтернет, які можуть викликати загрозу національній безпеці держави, передбачити можливості для постійного підвищення професійно-кваліфікаційного рівня співробітників органів системи ЗІБ держави в умовах інтенсивного розвитку ІКТ тощо.

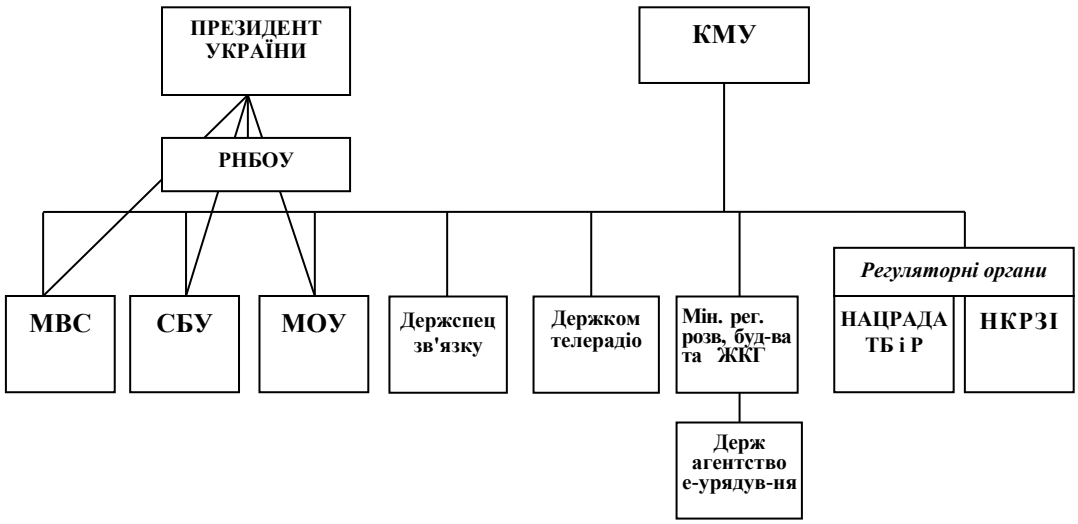


Рис. 1. Органи державної влади у сфері ЗІБ.

Вагомим чинником ефективності системи ЗІБ держави є забезпечення її інтелектуальної безпеки, насамперед у сфері економіки, науково-технічного розвитку, безпеки, оборони та правопорядку. Основними проблемами, що потребують вирішення у цьому контексті, є припинення «відтоку мізків», подолання відставання вітчизняної системи підготовки та підвищення кваліфікації державних та військовослужбовців, які задіяні у сфері ЗІБ держави, з урахуванням прискореного розвитку сфери ІКТ, появою значної кількості інновацій і, відповідно, розширення спектру протиправних дій.

Через неналежні умови праці, в тому числі відставання техніко-технологічного забезпечення державних органів, недостатній рівень соціального забезпечення службовців, відсутність механізмів мотивації незадовільною є безпека трудових ресурсів, низькою - надійність персоналу (переважання приватного інтересу над національними інтересами, схильність до кримінальних дій).

Частково з огляду на перелічені вище соціально-економічні причини, частково – через недостатню інформаційну, просвітницьку та ідейно-виховну роботу падає рівень моральності та патріотизму працівників державних органів, службовців правоохоронних та військових служб, невпинно погіршується імідж та престижність роботи в системі державного управління України.

Оскільки сьогодні актуальною є тенденція до перенесення політичного, економічного та воєнного протиборства між державами в інформаційну сферу особливої важливості набуває проблема недостатньої захищеності службовців системи ЗІБ від негативних інформаційно-психологічних впливів, відсутності навичок визначення та протидії таким видам негативного втручання у свідомість та психіку людини.

З огляду на зростаючу роль людського фактора для покращення кадрової складової системи ЗІБ України доцільно здійснення заходів за такими напрямами: організаційні, навчально-методичні, соціально-економічні та інформаційно-психологічні (рис.2).

Рис. 2. Напрями роботи з кадрами у системі ЗІБ.

Серед *організаційних заходів* виділяють такі як:

- прискорення реформування системи ЗІБ України з метою забезпечення її максимальної ефективності та здатності давати адекватну і оперативну відповідь реальним та потенційним загрозам в інформаційній сфері [3];

- оптимізація структури і складу діючих органів системи ЗІБ та створення єдиного координаційного органу у сфері інформаційної безпеки держави, формування системи професійного кадрового менеджменту у системі ЗІБ;

- проведення спеціальних процедур найму працівників, зокрема з метою «відсівання» невідповідних кандидатів, виявлення психологічних та етичних обмежень будь-якого виду на виконання посадових обов'язків. Так, психологічний відбір дозволяє не тільки з'ясувати морально-етичні якості кандидата, його слабкості, рівень стійкості психіки, але й можливі злочинні схильності, уміння зберігати таємницю [9];

- визначення повноважень та відповідальності у сфері діяльності з інформації з обмеженим доступом та документування добровільної угоди особи про нерозголошення відомостей обмеженого доступу;

- дотримання правил безпечної роботи з конфіденційною та таємною інформацією, навчання й інструктування співробітників щодо практичних дій із захисту інформації;

- здійснення систематичного контролю за роботою персоналу, що працює з конфіденційною інформацією, що є власністю держави, та державною таємницею, дотримання порядку обліку, зберігання та знищення документів і технічних носіїв службової і таємної інформації.

Сучасний стан розвитку інформаційного суспільства та ІКТ засвідчує потребу у прискоренні процесу оновлення професійних знань, умінь і навичок кадрів, задіяних у системі ЗІБ, у відповідності до актуальних вимог системи забезпечення інформаційної безпеки. З огляду на це необхідними *навчально-методичними заходами* є:

- удосконалення системи підготовки кадрів у галузі інформаційної безпеки з посиленням інформаційно-технологічного (розширення викладання нових технічних дисциплін «Основи кібербезпеки», «Хмарні технології» тощо) та інформаційно-психологічного компонентів освіти (дисципліни «Основи безпеки інформаційного середовища», «Інформаційна безпека особистості, суспільства і держави»), а також практичного спрямування освітніх програм;

- здійснення постійного підвищення кваліфікації, так званого навчання упродовж усього життя, у відповідності до розвитку інформаційних технологій, а також з урахуванням практичних напрацювань щодо попередження та ліквідації наслідків протиправних дій у сфері інформаційної безпеки;

- забезпечення тісного зв’язку з недержавними структурами з метою використання кращих зразків управління інформаційною безпекою, протидії несанкціонованим діям у сфері захисту інформації, підготовки кадрів, запозичення передового закордонного досвіду у цій сфері.

У наш час, коли на перший план виходить така форма встановлення переваги однієї країни над іншою як інформаційна війна - "цивілізована" колоніалізація однієї країни іншою [9] серед основних напрямів забезпечення інформаційної безпеки держави є удосконалення *інформаційно-психологічних заходів*, форм і способів протидії негативним інформаційно-психологічним впливам на персонал державних органів, особовий склад правоохоронних та військових формувань з метою послаблення їх готовності до захисту держави, деморалізації, дезінформації та погіршення морально-психологічного стану [8].

Враховуючи те, що метою інформаційної боротьби є захоплення й утримання інформаційної переваги над противником (як у воєнний, так і в мирний час) шляхом здійснення цілеспрямованого і комплексного впливу на свідомість і підсвідомість осіб, які приймають управлінські рішення, а також їх розробників, виконавців, нав’язування їм бажаних для противника рішень і керування їхньою поведінкою, необхідним є формування критичного мислення у всіх службовців та працівників, задіяних у системі ЗІБ держави, та оволодіння ними навичок розпізнавання та протидії прихованим інформаційно-психологічним впливам [3].

Окремими напрямами інформаційно-психологічних заходів є підвищення рівня поінформованості службовців та працівників державних органів, роз'яснення рішень політичного керівництва України та завдань, що стоять перед системою ЗІБ держави і кожним її суб'єктом, створення позитивного іміджу державної служби, служби у правоохоронних та військових органах, підвищення престижу їх діяльності.

Важливе значення для запобігання інформаційним загрозам має мотивація, економічне стимулювання і психологічна підтримка діяльності службовців та працівників, які забезпечують інформаційну безпеку держави.

Законодавство України гарантує забезпечення соціального захисту державних службовців, службовців правоохоронних та військових органів та членів їх сімей [1-3]. Водночас, недостатнє фінансове забезпечення, неможливість задоволення власних життєвих потреб та потреб своєї сім'ї, відсутність необхідного ділового та психологічного клімату в колективі часто мотивують працівників до здійснення протиправних дій.

Переманювання талановитих науковців і практиків, що володіють конфіденційною інформацією з питань інформаційної безпеки держави, підкуп, зовнішній тиск на співробітників, втягування їх у різні види залежності виступають зовнішніми факторами, які підсилюють негативний вплив на кадрову безпеку.

Необхідним є використання заходів матеріальної та нематеріальної мотивації працівників. У системі стимулювання службовців системи ЗІБ держави першочерговим стає обґрунтоване й справедливе матеріальне заохочення, достатні соціальний захист та медичне страхування, психологічна допомога. Крім матеріального стимулювання обов'язковим елементом є нематеріальна мотивація, наприклад залучення підлеглих до обговорення поточних питань, а також прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів й відповідне заохочення, просування по службових сходах, підвищення рівня професійної компетентності працівників через навчання та перепідготовку, заохочення ініціативи та творчого підходу до виконання поставлених завдань [9].

Таким чином, однією з передумов ефективного забезпечення інформаційної безпеки держави є посилення його кадрової складової через здійснення комплексу організаційних, навчально-методичних, соціально-економічних та інформаційно-психологічних заходів.

Список використаних джерел та літератури

1. Закон України від 06.12.1991 № 1934-XII «Про Збройні Сили України». Електронний ресурс. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1934-12
2. Закон України від 25.03.1992 № 2229-XII «Про Службу безпеки України». Електронний ресурс. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2229-12
3. Закон України від 16.12.1993 № 3723-XII «Про державну службу». Електронний ресурс. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/3723-12/page2
4. Закон України від 19.06.2003 № 964-IV «Про основи національної безпеки України». Електронний ресурс. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15
5. Закон України від 09.01.2007 № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Електронний ресурс. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16
6. Указ Президента України від 08.07.2009 № 514/2009 «Про Доктрину інформаційної безпеки України». Електронний ресурс. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/514/2009
7. Алещенко В., Сербін В. Проблеми захисту від негативного інформаційно-психологічного впливу противника. Електронний ресурс. – Режим доступу: http://www.immsp.kiev.ua/publications/articles/2010/2010_1/01_2010_Alechenko.pdf
8. Пєвцов Г., Залкін С., Сідченко С., Хударковський К. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: [монографія]. – Харків : Цифрова друкарня № 1, 2013. – 270 с.
9. Скляренко А. Забезпечення виконання персоналом політики інформаційної безпеки. Електронний ресурс. – Режим доступу: http://analiz.at.ua/publ/informacija/zakhist_informaciji/zabezpechennja_vikonannja_personalom_politiki_informacijnoji_bezpeki/3-1-0-34
10. Фомін В., Рось А. Сутність і співвідношення понять "інформаційна безпека", "інформаційна війна" та "інформаційна боротьба". Електронний ресурс. – Режим доступу: defpol.org.ua/site/index.php/en/publikaci/doc.../25-----q-q-q-q

Рабчун Д. І.
Державний університет телекомунікацій

Динамічні закономірності поведінки порушника інформаційної безпеки

Анотація. Розглянуто математичну модель системи захисту інформації, яка складається з двох об'єктів, що містять інформацію. Проведено аналіз впливу дій нападника на загальний результат інформаційного протистояння. Визначено важливість моделювання не тільки дій сторони захисту, а і сторони, яка здійснює напад на систему захисту.

Вступ. Використання математичної моделі при створенні або менеджменті систем захисту яка приведена в [1] дозволяє дати відповідь на питання: як оптимальним чином розподіляти наявні ресурси для захисту інформації? Але описаний підхід не враховує дій протилежної сторони (нападника), тобто пошук оптимального розподілу ресурсів ведеться в статичному режимі. Для переходу в динамічний режим потрібно розробити модель дій порушника інформаційної безпеки.

Постановка задачі. Для моделювання дій порушника використовується система з двох об'єктів, кожний захищається індивідуальною перешкодою (рис.1).

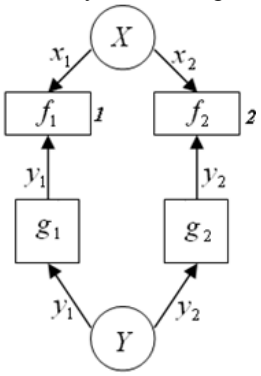


Рис.1 Схема системи захисту інформації

На рисунку позначено:

X та Y — загальні ресурси нападу та, відповідно, захисту;

g_1 і g_2 — частка загальної інформації на кожному з об'єктів ($g_1 + g_2 = 1$);

$f_k(x, y)$ — вразливість перешкоди, котра залежить від співвідношення ресурсів нападу і захисту (k – номер перешкоди) і разом з іншими перешкодами, які захищають об'єкт визначає вразливість об'єкта.

Цільова функція буде мати вигляд:

$$i(x, y) = g_1 f_1(x, y) + g_2 f_2(x, y) \qquad (1)$$

Така функція описує кількість інформації вилученої із системи, при інвестуванні певних ресурсів в інформаційне протистояння.

Так як цільова функція (1) залежить від ресурсів як сторони, що захищає, так і від сторони, що нападає на СЗІ, можна стверджувати, що $\max\ i(x, y)$ буде умовою оптимального розподілу ресурсів X сторони нападу на інформаційну систему.

Функції $f_k(x, y)$ задаємо у вигляді степеневих функції $f_k(x, y) = \dfrac{(x/y)^{n_k}}{c_k + (x/y)^{n_k}}$,

де n_k і c_k — параметри, котрі характеризують продуктивність витрат і визначаються специфікою об'єкта.

Мета дослідження. Пошук оптимального $\{x_k^0\}$ розподілу ресурсів нападника X по об'єктам, котрий максимізує функцію $i(x, y)$. Порівняння отриманих результатів із режимом в якому не враховується оптимізація ресурсів стороною X.

Результати досліджень і висновки. Шукані оптимальні розподіли залежать від параметрів розрахунку: співвідношень X/Y, g_k і значень n_k і c_k. За результатами досліджень зроблені висновки:

1) В залежності від параметрів системи протистояння в динамічному режимі може переходити (за певну кількість кроків N) в стан рівноваги — режим сідлової точки, тобто результати протистояння задовольняють обидві сторони і зміна розподілу ресурсів призведе тільки до програшу (рис.2,а).
2) В іншому випадку протистояння не виходить на режим сідлової точки (рис.2,б) і потрібно приймати рішення про модернізацію СЗІ, перерозподіл інформації на об'єктах або збільшення Y інвестицій в ІБ.

$i(x, y)$ $i(x, y)$

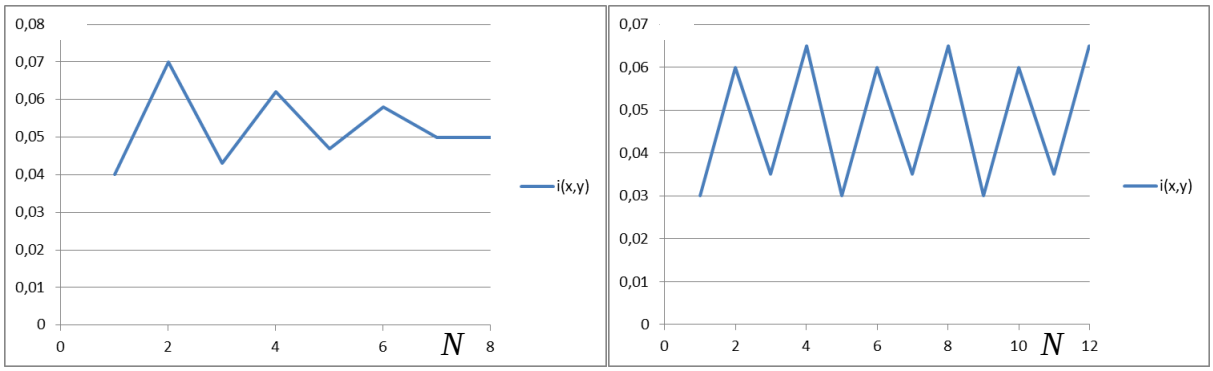


Рис.2 Динамічний режим інформаційного протистояння

Таким чином, проілюстровано вплив дій порушника ІБ на кількість втраченої інформації. Цей вплив проявляється в збільшенні $i(x, y)$, і ситуація, яка для сторони Y була оптимальною, стає програшною, і потребує коригування розподілу $\{y_k\}$.

Список використаної літератури

1. Левченко Є.Г., Рабчун А.О. Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації - 2010. - №1. - С. 16-23.
2. Левченко Є.Г., Прус Р. Б., Рабчун Д.І. Умови існування сідлової точки в багаторубіжних системах захисту інформації // Безпека інформації: наук.-практ. журнал - 2013. - №1. - С. 70-76.

Халапсіна О.А.
Державний університет телекомунікацій

Організаційно-технічне забезпечення управління інформаційною безпекою установи

Практика показує, що побудова комплексної системи інформаційної безпеки неможлива без послідовної реалізації заходів організаційного характеру. Адже можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлюються не технічними аспектами, а зловмисними діями, недбальством і халатністю користувачів або власних співробітників. У кожному конкретному випадку організаційні заходи носять специфічну для конкретної організації форму і зміст, які спрямовані на забезпечення безпеки активів підприємства в різних умовах.

Для забезпечення необхідного рівня інформаційної безпеки на підприємстві створюється комплексна система управління інформаційною безпекою (СУІБ).

Відповідно до стандарту ISO 27001, система управління інформаційною безпекою (СУІБ) - це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки».

Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

Основним завданням системи є забезпечення необхідного рівня доступності, цілісності і конфіденційності компонентів (ресурсів) інформаційної системи підприємства.

Для вирішення цього завдання використовується комплекс заходів, до числа яких входить система організаційних заходів.

Основна характеристика системи: це комплексність, тобто наявність у ній обов'язкових елементів, що охоплюють всі напрямки захисту інформаційних ресурсів підприємства.

Елементами системи є: правовий, організаційний, інженерно-технічний, програмно-апаратний і криптографічний. Організаційний елемент системи містить заходи управлінського, обмежувального та технологічного характеру, що визначають основи і зміст системи захисту, які спонукають персонал дотримуватися правил захисту конфіденційної інформації підприємства.

Елемент включає в себе регламентацію:

1) Формування та організацію діяльності служби безпеки та служби конфіденційної документації, забезпечення діяльності цих служб нормативно-методичними документами з організації і технології захисту інформації.

2) Складання і регулярного оновлення складу інформації, яка захищається підприємством, складання та ведення переліку паперових, машинописних та електронних документів.

3) Системи розмежування доступу персоналу до інформації, яка захищається.

4) Методів відбору персоналу для роботи з інформацією, яка захищається, методики навчання і інструктування співробітників.

5) Напрямів і методів виховної роботи з персоналом, контролю дотримання співробітниками порядку захисту інформації.

6) Технології захисту, обробки та зберігання паперових, машинописних та електронних документів; технології захисту електронних документів.

7) Порядку захисту цінної інформації фірми від випадкових або навмисних несанкціонованих дій персоналу.

8) Ведення всіх видів аналітичної роботи.

9) Порядку захисту інформації при проведенні нарад, засідань, переговорів, прийомі відвідувачів, роботі з представниками ЗМІ.

10) Обладнання та атестації приміщень і робочих зон, виділених для роботи з конфіденційною інформацією.

11) Пропускного режиму на території, в будівлі, приміщеннях, ідентифікації транспорту і персоналу фірми.

12) Системи охорони території.

13) Дій персоналу в екстремальних ситуаціях.

14) Організаційних питань придбання, встановлення та експлуатації технічних засобів захисту інформації та охорони.

15) Роботи з управління системою захисту інформації.

16) Критеріїв і порядку проведення оціночних заходів щодо встановлення ступеня ефективності системи захисту інформації.

В свою чергу організаційні заходи включають чотири основні компоненти:

вивчення обстановки на об'єкті;

розробку програми захисту;

діяльність з проведення зазначеної програми в життя;

контроль за її дієвістю та виконанням встановлених правил.

До числа розглянутих підсистем організаційного плану можна також віднести наступні заходи:

ознайомлення з співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;

організація надійної охорони приміщень і території проходження лінії зв'язку;

організація, зберігання і використання документів та носіїв конфіденційної інформації, включаючи порядок обліку, видачі, виконання і повернення;

створення штатних організаційних структур по захисту цінної інформації або призначення відповідального за захист інформації на конкретних етапах обробки і передачі;

створення особливого порядку взаємовідносин зі сторонніми організаціями та партнерами;

організація секретного і конфіденційного діловодства.

Виходячи з усього вищесказаного, приходимо до висновку, що саме організаційний елемент системи управління інформаційною безпекою на підприємстві є стержнем, основною (до 50-60 %) частиною комплексної системи інформаційної безпеки.

Це пов'язано з тим, що важливою складовою частиною організаційних заходів є підбір, розстановка і навчання персоналу, який буде реалізовувати на практиці систему управління інформаційною безпекою.

ЛІТЕРАТУРА:

1. А.А. Садердинов, В.А. Трайнёв, А.А. Федулов «Информационная безопасность предприятия» ИТК Дашков и К, 2005. – 336 с.

2. Е.Б. Белов, В. Лось, Р.В. Мещеряков, Д.А. Шелупанов «Основы информационной безопасности» Горячая линия – Телеком, 2006. – 544 с.

3. Петренко С.А., Симонов С.В. «Управление информационными рисками. Экономически оправданная безопасность» ДМК Пресс, 2004. – 384 с.

Чудін Д.Д.
Державний університет телекомунікацій

Основні етапи інформаційної атаки

На цей час одним з найбільш актуальних напрямів наукових досліджень в області забезпечення інформаційної безпеки є розробка методів і засобів виявлення атак і захист від атак на комп'ютерні системи (КС) та мережі. Атаки настільки ж різноманітні, як різноманітні системи, проти яких вони спрямовані.

Для виконання вказаних розробок необхідні постійні науково-дослідні роботи, які включають в себе попереднє вивчення і детальне опрацювання всіх можливих варіантів реалізації інформаційних атак. Як правило, такі роботи здійснюють за допомогою моделей, які дозволяють відтворити необхідні властивості і характеристики інформаційної атаки, а також провести оцінку рівня її небезпеки для КС. Моделі дозволяють якомога точно визначити ефективність існуючих і тих, що розроблюються, засобів захисту від інформаційних атак.

Атака на інформацію – це умисне порушення правил роботи з інформацією. Атаки на інформацію можуть принести підприємству величезні збитки. На сьогоднішній день майже 90% всіх атак на інформацію проводять нині працюючі або звільнені з підприємства співробітники.

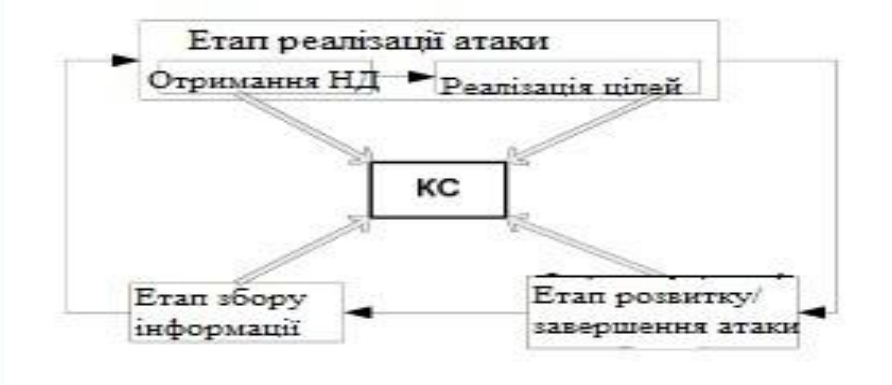
Атака на інформаційну систему називається дія чи послідовність дій порушника, які призводять до реалізації загрози шляхом використання вразливостей системи. Під вразливістю системи розуміється слабке місце КС, на основі

якого можлива успішна реалізація загрози. Загроза, в свою чергу – це потенційно можлива ситуація, явище чи процес, який може викликати нанесення збитків ресурсам системи.

Таким чином, зловмисник, для того щоб реалізувати атаку, моделює певну дію, яке призводить до очікуваного результату за допомогою деякого засобу, котрий використовує вразливості системи.

Інформаційна атака в загальному випадку може включати в себе три основні етапи:

1. Збір інформації – основний етап. Вибирається ціль атаки, збирається інформація про неї, відшукуються найбільш вразливі її місця, вибирається тип атаки.
2. Реалізація атаки. Порушник отримує несанкціонований доступ до тих ресурсів КС на які здійснювалась атака безпосередньо. Загалом це супроводжує порушення цілісності, конфіденційності і доступності інформації. Також можливе приховання слідів факту атаки.
3. Етап подальшого розвитку атаки – виконуються дії, які направлені на подальше продовження атаки на ресурси інших вузлів КС. В деяких випадках цей етап є завершальним.



Безпосередньо захист інформації від атаки проходить ті ж самі етапи, але з іншими цілями: збереження добре відомих нам цілісності, конфіденційності і доступності. З цього випливає, що спеціаліст із захисту інформаційної безпеки чи аналітик, проводить моделювання захисту інформаційної системи від загроз і атак на неї, спираючись на можливі засоби і методи, які можуть запобігти або попередити атаку. Можна виділити такі моделі захисту:

- Класична мандатна модель;
- Модель «Китайська стіна»;
- Модель елементарного захисту;
- Модель безпеки військової системи передачі даних;
- Суб'єктно-об'єктна модель;
- та інші.

Всі ці моделі можуть успішно вирішувати означені проблеми в залежності від вимог, які до них пред'являються. Всі вони базуються на взаємодії суб'єкта із об'єктом, що і виступає основним фактором для створення моделі. Загальна теорія моделювання має на увазі виконання всіх вимог, але існуючі реалізації теорії орієнтовані на виконання в повному обсязі тільки частини вимог, що значно обмежує області застосування кожної моделі. Варто відмітити і те, що, як і більшість технологій безпеки, моделювання захисту розвивається у взаємозв'язку з розвитком мережевих технологій.

д.т.н., с.н.с. Шевченко В.Л.
Державний університет телекомунікацій

Вплив тенденцій розвитку глобальної інформаційної інфраструктури на розвиток інформаційної інфраструктури силових відомств

Глобальна інформаційна інфраструктура (ГІІ) інтегрує інші інформаційні інфраструктури, зокрема й інформаційні інфраструктури силових відомств, незалежно від того бажають того останні, чи ні. Вплив відбувається як через безпосередньо підключення, так і через проникнення новітніх технологій всередину відносно консервативного силового сектору.

Поняття ГІІ запропоноване ще в 1994 році (Ель Гор), але насправді це було лише термінологічне визначення явища, яке де-факто вже набирало оберти і завдяки масштабам свого впливу на всі сторони життя людства потребувало упорядкування в масштабі планети.

Задекларована **мета ГІІ**– прискорення і збільшення економічного зростання завдяки розповсюдженню інформації і дистанційного співробітництва (зокрема, відкриття закордонних ринків і зменшення бар'єрів

несумісності стандартів). Завдяки ГІІ всі люди можуть отримати користь від інформаційних та телекомунікаційних технологій.

Основні **принципи ГІІ**:

- заохочення приватних інвестицій,
- конкуренція;
- гнучки рамки регулювання,
- відкритий доступ до мереж,
- універсальність послуг.

Отже без впровадження надсучасних (перспективних) мереж зв'язку не обійтись.

Основні **вимоги до перспективних мереж зв'язку.**

- Незалежність технологій надання послуг від транспортних технологій.
- Гнучкість та швидкість зміни пропускної спроможності.
- Мультімедійність з синхронізацією компонент в реальному часі.
- Інтелектуальність управління послугами.
- Інваріантність послуг щодо технології доступу.
- Багатооператорність.

Це веде до необхідності розвитку традиційних мереж зв'язку у напрямку **мультисервісних мереж.**

Складність сучасних технологій вимагає узгодження дій в сфері телекомунікацій за допомогою централізуючого, координуючого органу міжнародного рівня (МСЕ, Міжнародний союз електрозв'язку). Йому ж належить центральна роль в стандартизації процесу створення ГІІ. Діяльність МСЕ розподілена між секторами: радіозв'язку, електрозв'язку, стандартизації.

Основні принципи ГІІ, які необхідні для створення мереж наступного покоління (NGN, next generation network):

- пакетна комутація та
- єдина мережа для всіх видів трафіку, архітектура розподілена за незалежними рівнями.

До складу транспортної мережі NGN входять:

- транзитні та граничні вузли,
- контролери сигналізації,
- шлюзи для підключення традиційних мереж зв'язку.

При цьому вузол доступу повинен доставляти інформацію будь-якому термінальному пристрою на основі таких технологій:

- засобів аналогового доступу (МЗЗК, мереж зв'язку загального користування),
- засобів базового BRI та первинного PRI доступу ISDN,
- цифрових абонентських ліній xDSL,
- пасивних оптичних мереж,
- радіодоступу.

Оскільки жодна з перелічених технологій не може повною мірою забезпечити потреби мультисервісного доступу, то створюють абонентські концентратори, які об'єднують ці технології.

На початковому етапі МЗЗК може стати часткою конвергентної мережі завдяки шлюзам VoIP між МЗЗК і транспортною мережею IP/MPLS. Архітектура мереж NGN включає: сервери додатків, програмне забезпечення для підтримки (Application Programming Interface, API), прикладний програмний інтерфейс API, Softswitch - контролер медіашлюзів, обробник викликів, конвертор сигналізації, транспортні платформи, медіашлюзи.

Основні проблеми переходу до NGN:

- відсутність достатніх інвестицій;
- відсутність єдиної політики переходу до NGN;
- відсутність або недосконаліть стандартів щодо NGN;
- відсутність повної лінійки обладнання для NGN;
- несумісність обладнання різних виробників.

Мультисервісні мережі дозволяють надання в межах одної мережі як традиційних, так й інфо-комунікаційних послуг. Їх слід будувати на основі двухрівневої архітектури: регіонального та магістрального (включаючи міжрегіональний) рівнів.

Сучасні мережі гетерогенні, що змушує системних адміністраторів та інтеграторів витрачати левову частку свого часу на узгодження різнорідних компонент. Проблема слід вирішувати за допомогою сучасних технологій, наприклад, ATM (Asynchronous Transfer Mode), яка повинна дозволяти: передачу в одної мережі **комп'ютерного та мультимедійного** трафіку, чутливого до затримок; загальні транспортні протоколи для локальних та глобальних мереж; збереження існуючої інфраструктури фізичних каналів або фізичних протоколів (T1/E1, T3/E3, SDH STM-n, FDDI); взаємодію з наслідуваними протоколами локальних та глобальних мереж (IP, SNA, Ethernet, ISDN).

Мультисервісні мережі наступного покоління об'єднують в єдиній архітектурі:

- звичайний телефонний зв'язок,
- стільниковий зв'язок,
- ресурси мережі Інтернет,

- IP-телефонію,
- кабельне телебачення.

При цьому існуючі мережі комутації каналів (ТфОП, ISDN) зберігаються теж.

Основні етапи створення універсальної мережевої інфраструктури:

- ISDN (Integrated Services Digital Network), 1970.
- B-ISDN (broadband ISBN), 1988.
- NGN.
- IMS (IP Multimedia Subsystem) , 1998. Мультимедійна IP-орієнтована підсистема зв'язку, яка за багатьма ознаками дозволяє створити універсальну мережеву архітектуру, основним елементом якої є пакетна транспортна мережа (підтримує всі технології доступу, всі існуючі мережі, забезпечує реалізацію великої кількості інфокомунікаційних послуг).

Таким чином, темпи появи нових інфокомунікаційних технологій вимагають від силових відомств відповідної оперативності щодо їх реалізації в інтересах національної безпеки держави.

к.т.н., с.н.с. Щебланін Ю.М.
Державний університет телекомунікацій

АНАЛІЗ СТРУКТУРИ СПЕЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ

На сьогодні за допомогою інформаційної зброї протиборчі сторони здатні вирішувати стратегічні завдання, зокрема: наносити серйозної шкоди національним інтересам, підривати основи державності; дискредитувати державні органи і ускладнювати прийняття ними важливих рішень, паралізувати управління країною в кризових ситуаціях; створювати атмосферу напруженості в суспільстві, провокувати соціальні, політичні, національні та релігійні заворушення, ініціювати страйки, масові заворушення та інші акції економічного протесту, створювати атмосферу бездуховності і аморальності; дезорганізувати техносферу, економіку, систему комунікацій; підривати міжнародний авторитет держави та перешкоджати її співпраці з іншими країнам [1].

Одним з підходів до вирішення зазначених стратегічних завдань є проведення спеціальних інформаційних операцій спрямованих на підрив іміджу та довіри до політичного керівництва та держави і населення вцілому.

Зазначене питання є вкрай важливим для України, де навіть поверхневий аналіз дозволяє виявити проведення цілого ряду спеціальних інформаційних операцій, які доцільно класифікувати як повномасштабну інформаційну війну.

Відсутність своєчасної протидії таким операціям та відсутність державних органів з відповідними повноваженнями і можливостями значною мірою вплинула на розв'язання війни в східному регіоні нашої держави. Аналіз структури спеціальної інформаційної операції дозволить організувати ефективну протидію її проведенню та своєчасного виявлення етапів її підготовки.

Спеціальні інформаційні операції – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію шляхом впливу на її свідомість і поведінку за допомогою використання певним чином організованої інформації та інформаційних технологій для досягнення певної мети [1, 2].

Спеціальні інформаційні операції різних видів здійснюються за приблизно однаковою схемою. Виходячи із загальних положень системного аналізу, вона виглядає наступним чином [1-3]:

1. *Попередній етап*. На цьому етапі відбувається планування операції, зокрема визначення доцільності її проведення, цілей, завдань, сил і засобів, цільової аудиторії впливу, прийомів і методів впливу і т.ін.

2. *Інформаційний привід*. На цьому етапі спеціальної інформаційної операції необхідно вибрати або створити так званий інформаційний привід. Під інформаційним приводом слід розуміти подію (псевдоподію), яка може використовуватися як привід для пропагандистської кампанії або інформаційної операції. Вибір інформаційного приводу становить окрему проблему, яка детально розглянута в спеціальній літературі.

3. *«Розкрутка» інформаційного приводу.* Цей етап є основною частиною будь-якої інформаційної операції. Його суть полягає у використанні інформаційного приводу заради досягнення цілей операції, тобто для посилення, формування або руйнування певних психічних стереотипів і установок.

4. *Вихід зі спеціальної інформаційної операції або етап закріплення.* Найважливіше завдання цього етапу - забезпечення плавного завершення пропагандистської кампанії або інформаційної операції після досягнення поставлених цілей або через форс-мажорні обставини.

Етап планування спеціальної інформаційної операції.

На цьому етапі можливий наступний порядок діяльності:

1. Визначення мети.
2. Визначення об'єкта.
3. Аналіз сил і засобів, ресурсів, визначення виконавців.
4. Визначення методів і прийомів.
5. Розробка приблизного сценарію.
6. Визначення критеріїв оцінки успіху.

Етап створення інформаційного приводу.

Як інформаційний привід можна застосовувати практично будь-яку подію. Втім, набагато краще, якщо інформаційний привід дійсно є важливою подією. Це будь-яка подія, яка якимось чином співвідноситься з наявним, актуальними стереотипами аудиторії, порушує певні табу: акти святотатства, надзвичайне насильство і т.ін. Дослідження стереотипів - важлива проблема, яка вимагає глибокого наукового дослідження.

Відомо, що будь-яка система стереотипів і, тим більше, національна, в своїй основі, змінюється дуже повільно. Наприклад, за оцінками дослідників, зараз, як і раніше, люди сильно довіряють друкованому і, особливо, екранному слову.

Другий варіант інформаційного приводу - події, що безпосередньо впливають на людей, які становлять переважну більшість цільової аудиторії.

В переважній більшості випадків як інформаційний привід використовують негативні події, які набагато чіткіше позначаються на свідомості аудиторії.

На вибір (створення) інформаційного приводу повинні впливати, насамперед, характеристики цільової аудиторії, зокрема її національні, соціальні та інші стереотипи чи установки.

«Розкрутка» інформаційного приводу.

Цей етап фактично і є пропагандистською кампанією. Важливим є врахування вимог зворотного зв'язку під час звичайних пропагандистських кампаній, а в спеціальних інформаційних операціях він набуває ще більшого, ключове значення.

Закріплення або вихід із спеціальної інформаційної операції.

Кожна спеціальна інформаційна операція в своїй основі передбачає маніпулювання громадською або індивідуальною свідомістю. Основною ознакою маніпуляції є її незрозумілість для об'єкта. Іншими словами, розгадана маніпуляція, є невдалою. Точно так само, якщо об'єкт впливу розуміє, що проти нього проводиться спеціальна інформаційна операція, то він завжди може знайти методи протидії та зірвати її. Саме тому необхідно здійснювати «м'який» вихід зі спеціальної інформаційної операції. Часто цією вимогою нехтують, що призводить до значного, а іноді і катастрофічного зменшення ефективності операції. На цьому етапі необхідно вирішити завдання закріплення досягнутих результатів. Особливо це важливо в операціях, спрямованих проти суб'єктів прийняття рішень (політичного керівництва держави).

Література

1. Галамба М.М. Сутність, види та методи спеціальних інформаційних операцій. / М.М. Галамба // Юридичний журнал. [Электронный ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=2524.
2. Литвиненко А.В. Специальные информационные операции и пропагандистские кампании: моногр. / А.В. Литвиненко. [Электронный ресурс]. – Режим доступу до книги: http://click.hotlog.ru/?40793.
3. Богданович В.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: монографія / В.Ю.Богданович, І.С.Романченко, І.Ю.Свида.-Львів: АСВ, 2011.- 414с.

к.в.н. Якименко Ю.М.
Державний університет телекомунікацій

Напрями забезпечення безпеки інформації в організації

Оцінка інформаційної безпеки, як правило, спрямована на рішення конкретних проблем по досягненню необхідного рівня загальної безпеки організації. Ці критерії створювалися і широко використовуються при сертифікаційних випробуваннях захищеності автоматизованих систем загального призначення.

Головна увага при оцінці інформаційної безпеки приділяється забезпеченню збереження основних властивостей інформації: конфіденційності, достовірності та доступності.

Для того, щоб їх можна було застосувати до кожної організації, виникають певні труднощі, які залежать, насамперед, від її організаційної структури (архітектури) і умов інформаційно-аналітичної діяльності.

У той же час у відношенні інформації повинна бути забезпечена в першу чергу гарантія її цілісності (надійності - в документах при їх розробці, зберіганні і передачі адресатові тощо).

У відповідності зі стандартами США (Єдині системи - програмної та конструкторської документації) розроблені вимоги до забезпечення цілісності інформації та класифікація залежно від її значущості, які враховуються при сертифікації інформаційно - технологічних продуктів.

Системне забезпечення цілісності інформації в організаціях спрямовано на:
- забезпечення цілісності програмних засобів та інформації, що обробляється;
- фізичну охорону засобів обчислювальної техніки і носіїв інформації;
- наявність адміністратора (служби) захисту інформації в автоматизованих системах;
- періодичне тестування засобів захисту інформації (СЗІ) від несанкціонованого допуску (НСД) до неї;
- наявність засобів оперативного відновлення СЗІ від НСД;

- використання сертифікованих засобів захисту.

Створення захищеної зони, в якій встановлені засоби фізичної безпеки, роблять неможливим неконтрольований доступ сторонніх осіб без постійного або тимчасового пропуску. Тому для фізично ізольованої системи в цих умовах може ігноруватися загроза несанкціонованого доступу до комп'ютера або підключення до каналу зв'язку між комп'ютерами для перехоплення трафіку.

Персоналу організації може бути наданий доступ до всієї оброблюваної інформації і надані рівні права доступу. В цих умовах не є обов'язковим використання програм для управління доступом (за принципами дискретного управління доступом) і управління доступом до інформації не може організовуватися.

В організаціях, як правило, список файлів і програм, з якими працюють співробітники, чітко регламентований. Тому можна однозначно визначити всі інформаційні потоки і механізми безпеки інформації, що дозволяє організовувати управління доступом за принципами дискретного управління.

Неоднозначний підхід до вибору методів та засобів захисту спостерігається із-за відмінностей;
- у важливості оброблюваної інформації;
- між системами щодо компонент, структури та методів, використовуваних для обробки, зберігання і передачі інформації, які входять до їх складу ;
- між характеристиками і кількістю користувачів та обслуговуючого персоналу.

Слід зазначити, що сертифіковані засоби захисту ще недостатньо використовуються, особливо в комерційних організаціях України.

З урахуванням вимог до забезпечення безпеки інформації в організації все обладнання, програмне забезпечення та організаційні заходи, пов'язані із забезпеченням захисту інформації від НСД, можуть бути розділені на наступні підсистеми:
• Підсистема управління доступом.
• Підсистема реєстрації і обліку.
• Криптографічний підсистема.
• Підсистема забезпечення цілісності.

З урахуванням вище викладеного, як доповнення до напрямів системного забезпечення цілісності інформації в організаціях, пропонується мінімальний набір вимог до забезпечення безпеки інформації:
- гарантії передачі і прийому даних;
- цілісність мережних з'єднань;
- використання захищених каналів зв'язку;
- використання сертифікованих міжмережевих екранів.

Збереження цілісності інформації безпосередньо залежить від можливостей сучасних технічних систем, в яких вона функціонує.

Сучасні операційні системи (ОС) і системи управління базами даних (СУБД) розробляються і сертифікуються з урахуванням вимог до безпеки інформації. Саме ці системи успішно використовуються в інформаційних технологіях, критичних до безпеки інформації.

В якості об'єктів ОС визначені: робочі станції, сервери, мережі, домени, комунікаційні канали, порти, периферійні пристрої, диски, тома, каталоги, файли тощо).

До об'єктів СУБД відносяться: файли, індекси, таблиці, записи, поля записів, схеми, процедури тощо).

Знову створювана система захисту інформації в організації повинна бути атестована на дотримання вимог до забезпечення безпеки інформації в реальних умовах експлуатації. У деяких випадках ОС і СУБД повинні бути сертифіковані на більш високий рівень захищеності, ніж той, який забезпечується комерційними версіями, що призводить до необхідності їх подальшої модифікації і доопрацювання.

ОС і СУБД, пропоновані в якості основних засобів при створенні систем захисту інформації в організаціях, повинні бути оцінені по можливостям забезпечення системної безпеки.

Так, наприклад, стандартні засоби захисту інформації, що є в ОС Windows NT 4.0 і СУБД SQL Server 6.5 найбільше задовольняють пропонованим вимогам забезпечення безпеки інформації:
- можливість ідентифікації і аутентифікації користувачів при їх вході в систему (максимальна довжина пароля в Windows NT 4.0 - 14 символів, а в SQL Server 6.5 - 30);
- ідентифікація всіх звернень до об'єктів ОЗ по імені і його маркера безпеки;
- ідентифікація звернень до об'єктів СУБД в системі по імені;
- створення в ОС детальних журналів подій: запуску і зупинки системи, входу і виходу користувача із системи, доступу до об'єктів, запуску і завершення процесів, змін повноважень доступу суб'єктів і т. д.;
- реалізація дискреційної політики управління доступом до об'єктів ресурсів ОС з допомогою Object Manager і Security Reference Monitor.
- використання реєстру та відповідних модулів для перевірки цілісності системи при запуску;
- забезпечення цілісності засобів захисту СУБД шляхом ізоляції їх від користувачів з допомогою механізмів безпеки ОС і СУБД, а також з допомогою можливостей СУБД з оперативного відновлення баз даних.

Як показує практика експлуатації подібних систем у разі обробки конфіденційних документів і у великій їх кількості потрібно проводити періодичну очистку звільнених областей пам'яті, спостереження за передачею даних по мережі, налаштування міжмережевих екранів, шифрування даних і т. д. Тому такі системи вимагають внесення відповідних змін у механізми безпеки.

Для того, щоб сертифікувати механізми безпеки в Windows NT 4.0 і SQL Server6.5 на виконання вимог, що висуваються до них - для конкретних організацій і умов їх роботи, необхідно проводити додаткові дослідження і експерименти (тестування) у відповідності з розробленими програмою та методологією.

Для вирішення цього завдання мають бути спрямовані зусилля розробників технічних систем, з обов'язковим урахуванням думки операторів, які експлуатують ці системи.

Хропко Т.О.

Інформаційно-психологічний вплив як актуальна проблема інформаційної безпеки держави.

Сучасний етап розвитку суспільства характеризується переорієнтацією провідних країн світу на нові інформаційні принципи, обумовлює необхідність визначення нетрадиційних підходів до проблем забезпечення національної безпеки держави і насамперед її складової частини — інформаційної та воєнної безпеки.

Інформація перетворилася зараз на глобальний ресурс, використання якого дає змогу значно збільшити ефективність керування усіма життєвими сферами.

Головна інформаційна загроза для нас – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість,підсвідомість особистості, з метою нав’язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні.

Поєднання традиційних форм ведення інформаційної боротьби з останніми досягненнями в галузі інформаційних технологій почали істотно впливати на хід та результат розв’язання конфліктних ситуацій, досягнення поставлених цілей шляхом проведення інформаційно−психологічних операцій.

Тобто перевагами інформаційно−психологічних операцій є: практична відсутність людських втрат; порівняно невеликі витрати на проведення операції; відсутність ефекту помсти, оскільки переможені не відчувають свого програшу.

Дослідженням інформаційної безпеки та складових інформаційних впливів присвячені роботи О.Литвиненка , А.Маслоу, В.А.Ліпкана та ін.

Загальним джерелом загроз інформаційно-психологічної безпеки особистості є та частина інформаційного середовища суспільства, яка в силу різних причин, не адекватно відображає навколишній світ людини. Тобто інформація, яка вводить людей в оману, у світ ілюзій, не дозволяє адекватно сприймати навколишнє і самого себе.

Інформаційне середовище набуває для людини характер другий, суб'єктивної реальності. Ту її частину, яка містить інформацію, неадекватно відображає навколишній світ, і ті її характеристики і процеси, які ускладнюють або перешкоджають адекватності сприйняття і розуміння людиною навколишнього і самого себе, можна умовно позначити як "ілюзорна реальність". Незважаючи на свою ілюзорність, і навіть в силу своєї ілюзорності, але у формі уявній реальності, вона є основним зовнішнім джерелом загроз інформаційно-психологічної безпеки особистості.

В наш час проблема забезпечення інформаційної безпеки держави поки перебуває на стадії розроблення. Дана обставина обумовлена неадекватністю між формуванням інформаційної цивілізації і заходами із забезпечення інформаційної безпеки.

Отже, маніпулювання людьми використання різних засобів і технологій інформаційно-психологічного впливу стало досить звичайним явищем у повсякденному житті, економічній конкуренції та політичній боротьбі. Таким чином розуміння загроз інформаційно-психологічної безпеки особистості, механізмів їх дії і можливостей психологічного захисту стає не тільки теоретичною проблемою але і потребою соціальної практики і повсякденного життя людини.

Карпенко Є.М.
Державний Університет Телекомунікацій, м.Київ

Програмні засоби несанкціонованого одержання інформації

В залежності від мети проникнення на чужий віддалений комп'ютер зловмисник вибирає той чи інший діапазон пошуку IP-адрес. Якщо метою є отримання просто різної інформації (паролі на пошту, чи інші документи), то IP може бути довільним, вибраним зовсім випадково - від мінімального IP 000.000.000.000 до максимального IP 255.255.255.255.

Якщо хакеру знадобились паролі для доступу в Інтернет, то він буде перевіряти лише IP-діапазон свого провайдера. Якщо, наприклад, IP хакера 123.2.34.14, то потрібні адреси будуть в діапазоні від 123.2.34.1 до 123.2.34.255. Метод сканування діапазону також IP залежить від кінцевої мети хакера.

Зазначимо, що взнати IP свого комп'ютера можна, викликавши програму ipconfig (Start - Run - ipconfig), знаходячись в on-line режимі.

Для несанкціонованого отримання паролів доступу в Інтернет використовується сканер Shared Resource Scanner. Характеризується швидкодією, знаходить на комп'ютері файли із розширенням *.pwl, що зберігаються у системній

папці Windows. Отримані файли копіюються на комп'ютер хакера, де розшифровуються програмами PwlTool або HackPwl.

Такий підхід до зберігання паролів у вигляді окремого файлу на диску (кешування) спричинив багато проблем для користувачів, в яких кешування встановлювалось по замовченню. Оскільки, зазвичай, файл з паролями мав ту саму назву, що й ім' я користувача в системі. Тобто, якщо користувач при інсталяції Windows назвав себе як Thinker, то файл з усіма паролями буде розташовано тут: C:Windows Thinker.pwl

Для відключення кешування паролів для ОС Windows95/98 була передбачена програма System Policy Editor (Редактор системних правил) з комплекту ОС Windows95/ 98 Resource Kit, який був на компакт-диску разом із ліцензійною копією операційної системи. В нових версіях Windows кешування паролів відключено автоматично.

Отримання інформації (документи, файли). Для цього хакер може використовувати сканер xShareZ, що під'єднує локальні диски віддаленого ПК до своїх як сіткові. Або просто пише в броузері (програма для перегляду веб-сторінок) IP-адресу потрібного комп'ютера.

Найпоширенішою помилкою користувачів є розміщення текстового файлу з усіма паролями прямо на робочому столі - щоби не шукати довго. Тому рекомендується зберігати свої паролі на окремих носіях - дискетах, оптичних дисках, флеш-картах, тощо. В крайньому випадку пароль можна записати в зошиті, що зберігається у надійному місці.

На випадок втрати парольної інформації рекомендується завжди робити резервну копію і тримати її в іншому надійному місці. Також обережний користувач не повинен користуватись менеджером паролів (що пропонує запам' ятати його для зручності), а кожного разу при роботі вводити секретну інформацію.

При доступі до чужого комп'ютера хакер може взнати номер ICQ користувача, скопіювавши собі файл з розширенням *.dat, що знаходиться за таким шляхом - C:Program FilesICQicq(версія). Тоді за допомогою програми ICQr Information з файлу взнається пароль та номер.Багато недоліків мають і поштові клієнти. Наприклад, The Bat! дозволяє переглянути з віддаленого комп'ютера повні дані про з'єднання. А засоби програми Open Pass дозволять хакеру перетворити пароль, вказаний зірочками, у читабельну форму.

Сучасні комп'ютерні системи використовують програмні засоби різноманітного призначення в одному комплексі. Наприклад, типова мережа автоматизованого документообігу складається з операційної системи, програмних засобів управління базами даних, телекомунікаційних програм, текстових редакторів, антивірусних моніторів, засобів для криптографічного захисту даних, а також засобів ідентифікації та аутентифікації користувачів.

Головною умовою захищеності інформації в такій системі є забезпечення неможливості втручання у її функціонування з боку програм, присутність яких у системі є зайвою. Серед подібних програм, насамперед, необхідно зазначити програмні закладки, клавіатурні шпигуни та комп'ютерні віруси.

Олександр М.П.
Державний університет телекомунікацій, м. Київ

Системи захисту, з використанням систем відео спостереження

Системи відео спостереження є системи програмно-апаратних засобів, які реалізують функцію відеоспостереження, область дії та застосування яких обмежена географічно територією будівлі, підприємства, організації і т. і. Централізована система має один центр і деяку кількість відеокамер.

Децентралізована система являє собою сукупність кількох централізованих, об'єднаних логічно в одну структуру, але фізично розділених і здатних функціонувати незалежно систем.

Основною тенденцією сьогодення у розвитку систем відеоспостереження є інтеграція локальних систем відеоспостереження, побудова та впровадження системних рішень на потребу охорони громадського порядку, боротьби з «вуличною» злочинністю, та транспортною безпекою у межах окремих населених пунктів, автодоріг, місць скупчення людей, тощо (наприклад, проект «безпечне місто»).

За таких умов до систем відеоспостереження мають висуватися окремі вимоги щодо гарантованого запису інформації, її архівування та технічного захисту.

Актуальною задачею слід вважати розробку типової підсистеми захисту інформації системи відеоспостереження на основі аналізу та систематизації існуючих програмно-апаратних комплексів, пропонування на цій основі оригінальних рішень, які мали б на меті підвищити захищеність як інформації, що отримується та циркулює в таких системах.

Для того щоб здійснити системний комплексний підхід до систем безпеки у цій галузі, я пропоную розробку додаткового спектру послуг з організації віддаленого відео спостереження, інтеграції відео спостереження та системами контролю та управлінням доступом.

Пшоннік В.О.
Державний університет телекомунікацій

Розробка метода захисту RFID технології

На сьогодні велику популярність майже у всіх важливих з точки зору захисту інформації областях здобули RFID (англ. *Radio frequency identification*) мітки. Вони широко використовуються у бізнес центрах, будинках,тренажерних залах(як контроль доступу), у банківській справі (як аналог банківських карток), у магазинах (як засіб контролю за товаром), у метро (для оплати проїзду). Тому захисту інформації на них доцільно приділяти

більшу увагу.Особливо після того як на найбільшій конференції хакерів DEFCON було продемонстровано пристрій, який копіював код пасивного RFID ключа з відстані двох метрів. Проте представники платіжних систем говорять, що за шість років не було задокументовано жодного випадку подібного роду шахрайства, що є доказом достатнього рівня захисту для такого типу атак, бо наразі можливо провести лише одну транзакцію до блокування картки. Але ніщо не заважає злодіям за декілька годин скопіювати 10-20 карток.

Наразі використовується лише один засіб захисту від зчитування даних з RFID носіїв. Це мілко зерниста алюмінієва сітка, яка вшивається у гаманець чи спеціальний чохол для карток та буцімто унеможливлює зчитування за рахунок того, що ізолює носій від електромагнітного поля зчитувача.

Нажаль, це є доцільним лише у випадку банківських RFID міток.З картками доступу або ключами у виді брелока ця схема не є вдалою. Тому метою моєї роботи буде аналіз усіх недоліків даної технології та розробка метода, який зможе протидіяти зловмисному попиту, що зараз ще більше зростає.

Хоча мною ще не проводились дослідження, найбільш перспективним напрямком розвитку є локальне просторове зашумлення за допомогою електромагнітних полів.

RFID технологія у наш час отримала значне розповсюдження у всіх важливих сферах нашого життя. Проте я не знайшов слідів особливої зацікавленості у розвитку захисту цієї технології зі сторони провідних компаній які спеціалізуються на захисту інформації. Тому я маю мету провести дослідження цього питання та розробити метод захисту який зможе задовольнити такі вимоги як: надійність, простота, безпечність (для людини та інших приладів, що зазвичай з собою носить людина), низька вартість.

Боклан М.С.
Державний університет телекомунікацій , м. Київ

Система управління доступом на об’єктах інформаційної діяльності

Система контролю і управління доступом (СКУД) є одним з основних елементів сучасних систем безпеки. Поряд з іншими комплексами, такими як охоронно-пожежна сигналізація і комплекс відеоспостереження СКУД дозволяє створити інтегровану систему комплексної безпеки охоронюваних об'єктів. Судячи з останніх даних про продажі різних технічних засобів безпеки, споживачі виявляють найбільшу цікавість саме до СКУД. Темпи зростання її продажів на сьогоднішній день складають 15%, тоді як інші види охоронних систем мають більш скромні показники - 7%. З урахуванням цього має сенс розглянути деякі загальні та технічні аспекти перспективи розвитку системи контролю та управління доступом.

Перш за все, варто відзначити високий потенціал розвитку СКУД. На сьогоднішній день система контролю доступу є невід'ємною частиною комплексу безпеки, що охороняється і при цьому взаємодіє з іншими системами життєдіяльності будівлі і навіть із загальною системою управління підприємством. У першу чергу це відноситься до загальної системи управління будівлею, системі управління персоналом компанії і системі комерційного обліку.

Такий ступінь взаємодії та інтегрованості СКУД з іншими системами забезпечується наявністю прямого контакту з користувачами. Відбувається постійний обмін даними між СКУД і іншими інформаційними системами і комплексами про дії знаходяться в будівлі. Це істотно спрощує їх роботу і робить її більш ефективною, а так само сприяє зниженню витрат на енергоресурси. Зокрема наявність даних про точний час приходу або відходу співробітників компанії дає можливість контролювати, а при необхідності і регулювати мікроклімат і ступінь освітленості на робочому місці. Витрати на освітлення та підтримання комфортної температури і вологості складають до 60% від усіх витрат на енергоспоживання. Вибір оптимальних алгоритмів дозволяє скоротити ці витрати до 15%.

Ці ж дані, що надійшли до бухгалтерії і департамент кадрів компанії, дозволяють створити автоматичну систему розрахунку заробітної плати та інших нарахувань, а так само мати уявлення про відвідуваність і дисципліні кожного співробітника. Результатом цього є зниження витрат на утримання апарату бухгалтерії та поліпшення керованості підприємством. Але це не всі додаткові можливості, які може надати СКУД. Її застосування дозволяє об'єднати на єдиній карті комерційні та соціальні програми, такі як система внутрішнього розрахунку, медичне страхування, електронні гроші тощо.

Система СКУД може працювати на різних носіях, кожен з яких має свої можливості. На практиці застосовуються картки, проксіміті, CMART і RFID. Використання карток в якості універсального засобу ідентифікації та зберігання даних в значній мірі розширило можливості СКУД і забезпечило зростання її популярності. Пасивні проксіміті мають ряд переваг в порівнянні з магнітними і аналоговими носіями, але при цьому мають досить високу вартість (до 2 доларів) і маленький радіус дії (не більше 15 см). Систему CMART можна було вважати ідеальною, якби не її висока вартість, яка викликана досить складною конструкцією і наявністю вбудованого мікрочіпа. Але в ряді випадків всі ці недоліки компенсуються високим ступенем надійності, захищеності і багатофункціональності. А можливість використання CMART в якості платіжного засобу та зберігання персональних даних повністю виправдовує її високу вартість.

Основні очікування на ринку технічних засобів безпеки пов'язані з появою RFID. Ця технологія належить до класу hands-free і дозволяє значно спростити використання і підвищити ефективність використання СКУД. RFID або Radio Frequency Identification дозволяє здійснювати дистанційну ідентифікацію на заданій радіочастоті. Використання RFID дозволить пересуватися по будівлі, не пред'являючи карток або пропусків. Система здатна виробляти ідентифікацію на відстані 4 метрів. Транспондери, передавальні радіосигнал можуть використовуватися в якості міток для відстеження переміщення дорогого майна. На даному етапі використання RFID кілька обмежено через досить

великих витрат на придбання обладнання, а так само у зв'язку з низьким ступенем захисту від сторонніх випромінювань і екранування. За оцінками фахівців використання більш широкого діапазону випромінювання і зменшення вартості транспондера до більш прийнятною (близько 1 долара) дозволить більш активно впроваджувати цю різновид СКУД.

Використовуються і біометричні системи контролю. Вони відрізняються найбільшою надійністю, але через дуже високу вартість і складності не мають широкого застосування. Дана система використовує для ідентифікації сітківку очей, відбитки пальців, форму руки та інші біометричні дані. Поки біометрична система розпізнавання застосовується на військових і ядерних об'єктах, а так само в банківській справі. Але користувачів не влаштовує низька швидкість розпізнавання і часті помилкові спрацьовування, що ускладнює застосування цієї системи на об'єктах з великою кількістю співробітників. Основні перспективи розвитку експерти пов'язують з впровадженням даної системи ідентифікації для систем безпеки приватного житла. Найбільш перспективними є технології розпізнавання по сітківці ока і за формою руки.

Передбачається, що в найближчі 5 років буде створена більш досконала система ідентифікації, яка буде мати більш високу швидкість і мінімальна кількість помилкових спрацьовувань.

Прогрес розвитку систем СКУД очевидний. Це розвиток впливає і на підвищення ефективності інших систем. Причиною прогресу є активне впровадження сучасних технологій, які дозволяють удосконалювати цей напрям технічних систем безпеки. Сьогодні створено чимало різновидів СКУД. Фахівці з систем безпеки допоможуть вибрати найбільш оптимальну і ефективну конфігурацію.

Боклан М.С.
Державний університет телекомунікацій , м. Київ

Система управління доступом на об'єктах інформаційної діяльності

Система контролю і управління доступом (СКУД) є одним з основних елементів сучасних систем безпеки. Поряд з іншими комплексами, такими як охоронно-пожежна сигналізація і комплекс відеоспостереження СКУД дозволяє створити інтегровану систему комплексної безпеки охоронюваних об'єктів. Судячи з останніх даних про продажі різних технічних засобів безпеки, споживачі виявляють найбільшу цікавість саме до СКУД. Темпи зростання її продажів на сьогоднішній день складають 15%, тоді як інші види охоронних систем мають більш скромні показники - 7%. З урахуванням цього має сенс розглянути деякі загальні та технічні аспекти перспективи розвитку системи контролю та управління доступом.

Перш за все, варто відзначити високий потенціал розвитку СКУД. На сьогоднішній день система контролю доступу є невід'ємною частиною комплексу безпеки, що охороняється і при цьому взаємодіє з іншими системами життєдіяльності будівлі і навіть із загальною системою управління підприємством. У першу чергу це відноситься до загальної системи управління будівлею, системі управління персоналом компанії і системі комерційного обліку.

Такий ступінь взаємодії та інтегрованості СКУД з іншими системами забезпечується наявністю прямого контакту з користувачами. Відбувається постійний обмін даними між СКУД і іншими інформаційними системами і комплексами про дії знаходяться в будівлі. Це істотно спрощує їх роботу і робить її більш ефективною, а так само сприяє зниженню витрат на енергоресурси. Зокрема наявність даних про точний час приходу або відходу співробітників компанії дає можливість контролювати, а при необхідності і регулювати мікроклімат і ступінь освітленості на робочому місці. Витрати на освітлення та підтримання комфортної температури і вологості складають до 60% від усіх витрат на енергоспоживання. Вибір оптимальних алгоритмів дозволяє скоротити ці витрати до 15%.

Ці ж дані, що надійшли до бухгалтерії і департамент кадрів компанії, дозволяють створити автоматичну систему розрахунку заробітної плати та інших нарахувань, а так само мати уявлення про відвідуваність і дисципліні кожного співробітника. Результатом цього є зниження витрат на утримання апарату бухгалтерії та поліпшення керованості підприємством. Але це не всі додаткові можливості, які може надати СКУД. Її застосування дозволяє об'єднати на єдиній карті комерційні та соціальні програми, такі як система внутрішнього розрахунку, медичне страхування, електронні гроші тощо.

Система СКУД може працювати на різних носіях, кожен з яких має свої можливості. На практиці застосовуються картки, проксіміті, CMART і RFID. Використання карток в якості універсального засобу ідентифікації та зберігання даних в значній мірі розширило можливості СКУД і забезпечило зростання її популярності. Пасивні проксіміті мають ряд переваг в порівнянні з магнітними і аналоговими носіями, але при цьому мають досить високу вартість (до 2 доларів) і маленький радіус дії (не більше 15 см). Систему CMART можна було вважати ідеальною, якби не її висока вартість, яка викликана досить складною конструкцією і наявністю вбудованого мікрочіпа. Але в ряді випадків всі ці недоліки компенсуються високим ступенем надійності, захищеності і багатофункціональності. А можливість використання CMART в якості платіжного засобу та зберігання персональних даних повністю виправдовує її високу вартість.

Основні очікування на ринку технічних засобів безпеки пов'язані з появою RFID. Ця технологія належить до класу hands-free і дозволяє значно спростити використання і підвищити ефективність використання СКУД. RFID або Radio Frequency Identification дозволяє здійснювати дистанційну ідентифікацію на заданій радіочастоті. Використання RFID дозволить пересуватися по будівлі, не пред'являючи карток або пропусків. Система здатна виробляти ідентифікацію на відстані 4 метрів. Транспондери, передавальні радіосигнал можуть використовуватися в якості міток для

відстеження переміщення дорогого майна. На даному етапі використання RFID кілька обмежено через досить великих витрат на придбання обладнання, а так само у зв'язку з низьким ступенем захисту від сторонніх випромінювань і екранування. За оцінками фахівців використання більш широкого діапазону випромінювання і зменшення вартості транспондера до більш прийнятною (близько 1 долара) дозволить більш активно впроваджувати цю різновид СКУД.

Використовуються і біометричні системи контролю. Вони відрізняються найбільшою надійністю, але через дуже високу вартість і складності не мають широкого застосування. Дана система використовує для ідентифікації сітківку очей, відбитки пальців, форму руки та інші біометричні дані. Поки біометрична система розпізнавання застосовується на військових і ядерних об'єктах, а так само в банківській справі. Але користувачів не влаштовує низька швидкість розпізнавання і часті помилкові спрацьовування, що ускладнює застосування цієї системи на об'єктах з великою кількістю співробітників. Основні перспективи розвитку експерти пов'язують з впровадженням даної системи ідентифікації для систем безпеки приватного житла. Найбільш перспективними є технології розпізнавання по сітківці ока і за формою руки.

Передбачається, що в найближчі 5 років буде створена більш досконала система ідентифікації, яка буде мати більш високу швидкість і мінімальна кількість помилкових спрацьовувань.

Прогрес розвитку систем СКУД очевидний. Це розвиток впливає і на підвищення ефективності інших систем. Причиною прогресу є активне впровадження сучасних технологій, які дозволяють удосконалювати цей напрям технічних систем безпеки. Сьогодні створено чимало різновидів СКУД. Фахівці з систем безпеки допоможуть вибрати найбільш оптимальну і ефективну конфігурацію.

Рубан М.О.
Державний університет телекомунікацій

Акустичні сейфи

Сьогодні мобільні телефони є незамінними помічниками і постійними супутниками у повсякденному житті. Вони виконують як функцію основних засобів зв'язку, так і особистого органайзера, програвача, а смартфони - і функцію комп'ютера. Ми звикли зберігати в телефоні велику кількість особистих даних, які не повинні бути доступні стороннім особам.

На сьогоднішній день, коли зловмисникам доступна можливість встановлення на мобільні телефони спеціальних програм, які дозволяють використовувати телефон для прослуховування або отримування даніих що зберігаються в пам'яті мобільного, Ваш мобільний може перетворитися для Вас у пристрій, який становить загрозу незаконного отримання інформації та прослуховування.

Одним з таких способів є автоматична відповідь стільникового телефону на дзвінки з заданих номерів (ваш телефон автоматично «відповість на дзвінок», при цьому не повідомить Вас про те, що на нього надійшов виклик). У разі прийняття такого виклику Вашим телефоном, він автоматично перетворюється у прослуховуючий прилад, який здійснює запис і передачу звукової інформації на приймаючий пристрій. Приблизно так само буде виглядати передача інформації з Вашого мобільного на інший приймаючий пристрій. Подібна передача даних буде відбуваєтися абсолютно непомітно для власника телефону.

Для того, щоб забезпечити якісний захист мобільного телефону від прослуховування необхідно використовувати захисні пристрої, принцип роботи яких полягає у детектуванні електромагнітного поля навколо телефону. Коли на телефон надходить вхідний дзвінок, то рівень активності поля суттєво збільшується, і це фіксується приладом захисту, що обов'язково буде супроводжуватися звуковими і світловими сигналами, які власник телефону однозначно не пропустить.

Такі пристрої називаються акустичними сейфами. Особливість їх полягає в тому, що дані пристрої ніяк не заважають вести прослуховування, однак через те, що навколо прослуховується пристрої створюється акустична перешкода, з перехопленої інформації неможливо виділити що-небудь раціональне. Саме цей принцип дуже ефективний проти пасивного прослуховування, яка все більше набирає популярність із зростанням кількості смартфонів. Акустичні сейфи виробляються у різних форм-факторах: чохол, сфера, ладья, портмоне, та інші.

Таким чином, акустичні сейфи являють собою досить компактне та практичне рішення для захисту від прослуховування особистих засобів зв’язку. Темою мого дослідження є: принципи використання акустичних сейфів, їх види, та методи їх впровадження з метою комплексного захисту корпоративного та особистого мобільного зв’язку від витоку інформації шляхом прослуховуван

Г.В.Шевченко, завідувач кафедри вищої математики ДУТ О.В.Барабаш
Державний університет телекомунікацій

МАТЕМАТИЧНА МОДЕЛЬ РОЗПОДІЛУ ОБСЯГУ АСИГНУВАНЬ НА РІЗНІ ЗАСОБИ РЕКЛАМИ В ІНТЕРНЕТ-МЕРЕЖІ.

Розглядається задача розподілу рекламного бюджету при розміщенні реклами в інтернет середовищі із застосуванням інформаційних технологій. Дослідженню наявних сучасних інформаційних технологій, їх застосуванню та впливу на різні стадії створення і просування продукту присвячені дослідження у працях таких вчених, як: А. Богачевський, Н. Винер, Л. Вінарик, Дж. Веллінгтон, А. Макадаме, В. Мартін та ін. Враховуючи обмеженість практичних розробок а також різну ступінь впливу інформаційних технологій на розвиток бізнесу, виникла нагальна потреба в дослідженні застосування різноманітних інформаційних технологій в управлінні і

реалізації механізмів активізації розвитку в умовах переходу до інформаційного суспільства, що визначило актуальність роботи.

Головна мета побудови моделі – визначення об'єму реклами на кожному носії таким чином, щоб максимізувати досяжність до цільової аудиторії без порушення бюджетних обмежень. У відповідності з цим формулюється оптимізаційна задача максимізації цільової функції від змінних прийняття рішення, які відповідають кількості рекламної інформації на різних носіях в інтернет середовищі. Встановлюються критерії щодо цільової аудиторії. Для розв'язання поставленої задачі і визначення коефіцієнтів досяжності використовується метод визначення пріоритетів, що являється експертним методом, який застосовується для вибору кращого об'єкту з сукупності однорідних за групою критеріїв. З попарного порівняння критеріїв за важливістю випливає, що на першому місці за важливістю стоїть критерій посада, на другому – статок, на останньому – вік. Застосовується метод аналізу ієрархій для узгодження результатів, отриманих за допомогою методів оцінки. Перевірка показує, що виконується умова похибки. Таким чином, отримані бальні експертні оцінки, акумульовані в матриці, можна вважати адекватними реальним оцінкам. Отже, модель була сформульована таким чином, щоб реклама досягала саме тієї групи, для якої призначалась дана продукція, а не тієї групи, яка не є потенційним споживачем.

Иванюк Андрей Игоревич
Державного університету телекомунікацій , м. Київ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СИСТЕМЕ

Масштабный сбой в работе организаций, осуществляющих деятельность в банковском секторе, может привести к развитию системного кризиса всей платежной системы и, как следствие, к экономическому коллапсу в масштабе государства. Среди причин, способных вызвать подобный сбой, отдельной группой выделяются угрозы информационной безопасности организаций банковской системы. Данный вид угроз оказывает непосредственное влияние на операционный риск основной деятельности банка, а значит, сказывается на его бизнес-процессах [1]. От обеспечения безопасности информационной вычислительной системы банка сегодня во многом зависит бесперебойное, устойчивое и надежное функционирование бизнес-процессов, в частности репутация финансового учреждения, доля на рынке, снижение издержек.

Сложность защиты информации в банковском секторе определяется не только огромными массивами обрабатываемых данных и изощренностью средств, применяемых злоумышленниками для доступа к ним. Она характеризуется еще и тем, что банки, являясь частью единой финансовой системы государства, должны соответствовать жестким требованиям безопасности, но реализацию этих требований государство полностью возложило на сами кредитные организации .

Таким образом, к нынешним автоматизированным банковским системам предъявляются строгие требования как со стороны банков- пользователей, так и со стороны государственных и контролирующих органов. Но с другой стороны, банковское обслуживание, в частности дистанционное, должно быть простым и удобным для клиента, иначе предлагаемая услуга не станет массовой и не принесет банку ту прибыль, ради которой она вводилась. Однако чем проще доступ к услуге, тем сложнее обеспечить безопасность данных и не допустить незаконных транзакций. К тому же банковская система должна оставаться прозрачной для государственных надзорных и налоговых органов. В целом ИТ-инфраструктура крупного универсального банка включает до нескольких сотен информационных систем, каждая из которых может стать слабым звеном с точки зрения безопасности. Риски в банковской сфере высоки, разнообразны и связаны не только с криминалом, но и с потерей информации и оперированием недостоверными данными в результате технических сбоев или влияния человеческого фактора. Поэтому обеспечение информационной безопасности требует комплексного подхода, который включает правовые, организационные, технические, кадровые и другие аспекты, что связано с многогранностью задач, требующих решения. К созданию системы обеспечения информационной безопасности должны быть причастны не только служба информационной безопасности, ИТ-служба, но и топ-менеджмент, юридическая служба и другие структуры.

Поскольку обеспечение безопасности – это непрерывный процесс, то для него требуется непрерывный цикл мероприятий: планирование, реализация, проверка, действие. Следовательно, система менеджмента информационной безопасности должна стать частью общей системы

менеджмента банка. А эффективными способами минимизации риска информационной безопасности – составление политики информационной безопасности банка (в том числе с учетом результатов анализа и оценки данного риска), а также последующая реализация и совершенствование тсистемы менеджмента информационной безопасности банка в соответствии с этой политикой.

Литература

1. Шубин, А. Актуальные вопросы обеспечения информационной безопасности в банковской сфере / А. Шубин
2. Сучасні інформаційні технології.Інформаційна безпека.: Дубчак О.В., Рудюк Р.Г., Михайленко В.В., 2010.

Вальченко О.І., Гунченко О.М.
Державний університет телекомунікацій

БЕЗПЕКА ВИКОРИСТАННЯ РАДІОАКТИВНИХ МАТЕРІАЛІВ

Ядерні технології приблизили майбутнє і вже стали невід'ємною частиною нашого повсякденного життя. Атомні станції у багатьох із нас викликають страх. Частіше всього він пов'язаний із подіями 1986 року на Чорнобильській АЕС, 2011 року на АЕС Фукусіма-1 та із відсутністю інформації на скільки АЕС безпечні для навколишнього середовища і для кожного із нас. Із кожним днем зростає використання джерел радіації у різних галузях діяльності, які відрізняються від АЕС. Незважаючи на існування в конструкціях та експлуатації заходів безпеки, аварії із залученням радіаційних джерел виникають частіше, ніж аварії на реакторах. На відміну від аварії на реакторі, наслідки любої такої аварії, як правило, впливають тільки на невелике число людей, проте вплив на цю обмежену кількість людей може виявитися серйозним.

Як свідчить аналіз ряду публікацій [1-3], питання безпечного використання АЕС в літературних джерелах проаналізовано та відображено на відносно достатньому рівні. Безпека використання радіоактивних матеріалів, експлуатації радіаційних джерел у галузях діяльності не пов'язаних із атомними електростанціями, інформація про аварійні ситуації із такими матеріалами в літературних джерелах відображена недостатньо.

Розвиток атомної енергетики не має альтернативи як один із інструментів оптимізації паливно-енергетичного балансу та умови економічного розвитку. Оптимізація паливної корзини вимагає розширення частки АЕС у світі як мінімум до 25% [2-3].

У нинішній час неухильно зростає використання джерел радіації для медичного лікування, транспорту із використанням радіоактивних матеріалів, апаратури для опромінення, джерел радіації, що застосовуються в наукових дослідженнях, медицині та промисловості.

Радіаційні аварії можуть виникнути: в медичних закладах; на промислових об'єктах; в дослідницьких інститутах або навчальних закладах; на транспорті, що перевозить радіоактивні речовини; на підприємствах ядерно-паливного циклу; під час повернення супутників із ядерними енергетичними установками; на військових об'єктах, при терористичних актах або незаконній торгівлі радіоактивними речовинами.

Аварії, в результаті яких відбувається тяжке переопромінення людей, фактично рідкісні. Більшість випадків ураження людей від радіації були пов'язані із неправильним поводженням із закритими промисловими джерелами або ненавмисним опроміненням рентгенівськими променями при контролі якості.

Аналіз радіаційних аварії [1-4] свідчить про те, що основними причинами аварій є помилки людей та відмови обладнання. Недостатнє навчання, незнання, відсутність повірки та технічного обслуговування обладнання є основними факторами, які вносять вклад у помилки людей.

У результаті аналізу причин та наслідків радіаційних аварій можна набути наступних уроків:

- радіоактивні джерела, переміщенні з місця, указаного при реєстрації та ліцензуванні, можуть представляти серйозну небезпеку;
- усвідомлення населенням потенційної небезпеки від радіаційних джерел є важливим фактором зменшення вірогідності радіаційних аварій;
- необхідне маркування радіаційної небезпеки, яке знайоме для населення;
- державні компетентні органи повинні вести відповідний облік видів радіоактивних джерел, які знаходяться в державі та вимагати від користувачів вичерпну реєстрацію усіх джерел, що знаходяться у їх використанні.

Таким чином аналіз стану безпеки використання радіоактивних матеріалів дозволяє зробити наступні висновки:

- необхідно інтегрувати радіаційне аварійне реагування у загальну систему реагування на аварійні ситуації;
- у випадку багатьох радіаційних (не реакторних) аварій, пов'язана з радіацією небезпека найчастіше менше пов'язаної із іншими видами небезпеки (пожежа, небезпечні хімічні речовини);
- нерадіаційний аспект радіаційних аварійних ситуацій повинен майже завжди виступати на першому місці – пріоритетними аспектами є збереження життя, лікування пошкоджень, боротьба з пожежами та ін.;
- після того, як буде стабілізовано не пов'язані з радіаційним фактором аспекти ситуації, повинні бути початі негайні кроки для мінімізації радіаційного ризику для населення, аварійних робочих та навколишнього середовища;
- на ядерно та радіаційно-небезпечних об'єктах неможна застосовувати підходи, що характеризуються формулою: дозволено все, що не заборонено, там діє принцип: заборонено все, що не дозволено;
- досягнутий рівень забезпечення радіаційної та ядерної безпеки знижувати неможна;
- вимоги безпеки неможна мінімізувати, їх можна тільки оптимізувати.

ЛІТЕРАТУРА

1. Чернобыльская катастрофа / Под ред. В.Г. Барьяхтара – К.: Наукова думка, 1995. – 560 с.
2. Радиационная и химическая безопасность населения / Монография / В.А. Владимиров, В.И. Измалков, А.В. Измалков; МЧС России. – М.: Деловой экспресс, 2005. – 544 с.
3. INTERNATIONAL ATOMIC ENERGY AGENCY, Method for developing arrangements for response to a nuclear or radiological emergency, EPR-METHOD, IAEA, Vienna (2003). http://www.iaea.org.
4. INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Goiânia, IAEA, Vienna (1988). http://www.iaea.org.

Гунченко О.М. к.т.н, доц., Вальченко О.І., к.т.н., доц.
ДУТ

НЕБЕЗПЕКИ СОЦІАЛЬНОГО ХАРАКТЕРУ – ФАКТОР НЕСТАБІЛЬНОСТІ ДЕРЖАВИ

У непростий час проведення у країні широкомасштабних заходів економічного та політичного характеру особливе занепокоєння викликає загострення численних соціальних проблем, значне місце серед яких займають алкоголізм, наркоманія, бродяжництво тощо. Саме у зв'язку зі збільшенням кількості конфліктних ситуацій, економічною кризою та соціально-політичними негараздами в державі маргіналізація нації на сьогодні набуває тотальних темпів розповсюдження.

Ця тема є актуальною, оскільки боротьба з негативними соціальними проявами є серйозною міжнародною проблемою, яка викликає занепокоєння не тільки широких кіл громадськості, але і державних діячів.

Формування та розвиток засад ринкової економіки створили в Україні принципово нову соціальну та економічну ситуацію. Зараз все більшого значення набуває поділ суспільства за рівнем та джерелом багатства, наявністю чи відсутністю приватної власності. Водночас набувають сили і негативні чинники: формування нової соціальної диференціації та відповідних критеріїв її оцінки, що свідчить про нездорові відносини у суспільстві; надто різкий поділ на бідних та багатих; процеси збіднення та збагачення мають деформований характер.

За таких обставин різко зростають форми та розміри соціальних відхилень (злочинність, самогубство, алкоголізм, наркоманія тощо). Ці та багато інших форм збоченої поведінки в умовах занепаду системи соціального контролю стали загрозливими для суспільства.

Багато людей, стикаючись з проблемами матеріального характеру, не можуть їх подолати, і це не пов'язано зі слабкістю їх характеру, відсутністю сили волі, а з відсутністю необхідних умов, які б сприяли подоланню цих проблем. Це пояснюється незацікавленістю, байдужим відношенням влади до матеріального та психологічного стану населення, зокрема незахищеного та з низьким рівнем достатку. Звідси з'являється негативна девіантна поведінка людей, що являє собою поведінку, яка відхиляється від загальноприйнятих, соціально схвалюваних, найбільш поширених і усталених норм у певних спільнотах в певний період їх розвитку.

Таким чином, до девіантної поведінки можна віднести низку шкідливих звичок людини, що являють собою небезпеки соціального характеру.

Соціальні небезпеки можуть бути класифіковані за певними ознаками:

1. За природою можуть бути виділені наступні групи небезпек:

а) небезпеки, що пов'язані із психічним впливом на людину (шантаж, шахрайство, злодійство, моббінг та ін.);

б) небезпеки, що пов'язані з фізичним насильством (розбої, бандитизм, терор);

в) небезпеки пов'язані із уживанням речовин, що руйнують організм людини (наркоманія, алкоголізм, паління);

г) небезпеки, що пов'язані із хворобами (СНІД, венеричні захворювання, гепатит, туберкульоз та ін.);

д) небезпеки суїцидів.

2. За масштабами подій соціальні небезпеки можна розподілити на: локальні; регіональні; глобальні.

3. За статтю та віком розрізняють соціальні небезпеки, що характерні для дітей, молоді, жінок, чоловіків, людей похилого віку.

4. За організацією соціальні небезпеки можуть бути випадковими та навмисними.

В основу визначення соціальних небезпек, що викликані низьким духовним рівнем, закладено цінності і компоненти суспільства та людини.

Існують два ціннісні компоненти, співвідношення між якими характеризує стан суспільного життя.

Перший ціннісній компонент — цінності культури суспільства. Другий ціннісний компонент — ціннісна орієнтація особистості. Зв'язок між цими двома крайніми компонентами культури — найважливіший цементуючий і стимулюючий початок всього суспільного життя. І навпаки — порушення цього зв'язку визначає глибоку духовну кризу.

На фоні змінених орієнтирів суспільство потерпає від соціальних небезпек, які викликали зміни і втрати загальнолюдських цінностей і орієнтацій значної кількості населення.

Визначені соціальні небезпеки формують в людському середовищі "групи ризику". "Групи ризику" впливають на стан суспільства шляхом підвищення чисельності кримінальних злочинів, втягування в свої лави все нових представників здорової частини суспільства, впливу на стан здоров'я оточуючих їх людей, погіршують генофонд нації. Вищезгадані негативні явища в суспільстві створюють негативне коло, причини якого, в більшості випадків, пов'язані між собою.

Загостреність обставин викликають також незадовільний стан умов праці, проживання і побуту. Вся сукупність обставин збільшує ступінь соціального напруження. Такий розвиток подій завжди, навіть в ретельно організованих суспільних змінах, супроводжується виникненням стихійних угруповань, які здійснюють свої плани наживи за рахунок мародерства і вандалізму серед населення, що в своєму подальшому розвитку закінчується тяжкими наслідками актів тероризму.

Необхідність усвідомлених знань розвитку соціально небезпечних факторів пов'язана з розумінням — куди може привести сукупний їх розвиток і як може потерпіти населення від необачливих дій стихійного характеру [1].

Соціальна напруга поглиблює розвиток і поширення шкідливих звичок людини. Шкідливі звички дезорганізують людину, послаблюють її волю, знижують працездатність, погіршують здоров'я і скорочують тривалість життя. Чим

раніше вони утворюються, тим згубніше діють і тим складніше їх позбутися. Ці звички приносять безліч бід і страждань, завдають великої економічної, соціальної та моральної шкоди суспільству. Як соціальні проблеми вони впливають і на фінансову сферу держави.

Хропко Т.О.
Державний університет телекомунікацій

Деструктивний інформаційно-психологічний вплив як актуальна загроза інформаційній безпеці держави

Сучасний етап розвитку суспільства характеризується переорієнтацією провідних країн світу на нові інформаційні принципи, обумовлює необхідність визначення нетрадиційних підходів до проблем забезпечення національної безпеки держави і насамперед її складової частини — інформаційної безпеки.

Інформація перетворилася зараз на глобальний ресурс, використання якого дає змогу значно збільшити ефективність керування усіма життєвими сферами.

Головна інформаційна загроза для нас – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні.

Поєднання традиційних форм ведення інформаційної боротьби з останніми досягненнями в галузі інформаційних технологій почали істотно впливати на хід та результат розв'язання конфліктних ситуацій, досягнення поставлених цілей шляхом проведення інформаційно-психологічних операцій. Тобто перевагами інформаційно-психологічних операцій є: практична відсутність людських втрат; порівняно невеликі витрати на проведення операції; відсутність ефекту помсти, оскільки переможені не відчувають свого програшу.

Дослідженням інформаційної безпеки та складових інформаційних впливів присвячені роботи О.Литвиненка, А.Маслоу, В.Л.Бурячка та ін.

Загальним джерелом загроз інформаційно-психологічный безпеці особистості є та частина інформаційного середовища суспільства, яка в силу різних причин, не адекватно відображає навколишній світ людини. Тобто інформація, яка вводить людей в оману, у світ ілюзій, не дозволяє адекватно сприймати навколишнє і самого себе.

Інформаційне середовище набуває для людини характер другої, суб'єктивної реальності. Ту її частину, яка містить інформацію, неадекватно відображає навколишній світ, і ті її характеристики і процеси, які ускладнюють або перешкоджають адекватності сприйняття і розуміння людиною навколишнього і самого себе, можна умовно позначити як "ілюзорна реальність". Незважаючи на свою ілюзорність, і навіть в силу своєї ілюзорності, але у формі уявної реальності, вона є основним зовнішнім джерелом загроз інформаційно-психологічній безпеці особистості.

В наш час проблема забезпечення інформаційної безпеки держави поки перебуває на стадії розроблення. Дана обставина обумовлена неадекватністю між формуванням інформаційної цивілізації і заходами із забезпечення інформаційної безпеки.

Отже, маніпулювання людьми, використання різних засобів і технологій інформаційно-психологічного впливу стало досить звичайним явищем у повсякденному житті, економічній конкуренції та політичній боротьбі. Тому розуміння загроз інформаційно-психологічній безпеці особистості, механізмів їх дії і можливостей психологічного захисту стає не тільки теоретичною проблемою але і потребою соціальної практики і повсякденного життя людини.

Спасітєлєва С.О. к.ф.-м.н.
Державний університет телекомунікацій

Створення безпечних додатків платформи .NET з використанням Ms SQL Server 2014

MS SQL Server 2014 забезпечує посиленну безпеку Advanced Security (SQL Server Audit, Transparent Data Encryption), розширення Common Language Runtime Microsoft .NET, що дозволяє додаткам, розробленим мовами платформи .NET, реалізовувати збережені процедури та різні функції. Сучасні системи баз даних містять широкий набір процедур та функцій, які створюються для розв'язку конкретних прикладних задач та для розширення функціональності сервера [1]. Запити до бази даних можуть бути задані за допомогою як традиційного Transact-SQL, так і Visual C#, Visual Basic .NET, C/C++, Java, Linux, PHP. Недостатня компетентність розробників клієнтських додатків може скласти значну загрозу безпеці систем баз даних. Доповідь присвячена розгляду підходів та засобів СУБД MS SQL Server 2014, які дозволяють запобігти атакам на сервер із клієнтського додатку.

Одним із базових принципів створення безпечних додатків є принцип надання мінімальних привілеїв необхідних для розв'язку поставленої задачі, який реалізовано в MS SQL Server за рахунок відключення за замовчуванням значної кількості функцій, таких як застосування Microsoft .NET Framework в ядрі СУБД, SQL Service Broker Network

Connectivity, доступу до аналітичних служб за допомогою протоколів HTTP, SQL Server Agent, Data Transformation Services тощо [2].

Виконання .NET-коду в ядрі СУБД є потенційно небезпечним, тому керованому коду слід присвоювати мінімально необхідний рівень привілеїв. При завантаженні зборки необхідно вказати один із трьох рівнів безпеки: SAFE (доступ до зовнішніх ресурсів не дозволяється), EXTERNAL_ACCESS (дозволяється доступ до файлів, мережевих ресурсів, реєстру, змінних оточення), UNSAFE (дозволяється доступ до всіх ресурсів в тому числі до некерованого коду). Якщо зборка в процесі виконання порушить правила безпеки, вказані при її завантаженні, тоді загальномовне середовище виконання (Common Language Runtime) згенерує виняток і виконання коду буде припинено.

З метою підтримки стабільності роботи СУБД будь-який програмний модуль має виконуватися у контексті користувацької сесії, яка його викликала с привілеями, які необхідні для даного контексту, при цьому програмний модуль не має звертатися до ресурсів за межами сервера. В іншому випадку із програмного модуля можливим є неавторизований доступ до даних. MS SQL Server дозволяє вказувати контекст безпеки, в якому будуть виконуватися оператори програмного модуля, а саме обліковий запис, який використовується при перевірці дозволів на використання об'єктів на які посилається процедура або функція. Це може бути обліковий запис користувача, який викликав процедуру або обліковий запис користувача-розробника процедури або інший обліковий запис.

Однією із можливостей MS SQL Server, яка реалізує принцип мінімальних привілеїв, є дозвіл виконувати користувацькі процедури та функції з правами іншого користувача. Для цього можна використати оператор EXECUTE AS. Цей оператор надає гнучкий механізм управління правами, які надаються виконуваному коду, і не пов'язані з правами самого користувача. Ця функціональність може застосовуватися для безпечного управління правами користувачів. Конструкція EXECUTE AS, яка вказується при створенні відповідного об'єкту бази даних, задає обліковий запис користувача, який MS SQL Server буде застосовувати для перевірки прав доступу до об'єктів використаних в процедурі або функції. Використання конструкції EXECUTE AS дозволяє виключити циклічне призначення та перевірку прав доступу при виконанні операторів SELECT, INSERT, UPDATE, DELETE и EXECUTE, а також відкриває безпосередній доступ до об'єктів бази даних.

До базових принципів, які забезпечують безпеку додатків баз даних і широко застосовуються в СУБД MS SQL Server, можна віднести використання представлень, збережених процедур, параметризованих запитів та засобів перевірки користувацького введення. Відмова від генерації команд, запитів, які динамічно формує користувач і виконує на сервері на користь вищеперерахованим засобам дозволяє значно зменшити небезпеку виконання додатків.

Представлення можна використовувати для забезпечення безпечного доступу до об'єктів бази даних, обмеження доступних користувачу операцій для роботи з даними. Використання представлень дозволяє ізолювати додатки від внесення змін в схеми даних, що спрощує супроводження клієнтських додатків.

Для виконання більшості операцій з даними додатку слід використовувати збережені процедури або параметризовані запити а не динамічно розроблені користувачем запити. З точки зору безпеки динамічно сформовані запити мають значні недоліки. Вони дозволяють виконувати атаки типу SQL Injection (введення даних, які ініціюють виконання неавторизованого запиту) або здійснювати неавторизований доступ до даних. Застосування збережених процедур і параметризованих запитів мають значні переваги. З точки зору безпеки додаток не має використовувати конструкції SELECT, INSERT, UPDATE и DELETE для запитів до бази даних, але може звертатися до збережених процедур, які виконують подібні операції. Використання збережених процедур дозволяє відмовитися від надання користувачам прав доступу до таблиць, дозволяє зробити клієнтські додатки незалежними від схеми бази даних, що дозволяє змінювати схему без зміни самого додатку. Це спрощує супроводження таких додатків. Використання збережених процедур дозволяє виконувати операції над конфіденційними даними на сервері і не надавати їх клієнтському додатку.

Перевірка введених даних є важливим засобом при створенні безпечних клієнтських додатків. Такі фрагменти коду, як перевірка відповідності типів введених даних типам в СУБД, використання регулярних виразів для перевірки користувацького введення, екранування спеціальних символів дозволяють захистити базу даних.

Для створення безпечних клієнтських додатків необхідно використовувати всі вищеописані можливості MS SQL Server, такі як виконання додатків від імені облікових записів з мінімально необхідними привілеями, мінімізація привілей для керованого коду, відключення усіх непотрібних служб та опцій, широке використання збережених процедур, представлень, параметризованих запитів та перевірки введених користувачем даних.

Література

1. Lobel Leonard, Brust Andrew. Programming Microsoft SQL Server 2012 (Developer Reference).– O'Reilly Media Inc, 2012. – 816 pp.
2. Кайли Д. SQL Server 2012: совершенствуем защиту даннях. Эволюция безопасности / Д. Кайли // Windows IT Pro – 2012. – № 6. – С.18-20.

Крицький Г.Г.
Державний університет телекомунікацій

Розподіл обов`язків персоналу в системі управління інформаційною безпекою

Бурхливий розвиток інформаційних технологій призвів до інформаційної революції, внаслідок чого основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки.

Необхідно чітко визначити відповідальність за захист окремих ресурсів, за виконання конкретних процедур, пов'язаних з безпекою. Політика інформаційної безпеки повинна містити загальні правила з розподілу посад й обов'язків, пов'язаних з інформаційною безпекою.

Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту (вищу,середню спеціальну, спеціальні курси підвищення кваліфікації у галузі ТЗІ тощо) та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту.

Для проведення окремих заходів з захисту інформації в АС, які пов'язані з напрямком діяльності інших підрозділів організації, керівник організації своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов'язків, допущені ними порушення встановленого порядку захисту інформації в АС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими (функціональними) інструкціями.

Безпосереднє керівництво роботою СЗІ здійснює її керівник. У випадку, коли СЗІ є структурною одиницею підрозділу ТЗІ (служби безпеки організації) – керівник цього підрозділу (заступник керівника). Призначення і звільнення з посади керівника СЗІ здійснюється керівництвом організації за узгодженням з особами, що відповідають за забезпечення безпеки інформації (керівник підрозділу ТЗІ, керівник служби безпеки та ін.).

На час відсутності керівника СЗІ (у зв'язку з відпусткою, службовим відрядженням, хворобою тощо) його обов'язки тимчасово виконує заступник керівника СЗІ, а у разі відсутності такої посади – керівник одного з підрозділів або інший кваліфікований співробітник СЗІ. Призначення на цю посаду позаштатних або тимчасово працюючих співробітників забороняється.

За посадами співробітники СЗІ поділяються на такі категорії (за рівнем ієрархії):

- керівник СЗІ;
- адміністратори захисту АРМ (безпеки баз даних, безпеки системи тощо);
- спеціалісти служби захисту.

Розподілу обов'язків передбачає такий розподіл ролей і відповідальності, щоб лише одна людина не могла порушити і критично важливий для організації процес або створити пролом у захисті на замовлення зловмисника. Зокрема, його реалізація може попередити зловмисні або некваліфіковані дії персоналу.

Простота означає, що механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або виконанням дій, що вимагають значних додаткових трудовитрат при звичній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (наприклад, запровадження декількох паролів та імен і т. п.). Крім того, простота дає можливість формально або неформально доводити коректність захисту.

Майже завжди вжиті заходи і встановлені засоби захисту, особливо в початковий період їхньої експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівня захищеності засоби захисту повинні мати певну гнучкість. Особливо важливою ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійсню вати на працюючій системі, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом змінюють ся. В таких ситуаціях властивість гнучкості може врятувати власники АС від необхідності вжиття кардинальних заходів для повної заміни засобів захисту на нові. Керованість дозволяє перевіряти узгодженості конфігурацій різних компонентів і здійснювати централізоване адміністрування.

ДОВГАНЬ О.Д., к.ю.н, с.н.с. Національна бібліотека України імені В.І.Вернадського

НАЦІОНАЛЬНИЙ ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ - ІНФОРМАЦІЙНА БЕЗПЕКИ: СПІВВІДНОШЕННЯ

Процес суспільної структуризації ставить нові проблеми, пов'язані з дослідженням теми інформаційного суверенітету. Адже з диференціацією основного поняття потрібний відповідний підхід до аналізу інформаційної структури базових інформаційних ресурсів, відповідної системи соціальних інформаційних баз, на основі яких існують і розвиваються всі соціальні складові суспільства як єдиного цілого.

Таким чином, якщо представити сьогоднішні уявлення про інформаційний суверенітет в більш концентрованому вигляді, не використовуючи у визначенні в якості опорного елемента посилань на суверенітет державний, дане визначення можна представити як межі контролю інформаційних ресурсів, необхідних для існування і розвитку особи і суспільства, держави і нації, обумовлені специфікою їх призначення, характерними для них засобами досягнення суспільнозначимих цілей, самобутністю і підтвердженою суспільною практикою традицією.

Таке формулювання охоплює всі рівні суверенності над інформаційними ресурсами та можливостями їх використання на рівні державному, національному, на рівні соціальних структур сучасного суспільства, надає можливість формування конструктивної ієрархії цих рівнів. Крім інформаційних ресурсів, пов'язаних із організацією безпеки і розвитку суверенів цих ресурсів, дане визначення є перспективним для вдосконалення правової бази, пов'язаної із гарантуванням інтелектуальної власності, прав на використання інформаційних, інформаційно-аналітичних продуктів на внутрішньому і зарубіжних ринках інформації. Воно також відображає сучасний підхід до уявлень про межі і можливості контролю над суверенними інформаційними ресурсами, що визначаються не просторовими обмеженнями, а розвитком відповідної правової системи на базі організаційно-технічних, технологічних засобів контролю інформаційного суверенітету, а також формами інформаційної протидії проявам інформаційного тиску в мережі соціальних комунікацій.

Важливим видається також те, що дане визначення пов'язує сучасний інформаційний суверенітет із відповідною інформаційною традицією, збереженням самобутності суверенів інформаційних ресурсів в умовах розвитку глобального інформаційного простору.

Ефективність функціонування загальноукраїнської, як власне, і всяких інших інформаційних баз прямо залежить як від змістовного їх наповнення, так і від якості самої роботи з інформацією, дотриманням необхідних пропорцій між організацією роботи структур, що займаються виробництвом, збереженням, розповсюдженням інформації, що здійснюють її використання в суспільних інтересах, в реалізації актуальних проектів національного розвитку. І забезпечення цих показників ефективності є важливим завданням сучасної інформаційної безпеки.

При організації вітчизняної інформаційної безпеки важливим є аналіз механізмів використання ресурсів глобального інформаційного простору в інтересах національного розвитку. При цьому предметом вибіркового комплектування вітчизняних інформаційних баз є, в ідеальному варіанті, всі глобальні ресурси, а об'єктом національної безпеки лише ті з них, що введені до національних інформаційних баз, відповідно адаптовані і необхідні для розвитку нації чи держави.

У зв'язку цим набуває актуальності проблема наукового аналізу відповідності наявної інформаційної бази специфіці розвитку внутрісуспільних процесів у сучасній Україні, об'єктивного виявлення характерних особливостей, закономірностей цього розвитку, впливів активізації глобальних процесів на розвиток нашого суспільства, на забезпечення належного інформаційного суверенітету держави і суспільства. Напрацювання із сфери теоретичного обґрунтування інформаційних процесів поступово входять і в сферу методики організації сучасної інформаційної діяльності, і в сферу законотворчості, в практику формування системи інформаційного права, важливість і актуальність якої на етапі входження нашого суспільства в інформаційний етап розвитку важко переоцінити.

Процес суспільної структуризації ставить нові проблеми, пов'язані з дослідженням теми інформаційного суверенітету і його забезпечення розвитком відповідної суспільної діяльності. Даний розвиток має враховувати наявний нині процес диференціації суверенних інформаційних ресурсів у зв'язку з активним розвитком соціальної диференціації суспільства. Дані процеси не повинні призвести до розпорошеності ресурсу, що становить інформаційну основу розвитку нації чи держави.

У зв'язку з цим для вироблення сучасних методик організації інформаційної безпеки відчувається потреба в дещо більшій універсалізації визначення, в якому передбачалися б всі рівні суверенності над інформаційними ресурсами та можливостями їх використання: державний, національний, рівень нових соціальних структур сучасного суспільства, надає можливість формування конструктивної ієрархії цих рівнів. Визначення має бути перспективним для вдосконалення правової бази, пов'язаної із гарантуванням інтелектуальної власності, прав на використання інформаційних, інформаційно-аналітичних продуктів на внутрішньому і зарубіжних ринках інформації. Воно має відображати сучасний підхід до уявлень про межі і можливості контролю над суверенними інформаційними ресурсами, що визначаються не просторовими обмеженнями, а розвитком відповідної правової системи на базі організаційно-технічних, технологічних засобів контролю інформаційного суверенітету, а також формами інформаційної протидії проявам інформаційного тиску в мережі соціальних комунікацій. Визначення має пов'язувати сучасний інформаційний суверенітет із відповідною інформаційною традицією, збереженням самобутності суверенів інформаційних ресурсів в умовах розвитку глобального інформаційного простору.

З урахуванням даної тенденції дослідниками запропоноване визначення інформаційного суверенітету як межі контролю необхідних для існування і розвитку соціальних структур інформаційних ресурсів, обумовлені специфікою призначення цих структур, характерними для них засобами досягнення суспільнозначимих цілей, відповідною самобутністю і підтвердженою суспільною практикою традицією.

Об'єктом інформаційного суверенітету є суверенні інформаційні ресурси – масиви інформації, без яких не можливе існування і розвиток нації чи держави. «Інформаційна основа діяльності в усіх сферах життя суспільства є фундаментом, або стратегічним ресурсом, соціального розвитку й прогресу. За значущістю та специфічністю інформаційний ресурс перевищує всі інші, але, як і всі інші, має свій життєвий цикл: Добування – Нагромадження – Систематизація – Зберігання – Використання – Нарощування».

Процес сучасної реструктуризації інформаційного ресурсу сьогодні у все більшій мірі набуває усвідомленого, прогнозованого характеру, що має ефективно враховуватись в організації інформаційної безпеки. Даний процес проявляється і в відповідних організаційних заходах, і в інвестиційній політиці, і в виробленні певних принципів творення і збагачення інформаційних баз.

Зазначений вище процес вдосконалення функціональних зв'язків, контурів саморегулювання і саморозвитку є важливою складовою реструктуризації сучасних соціальних інформаційних баз в цілому і системи суверенних інформаційних ресурсів зокрема. Даний процес є дуже важливим для окреслення меж сучасного об'єкта національної інформаційної безпеки. Оскільки суверенні інформаційні ресурси в масштабах нації, держави фактично є рознесеними у відповідності із структурою соціальних складових суспільства, відповідних центрів зберігання інформації, в розвитку інформаційних обмінів зростаючого значення набувають соціальні інформаційні комунікації, насамперед ті з них, що вибудовуються на базі електронних технологій і обслуговують обіг електронних ресурсів і являють собою певну мережу. При застосуванні цієї мережі для організації обігу суверенних ресурсів, контроль за її функціонуванням здійснюється відповідними національними засобами.

Таким чином бачимо, що захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки і може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Організація безпеки системи соціальних інформаційних комунікацій зі зростанням ролі інформаційних ресурсів у забезпеченні соціального прогресу людства набуває все більшого значення.

Використана література

1. *Олійник О. В.* Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави/ О.В.Олійник, О.В.Соснін, Л.Є.Шиманський. – http://www.niss.gov.ua/book/Sosnin_2.htm. – С. 2.

2. KeeIy B. Humanitarian Intervention and Sovereignty // Konrad Adenauer StiftungArbeitspapier. – 1995. – P. 22-23; Thomas C. New States, Sovereignty and Intervention. – N. Y.: Gower, 1985. – P. 9 - Ю.

3. Hoffmann S. The Politics and Ethics of Military Intervention // Survival. – 1996. – Vol. 37. – № 4. – P. 37.

4. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій/ НАН України, Нац. б-ка України ім..В.І.Вернадського. – К.:НБУВ, 2011 .- С.14.

5. *Марутян Р.* Національні інформаційні ресурси як першооснова інформаційного суверенітету України/ Р. Марутян // Актуальні проблеми міжнародної безпеки: український вимір. – К.: ВД «Стилос», 2010. – С. 496.

6. *Степко О. М.* Аналіз головних складових інформаційної безпеки держави/ О. М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. – Сер.: Економіка, право, політологія, туризм. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – Вип. 1 (3). – С. 83 .

к.ф.-м.н., Мусієнко А.П., д.т.н., професор Барабаш О.В.
Державний університет телекомунікацій, Київ

Самодіагностування телекомунікаційних мереж на основі гнучких структур перевірочних зв'язків

Вступ. Самодіагностування − це процес визначення відмов ситуації в системі шляхом узагальнення результатів взаємних перевірок функціональних блоків об'єкта. Даний вид діагностування відноситься до тестового діагностування та дозволяє діагностувати технічний стан об'єктів, в яких можливо розбивка на функціональні блоки, які мають можливістю виконання тестових перевірок інших функціональних блоків. До класу таких об'єктів і відноситься обчислювальні системи, що поєднують кілька обчислювальних машин, що працюють під управлінням загальної операційної системи, з'єднаних загальною шиною і які вирішують безліч взаємопов'язаних завдань. Вперше ідея самодіагностування була запропонована в роботі Препарата Ф. Надалі метод самодіагностування отримав розвиток у роботах Пархоменка П.П., Согомоняна Е.С., Коваленка А.Е., Гуляєва В.А., Машкова В.А., Барабаша О.В. та інших. У цих роботах дослідження проводилися в напрямку розвитку діагностичних моделей і вдосконалення методів діагностування з централізованим і розподіленим діагностичним ядром, при якому повинен реалізовуватися заданий набір тестових перевірок. Залежно від послідовності виконання перевірок загальний метод можна розбити на два види: послідовне і паралельне самодіагностування. Найбільшого поширення набуло паралельне

самодіагностування з розподіленим діагностичним ядром. Однак при реалізації паралельного самодіагностування викликає ряд проблемних питань: яким чином здійснити накопичення діагностичної інформації в діагностичному ядрі; яким чином вибрати обчислювальний модуль системи, якому можна довірити виконання аналізу діагностичної інформації; яким чином виконати самодіагностування із заданою вірогідністю.

Актуальність розробки методики самодіагностування з блукаючим діагностичним ядром обумовлена необхідністю підвищення достовірності діагностування та необхідністю виконання фонового діагностування в процесі виконання обчислювальною системою основних завдань.

Нашою метою є розробка методики самодіагностування телекомунікаційної мережі на основі гнучких, випадкових структур перевірочних зв'язків.

Пропонована стратегія оперативного самодіагностування може знайти застосування не тільки в телекомунікаційних мережах, а й у будь-яких обчислювальних системах, що складаються з великого числа модулів. Виконання оперативного самодіагностування в цих системах дозволить забезпечити максимальну стійкість телекомунікаційних мереж та їх систем діагностування, яка буде здатна виявляти несправності при відмовах в самих засобах контролю за рахунок використання «блукаючого» ядра.

д.т.н., професор, Барабаш О.В., к.ф.-м.н.Мусієнко А.П.
Державний університет телекомунікацій, Київ

Функціональна стійкість процесів управління на основі інтелектуалізації телекомунікаційної мережі

В доповіді обґрунтуванні основні положень концепції забезпечення функціональної стійкості процесів управління на основі інтелектуалізації телекомунікаційної мережі.

Основною особливістю функціонально-стійких систем являється їх здатність деградувати на структурному рівні до повної відмови системи, тобто виключати зі структури несправні елементи, перебудовувати структуру, настроювати параметри системи для пристосування (адаптації) до нових умов експлуатації. Основним засобом забезпечення функціональної стійкості є введення надмірності при їх проектуванні.

Разом з тим, такий підхід, не може бути використаний в розподілених інтелектуалізованих системах управління, ключовим елементом яких є розподілена база знань. На відміну від технічних систем, база знань не може деградувати, виключаючи з роботи окремі свої модулі, оскільки утворилися в такому випадку розриви не забезпечать нормальне її функціонування, а висновок, зроблений на такій базі знань, не буде володіти необхідною достовірністю.

У такому випадку необхідний дещо інший підхід до визначення поняття і формування етапів забезпечення функціональної стійкості інтелектуальної системи автоматичного управління.

Під функціональною стійкістю розподіленої інтелектуалізованої системи управління в даній доповіді розуміється її властивість зберігати протягом заданого часу виконання своїх основних функцій в умовах протидії зовнішніх дестабілізуючих факторів.

Основна відмінність стійкості функціонування від функціональної стійкості полягає в наступному: стійкість функціонування характеризує поведінку координат незбуреного і збуреного руху системи, а функціональна стійкість характеризує відхилення основних функцій від координат при збуреному і незбуреному русі

$$\forall\theta>0\Rightarrow\delta>0,\ \rho(z_0,z_0')<\delta\Rightarrow\rho[f(z_0),f(z_0')]<\theta,\ \ \forall t\in[0,\infty),$$

де $f(z)$ − функція від координати руху системи, яка характеризує основні вимоги, що пред'являються до системи.

Отже, на основі проведених досліджень отримала подальший розвиток існуюча теорія функціональної стійкості складних технічних систем в контексті деталізації цієї властивості для інтелектуальної системи автоматичного управління. Напрямком подальших досліджень в цій області може бути широке коло питань, присвячених моделям визначення показників функціональної стійкості перспективних систем автоматичного управління.

канд. істор.наук, доцент КИРИЛЕНКО О. Г.
Національна бібліотека України імені В. І. Вернадського

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ПРОДУКЦІЇ НАУКОВИХ БІБЛІОТЕК

Підвищення ролі інтелектуальної діяльності в інформаційному суспільстві актуалізує проблеми захисту об’єктів інтелектуальної власності в бібліотечно-інформаційних установах. Практика показує, що бібліотекознавча наука впритул підійшла до дослідження проблем інтелектуальної власності на інформаційні продукти і послуги, що динамічно розвиваються в процесі бібліотечно-бібліографічної та інформаційно-аналітичної діяльності наукових бібліотек.

В умовах інформаційного суспільства наукова бібліотека є глобальним центром суспільних комунікацій який продукує та поширює інформаційну продукцію і знання. Сучасні інтегровані електронні ресурси наукової бібліотеки створені внаслідок наукового опрацювання значних за обсягом документно-інформаційних потоків слід розуміти як результат і продукт інтелектуальної діяльності, що потребує побудови відповідної системи захисту. Для наукової бібліотеки електронні інформаційні продукти і віртуальні сервіси є ключовими об’єктами інтелектуальної діяльності, що обумовлюють сучасний рівень задоволення інформаційних потреб користувачів.

Виходячи з визначених організаційних засад формування інтелектуального бібліотечно-інформаційного потенціалу одним з важливіших завдань великої наукової бібліотеки на шляху до захисту власної інтелектуальної продукції на державному рівні є трансформація різних напрямів її діяльності відповідно до міжнародних вимог охорони інтелектуальної власності.

У заходах з модернізації діяльності Національної бібліотеки України імені В. І. Вернадського (далі - НБУВ) на 2014-2015 рр. в напрямку інтеграції з бібліотеками та інформаційними установами передбачено реальні кроки діяльності бібліотеки у формуванні єдиного національного інформаційного простору та захисту об'єктів інтелектуальної власності. Зокрема, НБУВ планує активізувати роботи зі створення загальнонаціональної електронної бібліотеки «Україніка», розробити проект Єдиного реєстру цифрових інформаційних ресурсів бібліотек України, запровадити уніфіковану систему реєстрації та захисту інтелектуальної власності на об'єкти представлені бібліотекою в мережі Інтернет.

Реальним кроком на шляху до уніфікації роботи з електронними інформаційними ресурсами стало створення в НБУВ "Комісії з приймання завершених розробок бібліотечно-інформаційних сервісів та баз даних", одним з важливих напрямів діяльності якої є впровадження уніфікованих форм документації введення в експлуатацію бібліотечно-інформаційних продуктів. Діяльність цієї комісії повинна сприяти уніфікації і координації робіт з експертизи завершених розробок бібліотечно-інформаційних сервісів та баз даних, поліпшення взаємодії між підрозділами розробниками, співвиробниками та користувачами інформаційної продукції бібліотеки.

З метою запровадження єдиної системи прийняття результатів здійснених розробок, паспортизації створених у НБУВ об'єктів інтелектуальної власності, обліку об'єктів інтелектуального права, захисту інтелектуальних та майнових прав НБУВ та її працівників у цьому році створено відділ з охорони інтелектуальної власності. Серед основних напрямів діяльності відділу визначено:

взаємодія з органами виконавчої влади, українськими та іноземними інноваційними структурами, підприємствами, установами, організаціями усіх форм власності, діяльність яких пов'язана з охороною інтелектуальної власності;

дослідження проблем охорони інтелектуальної власності та авторського права в бібліотечно-інформаційній сфері;

забезпечення систематичної роботи з правової охорони інтелектуальної власності НБУВ та технічної безпеки інформаційних ресурсів;

розробка нормативних документів НБУВ, розгортання роботи з прийняття здійснених розробок;

реєстрація торгових марок, майнових прав та прав інтелектуальної власності НБУВ у встановленому в Україні порядку;

розробка та впровадження нормативних документів НБУВ, що відповідно до чинних нормативних актів регулюють порядок передачі авторами та правовласниками невиключних прав НБУВ на поширення в мережі Інтернет творів друку.

В перспективі дослідження проблем захисту інтелектуальної власності в інформаційно-комунікаційній діяльності бібліотек повинно сформувати єдині підходи до організації та використання інтелектуального потенціалу бібліотечно-інформаційної сфери в національному інформаційному просторі.

ПОЛІЩУК Р. В.
Національна бібліотека України імені В. І. Вернадського

БЕЗПЕКА РЕСУРСІВ ВІДКРИТОГО ДОСТУПУ В БІБЛІОТЕЧНО-ІНФОРМАЦІЙНИХ УСТАНОВАХ: ПРАВОВІ АСПЕКТИ

Основою сучасного інформаційного права є положення про невід'ємне право людини на вільний доступ до інформації. Одночасно важливим є створення правового захисту інтелектуальної власності в системі використання інформаційних ресурсів (збереження авторських прав).

Основні риси інформаційного суспільства і завдання, що стоять перед бібліотеками, охарактеризувала Маргарет Хейнс (виконавчий директор Британської комісії з бібліотек і інформації). Вона наголосила, що бібліотеки та інформаційні центри діють у швидкомінливому зовнішньому оточенні, де вільний доступ до інформації становить основу демократичного суспільства, а інформація має бути доступною, організованою і керованою та водночас — міжнародним товаром. Вирішення цих питань потребує перегляду та вдосконалення законодавчих норм як на міжнародному рівні, так і на загальнодержавному.

Актуальним завданням є не тільки удосконалення законодавства в галузі авторського права та використання інформації, а найголовніше – це його виконання, правильне застосування ряду положень, спрямованих на захист авторських прав та вільний доступ громадян до бібліотечних фондів та електронних ресурсів.

Міжнародне бібліотечне співтовариство намагається захистити право користувачів на вільний доступ до електронних документів та їхнє копіювання, але більшість держав приймають рішення про обмеження копіювання електронних документів у бібліотеках.

Авторське право в Україні — це частина цивільного законодавства, і воно регулює відносини із використання творів науки, літератури і мистецтва. Для правомірного використання об'єктів авторського права і суміжних прав у мережі Інтернет, необхідно отримати дозвіл від суб'єктів авторського права і суміжних прав.

Законодавство у сфері авторського права передбачає, що використання твору є правомірним лише після попереднього письмового дозволу авторів чи інших осіб, що мають авторське прав на твори (статті 15, 33 Закону).

Важливі питання у сфері охорони авторського права виникають при розповсюдженні електронних документів та використанні ресурсів відкритого доступу.

Режими доступу утворюють системи з різними параметрами: від вільного використання в Інтернеті щоденно до повного доступу адміністратора в цілях підтримки працездатності електронного документа. Розглядаються варіанти використовувати мережеві електронні документи в режимах вільного доступу в Інтернеті, обмеженого доступу в Інтернеті, доступу в локальній мережі Бібліотеки.

Нині Україна має систему інформаційного законодавства, яка частково забезпечує функціонування правового поля – це і галузі та розділи законодавства України, присвячені питанням інформаційного права; це інформаційно-правові норми Конституції України, які закріплюють інформаційні права і свободи; а також деякі інформаційно-правові норми, що стосуються інших галузей законодавства.

Функціональна спрямованість бібліотеки вже давно вийшла далеко за межі зберігання та надання доступу до інформації.

Варто відзначити, що запровадження в обіг документів шляхом розміщення в електронному середовищі та надання їм відкритого доступу сприяє покращенню обміну інформацією серед вчених, а також активізації діяльності бібліотеки.

Існуюча законодавча база та правові документи забезпечують неефективний захист інтересів власників інформаційних продуктів. Нечітке визначених положень негативно впливають на правові та інші відносини осіб, які задовільняють, власників і користувачів бібліотек. Складність полягає в розробленні «балансу» інтересів, який дозволив би надати належну охорону авторського права – виробникові інформаційних продуктів та послуг, розширення прав посередників та представити інтереси користувача послуг.

к.ф.н., доцент Омецінська О.Б. - Державний університет телекомунікацій;
аспірант Сергієнко І.-В. О. - Державний університет телекомунікацій

ВРАХУВАННЯ ФОРМИ МОДУЛЬОВАНОГО ІМПУЛЬСУ ПРИ РОЗРАХУНКУ ПРОПУСКНОЇ СПРОМОЖНОСТІ ВОЛОКОННО-ОПТИЧНОГО ЛІНІЙНОГО ТРАКТУ

За постійного зростання швидкості передавання інформаційних сигналів по волоконно-оптичних лініях зв'язку (ВОЛЗ) постає проблема створення оптичного лінійного тракту (ОЛТ) з підвищеною пропускною спроможністю. Хроматична дисперсія імпульсу в одномодовому оптичному волокні (ООВ) є одним із основних чинників, що обмежує пропускну спроможність ОЛТ.

Для кількісної оцінки впливу динамічного розширення спектра передавача на обмежену за хроматичною дисперсією довжину лінійного тракту ВОЛЗ будемо вважати, що модульований послідовністю бітів сигнал від передавача на вході в ООВ аналітично описується супергаусівськими імпульсами з початковою модуляцією, а саме:

$$u(z=0,T)=\exp\left[-\frac{1-i\alpha}{2}\left(\frac{T}{T_0}\right)^{2m}\right], \qquad (1)$$

де z – відстань, яку проходить імпульс вздовж ООВ; T – час в системі відліку, яка рухається разом з імпульсом зі швидкістю $v_{гр}$, що відповідає груповій швидкості поширення хвильового пакету на центральній частоті ω_0 імпульсу,

$$T=t-\frac{z}{v_{гр}}; \qquad (2)$$

T_0 – напівширина імпульсу на рівні $1/e^{1/2}$ його амплітуди $|u(0, T|$; α – параметр частотної модуляції імпульсу в передавачі, рад; m – параметр крутизни фронту.

Якщо m = 1, то (1) відповідає Гаусовому імпульсу з частотною модуляцією. Для апроксимації імпульсів від напівпровідникових лазерів більшою мірою підходить супергаусівський імпульс із значенням параметра $m > 1$. За великих значень m форма такого імпульсу наближається до прямокутної з різким переднім та заднім фронтами. Якщо визначити тривалість T_p наростання інтенсивності від 10% до 90% її пікового значення, то у відповідності до (1) одержимо: $T_p \approx T_0/m$, тобто параметр m можна визначити, замірюючи T_p і T_0.

Авторами [1] знайдено аналітичний вираз для коефіцієнта k розширення початкового імпульсу з частотною модуляцією, що описується формулою (1), за його розповсюдження по ООВ. Цей вираз можна записати у вигляді

$$k = \frac{\sigma}{\sigma_0} = \tag{3}$$

$$= \left[1 + \frac{\Gamma\left(\frac{1}{2m}\right)}{\Gamma\left(\frac{3}{2m}\right)} \alpha sign(D) Z + \frac{m^2 \Gamma\left(2 - \frac{1}{2m}\right)}{\Gamma\left(\frac{3}{2m}\right)} 1 + \alpha^2 \ Z^2 \right]^{1/2},$$

де Γ – гамма-функція; sign$D$ – знак питомої хроматичної дисперсії ООВ; $Z = z/L_D$ –безрозмірна величина шляху імпульсу вздовж ООВ; L_D - дисперсійна довжина,

$$L_D = \frac{2\pi c T_0^2}{\lambda_0^2 |D|}; \tag{4}$$

σ – середньоквадратична тривалість імпульсу після проходження ним ділянки ООВ довжиною z, σ_0 – середньоквадратична тривалість початкового супергаусівського імпульсу при $z = 0$, що має значення

$$\sigma_0 = T_0 \left[\frac{\Gamma\left(\frac{3}{2m}\right)}{\Gamma\left(\frac{1}{2m}\right)} \right]^{\frac{1}{2}}. \tag{5}$$

Згідно з виразом (3) за умови $\alpha \times signD > 0$, як і за відсутності чірпу імпульсу від передавача ($\alpha = 0$), імпульс безперервно розширюється в процесі його слідування по ООВ. Навпаки, у разі протилежних знаків α-параметра чірпу імпульсу від передавача та коефіцієнта D хроматичної дисперсії волокна, імпульс спочатку звужується до деякої мінімальної величини його середньоквадратичної тривалості, а за подальшого слідування по волокну – розширюється. В цьому випадку взаємодія чірпованого імпульсу від передавача з хроматичною дисперсією імпульсу у волокні може бути використана для досягнення максимальної довжини обмеженої за хроматичною дисперсією довжини регенераційної ділянки ВОЛЗ.

Література

1. Anderson D., Lisak M. Propagation characteristics of frequency-chirped super-Gaussian optical pulses. Opt.lett., 11, 569 (1986)

Зоценко В.С., зав. каф. Вищої математики , Барабаш О.В.
Державний університет телекомунікацій, Київ

Застосування неорієнтованих графів для оцінки зв'язності телекомунікаційних мереж

Для опису структури та оцінки параметрів функціонування телекомунікаційної мережі доцільно використовувати математичну модель на основі неорієнтованого графа.

Граф позначається як $G = V, L$, $V = v_i$, $L = l_{ij}$, $i, j = 1,2, \ldots, n$, де

V – це множина вершин графа, якій відповідає множина вузлів комутації. Потужність множини дорівнює n.

L – це множина ребер графа, якій ставиться у відповідність множина ліній передачі інформації між вузлами комутації.

Оскільки канали передачі інформації в телекомунікаційній мережі двосторонні, то в графі $G(V,L)$ відсутні орієнтовані ребра.

Також будемо вважати, що в графі відсутні петлі та кратні ребра.

Граф може бути заданим трьома способами:

- матрицею зв'язності розміру $n \times n$
- списками зв'язності розміру $1 \times m$; $m = L$;
- матрицею інцидентності розміру $n \times m$.

При дослідженні графових моделей будемо використовувати такі інваріанти (параметри) графів:

1) потужність множини вершин $n = m_v = V$;
2) потужність множини ребер $m_L = L$;
3) локальні степені вершин (валентність) - число інцидентних ребер по відношенню до вершини v_i: $a_i = deg\ v_i$
4) характеристичні числа матриці суміжності графа (слід графа) λ_i, i=1,2,…,n, які є рішенням матричного рівняння: $A - \lambda E = 0$,

де A – матриця суміжності графа,

$\lambda^T = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ – вектор характеристичних чисел;

$E = e_{ij}$ – одинична матриця:

5) число вершинної зв'язності (вузлової зв'язності) $\chi(G)$;
6) число реберної зв'язності $\lambda(G)$.

На основі отриманих відомостей, ми маємо уявлення про надійність функціонування мережі та можемо оптимізовувати її параметри відповідно до заданих потреб.

В доповіді пропонується використовувати всі зазначені параметри неорієнтованих графів для обчислення зв’язності телекомунікаційної мережі

Онищенко В.В.
Державний університет телекомунікацій,

БЕЗПЕКА ІНФОРМАЦІЇ В ТРАНКІНГОВИХ СИСТЕМАХ РАДІОЗВ’ЯЗКУ СТАНДАРТА TETRA

Сучасний етап розвитку мереж професійного мобільного радіозв'язку (ПМР) характеризується впровадженням цифрових технологій на базі відкритих міжнародних стандартів і розширенням сфери застосування ПМР для завдань управління об'єктами, передачі відеозображень та іншої широкосмугової інформації. Використання ПМР в цих системах вимагає підвищеної уваги до проблем інформаційної безпеки, особливо у зв'язку із збільшеним рівнем загроз, в тому числі терористичного характеру.

У доповіді розглядаються питання інформаційної безпеки найбільш популярного стандарту транкінгового зв'язку TETRA.

TETRA – провідний відкритий цифровий стандарт ПМР, підтримуваний багатьма виробниками обладнання інфраструктури мереж та/або абонентських терміналів TETRA. Стандарт створювався як єдиний загальноєвропейський цифровий стандарт. Тому до квітня 1997 абревіатура TETRA означала трансєвропейське транкінгове радіо (Trans-European Trunked Radio). Однак, інтерес, проявлений до стандарту в інших регіонах, призвів до того, що зараз TETRA розшифровується як Наземне транкінгове радіо (Terrestrial Trunked Radio).

Стандарт TETRA забезпечує два рівня безпеки переданої інформації: стандартний рівень, який використовує шифрування в радіоканалі, і високий рівень, що забезпечується за допомогою наскрізного шифрування із застосуванням оригінальних криптографічних алгоритмів.

Основними механізмами забезпечення безпеки інформації в стандарті TETRA є: аутентифікація абонентів; шифрування інформації; забезпечення секретності абонентів.

Аутентифікація абонентів здійснюється на основі головного ключа (K-key) і унікального номера TEI. Номери TEI (TETRA Equipment Identities) є унікальними для кожного абонентського терміналу TETRA – не існує двох радіостанцій з одним і тим же ідентифікатором. Номер TEI складається з 15 цифр і включає в себе складальний код FAC (Final Assembly Code), код підтвердження TAC (Type Approval Code), а також електронний серійний номер ESN (Electronic Serial Number) і резервний номер SPR (Spare). Двозначний складальний код вказує на виробника і місце збірки. Абонентський термінал з неправильним ідентифікатором не допускається до ресурсів системи TETRA.

Шифрування інформації є опціональною особливістю кожної конкретної системи стандарту TETRA.

Секретність же параметрів абонента забезпечується за допомогою кодового захисту конфігурації абонентського терміналу та присвоєння ідентифікаторів-псевдонімів.

Левицький В.О.
Державний університет телекомунікацій

Необхідність інформаційних технологій в бізнесі.

Одним з результатів науково-технічного прогресу є створення інформаційних технологій, впровадження та використання яких впливає на економічний розвиток бізнеса.

Під інформаційними технологіями розуміють: по-перше, комплекс взаємопов'язаних наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і зберіганням інформації; по-друге, обчислювальну техніку, методи організації і взаємодії з людьми та виробничим устаткуванням, практичні додатки, а також пов'язані з усім цим соціальні, економічні і культурні проблеми.

Зупинимося детальніше на спеціалізованих програмних продуктах, оскільки саме їм приділяється більше уваги з боку бізнес-спільноти. На сьогоднішній день існує значна кількість програмних продуктів вітчизняних і зарубіжних розробників, спрямованих на оптимізацію діяльності компаній незалежно від специфіки виробленої ними продукції чи послуг. Адаптація програмних продуктів під специфіку компаній була досягнута за допомогою модульності даних інформаційних систем.

Під модульністю слід розуміти здатність системи надавати користувачам можливість налаштовувати і вибирати функції виходячи із специфіки та складності діяльності підприємства. Таким чином, компанії-розробники створили гнучкі системи автоматизації, що дозволяють формувати єдину систему, що складається з окремих модулів, інтегрованих між собою. На рис.1 описалні інформаційні технології які грають основну ролі у роботі підприємства

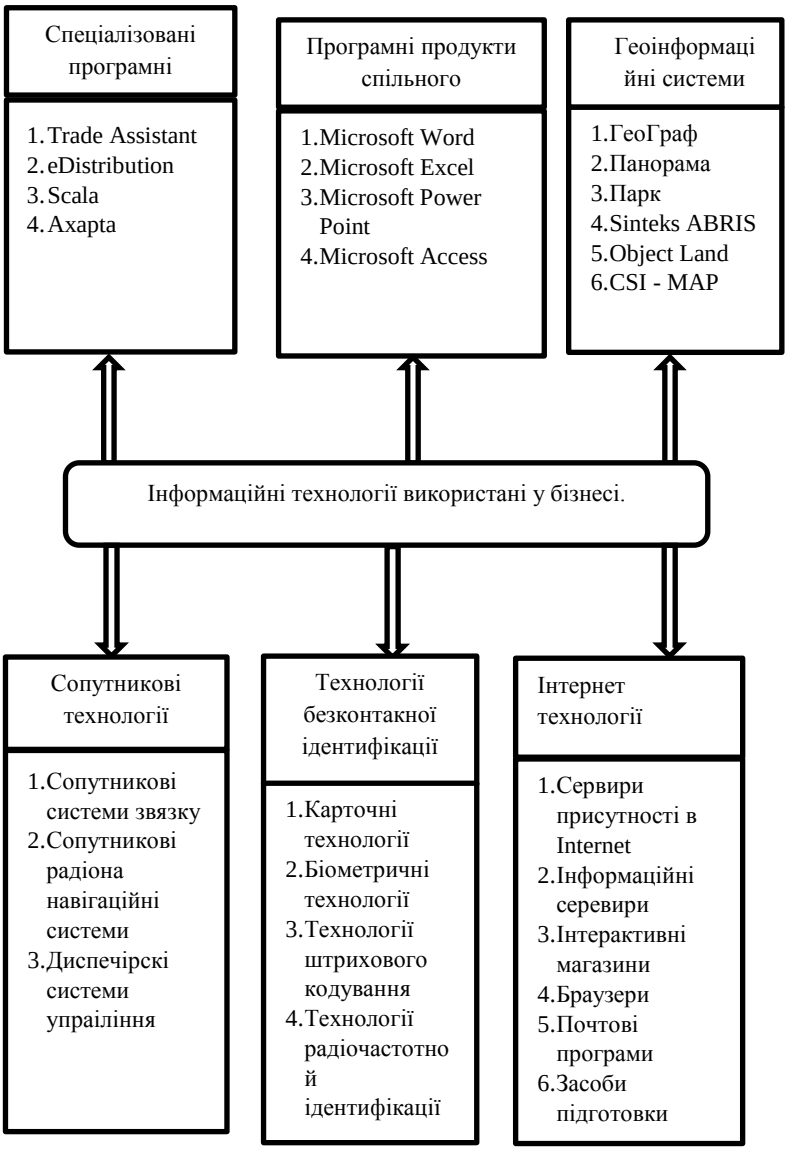


Рис. 1 - Інформаційні технології, які використовуються в сфері бізнесу.

Левицький В.О.
Державний університет телекомунікацій

Користь аудиту інформаційної безпеки

Інформація є одним із найважливіших та найцінніших ресурсів підприємства. Вона може бути як засобом досягнення безпеки, так і вразливим місцем підприємства. З розвитком інформаційних технологій стрімко зростає ризик втрати або змінення інформації. Саме в той момент коли настає загроза інформаційна система потребує захисту. Пошук шляхів вирішення проблем безпеки повинен здійснюватися не тільки за рахунок сил самого підприємства, але й при залученні зовнішніх консультантів, а саме аудиторів**.** Деякі задачі вирішує незалежне аудиторське дослідження. Аудит в інформаційній системі дає змогу вдосконалити систему захисту інформації підприємства, впровадити технології, підвищити ефективність існуючих механізмів безпеки його інформаційних систем і, як наслідок, покращити надійність функціонування підприємства. У цьому реченні двічі є слово підприємства – залиш одне. Важлива роль у цьому напрямі належить аудиту ІБ підприємства, який стає все більш затребуваним на ринку.

Аудит інформаційних Систем (аудит ІС) – це системний процес, відповідно до стандартів та процедур аудиту, отримання і оцінки об’єктивних даних щодо поточного стану інформаційної системи, щоб з'ясувати їх відповідність визначеним критеріям, надання рекомендацій аудиту замовнику.

До функцій аудиту ІС відносять:

• аналіз бізнес-процесів, технологій та структури ІС;
• відповідність політики управління ризиками;
• систему моніторингу ризиків та контролю ризиків;
• об’єктивне оцінювання ризиків, перевірка результатів, здійснених бізнес-підрозділами;

• ідентифікацію потенційних проблем і ризиків;
• об’єктивний аудит проблемних ситуацій та уразливих місць, та повноту заходів їх вирішення;
• аналіз звітів моніторингу та контролю з поліпшенням існуючої роботи управління ризиками;
• аналіз та надання керівництву організації повного профілю ризиків, висновків та рекомендацій щодо стратегії управління ризиками.

Необхідність набуття теоретичних і практичних розробок у вирішенні проблем посилення безпеки підприємства у інформаційних системах дало змогу сформувати наступні висновки. В умовах стрімкого розвитку інформаційних технологій виникла необхідність захищеності та збереження інформаційних ресурсів підприємства для протистояння зовнішнім і внутрішнім загрозам його безпеки. З метою посилення безпеки підприємства у сфері інформаційних технологій та її дотримання на належному рівні пропонується проведення аудиторського дослідження.

Значення аудиту для посилення безпеки підприємства із застосуванням інформаційних технологій залишається достатньо обґрунтованим, оскільки він здатний стати реальним засобом ліквідації загроз його діяльності у сфері інформаційної безпеки.

Перлік посилань:
1.http://www.itsway.kiev.ua/index.php?language=ua&main_managemen=services&managemen=audit
2. Подольский В.И. Компьютерный аудит: [Практ. пособие] / В.И. Подольский, Н.С. Щербакова, В.Л. Комиссарова; под. ред. проф. В.И. Подольского. – М.: ЮНИТИ-ДАНА, 2004. – 128 с.

д.т.н., с.н.с. Дружинін В.А.,Батрак Є.О.
Державний університет телекомунікацій, м. Київ

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ БАГАТОПОЗИЦІЙНИХ СИСТЕМ РАДІОЛОКАЦІЇ ІЗ ЗМІННОЮ ПРОСТОРОВОЮ КОНФІГУРАЦІЄЮ

Сучасні концепції розвитку радіотехнічних систем із змінною просторовою конфігурацією орієнтовані на створення багатофункціональних засобів спостереження, використання яких дозволило б отримувати якісну інформацію про об’єкти моніторингу з урахуванням зростаючих вимог до оперативності й точності визначення їх параметрів в реальному масштабі часу в умовах складної сигнально-завадової обстановки. На даний час в провідних країнах світу одним із пріоритетних напрямків є розвиток літакових радіотехнічних систем огляду (РТСО) із синтезованою апертурою (СА). При цьому, недостатньо відображені в публікаціях структури побудови відповідних систем спостереження, реалізація яких дозволила б вирішити проблему забезпечення необхідної роздільної здатності системи за кутовими координатами в передній зоні огляду для подальшого виявлення, супроводження та класифікації об'єктів спостереження. Недостатньо дослідженими є задачі: забезпечення внутрішньо системної електромагнітної сумісності визначених систем та необхідного рівня їх завадостійкості при функціонуванні в умовах інформаційної невизначеності, синхронізації роботи радіолокаційних елементів даних систем спостереження та просторово-часової обробки радіолокаційної інформації від об’єктів спостереження. Проблема створення радіолокаторів із синтезованою апертурою (РСА) для передньої зони огляду на базі бортових радіотехнічних засобів (БРТЗ) розглядається в роботах Кондратенкова Г.С., Фролова О.Ю., Орлова М.С. і пропонуються її вирішення або у вигляді допплерівського звуження променя (ДЗП) з визначенням неоднозначності за допплерівською частотою, що вимагає помітного збільшення часу синтезування, або шляхом використання спеціальних діаграм спрямованості, що представляє певні труднощі в реалізації. Одним із перспективних напрямків вирішення даної проблеми є створення методологічного апарата, використання якого дозволило б реалізувати режим багатопозиційного прийому радіолокаційної інформації на інтервалах часу СА відповідної системи у передньо-боковій зоні огляду за рахунок прийому радіолокаційної інформації бортовими РТСО, носії яких знаходилися в одній площині. Визначена проблема може розглядатися для радіолокаційних систем авіаційно-наземного базування зі змінною відносною просторовою конфігурацією (РЛС АНБ ЗВПК), носіями бортових радіолокаційних засобів (БРЛЗ) в яких розглядаються дистанційно пілотовані літальні апарати (ДПЛА), що мають ряд важливих переваг у порівнянні з пілотованими літаками.

к.т.н. Цитрицька Л.М.
Державний університет телекомунікацій, Київ

Знаходження мінімального остовного дерева за допомогою матриці інцидентності

В доповіді пропонується метод знаходження мінімального остовного дерева, який базується на представленні дерева матрицею інцидентності.

В основі розробки телекомунікаційних мереж виникає задача про з'єднання n вузлів в єдину телефонну мережу з мінімальною сумарною вартістю з'єднань. Ця задача може бути вирішена за допомогою матричного методу

знаходження мінімального остовного дерева. Мінімальна остовное дерево (або мінімальне покривне дерево) у зв'язаному зваженому неорієнтовному графі – це дерево цього графа, що має мінімальну вагу суми його ребер.

Проблема знаходження мінімального остовного дерева, виникла ще в 1909 році. Математиками розроблена група алгоритмів, побудованих на нарощуванні дерева: існує тільки одна нетривіальна компонента і вона поступово нарощується додаванням « безпечних» ребер. Всі алгоритми використовують візуальну оцінку графів.

Представлений метод полягає в наступному: зв'язний, неорієнтований граф без петель з вагами на ребрах *G(A,P), A* – множина вершин, *P*-множина ребер, представляється матрицею інцидентності *U.* Ребра графа нумеруються в тому порядку, в якому їх краще вводити в дерево (в порядку зростання ваг).

Використовується теорема*:* кожне дерево з n вершинами має в точності n-1 ребро. В зв'язному графі з *m* вершинами завжди можна виділити *m-1* ребро, які утворюють дерево, тобто суграф без циклів. Тому, для виконання умови теореми, матриця інцидентності повинна мати *m-1* незалежний стовпець, тобто її ранг повинен дорівнювати *m-1*. Використовуючи операції над матрицею *U,* які не пошкодять її рангу, знаходимо одиничну матрицю з *m-1* стовпців, які відповідають гілкам дерева.

Основна відмінність представленого методу полягає в тому, що відпадає потреба в візуальному оцінюванні графа, він легко програмується і достатньо формалізований.

Список літератури

1. Эйдельман С.Д., Сирченко З.Ф. Основы дискретной математики. Графы- Киев, КВИРТУ, 1980.-110 с.
2. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ, 2-е изд. — М.: Вильямс, 2005. — 1296 с.

Курінний С.В, Сосюра А.О.
Державний Університет Телекомунікацій

ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ ЯК СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

Особливості рукописного підпису

Організаційне забезпечення електронного цифрового підпису (ЕЦП) здійснюється відповідно до законодавства держави, на території якої використовується такий засіб ЕЦП. Якщо такого законодавства немає, правове регулювання в галузі застосування засобів ЕЦП здійснюється на основі нормативних актів адміністративних органів.

У ст. 4 Закону "Про електронний цифровий підпис" зазначено, що електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами — суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Статтею 3 Закону № 852 визначено, що електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному в сертифікаті.

Власноручний підпис під документом віддавна вважається доказом того, що людина, яка підписала цей документ, ознайомилася з ним і згодна з його змістом. Тобто рукописний підпис є одним із засобів ідентифікації особи, в основу якого покладено гіпотезу про унікальність особистих біометричних параметрів людини. Чому ж підпис заслужив таку довіру? Основні причини такі:

Дійсність підпису можна перевірити (його наявність у документі дає змогу переконатися, чи справді він був підписаний людиною, що володіє правом ставити цей підпис);

Підпис не можна підробити (справжній підпис - доказ того, що саме та людина, якій він належить, поставила цей підпис під документом);

Підпис, що вже стоїть під одним документом, не може бути використаний ще раз для підписання іншого документа (підпис — невід'ємна частина документа і його не можна перенести в інший документ);

Підписаний документ не підлягає ніяким змінам;

Від підпису неможливо відректися (той, хто поставив підпис, не може згодом заявити, що він не підписував цей документ).

Насправді жодна з перерахованих властивостей підпису на всі 100 % не виконується. У нашому сучасному криміналізованому суспільстві підписи підробляють і копіюють, від них відрікаються, а в уже підписані документи вносять довільні зміни. Тобто застосування рукописного підпису не позбавлене недоліків:

- недостатній ступінь захисту (коли необхідна підвищена достовірність відомостей, що містяться у документі, використовують додаткові засоби захисту: наявність додаткових рукописних підписів, печатки юридичних осіб, засвідчення у нотаріуса, спеціальні бланки тощо);
- нерозривний фізичний зв'язок з матеріальним носієм (рукописний підпис можливий тільки на документах з матеріальною природою, тому особа, що підписує документ, має безпосередньо контактувати з матеріальним носієм цього документа);
- розбіжності між оригіналом та копіями, отриманими засобами копіювально-миожильної техніки (копії не мають тієї юридичної сили, яку має оригінал документа);
- ніяким чином не забезпечує аутентифікацію документа, тобто його цілісність і незмінність (без додаткових засобів захисту рукописний підпис не гарантує незмінності вмісту документа під час його збереження або транспортування).

Особливості електронного цифрового підпису

Застосування глобальних комунікацій в економічній діяльності та повсякденному житті зумовило появу принципово нового виду відносин, пов'язаних з обміном інформацією без використання паперових носіїв, тобто за допомогою електронних документів. Під електронним документом мають на увазі документ, в якому інформацію подано в електронній формі та який містить необхідні реквізити (у тому числі електронний цифровий підпис).

Електронний цифровий підпис (ЕЦП) є реквізитом електронного документа і призначений для його захисту від підробки. ЕЦП має не фізичну, а логічну природу. Під час побудови цифрового підпису замість звичайного зв'язку між печаткою або рукописним підписом та аркушем паперу простежується складна залежність між документом в електронному вигляді, секретним і загальнодоступним (відкритим) ключами, а також цифровим підписом. Складність підробки ЕЦП зумовлена дуже великим обсягом математичних обчислень.

ЕЦП може мати цілком "буквений" вигляд, але частіше він поданий у вигляді послідовності довільних символів. Цифровий підпис може зберігатися разом з документом, наприклад, стояти на його початку, в кінці або в окремому файлі (природно, що в останньому випадку, перевіряючи підпис, необхідно мати у своєму розпорядженні як сам документ, так і файл, що містить підпис).

Електронний цифровий підпис — це засіб, що дає змогу на основі використання криптографічних методів визначити авторство і дійсність документа. При цьому електронний цифровий підпис має такі переваги:

- дематеріалізація документів (незалежність ЕЦП від носія дає можливість використовувати його в електронному документообігу й установлювати договірні взаємовідносини без безпосереднього контакту між фізичними або юридичними особами);
- рівнозначність копій (логічна природа ЕЦП дає змогу не розрізняти копії одного документа та зробити їх рівнозначними);
- додаткова функціональність: в основі механізму ЕЦП лежить криптографія, тому ЕЦП є не тільки засобом ідентифікації, а й засобом аутентифікації документа (в електронний документ, підписаний ЕЦП, не можна внести зміни, не порушивши підпису);
- автоматизація (створення, застосування, засвідчення та перевірка ЕЦП виконується із застосуванням програмних та апаратних засобів обчислювальної техніки, тому добре автоматизується);
- порівнянність захисних властивостей (об'єктивна оцінка сертифікованих програмних та апаратних засобів обчислювальної техніки, призначених для створення ЕЦП (далі — засобів ЕЦП), базується на чіткому математичному аналізі, а не на гіпотезі про унікальність біометричних параметрів людини);
- масштабованість (виходячи з оцінки захисних властивостей ЕЦП, у цивільному документообігу можна використовувати найпростіші засоби ЕЦП, у службовому — сертифіковані для секретної інформації — спеціальні засоби ЕЦП).

Усі наведені властивості ЕЦП широко використовуються в електронній комерції. Однак у використанні ЕЦП є й недоліки. Хоча електронний документообіг з електронним підписом сприяє підвищенню продуктивності праці, але виводить механізм підпису з-під контролю звичайними методами (візуальними) та може створювати ілюзію благополуччя. Тому для використання ЕЦП необхідне спеціальне технічне, організаційне та правове забезпечення.

Література:

1. Сергієнко Дмитро. Україні – електронний документообіг // Юридичний журнал. №2/2002.
2. Симонович П.С. Регулирование электронной цифровой подписи нормами права: международный опит // «Журнал российского права»
3. Закон України «Про електронні документи й електронний документообіг» від 22.05.2003 р. № 851-IV.
4. Закон України «Про електронний цифровий підпис» від 22.05.2003 р. №852-IV.

СОЛОДКА О.М.
НА СБ України

Інформаційна безпека людини в умовах інформаційного суспільства

Зростаюче значення інформаційних ресурсів у суспільному житті, об'єктивна потреба підвищення ефективності використання інформації як суттєвого фактора прискорення суспільного прогресу – все це дало підстави до визначення нинішнього етапу розвитку людства як інформаційного.

Сутність інформаційного суспільства була визначена ще 1993 року Комісією Європейського Союзу як суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

У підсумкових документах Всесвітнього саміту з питань інформаційного суспільства (2003–2005) визначено, що інформаційне суспільство – це суспільство, орієнтовне на людей, відкрите для всіх і спрямоване на розвиток, в якому кожний може створювати інформацію і знання, мати до них доступ, користуватися і обмінюватися ними, даючи змогу конкретним особам, громадам і народам повною мірою реалізувати свій потенціал, сприяючи своєму сталому розвитку і підвищувати якість свого життя [1].

А Окінавська хартія глобального інформаційного суспільства від 22 липня 2000 року під поняттям «інформаційне суспільство» розуміє суспільство, економіка якого базується на інформаційних технологіях і яке соціально трансформується з метою допомогти індивідам та спільнотам використовувати знання та ідеї, що допомагає людям втілити їх потенціал та реалізувати їх прагнення [2].

Відповідно до національного законодавства інформаційне суспільство – це суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя [3].

Відтак, виходячи з вище наведених визначень, можливо констатувати, що інформаційне суспільство перш за все орієнтоване на задоволення інформаційних потреб людини, оскільки саме вона є найвищою цінністю. Згідно зі ст. 3 Конституції України людина, її життя і здоров'я, честь та гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю, а людина і громадянин – їхні конституційні права і свободи – визначені у законодавстві України об'єктами національної безпеки.

Разом з цим, зворотною стороною розвитку інформаційних технологій, які суттєво полегшують комунікацію, стала поява тенденцій до негативних процесів у частині посягань на інформаційну безпеку.

У Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" інформаційна безпека визначена як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [3].

В рамках аналізу питань забезпечення інформаційної безпеки звертають усе більшу увагу на необхідність розробки проблематики інформаційно-психологічної безпеки особистості, адже без докладного аналізу цих проблем неможливий подальший стійкий розвиток суспільства.

На сьогоднішньому етапі, завдяки ефективності інформаційного впливу на свідомість, засоби масової інформації, особливо у нашій державі, стали ідеальним засобом для проведення інформаційно-психологічного впливу, який полягає в цілеспрямованому створенні та поширенні спеціально підібраної інформації, що позитивно або негативно впливає на психіку і поведінку окремих осіб або населення загалом з метою досягнення переваг для суб'єкта впливу. Така ситуація пояснюється тим, що, зокрема в Україні, доступ до мережі Інтернет є неоднорідним, як щодо вікових категорій, так і соціальних, і більшість населення все ж таки отримує інформацію з телебачення та друкованих ЗМІ, що й створює умови для можливості маніпулювання масовою свідомістю.

Окрім цього, засилля телевізійного продукту виключно іноземного виробництва або проіноземного зразка (російських серіалів, західних розважальних шоу) створило умови для поширення невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності, небажання самоідентифікації.

Надзвичайна популярність соціальних мереж як засобу комунікації та спілкування людей з різних частин не лише однієї країни, а й світу, попри позитив, актуалізує питання «інформаційної правосвідомості особи», оскільки розміщуючи свою персональну інформацію, власники, як правило, на задумуються про негативні наслідки її неправомірного використання третіми особами, здебільшого перекладаючи відповідальність за це на державу. До того ж за повідомленнями на сторінці конкретної особи можна визначити її плани, місцезнаходження, уподобання. Відтак, інформатизація в умовах інформаційного суспільства призводить до того, що всі людські прояви стають фактично контрольованими.

Загалом, вирішення наявних проблем забезпечення інформаційної безпеки особи в сучасних умовах полягає в наступному:

1) у необхідності кардинальної зміни національної інформаційної політики щодо створення національного інформаційного продукту, актуалізації питання національних традицій, поваги до сімейних цінностей та нації загалом, адже національна свідомість населення держави, яка побудована за національною ознакою, передбачає усвідомлення

нацією своєї спільності у межах певної території (а не класу чи цілого світу), ототожнення членів нації з певною мовою, культурою, традиціями. Завдання держави, у даному випадку, не встановити контроль за діяльністю ЗМІ та наповненням Інтернет-ресурсів (за виключенням випадків поширення шкідливої інформації), а забезпечити умови для формування раціонального, критичного мислення на основі принципів свободи вибору, забезпечення прав свободи слова та доступу до інформації;

2) забезпеченні доступу громадян до інформації не лише створенням юридичного механізму, що здебільшого стосується публічної інформації, а шляхом практичного забезпечення розвитку програми інформатизації з метою «інтернетизувати» більшу кількість населення;

3) формуванні інформаційної правосвідомості громадян шляхом введення до програми навчання спеціальних курсів з роз'яснення поняття «персональні дані» та інших видів інформації вже у школі, донесення до суспільства негативних наслідків використання соціальних мереж, негативного інформаційного впливу тощо.

Особливість сучасного етапу формування інформаційного суспільства полягає в тому, що розширення джерел отримання інформації створює умови для величезної кількості протиправних посягань.

Відтак, поряд із положеннями про побудову в Україні розвинутого інформаційного суспільства, впровадження новітніх інформаційних технологій, забезпечення конституційних прав людини і громадянина на свободу слова та вільний доступ до інформації мають бути і механізми забезпечення інформаційної безпеки особи:

- захист національних традицій, моральних і культурних цінностей, популяризація українського продукту;
- правові механізми виявлення, фіксації, кваліфікації, блокування та видалення з українського сегмента мережі Інтернет інформації, поширення якої заборонено законодавством України тощо;
- формування інформаційної культури і правосвідомості громадян.

Важливо зазначити, що основою вище зазначених змін є створення умов забезпечення поваги до людини, її гідності, створення належного соціального забезпечення.

Список використаних джерел

1. Кісілевич-Чорнойван О. М. Міжнародне інформаційне право. — К. : ДП «Вид. дім «Персонал», 2011. — С. 39 – 45.
2. Європа і всесвітнє інформаційне суспільство. Рекомендації Європейської Ради: звіт групи М.Бангемана від 05.12.93 р. Комісії Європейського Союзу [Електронний ресурс] // Режим доступу : //www.europa.eu.int/com.
3. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 9 січня 2007 року № 537-V // Відомості Верховної Ради України, 2007. – № 12. – Ст.102.

Чередніченко О.О.
Державний Університет Телекомунікацій

Аудит інформаційної безпеки організації та систем

Аудит інформаційної безпеки - це системний процес одержання об'єктивних якісних и кількісних оцінок поточного стану безпеки організації або інформаційної системи. В Україні, аудит інформаційної безпеки організацій та інформаційних систем, проводиться на відповідність таким вимогам:

- Нормативних документів у галузі технічного захисту інформації (НД ТЗІ).
- ISO\IEC 27001:2005.
- PCI DSS.

На даний час, за умов стрімкого розвитку інформаційних технологій виникає необхідність захищеності інформаційних ресурсів організацій та підприємств для боротьби із зовнішнім і внутрішнім загрозами. З метою посилення інформаційної безпеки та утримання її на належному рівні, пропонується проведення аудиту. Процес аудиту повинен проходити в декілька етапів:

1. Вивчення поточного стану ІБ в організації.
2. Порівняння цих результатів відповідно до стандартів та аналогічним об'єктам дослідження.
3. Розробка рекомендацій для організації, що стосуються посилення інформаційної безпеки
4. Оформлення та подання результатів.

Зараз, в Україні, ефективність проведення аудиту в сфері інформаційної безпеки не є дуже великою і вистачає різних проблем, але все ж прогрес відбувається. Я вважаю, що аудит здатний стати реальним засобом ліквідації різного типу загроз в сфері ІБ.

Перелік посилань:

1) http://eztuir.ztu.edu.ua/3149/1/9.pdf

Чередніченко О.О.
Державний Університет Телекомунікацій

Функціональний та процесний підходи до УІБ

Початок нового тисячоліття в усьому світі ознаменувався бурхливим розвитком не тільки техніки і технологій, а й якісно новим рівнем ведення управління. Перед керівниками підприємств гостро постає питання про створення такої системи управління, яка б враховувала нові умови роботи в ринкових відносинах і сприяла б посиленню конкурентоспроможності підприємств.

Сьогодні в Україні в сфері УІБ, як правило, застосовує функціональний підхід, що має ряд недоліків. Вдосконаленим методом управління є процесний підхід, який створює кращі передумови пристосовування до змінного, динамічного і часто непередбачуваного середовища. Багатообіцяючим виявляється застосування процесного підходу до системи управління організацією. Цей підхід дозволяє розглядати діяльність організації як систему взаємопов'язаних і взаємодіючих процесів, кінцевими цілями виконання яких є створення продуктів або послуг, що представляють цінність для зовнішніх і внутрішніх споживачів.

При функціональному підході до управління перед кожною структурною одиницею організації закріплено ряд функцій, описана область відповідальності, сформульовані критерії успішної та неуспішної діяльності. Як правило, і зв'язки між структурними одиницями слабкі, а зв'язки по лінії начальник-підлеглий - сильні. Підлеглий відповідає тільки за доручені йому функції і, можливо, за діяльність свого підрозділу в цілому.

Процесний підхід розглядає функції управління як взаємопов'язаний процес управління. Він є загальною сумою всіх функцій, серією безперервних взаємопов'язаних дій. При цьому підході до управління кожна структурна одиниця забезпечує виконання конкретних процесів, в яких вона бере участь. Зв'язки між структурними одиницями при такому підході значно сильніші, ніж у випадку функціонального підходу, але зв'язки між структурними одиницями по лінії начальник-підлеглий дещо слабші.

Отже, процесний підхід є якіснішим і ефективнішим за функціональний, але для його впровадження потрібно більше часу, можливостей і затрат.

Перелік посилань:

1. http://www.scienceforum.ru/2014/715/6937
2. http://bibliofond.ru/view.aspx?id=561964

Белоусов М.О., Ткач М.М., Почтарьов І.С.
Державний університет телекомунікацій

Програма автоматизації розрахунку зони радіопокриття базової станції

В доповіді обґрунтовано доцільність використання розробленої програми автоматизації розрахунку зони радіопокриття базової станції при попередньому плануванні мережі в MathCad, що дозволяє знайти число базових станцій, які необхідно встановити для обслуговування з необхідною якістю заданої кількості абонентів; визначити доцільність застосування секторних антен для зменшення взаємних перешкод між станціями, що працюють у тому самому частотному каналі і розташовані в різних стільниках; знайти параметри, що визначають необхідну енергетику базових станцій.

Системи зв’язку з рухомими об’єктами через принципове обмеження на випромінювану ними потужність, що накладається органами державного регулювання, не в змозі однією базовою станцією (БС) забезпечити радіопокриття великого за територією регіону через затухання радіохвиль. Тому вони будуються за принципом поділення регіону на певну кількість зон - стільників порівняно невеликої площі.

Завданням частотно-територіального планування є визначення оптимальної кількості і конфігурацій розташування БС, а також вибір розподілу частот або груп частот для кожного стільника, які забезпечують покриття максимальної території при мінімальних матеріальних витратах і максимальній кількості каналів зв'язку в заданому діапазоні частот це, очевидно, багатоваріантне завдання, при рішенні якої враховується велика кількість найрізноманітніших чинників.

Тому, використання програм комп’ютерної математики при автоматизації розрахунку зони радіопокриття БС дозволяє значно спростити і підвищити точність планування мережі.

Система стільникового зв’язку - це система масового обслуговування, особливістю якої є те, що тільки мала частина користувачів при великій їх загальній чисельності одночасно має потребу в послугах. Тому певною кількістю каналів зв’язку можна обслужити набагато більшу кількість користувачів. Потік заявок на послугу зв’язку (трафік) є випадковою величиною, що вимірюється в Ерлангах, причому його максимальне значення виявляється у час найбільшого навантаження доби.

Розроблений алгоритм дозволяє знайти всі необхідні параметри частотного плану стільникової МПР. При складанні повного частотного плану необхідно, знаючи число частотних каналів, що приходяться на кожну БС, і конфігурацію кластера, використовуваного для побудови стільникової мережі, визначити конкретні номінали частот, що виділяються для роботи всіх БС одного кластера. Причому повинні бути зведені до мінімуму перешкоди між

стільниками, у яких застосовуються сусідні частотні канали, а також інтермодуляційні перешкоди між частотними каналами, задіяними в одному секторі стільника.

Запропонована процедура розрахунку основних параметрів частотного плану стільникової мережі рухомого радіозв'язку, розгорнутої в місті, дозволяє знайти число базових станцій, які необхідно встановити для обслуговування з необхідною якістю заданої кількості абонентів; визначити доцільність застосування секторних антен для зменшення взаємних перешкод між станціями, що працюють у тому самому частотному каналі і розташовані в різних стільниках; знайти параметри, що визначають необхідну енергетику базових станцій.

За визначеним алгоритмом розрахунку зони радіопокриття в інтегрованому середовищі MathCad розроблена програма автоматизації розрахунку зони радіопокриття базової станції.

Козовий В.Є., Волуйко І.В., Струк С.Є.
Державний університет телекомунікацій

Вибір оптимального сценарію розвитку IPTV

В доповіді розказано про вибір оптимального розвитку IPTV. За мережевою статистикою виконується оцінка якісних параметрів IPTV. Проведено експеримент по оцінці впливу мережевих параметрів на показники якості. Також проведено порівняння технологій доступу перспективи реалізації концепції FTTx.

У споруджуваному будинку можна вибрати і прокласти ту кабельну систему, яка здасться найкращою, скажімо, кручену пару (для Ethernet) або навіть оптику. У вже заселеному будинку «дійти» до абонента новим кабелем не завжди просто – можливо, в окремих випадках доцільно використовувати на останніх метрах безпроводові системи Wi–Fi.

Неможливо, навіть просто перелічити все різноманіття чинників, що визначають вибір схеми побудови мережі FTTx.

Fiber To The X – поняття, що описує загальний підхід до організації кабельної інфраструктури мережі доступу, в якій від вузла зв'язку до певного місця (точка «x») доходить оптоволокно, а далі, до абонента, – мідний кабель (можливий і варіант, при якому оптика прокладається безпосередньо до абонентського пристрою). Таким чином, FTTx – це тільки фізичний рівень. Однак фактично дане поняття охоплює і велике число технологій канального й мережного рівня. З широкою смугою система FTTx нерозривно пов'язана можливість надання великої кількості нових послуг.

У сімейство FTTx входять різні види архітектур:

• FTTN (Fiber to the Node) – волокно до мережевого вузла;
• FTTC (Fiber to the Curb) – волокно до мікрорайону, кварталу або групи будинків;
• FTTB (Fiber to the Building) – волокно до будівлі;
• FTTH (Fiber to the Home) – волокно до помешкання (квартири або окремого котеджу).

На сьогоднішній день FTTN (Fiber to the Node) використовується в основному як швидко впроваджуване рішення там, де існує розподільча «мідна» інфраструктура і прокладка оптоволокна нерентабельна. Всім відомі пов'язані з цим рішенням труднощі: невисока якість надаваних послуг, обумовлене специфічними проблемами лежать в каналізації мідних кабелів, істотне обмеження по швидкості і кількості підключень в одному кабелі.

Очевидно, що запланований набір послуг і необхідна для їх надання смуга пропускання мають найбезпосередніший вплив на вибір технології FTTx. Чим вище швидкість доступу і чим більше набір послуг, тим ближче до терміналу повинна підходити оптика, а саме потрібно використовувати технології FTTH. Якщо ж пріоритетом є збереження наявної інфраструктури та обладнання, найкращим вибором буде FTTB.

Побудова мереж доступу FTTx – на сьогоднішній день найперспективніший спосіб розширення смуги пропускання каналів зв'язку до кінцевих користувачів і пропозиції їм нових високошвидкісних послуг. При цьому вибір місця для точки «x» – межі між оптикою і міддю – залежить від цілого ряду чинників.

Могилевський В.Б., Малов О.І.
Державний університет телекомунікацій

Проблеми реалізації технології «cloud computing» в телекомунікаційній мережі

В доповіді оцінюється ефективність технології «Cloud computing», обґрунтовується можливість її застосування. Обґрунтовуються практичні рекомендації по використанню технології «cloud computing» для підвищення працездатності обробки інформації.

Сучасний рівень інформатизації і комп'ютеризації українського суспільства, впровадження безлічі інтерактивних мультимедійних інфо-комунікаційних послуг практично в усі сфери громадської діяльності, вдосконалення засобів зв'язку і обробки даних, цифровізація радіо і телевізійного мовлення обумовлюють інтеграцію ряду телекомунікаційних послуг в єдину багатофункціональну інтерактивну мультимедійну підсистему і диференціацію завдань обробки даних і додатків по пріоритетності окремих показників якості передачі інформації. Основні підходи в рішенні цілого комплексу завдань, що стоять перед розробниками у зв'язку з кардинальними змінами в системах управління телекомунікаційними ресурсами визначені законом України "Про концепцію Національної програми інформатизації", постановами Кабінету Міністрів України "Про концепцію розвитку зв'язку України", "Про затвердження Державної цільової науково - технічної програми створення державної інтегрованої інформаційної системи забезпечення управління рухомими об'єктами(зв'язок, навігація, спостереження) ". Ряд концептуальних

проблем, в першу чергу пов'язаних з необхідністю забезпечення показників якості обслуговування, до яких, відповідно до стандартів Міжнародного союзу електрозв'язку, пред'являються підвищені вимоги, обумовлюють актуальність проведення прикладних досліджень на шляхи створення і впровадження перспективних засобів і систем зв'язку, а також розробки нових методів управління процесами обробки і передачі інформації.

Для оцінки реалізації технології «Cloud computing» в якості основного матеріалу, взяті основні дані про технологію, а також графіки про можливості використання технології «Cloud computing», шляхи розвитку та проблеми реалізації даної технології.

Хмарні технології та надання програмного забезпечення «як послуга» знаходяться на самому початку життєвого циклу. Принцип організації надання послуг «хмарних обчислень» поки не визначений. Існуюче розмаїтість маркетингових підходів до надання даних послуг вводить споживачів в оману. Найбільш відомими способами надання послуг є хостинг і здача програмного забезпечення в оренду.

Проте, найбільш просунуті бізнеси (особливо це стосується підприємств, що працюють у сфері інформаційних та комунікаційних технологій) вже користуються різними хмарними сервісами і знаходять їх застосування зручними й економічно доцільними. Більшість респондентів визнало, що в найближчому майбутньому з великою ймовірністю стануть використовувати різні хмарні сервіси і набувати послуги за схемою SaaS.

Найбільш ймовірними позитивними наслідками застосування SaaS і Cloud computing - визнають прискорення процесів впровадження нових технологій і економію на придбанні інфраструктурних рішень. Найбільш важливим чинником, що заважає розвитку хмарних рішень, визнали - низьку якість послуг зв'язку та особливості бізнес-менталітету, включаючи низьку інноваційну активність бізнесу. Найменш важливим фактором названі піратство і нерозвиненість ринку SaaS і хмарних додатків.

Слід зазначити наступні кроки, які сприятимуть розвитку ринку: збільшення інформованості споживачів про хмарних технологіях та підвищення інформаційної безпеки пропонованих рішень.

Талабко О.Ю., Евтушенко В.К., Олійник О.Ю.
Державний університет телекомунікацій

Розробка імітаційної моделі систем ідентифікації трафіку і управління чергами в тк мережі

В доповіді оцінюється ефективність розроблених методів ідентифікації трафіку і динамічного управління чергами у багатопротокольних вузлах зв'язку, обгрунтовується достовірність отриманих результатів. Обгрунтовуються практичні рекомендації по використанню розроблених методів для підвищення оперативності передачі даних в телекомунікаційних мережах.

Сучасний рівень інформатизації і комп'ютеризації українського суспільства, впровадження безлічі інтерактивних мультимедійних інфо-комунікаційних послуг практично в усі сфери громадської діяльності, вдосконалення засобів зв'язку і обробки даних, цифровізація радіо і телевізійного мовлення обумовлюють інтеграцію ряду телекомунікаційних послуг в єдину багатофункціональну інтерактивну мультимедійну підсистему і диференціацію завдань обробки даних і додатків по пріоритетності окремих показників якості передачі інформації.

В якості основного інструментарію імітаційного моделювання використовуємо середовище символьної математики MathCAD. В якості об'єкту моделювання виберемо фрагмент ТКС, що має багато зв'язкову топологічну структуру.

В імітаційній моделі підсистеми параметричної ідентифікації трафіку реалізована процедура n- мірного шкалування на основі, якій приймається рішення про розбиття інформаційного трафіку по категоріях і напрям його на різні мережеві облаштування(порти) багато-протокольного вузла зв'язку.

Проведений аналіз і дослідження показали, що основою системи управління чергами у багато-протопротокольному вузлі зв'язку є підсистеми установки первинних параметрів і динамічного розподілу ресурсів.

Вхідними даними для вказаних підсистем є в першу чергу імовірнісно-тимчасові характеристики інформаційного потоку, такі як інтенсивність інформаційного потоку, час очікування інформаційних пакетів в черги, джиттер затримки, а також статистичні дані про поведінку інформаційного потоку різних служб прикладного рівня.

Функціонування усіх приведених підсистем має на меті реалізацію принципу справедливого розподілу мережевих ресурсів з урахуванням пріоритетного обслуговування трафіку мультимедійних служб.

Таким чином, розроблена імітаційна модель систем ідентифікації трафіку і управління чергами у багатопротокольних вузлах зв'язку телекомунікаційної мережі дозволяє здійснювати збір і статистичну оцінку вхідного інформаційного потоку, ідентифікувати різні інтерактивні і інші мережеві служби прикладного рівня, робити динамічний перерозподіл ресурсів у облаштуваннях обслуговування багато-протокольного вузла зв'язку, імітувати функціонування підсистем ідентифікації трафіку, імітувати функції збору статистичних даних, управління і обслуговування компонентів телекомунікаційної мережі. Результати імітаційного моделювання дозволяють оцінити ефективність методу підвищення оперативності передачі даних в телекомунікаційній мережі і обгрунтувати достовірність отриманих результатів.

д.т.н.,професор Богданович В.Ю
Державний університет телекомунікацій,м.Київ

Отработка стратегии и тактики гибридной войны XXI-го столетия на территории Украины

Практически все военные конфликты конца XX-го – начала XXI-го столетий, происходившие в тех или иных уголках нашей планеты, развивались и протекали не по классическим схемам из учебников по военному искусству.

Современный мир пребывает в состоянии системной неустойчивости, разбалансированности и хаоса. К вызовам и угрозам эпохи холодной войны добавились качественно новые опасности и угрозы, носящие глобальный характер. Мир ни в коем случае не стал более стабильным и предсказуемым: войны непрерывно сотрясают нашу планету. И за относительно короткое время благополучные некогда страны и регионы ввергаются в состояние разрухи, деградации и хаоса. Ирак, Югославия, Ливия, Сирия – список государств, сполна ощутивших на себе специфику войн современного типа, пополнился Украиной. Несмотря на все различия между этими государствами, произошедшие в них события имеют много общего. Это позволяет некоторым аналитикам утверждать, что в мире существуют силы, которые **управляют** этими разрушительными процессами и пользуются ими в своих интересах, манипулируя при этом общественным сознанием как на глобальном уровне, так и внутри отдельных стран [1].

Если абстрагироваться от политического содержания современных военных конфликтов, то можно заметить, что все они имеют некоторые общие черты, отличающие их от традиционных войн прошлого. Современные войны, прежде всего, возникают, как правило, в формате внутригосударственного конфликта и быстро приобретают международное измерение.

Вспыхнувший внутригосударственный конфликт в любой стране незамедлительно получает оценку Запада, в которой одна из сторон без долгих колебаний немедленно объявляется «легитимной». В качестве такой стороны может выступать национальное правительство, внутренняя оппозиция или даже некие внешние акторы. Под эту оценку через механизмы ООН и других межгосударственных структур с использованием мировых средств массовой информации «подгоняется» позиция международного сообщества, что позволяет сфабриковать международный ярлык легитимности фактически любому государственному перевороту [2] .

Военные конфликты нового типа, как правило, не имеют четко выраженных временных параметров: у них нет четкого начала и конца. Эти конфликты могут «замораживаться» на годы, внезапно переходить в «горячую» стадию, снова затухать, чтобы вновь обостриться в будущем. Такой конфликт может возникнуть в Крыму.

Военные действия в ходе современных военных конфликтов приобретают асимметричный характер, когда на поле боя сталкиваются регулярные вооруженные силы и иррегулярные формирования всех мастей. Это требует от регулярных войск соответствующей специальной подготовки для действий против иррегулярных формирований. Одновременно создаются условия для специальных действий и широкого применения сил специальных операций [3].

В условиях войны «управляемого хаоса» расцветает такое явление, как «приватизация войны». К традиционным двум сторонам военного конфликта добавляются другие акторы – независимые племена, уголовные банды, батальоны «добровольцев» и другие организованные вооруженные формирования, в том числе частные вооруженные формирования (ЧВК), чаще всего иррегулярного типа. Действуя самостоятельно, не подчиняясь ни одной стороне конфликта, эти формирования активно способствуют нагнетанию хаоса и препятствуют процессам мирного урегулирования. В силу специфики состава участников военного конфликта и их возможностей сами военные действия часто ведутся с военной точки непрофессионально. Лидеры иррегулярных формирований не имеют, как правило, специального военного образования и воюют «по понятиям», что вносит дополнительный хаос и неразбериху, приводит к неоправданным жертвам со всех сторон.

Хаос в зоне военного конфликта проявляется в первую очередь в отсутствии слаженной системы управления вооруженными формированиями, эффективной системы иформационного обеспечения. Планирование боевых действий осуществляется наспех и бессистемно, что негативно отражается на их ходе и исходе.

В ходе боевых действий стороны широко применяют весь арсенал доступного им вооружения, не задумываясь о последствиях и нарушениях норм и принципов международного гуманитарного права. В качестве целей для поражения нередко выбираются ключевые объекты инфраструктуры, энергоснабжения, экологически опасные объекты и др. При этом больше всего страдает мирное население на территории конфликта. Ввергнутые в состояние войны жители оказываются перед выбором: бежать куда глаза глядят или оставаться под бомбежками и обстрелами. Старики, женщины и дети гибнут первыми. Массовые казни, террор и запугивание, насилия и грабежи становятся жестокой реальностью. Наступает гуманитарная катастрофа. Именно это мы наблюдаем сегодня и в Сирии, и в Украине.

События последних лет свидетельствуют, что в результате целенаправленного внешнего вмешательства под благовидными целями развития демократии и защиты прав отдельных обиженных граждан более-менее стабильные государства оказываются ввергнутыми в хаос, в гражданскую войну. В результате десятки тысяч граждан становятся жертвами, миллионы – беженцами, а само государство фактически переходит под внешнее управление реальных заказчиков этой войны.

Анализ таких войн показывает, что их проведение требует длительных многолетних подготовительных действий и больших ресурсов. Ведь необходимо подорвать нравственные и моральные устои наиболее активной части

населения, внушить ему абсурдную мысль, что у него появился враг, который посягает на его суверенитет, свободу и только, если его уничтожить, то завтра само собой наступит светлое будущее!

Те события, которые с конца 2013 года стремительно развернулись в Украине, являются результатом многолетней работы спецслужб геополитических противников России. В настоящее время попытки противодействовать новой технологии войны, опираясь на старую теорию, чреваты такими же катастрофическими последствиями, как и 75 лет назад, за одним исключением: тыла, куда можно отступать и эакуировать стратегически важные предприятия, не будет. Сегодня боевые действия разворачиваются на территории страны – жертвы агрессии и куда бежать и что делать в таких условиях, никто не знает.

Введенные в конце XX-го столетия понятия «война управляемого хаоса», «цветная революция», «гибридные войны» и «гибридные угрозы», как представляется, относятся к новому виду конфликтов современности, в основе которых лежат разработанные на Западе подрывные инновационные технологии. Отдельное место в списке инновационных подрывных технологий занимают так званые «цветные» революции, осуществляемые с применением технологий «управляемого хаоса». При этом такие технологии рассматриваются в качестве средства демократического, ненасильственного захвата власти в ходе государственного переворота с целью передачи страны-мишени под внешнее управление [2].

Опыт «цветных» революций в Египте, Ливии, Сирии, Грузии, Украине показывает, что, от политического шантажа на начальном этапе в ходе относительно мирных демонстраций, противоборствующие стороны в результате искусных манипуляций со стороны зарубежных заказчиков и внутренних заинтересованных акторов и «агентов влияния» в дальнейшем переходят к силовому противостоянию. При этом отсутствие решительной реакции властей на первоначальные отдельные акты использования силы радикальной оппозицией и умело спровоцированными на это правоохранительными органами приводит к эскалации конфликта с последующим «скатыванием» страны к гражданской войне.

Заказчики «цветной» революции прогнозируют развитие событий именно по такому сценарию и заранее готовят и аккумулируют силовые и информационные ресурсы, продвигают новых лидеров, альтернативных действующей власти. Для продавливания своих планов они не останавливаются перед прямым вмешательством во внутренние дела суверенных государств, как это было, например, во время известных визитов в Украину высокопоставленных представителей Госдепа и конгресса США, директора ЦРУ, екс-посла США в Украине С.Пайфера, политической элиты Евросоюза и др.

В подобных условиях бездействие властей, парализованных страхом и угрозами преследования со стороны международного сообщества, или бегство из страны ее руководителей приводит к развязыванию в стране гражданской войны. В дальнейшем приходит очередь использования технологий войны нового типа – «гибридной войны». «Цветная» революция, таким образом, может рассматриваться лишь как начальный этап такой войны [2].

Следует отметить, что стратегия «гибридных войн» разрабатывается на Западе в течение ряда лет, однако до сих пор нет четкого единого определения такой войны.

На высоком официальном уровне термин «гибридная война» впервые прозвучал на саммите НАТО в сентябре 2013г. в Великобритании. Под такой войной альянс понимает проведение широкого спектра прямых боевых действий и тайных операций, осуществляемых по единому плану вооруженными силами, партизанскими (невоенными) формированиями и включающих также действия различных гражданских компонентов [2]. В «гибридной войне» аналитики НАТО прелагают более активно привлекать силы полиции и жандармерии для пресечения нетрадиционных угроз, связанных с пропагандистскими кампаниями и действиями местных сепаратистов. Отдельно выделяются специальные информационные операции, информационное и кибернетическое оружие. Государства, втянутые в «гибридную войну», обычно видят для себя комплекс «гибридных» угроз, включающий угрозы различного типа: традиционные, нестандартные, масштабный терроризм, а также подрывные действия, в ходе которых используются технологии для противостояния превосходящей военной силе.

Особенностью «гибридных» угроз является их строго целенаправленный, адаптивный по отношению к государству-мишени и конкретной политической ситуации характер. По образному выражению, такие угрозы формируются под конкретную страну, как шьется костюм по индивидуальному заказу [1]. Комплекс гибридных угроз обладает рядом характеристик, обеспечивающих его эффективное применение на всех этапах гибридной войны. Такой комплекс благодаря уникальной синергетике обладает гораздо большей разрушительной силой, чем простая сумма входящих в него угроз. Эта особенность обусловливает их мощный разрушительный потенциал. Синергетический эффект от воздействия угроз этого вида обеспечивается реализацией системы комплексных и взаимозависимых подготовительных и исполнительных мероприятий, связанных с координацией деятельности значительного количества участников, действующих на территории страны-мишени и за ее пределами. Успеху способствует умелое использование факторов, обусловливающих высокую динамику развития обстановки и придания процессам необходимой направленности с использованием как невоенных, так и военных решений.

Целенаправленный характер и высокая динамика перехода «гибридных» угроз из категории потенциальных к реально действующим требуют тщательной предварительной проработки на государственном уровне мер по противодействию. В первую очередь требует особого внимания своевременное вскрытие комплекса проводимых мероприятий по подготовке противника к «гибридной» войне, начиная от планирования первоначальных этапов ненасильственных действий и вплоть до перехода к жесткой силовой конфронтации. Эта задача успешно может быть решена в ходе проведения комплексного мониторинга угроз национальной безопасности [3]. Для этого должны быть

формально выделены признаки подготовки противника к «гибридной» войне. Такими признаками со стороны страны-агрессора обычно выступают:

– формирование источников устойчивого финансирования протестного движения, а затем вооруженных формирований как со стороны внешних заинтересованных сил, так и с использованием внутренних возможностей;

– выявление (формирование, поддержка) протестных общественных групп, способных участвовать в планируемых акциях ненасильственного, а затем и силового характера, вплоть до гражданской войны;

– определение практических лозунгов, максимально приближенных к реальным требованиям протестных общественных групп, действия которых в итоге могут использоваться для делегитимации и слома существующей власти;

– определение (создание, поддержка) политических объединений и подготовка лидеров, способных возглавить политические протестные акции;

– подготовка в специализированных лагерях полевых командиров и боевиков для силовых акций, организация мобилизационных пунктов за рубежом и маршрутов переброс наемников;

– обеспечение поддержки оппозиции и осуществление ее экспансии в регионы, прежде всего за счет координированного использования контролируемых оппозицией электронных отечественных и зарубежных СМИ. Немаловажное место отводится завоеванию поддержки со стороны международных организаций и международной общественности;

– организация сетевых структур управления подрывными действиями, снабжения, связи и мониторинга обстановки;

-активизация внедрения обменных программ, главной (но не единственной) целью которых может быть выращивание политиков для страны-мишени, способных в дальнейшем выполнять задачи «агентов влияния»;

-развертывание и поддержка сети неправительственных организаций Запада, формирование сети «агентов влияния», внедрение программ, целью которых является политическая переориентация населения страны в целом или ее отдельных регионов;

-поддержка радикальных, в том числе неофашистских организаций, радикально-экстремистских сект («Хизб-ут-Тахрир», «Сулеймандживилар»), запрещенных в других государствах, международных религиозных организаций (например, «Нурджулар») и др.;

-проведение специальных информационных операций (СИО), направленных против субъектов, принимающих стратегические решения;

-проведение СИО, направленных на компроментацию и нанесение ущерба имиджу отдельным личностям из состава высшего военно-политического руководства страны;

-проведение СИО, направленных на политическую (экономическую) дестабилизацию государства;

-проведение СИО, направленных на подрыв обороноспособности государства;

-проведение СИО, направленных на разрушение духовного наследия и пересмотр итогов Великой отечественной войны;

-проведение СИО, направленных на формирование «нужного» общественного мнения для поддержки тех или иных политических акций, програм, действий отдельных политических структур или отдельных личностей;

-поддержка усилий по переформатированию информационного пространства и установление контроля за эксперным пространством страны;

-лоббирование законодательного обеспечения навязываемых реформ, программ развития или политического курса (например, курса на интеграцию в НАТО).

С учетом масштабов и реального характера «гибридных» угроз успешное решение комплекса задач по обеспечению национальной безопасности Украины может быть достигнуто за счет выхода из-под внешнего управления США, консолидации общества, укрепления обороноспособности страны, развития связей с союзниками и партнерами, умелым использованием потенциала существующих структур обеспечения международной безопасности и решительным противодействием попыткам деструктивного влияния в сфере международных отношений. Для этого в системе обеспечения национальной безопасности целесообразно создать систему противодействия «гибридным» угрозам. Для эффективного функционирования этой системы необходимо выработать и внедрить в практику систему критериев и признаков, позволяющих оперативно, с использованием преимущественно количественных методов проводить оценку способности страны противостоять подрывной деятельности с целью исключить возможные попытки спровоцировать на территории Украины или отдельных ее частей гибридные войны.

Особое внимание должно быть уделено работе с молодежью, которая представляет собой первоочередной объект воздействия для технологов гибридных войн, а также с мигрантами, недопуская создания этнических анклавов в крупных городах и в регионах, поскольку использование современных информационно-коммуникационных технологий позволяет в рамках сетевой организации оперативно создавать с участием мигрантов мощные источники дестабилизации обстановки в различных районах страны.

Анализ известных «гибридных» войн показывает, что при подготовке «гибридной» войны ее потенциальные участники заблаговременно объединяются в сеть, которая охватывает прежде всего столицу и другие крупные города. При этом для сетевых форм управления подготовкой и развертывания действий характерно на начальном этапе отсутствие четко выраженного единого центра. Такие структуры получили название полицентрических. Сетевая организация имеет горизонтальную архитектуру, для которой в отличие от жесткой иерархической пирамиды присущи взаимосвязанность ячеек (групп) сети и непрерывный обмен информацией между ними в масштабе времени,

близком к реальному. Это обеспечивает выживаемость и работоспособность всей структуры в хаосе гражданской войны, как, например, в Ливии и Сирии.

В современных условиях объявленная руководством Украины антитеррористическая операция имеет все признаки гражданской войны, которая носит характер «гибридной».

Деятельность государства по организации системы противодействия этой «гибридной» войне требует соответствующего нормативно-правового обеспечения, согласованного с международно-правовой базой, а таже внесения новых положений в теорию и практику военного искусства и обеспечения обороноспособности государства.

Список использованной литературы

1.Изборский клуб.. Электронный ресурс. - Режим доступа: http://www.dynacon.ru/content/articles/4224/
2.Александр Бартош. Гибридные войны в стратегии США и НАТО. Электронный ресурс. - Режим доступа: http://nvo.ng.ru/concepts/2014-10-10/1_nato.html.
3.Богданович В.Ю., Скулиш Є.Д., Свида І.Ю Теоретико-методологічні основи забезпечення національної безпеки України (в 7 томах). Том 1. Теоретичні основи, методи і технології забезпечення національної безпеки України: за заг. ред.. Є.Д.Скулиша К.: Наук.-вид. відділ НА СБ України. 2012. - 548 с.

аспірант Складанний П.М.
Державний університет телекомунікацій

Технології обґрунтування прийняття рішень в інтелектуальній системі захисту інформації

Інформаційні системи (ІС) стають сьогодні одним з головних інструментів управління бізнесом, найважливішим засобом виробництва сучасного підприємства. Однак їх застосування інформаційних технологій неприпустимо без підвищеної уваги до питань інформаційної (комп'ютерної) безпеки через наявність загроз захищеності інформації. Опубліковані дані про збитки світовій економіці від комп'ютерних атак свідчать про те, що застосовувані в сучасних ІС традиційні комплекси систем захисту інформації (СЗІ) практично не дозволяють забезпечувати виконання вимог щодо захисту інформації протягом усього періоду функціонування ІС. Критична ситуація у сфері інформаційної безпеки посилюється до того ж з появою невідомих раніше типів інформаційних впливів і використанням глобальної мережі для зовнішніх і внутрішніх електронних транзакцій підприємства. Все це веде до розуміння того, що:

1) без належного ступеня захисту інформації впровадження інформаційних технологій і зокрема, інформаційних систем може виявитися економічно невигідним;

2) забезпечення інформаційної безпеки гарантує збереження конфіденційності, цілісності, доступності з імовірністю, пропорційною витратам;

3) забезпечення інформаційної безпеки повинно бути не одноразовою дією, а постійним процесом.

Враховуючи те, що сучасним СЗІ властивість інтелектуальності не притаманна, основна на сьогоднішній день наукова проблема в області побудови таких систем полягає у забезпеченні автоматизованої або автоматичної підтримки прийняття рішень з усього комплексу вирішуваних ними задач. Це викликає потребу в:

1)формування концепції побудови інтегральної моделі загроз в інформаційному середовищі об'єкта інформатизації, в якій загрози розглядатимуться як канали несанкціонованого доступу, витоку і деструктивних впливів (НСДУВ): з одного боку, на множині елементів фізичного середовища поширення носія інформації,а з іншого боку, на множині компонентів загроз (етапах дій зловмисника);

2) розробленні комплексної методики організаційно-технічного управління захистом інформації на об'єкті інформатизації, що має включати в себе методику синтезу раціональних наборів засобів захисту інформації, що складаються з сумісних програмно-апаратних продуктів та методику чисельної оцінки рівня захищеності інформації на об'єкті інформатизації, засновану на використанні інтегральної структурної вербальної моделі загроз;

3) розробленні алгоритму вибору оптимальних варіантів реагування СЗІ, в якому може бути реалізовано модернізований метод прийняття рішень в умовах ризику в реальному часі з реагування в потенційно небезпечних ситуаціях в умовах невизначеності інформаційних впливів;

4) розробці і впровадженні інфраструктурного ПЗ, в якому мають бути реалізовані математичні методи прийняття рішень з управління СЗІ.

Реалізація комплексу запропонованих заходів дозволить підвищити ефективність захисту периметра на об’єкта інформатизації приблизно на 30%, а сумарний показник захищеності на 5-6%.

к.т.н. Семко В.В.
Дердавний університет телекомунікацій

Концепція топологічного систуаційного аналізу та синтезу в "малому" управління об'єктом в умовах конфлікту, невизначеності поведінки та варіативної множини об'єктів спостереження

В загальному випадку під конфліктом розуміють ситуацію, в якій кожна зі сторін намагається зайняти позицію несумісну з інтересами іншої сторони.

При аналізі конфліктів в технічних системах [1, 2, 3] конфлікт визначається як взаємодія об'єктів (технічних систем) , що мають несумісні цілі і способи їх досягнення, діяльність яких так чи інакше пов'язана з постановкою і рішенням завдань управління, з прогнозуванням і прийняттям рішень, а також з плануванням цілеспрямованих дій.

Дослідження та аналіз об'єктів (учасників) конфлікту здійснюється за методологією системного аналізу, як напряму методології наукового пізнання, в основі якого лежить розгляд об'єктів як систем. При дослідженні конфлікт розглядається як цілісне явище, з певним розмаїттям типів зв'язків між його елементами, об'єктами, системами, зовнішнім середовищем, тощо, які мають бути зведені в єдину теоретичну концепцію, що різнобічно і глибоко відбиває реальні особливості явища конфлікту, яке досліджується [2, 3, 4, 5]..

При дослідженні конфліктів в технічних системах доцільним є застосування :

- системно-структурного аналізу конфлікту, як дослідження явища в цілому, яке складається з системи підструктур, які, у свою чергу, складаються з елементів, і в якості підсистем входить в систему більш високого рівня;
- системно-функціонального аналізу конфлікту, як дослідження з метою визначення усіх основних взаємозв'язків конфлікту із зовнішнім середовищем, в якому конфлікт розвивається, у виявленні характеру і способів впливу одних елементів і підструктур конфлікту на інші (біфуркації).

Для досліджень доцільним є використання інтегрально-топологічних методів аналізу складних нелінійних систем, які базуються на використанні математичних моделей опису властивостей динамічних процесів, пов'язаних з об'єктами як системами. При цьому під інтегрально-топологічними методами розуміють сукупність методів, які базуються на аналітико-комп'ютерних методах, методах нелінійної інтегральної інваріантності, що призначені для одержання топологічних структур просторів спостереження, поведінки та рішення для синтезу та вибору управлінь в "малому".

Надалі при дослідженні методів синтезу та вибору рішень по управлінню об'єктом в умовах невизначеності будемо розглядати оптимізаційні методи та структури об’єкту управління (ОУ), в яких ці методи управління конфліктом в "малому" можуть бути реалізовані.

Я якості методів дослідження застосуємо методи функціонально-структурного аналізу, методи опису топологічних простору пошуку, станів та рішень, методи ситуаційного управління щодо опису моделі взаємодії об'єктів в просторі спостереження та синтезу стратегій (рішень) і вибору рішення в просторі рішень за умов конфлікту та невизначеності.

Інтегрально-топологічні методи дослідження та аналізу складних нелінійних систем в просторі спостереження (ПС) дозволяють виявити характеристики взаємодії кінематичної моделі ОУ та об’єкту спостереження (ОС), які включають параметри безпечного розв'язання конфлікту при синтезі та виборі рішень з врахуванням невизначеності [4], а саме:

- значення припустимої дистанції зближення ОУ з ОС;
- координати ОС в просторі спостереження;
- інтервали часу спостереження ОС в просторі спостереження;
- координати вершин простору спостереження в просторі існування конфлікту;
- координати цільової точки переміщення ОУ в просторі спостереження;
- обмеження кінематичних характеристик ОУ та ОС;
- цілі переміщення ОС.

Зазвичай вирішення задачі взаємодії ОУ з множиною ОС в ПС породжує збільшення розмірності моделі процесу управління і, як наслідок, поліноміальне збільшення складності адекватного до моделі процесу управління, тобто $N = \frac{(m+1)^2}{2} n$, де m - мірність вектору фазових характеристик ОС; n - кількість ОС. Таким чином збільшується час розв'язання задачі конфлікту, що може призвести до ефекту "доміно" та неконтрольованому зростанню часу обчислень. Виходячи з наведених міркувань, можна зробити висновок про те, що інтегральне врахування складності моделі взаємодії ОУ з множиною ОС в ПС призведе лінійного збільшення складності, а саме отримаємо $N = (m+1)n$. Ці міркування складають сутність підходу до розрахунку та формування простору рішень, як підпростору ПС, при вирішенні задачі конфлікту, що дозволяє достатньо просто врахувати топологічну складність конфлікту.

1. Берж К. Общая теория игр нескольких лиц / К.Берж. - М.: Физматгиз, 1961. - 126с.
2. Павлов В.В. Конфликты в технических системах / В.В.Павлов. - К: Вища школа, 1982. - 184с.
3. Павлов В.В. Начала теории эргатических систем / В.В.Павлов - К.: Наук. думка, 1975. - 240с.
4. Семко В.В., Модель конфлікту взаємодії об’єктів кібернетичного простору / В.В.Семко //Проблеми інформатизації та управління. - 2012. - Вып. 2(38). - С.88-92.
5. Семко В.В. Применение метода интегрального усечения вариантов при синтезе стратегий управления подвижным объектом / В.В.Семко, В.В.Павлов //Кибернетика и вычислительная техника. - 1989. - Вып. 84. - С.1-6.

к.е.н., доцент Іщук Г.П.
Державний університет телекомунікацій

Особливість оцінювання результатів АІБ промислових та фінансових організацій

Специфіка оцінювання результатів АІБ у промислово-фінансових організаціях за об'єктивними і суб'єктивними причинами створення проблем в ІС.

Обсяг послуг в Україні, наданих суб'єктами телеком-ринку за січень-жовтень 2014 р. склав 59,44 млрд. грн., в т.ч. населенню - 16 млрд. грн. Приріст у порівнянні з аналогічним періодом 2013 р. склав 35,6 млн. грн. Послуг телеком-компаній за десять місяців 2014 р. надано на 40,67 млрд. грн, в т.ч. населенню - 14,4 млрд. грн. Комп'ютерного програмування і надання інших інформаційних послуг - 11,35 млрд. грн. (в т.ч. населенню - 474,9 млн. грн). Приріст на ринку ІТ склав 31% (2,68 млрд. грн). Основою ефективності будь-якої сучасної діяльності є довіра до інформації і впевненість суб'єктів бізнесу в надійності ІБ. Вона пронизала народне господарство, галузі, інфраструктуру. Розвиток ІТ сприяє одержанню надприбутків організаціями різних форм власності але примножує ризики їх діяльності. Проблеми ІБ насамперед залежать від розвитку ІТ, які в економічних сферах різні. Якщо, наприклад, у промислового підприємства раптом зникне вся інформація, у нього залишиться вироблена продукція, яку можна продати і створити нову ІС. Тобто у підприємства залишається можливість повного чи часткового відновлення своєї діяльності, оскільки його ІС менш інтегрована у спосіб виробництва.

Фінансово-кредитні установи відрізняються тим, що їх засоби складаються з позичених та виданих у позику. Якщо ці установи раптово опиняються без своєї ІС - вони одночасно втрачають головні засоби виробництва і свою «пам'ять». Гроші та інформація – речі нематеріальні, виконують лише роль сировини у виробництві банківських послуг. Можна стверджувати, що, інформатика не просто супроводжує виробничий процес, який у випадку несправностей може стати менш ефективним без неї, а сама по собі є цим процесом. Забезпечення безпеки систем збору, обробки, зберігання і передачі інформації про кредитно-фінансові потоки стало обов'язковою умовою для взаємозалежних галузей економіки: галузеві ризики можуть створити серйозні наслідки для економіки країни, стати можливим фактором породження в ній системної кризи. Для безпеки ІС бізнесу організацій характерні наступні основні фактори (вразливості), які можуть бути джерелами інформаційних ризиків: 1) велика змінність, безперервне удосконалення ПЗ; 2) неадекватна складність операційного середовища щодо завдань вирішення; 3) інформаційна та телекомунікаційна потужності на мікро-, мезо-, макро- економічних рівнях багаторазово перевищують кількість клієнтських електронних платежів, об'єктивно створюючи, ресурсний дефіцит.

Особливість АБС в тому, що вона розвиваються з суб'єктивних причин (бажань) підтримати змінність системи, не як спеціалізована, а супер універсальна система, яка вимагає обов'язкової ресурсної і функціональної надлишковості. Із збільшенням змінності АБС постійно зростає надлишковість, особливо із часом. Чим менше часу відводиться практично на реалізацію змінності, тим більше потрібно ресурсної надлишковості. Будь-яка надлишковість, з точки зору фахівців ІБ, небезпечна - особливо функціональна, оскільки вона є внутрісистемною і не піддається блокуванню чи контролю. Таким чином, практично склалася ситуація, коли функціональна надлишковість АБС багаторазово перевищує реальні потреби з усіма наслідками, що витікають з цього. Взагалі, безпека - це прагнення порядку (ролі і відповідальності, прав і обов'язків). Із незначної кількості діючих специфічних для безпеки методів (стандартів забезпечення безпеки на різних стадіях життєвого циклу систем, процесів, продукції, довіри до персоналу тощо), кожен підсилює впевненість у ІБ, зменшує невизначеність (ризик). Це спонукає передбачати не тільки заходи, пов'язані з ІТ (криптозахист, програмні засоби адміністрування справ користувачів, їхньої ідентифікації і аутентифікації, «брандмауери» для захисту входів-виходів мережі тощо, але і адміністративного, технічного характеру, включаючи жорсткі процедури: 1) контролю фізичного доступу до АБС; 2) синхронізації й обміну даними між модулем адміністрування безпеки АБС і системою охорони. Усі дослідження у сфері ІБ об'єднані та сформовані на чотирьох рівнях її підтримки: законодавчому, адміністративному, процесуальному, технічно-програмному. Із великої кількості методів довіри, орієнтованих на різні сутності безпеки (або їх об'єднання) насправді небагато прямо чи опосередковано (непрямо) можуть стосуватися ІБ. Наприклад, такий метод довіри як сертифікація системи менеджменту якості організації ІСО 9000, може опосередковано сприяти формуванню довіри ІБ. Хоч він був розроблений для промислових підприємств, проте містить елементи довіри до процесу, що може застосовуватись для ПЗ, по суті, програмних продуктів і систем безпеки. Взагалі, будь-які превентивні заходи, що зменшують невизначеність, надають переконливі дані щодо їх правильності або/і додають, підвищують впевненість, формують основу довіри безпеки. Замовник АІБ або керівництво організації, яку перевіряють, в аудиторському висновку одержує: кількісну та якісну характеристику стану ІБ; рівень використання результатів АІБ та СІБ; упевненість у результатах; простоту розуміння результатів; виконання положень моделі оцінки; точність процедур оцінювання; повторюваність і відтворення результатів. За результатами АІБ та СІБ створюється модель прийняття рішень з планування і реалізації превентивних заходів, корекції процесів системи забезпечення ІБ.

Рівень використання результатів АІБ (модель) керівництвом організації або відповідальним за забезпечення ІБ буває різним, інколи навіть не використовується. Впевненість замовника в результатах АІБ залежить від багатьох факторів: а) правильно підібраних і використаних методів вимірювання, показників та моделей їх об'єднання; б) правдивої інтерпретації результатів; в) виконання аналітичних процедур, що попереджують спотворення даних та їх невірну інтерпретацію; г) гарантії у професіоналізмі аудиторів; д) регулярної участі в консультаціях і обговоренні проміжних результатів оцінювання; е) своєчасності перевірок, які мають проводитися за графіком, встановленим за програмою АІБ; є) ефективності перевірки, яка оцінюється співвідношенням витрат на виконання

процесу АІБ і цінності інформації, яку він надає; ж) задоволення споживача, що залежить від якості і ефективності проведення АІБ та рівня очікуваної вигоди від виконання процесу. У результатах АІБ його замовник переконується тоді, коли розуміє категоріальний апарат аудитора і запропонований алгоритм визначення значення показників, сприймає лаконічні пояснення логічних висновків і точність рекомендацій, може самостійно відслідкувати відповідність процесу. Замовник АІБ має знати, що зміна послідовності, підміна його процедур може призвести до втрати або підміни даних, невірних результатів, неправдивої їх інтерпретації. Виконання положень моделі оцінки замовник АІБ має самостійно чітко оцінювати за послідовністю процедур вимірювання, шкалою вимірювання, одиницями вимірювання і моделлю об'єднання показників. Точність процедур оцінювання сторін АІБ заслуговує на особливу увагу і залежить від :

- суб'єктивного фактору (неякісне виконання процедур керівником, виконавцем, аудитором);
- методу вимірювання (ручного, автоматизованого);
- помилки (систематичної, випадкової);
- вибіркового використання джерел свідоцтва аудиту;
- невідповідності одержаних (вхідних) даних;
- відсутності даних, що знаходяться у межах визначених значень порогу;
- різного рівня компетентності осіб, що беруть участь у процедурі вимірювання;
- компетентності аудиторів, що не відповідає вимогам;
- проведення модернізації (або зміни) інструментальних засобів, що призвело до зміни алгоритму визначення значення показників, не відповідному моделі оцінки.

Фахівці ІБ, після події 11.09.2001р., звернули особливу увагу на необхідність розвитку нового виду - аудиту управління безперервністю бізнесу і його відбудови після збоїв. Це виправдано, оскільки щорічно збільшується число таких інцидентів, як: теракти, збій телекомунікаційних та енергетичних систем, серверів, форс-мажорних обставин, примусової евакуації, техногенних катастроф тощо. Життя показало, що однією з основних компонент виживання успішного бізнесу в екстремальних умовах є наявність підготовлених технічних рішень, діючого плану безперервності бізнесу, а також впровадження корпоративних регулюючих норм у сфері підтримки неперервності. Так виникли нові плани: а) План безперервності бізнесу; б) План відбудови після збоїв (складова частина попереднього плану). План «Управління безперервністю бізнесу» включає процеси, методи, техніку управління, спрямовані на забезпечення безперервності функціонування критичних бізнес-процесів.

Щодо ситуації з ІБ в Україні, за даними НБУ, близько 60% вітчизняних комерційних банків перебувають у повній або частковій власності компаній, зареєстрованих в офшорних зонах. Тому питання ІБ, зокрема АІБ банківської системи України, на сьогодні набуває особливої актуальності.

Список використаних джерел

1. Курило А.П., Зефиров С.П., Голованов В.Б. и др. Аудит информационной безопасности. М.: Изд. группа «БДЦ-пресс»,- 2006,- 304 с. , с вкл..
2. Постанова НБУ від12 листопада 2002 р. «Про затверджене Інструкції про складання проміжної (квартальної) фінансової звітності банків України».
3. Доктрина інформаційної безпеки України. Затверджено Указом Президента України від 8 липня 2009 р. № 514/2009.
4. Закон України «Про концепцію національної програми інформатизації» від4 лютого 1998 р.№ 75/98-ВР// Відомості ВРУ.-1998.-№27-28.-ст.182.
5. ИТ-компании в Украине нарастили предоставление услуг на 31%. 24.11.2014 р. ЛІГАБізнесІнформ. www.liga.net

к.е.н., доцент Г.П. Іщук
Державний університет телекомунікацій

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ІНФОРМАЦІЙНО-ЕКОНОМІЧНОЇ ХАОТИЧНОСТІ

Розглядається зарубіжний досвід вивчення та вирішення проблем управління інформаційною безпекою в умовах турбулентної економіки в якій повинні працювати компанії ефективно і стабільно.

Коли в країні зникають стабільність і прогнозованість та починають діяти протилежні, нещадні сили, що ведуть її до спаду або затяжної кризи, є необхідність у створенні системи, яка б застрахувала від ризиків і відреагувала на невизначеність. У розвинених країнах вона вже створена, працює і має назву - система хаотики (раннього попередження і розроблення сценарію швидкого реагування на інциденти під час спадів та турбулентності). В сучасних умовах всі країни живуть з ризиком (що вимірюється) та невизначеністю (що не вимірюється) і більшість

компаній працює в умовах самовідновлювальної рівноваги без системи хаотики а УІБ в них розрізнене та недостатнє. Турбулентність завжди супроводжується хаосом, ризиком, невизначеністю, агресивністю, неспокійною поведінкою, що нині стає новою нормальністю для галузей, ринків, компаній. Така «нормальність» з періодичними, стрибкоподібними сплесками процвітання і тривалого спаду, досягає кризи або навіть депресії. Зарубіжна практика свідчить, що турбулентність має одночасно два основних ефекти. Перший ефект – уразливість, від якої компанії потребують захисту, другий - можливість, яку потрібно використати. Для одних компаній період спаду - це скрутний час, а для інших – це час можливостей. Чередування позитивних та негативних змін створює турбулентність - явище, що властиве майже всіх країнам створеними новими умовами буття, нової «нормальності".

В Україні інформаційно-економічні умови постійно нестабільні і звикати бізнесу до світової „хаотики" не надто складно - в цих умовах він вже працює. У поняття „хаотика" (походить від англ.) закладено більш глибоке поняття ніж в його слово-прообраз „хаос". Воно включає і хаотичний стан – оточення компанії, в якому вона функціонує, і систему управлінських дій, яких керівництво має дотримуватись та впроваджувати на різних рівнях. Така «нормальність» виходить за межі проривних інновацій і включає великі потрясіння та жорсткість. Хаотика пропонує нові потужні сили для рішучого і якнайшвидшого подолання підвищених рівнів турбулентності та хаосу. У кожній компанії наступає стратегічно переломний момент, коли стара стратегія не спрацьовує і потребує заміни на нову із забезпеченням подальшого стабільного функціонування. Якщо УІБ не зможе ефективно працювати під час хаосу, компанія швидко слабшатиме або загине. Через хаос і страх все втратити зростає відхилення від норми в глобальних розмірах і щоб вижити обов'язково має підвищитися рівень прозорості управлінських рішень на всіх рівнях, жорсткість та ретельність перевірки з боку керівництва компанією. В цей період абсолютної невизначеності від керівництва вимагається оперативно реагувати на внутрішні, міждержавні та світові економіко-інформаційні події. Стратегічно переломні моменти відбуваються дедалі частіше і компаніям доведеться оперативно їх виявляти та реагувати. До критичних факторів, які спричиняють хаос та ризики в бізнесі зарубіжні фахівці відносять: а) технічний прогрес та інформаційну революцію; б) руйнівні технології та інновації; в) швидке зростання інших суб'єктів інформаційного ринку та гіперконкуренцію; г) державні інвестиційні фонди; д) довкілля; е) підвищення компетентності учасників ринку та ін. Між бізнес-циклами в часи нормальної економіки та турбулентної економіки можна побачити такі контрасти.

Ознака	: Нормальна економіка	: Економіка нової «нормальності»
Економічні цикли	передбачувані	немає
Зростання/різкі зростання	визначаються (5-7 років)	непередбачувані, мінливі
Спади, кризи	визначаються (10 років)	непередбачувані, мінливі
Можливий вплив факторів	низький	високий
Загальна структура інвестицій	розширюються, широкі	обережні, цільові
Ставлення до ринкового ризику	прийняття	уникнення
Стан споживачів	упевненість	невпевненість
Уподобання клієнтів	стійкі, еволюціонують	страх, прагнення безпеки

Як застерігав Шумпетер Й., що радикальні інновації призводять до „творчого руйнування" на стільки, наскільки потрібні динамічній економіці. Руйнівна технологія змінює правила, що уможливить створення хаосу в усій галузі, особливо це стосуватиметься «старожилів», які не приділяти уваги турбулентності, що непомітно наростала аж поки не стало надто пізно. Прорив відбувається тоді, коли продукт відповідає новому або зростаючому сегменту ринку, який не обслуговується існуючими компаніями галузі. Гіперконкуренція відбувається тоді, коли технології або продукти настільки нові, що спонукають до зміни стандартів та правил, у результаті чого конкурентні переваги не можуть бути довготривалими. Швидкість руйнівної турбулентності створеної гіперконкуренцією, управляється глобалізацією. Привабливішою є продукція, більш сегментована на смаки споживачів, припиненням регулювання та винайденням нових бізнес-моделей, усім, що спричиняє структурну неврівноваженість, падіння бар'єрів для входження на ринок та усунення промислових лідерів. У зарубіжній літературі визначено стратегії гіперконкуренції для руйнування. 1. Задоволення зацікавленої сторони – ключ до завоювання кожної динамічної взаємодії з конкурентами. 2. Стратегічне передбачення – процес пошуку нових знань для прогнозування майбутніх потреб споживачів. 3. Швидкість є вирішальною, щоб скористатися можливостями та відреагувати на контратаки конкурентів. 4. Несподіванка збільшує здатність компанії приголомшувати конкурентів, зайняти кращу позицію до того, як конкурент зможе нанести відповідний удар. Також визначено тактику гіперконкуренції для руйнування. 1. Сигнали, що оголошують стратегічний намір домінувати на ринку або маніпулювати майбутніми ходами суперників. 2. Правила зміни ринку, що створюють величезні руйнування для конкурентів. 3. Одночасні або послідовні атаки , що використовують різні дії, щоб ввести в обману або задурити голову конкуренту.

В умовах хаосу конкурентні переваги нетривалі і перевага у тих, хто знаходить можливості за існуючих умов, якими б вони не були. По суті, це природний відбір хаосом, в ході якого вирішується які компанії стануть переможцями, а які програють. У сучасному світі не сховатися, а достовірність - це ключ, і якщо є хоч одна ознака недостовірності новини поширюються між споживачами як вірус, ось чому планування послуг таке важливе. У розвинених країнах будь-яку компанію сприймають лише як послугу, а люди купують її досвід, а не продукт чи послугу. Якщо досвід не виправдовує очікувань, компанія заплатить високу ціну. Компанії, які виготовляють неякісні вироби або послуги, зникають швидше, ніж раніше. Прогресивні компанії частіше вчаться миттєво

удосконалювати навички, системи, процеси, заходи щодо регулювання, виявлення і передбачення турбулентності у своєму середовищі та визначення слабких місць, уразливостей і можливостей, які створює хаос. Звідси можемо винести уроки. Перший - ризик вимірюється, а отже, може бути керованим, а невизначеність - ні. Другий - у світі блискавично посилюється взаємозалежність і взаємозв'язок. Якщо певна компанія професійно, якісно моделює і прогнозує ситуацію, будь-хто з її акціонерів може створити турбулентність, яка може швидко зруйнувати компанію. Третій - хаос може гарантувати усім керівникам, фахівцям з ІБ, командам менеджерів відсутність гарантій. До найпоширеніших помилок, яких припускаються лідери бізнесу в період турбулентності, відносять рішення стосовно: а) розподілу коштів, що руйнують основну стратегію та корпоративну культуру; б) скорочення витрат за всіма напрямами замість цілеспрямованих та виважених дій; в) збереження непродуманого руху грошових коштів, що створює ризик для основних партнерів; г) скорочення витрат на збут, бренд та розроблення нової продукції; д) зменшення обсягу продажів та цінові знижки; е) віддалення від клієнтів через зниження витрат на збут; є) скорочення витрат на навчання та розвиток під час економічної кризи; ж) недооцінювання постачальників та дистриб'юторів.

Приймаючи швидкі непродумані рішення, ризик неефективного УІБ загрожує компанії. З другого боку, загальне скорочення персоналу – завжди помилка. Із закінченням кризи, дефіцитним ресурсом для більшості компаній будуть талановиті працівники, а не капітал. До найбільших маркетингових помилок, яких часто припускаються компанії і яких варто уникати відносять: а) прагнення залучити нових клієнтів, ігноруючи основних; б) скорочення витрат на маркетинг; в) приховування правдивої інформації від клієнтів компанії та зацікавлених сторін.

В період турбулентності інформаційного-економічного середовища, компанія може припуститися таких найбільших помилок: звільнення талановитих працівників; скорочення витрат на технології; зниження ризиків; припинення розроблення продукції; заміна керівників, орієнтованих на зростання, на керівників, які скорочують витрати; відхід від глобалізації; відмова керівництва від інновації як основної стратегії; зміна показників результативності; посилення ієрархії замість співпраці; замикання у чотирьох стінах.

У літературі знаходимо перелік помилок, яких найчастіше припускаються компанії стосовно своїх партнерів у період турбулентності: дублювання функцій; складні контракти; неоптимальні системи оцінювання продуктивності; недостатнє розроблення продукції /специфікацій; процес вибору відповідно до єдиного критерію; фізичне віддалення від ключових постачальників та дистриб'юторів; збереження надто великої кількості постачальників; відмова від інвестування в навчання постачальників та дистриб'юторів; відмова від інвестування у зв'язок з постачальниками і дистриб'юторами.

У період хаосу традиційний трирічний стратегічний план застаріває і стає непридатним для використання. Традиційний підхід до розроблення стратегії потребує точних прогнозів, що часто призводить до недооцінювання керівниками невизначеності та хаосу, зумовлених непередбачуваною та повторною турбулентністю з її раптовими та непостійними змінами. Сучасне УІБ вимагає нового напряму думок, ефективного планування, правильних стратегій та сміливості відійти від традиційного мислення. Турбулентність може відбуватися на макрорівні (світова економіка, регіональна чи економіка країни) і на мікрорівні (в окремій галузі чи компанії). Передбачити її неможливо, отже визначення її ознак на ранній стадії стає одним з вирішальних факторів успіху компанії в майбутньому. Лідери бізнесу мусять оцінювати всю сукупність макроекономічних результатів, створювати таку ж сукупність сценаріїв з відповідними стратегічними реакціями, а потім вживати заходів, щоб їхні компанії реагували швидше, були більш стійкими та життєздатними. Кожній компанії доводиться враховувати додаткові тенденції та події як на галузевому рівні, так і на рівні компанії, щоб урізноманітнити сценарії поведінки. Менеджерам доведеться як найшвидше створити стратегічні та тактичні варіанти захисту та нападу для найбільш ймовірних сценаріїв. Коли компанія розвивається через дію хаотики, мета – досягнення компанією високого рівня стабільності. В літературі знаходимо стислий перелік напрямів поведінки, які можуть бути корисними в умовах прискорення темпу змін: особисте залучення керівництва теж має зростати, для розуміння суті справ і «вимкнення» ним фільтрів та цензури. Лідери бізнесу повинні усвідомити невідповідність стратегії новим умовам.

Керівництво не повинно покладатися на двосхемну стратегію (одна схема для економічного зростання, друга – для спаду), яку треба постійно корегувати, або навіть відкинути, якщо цього потребує ринкова ситуація. Ця стратегія , що придатна для нормальних ситуацій, зовсім непридатна для хаосу. Управління в умовах хаотичності – це систематизований підхід до виявлення, аналізу та реагування на турбулентність та хаос, а система управління складається з таких елементів як: виявлення джерел турбулентності через створення систем раннього попередження; реагування на хаос через створення ключових сценаріїв; вибір стратегії, що ґрунтується на визначенні пріоритету сценарію та ставлення до ризику. Оскільки турбулентність виникає несподівано, її можна лише частково виявити або не виявити і одразу слід управлінцям ІБ вирішити які її прояви можна використати на користь фірмі, а які мінімізувати або навіть усунути, інакше в компанії виникне хаос. Лідери бізнесу, створюючи формальну систему раннього попередження, передусім розглядають інформацію про інфокомунікаційний ринок, яку раніше не розглядали і згодом сприйняли як сюрприз. Більшість несподіванок трапляється не через недостатню кількість ранніх ознак, а через невміння їх розпізнавати. Ключові напрями, які треба контролювати включають покупців та канали збуту, конкурентів та виробників товари-замінники, впливових осіб, найновіші наукові розробки та технології, політичні, правові та соціальні сили.

Розроблення превентивних заходів та системи раннього попередження і реагування на думку більшості зарубіжних теоретиків та практиків потребує вивчення, обговорення і дослідження планових демографічних показників та урядової політики. Коли керівництво починає розглядати створення ефективної системи раннього попередження ІІІБ в своїх компаніях, потрібно визначитися із завданнями. Окрім попереджень та сигналів тривоги, ці завдання мають включати виявлення та зниження ризику, невизначеності та вразливості, а також розпізнавання та використання можливостей.

Актуальним завданням є підвищення поінформованості та навчання персоналу УІБ в компаніях, оскільки переважно керівники бачать ранні ознаки але не вміють зрозуміти їх значущості та реагувати на них.

Література

1.Діброва Т.Г. Маркетингова політика / Навч. посібник/ Т.Г.Діброва.-К.: Видавничий дім «Професіонал».2009.-320с.

2.Котлер Ф., Дж.А.Касліоне. Хаотика: управління та маркетинг в епоху турбулентності. (пер. з англ.).-К.: Хімджест, ПЛАСКЕ.-2009.-208с.

3.Пацалюк К.О. Маркетингові комунікації в сучасних умовах менеджменту. Вісник ЖТДТУ .2013.№1(63). С.294-295.

4. www.management.com.ua/interview/int190html.

І. В. Мордас
Державний університет телекомунікацій

НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

На сучасному етапі глобальних трансформацій загострюються суперечності та диспропорції у питаннях реформування усіх сфер суспільства, що зрештою веде до створення комплексу відповідних загроз національним інтересам в інформаційній сфері. Це створює нагальну необхідність їх конкретизації та формування дієвих механізмів забезпечення, що і визначає актуальність теми і мету дослідження.

Сьогодні можна виділити чотири основні складові національних інтересів України в інформаційній сфері.

Перша складова полягає у дотриманні конституційних прав і свобод громадян України щодо отримання інформації і користування нею. Для цього необхідно:

- підвищити ефективність використання інформаційної інфраструктури держави;
- удосконалити систему формування, зберігання і використання інформаційних ресурсів;
- оптимізувати механізми правового регулювання відносин в інформаційній сфері.

Друга складова полягає в інформаційному забезпеченні державної політики України. Для цього необхідно:

- зміцнити довіру до державних засобів масової інформації;
- прискорити формування відкритих державних інформаційних ресурсів.

Третя складова полягає у розвитку сучасних інформаційних технологій та вітчизняної індустрії інформації. Для цього необхідно:

- удосконалювати інфраструктуру єдиного інформаційного простору України;
- розвивати вітчизняну індустрію інформаційних послуг;
- розширювати виробництво конкурентоспроможних інформаційних продуктів;
- забезпечувати державну підтримку вітчизняних наукових досліджень в інформаційній сфері.

Четверта складова полягає у надійному захисті інформаційних ресурсів від несанкціонованого доступу та технічних розвідок, а також забезпеченні безпеки інформаційних систем. Для цього необхідно:

- прискорити розвиток вітчизняного виробництва апаратних і програмних засобів захисту інформаційних ресурсів;
- розширювати міжнародне співробітництво щодо розвитку, безпечного використання і протидії загрозам в інформаційній сфері.

Сьогодні лише системний аналіз усіх чотирьох складових національних інтересів України в інформаційній сфері та реалізація запропонованих заходів може гарантувати забезпечення національної безпеки та вихід держави на якісно новий інформаційний рівень.

Семко О.В.
Національний авіаційний університет

Інформаційно-телекомунікаційна система видачі медичних довідок

Впровадження інформаційно-телекомунікаційної системи (ІТС) видачі медичнгих довідок водіям і кандидатам у водії транспортних засобів забезпечує виконання вимог щодо удосконалення діяльності медичних комівсій та сприяє вдосконаленню медичного забезпеченню у сфері безпеки дорожнього рухудорожнього руху.

Технологічні рішення, впроваджені в ІТС, дозволяють значно скоротить часові та матеріальні витрати, а також вирішити проблему нестачі кваліфікованих фахівців з інформаційних технологій в медичній галузі.

Мета і актуальність створення та впровадження ІТС обумовлена необхідністю:

- вдосконалення медичного забезпечення безпеки дорожнього руху, визначення здатності кандидатів у водії і водіїв до безпечного керування транспортними засобами, відсутності у водія медичних протипоказань до керування засобом відповідної категорії, попередження причин та умов виникнення дорожньо-транспортних пригод;

- забезпечення діяльності медичних комісій з оглядів кандидатів у водії та водіїв транспортних засобів, обліку забезпечення та використання закладами охорони здоров'я бланків Медичної довідки щодо придатності до керування транспортним засобом;

- забезпеченням взаємодії з іншими інформаційно-телекомунікаційними системами при отриманні похідних даних;

- забезпеченням взаємодії з інформаційно-телекомунікаційними системами ДАЇ МВС України та інших міністерств та відомст України в межах їх компетенції;

- оприлюднення інформації щодо оглядів кандидатів у водії та водіїв транспортних засобів, обліку забезпечення та використання закладами охорони здоров'я бланків медичної довідки щодо придатності до керування транспортним засобом в межах діючого законодавства України.

Виходячи з того, що ІТС призначена для збирання, накопичення, зберігання, обробки, надання медичної інформації та персональних даних, для автентифікації та ідентифікації суб'єктів і об'єктів системи, також забезпечення вимог цілісності, конфіденційності, доступності та спостережності застосовуються носії ключової інформації (НКІ).

Основними інформаційними потоками ІТС при обміні повідомленнями між об'єктами та суб'єктами ІТС є такі що забезпечують:

- взаємодію кандидатів у водії та водіїв з персоналом медичної комісії при проходженні медичного огляду та формування відповідного документу щодо результатів медичного огляду лікарями медичної комісії;

- взаємодії автоматизованих робочих місць (АРМ) видачі медичних довідок, які розміщуються в медичних комісіях при проведенні медичного огляду кандидатів у водії та водіїв транспортних засобів з програмно-апаратним комплексом (ПАК) ІТС відповідних підрозділів МОЗ України.

Дані від медичної комісії, як суб'єкту ІТС, проходіть автентифікацию, ідентифікацію, дешифрування і у підписаному електронним сертифікатом (електронною печаткою) вигляді за електронним цифровим підписом підсистеми ведення баз даних (ПВБД) заносяться до бази даних (БД) з унікальним реєстровим номером, який є похідним від даних про медичну комісію.

Після розміщення в БД ПВБД надсилає в АРМ видачі довідок номер довідки, підписаний ЕЦП ПВБД та зашифрований з використанням НКІ. Після розшифрування номеру довідки здійснюється її друк на бланку.

к.т.н., с.н.с. Курченко О. А., Храпач Г.С.
Державний університет телекомунікацій

Аспекти забезпечення інформаційної безпеки на підприємстві

Система інформаційної безпеки кожного підприємства цілком індивідуальна. Її повнота та дієвість залежать від існуючої в державі законодавчої бази, від обсягу матеріально-технічних та фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості забезпечення безпеки бізнесу, а також від досвіду роботи керівників служб безпеки підприємств.

Надійний захист інформаційних активів підприємства можливий лише при комплексному та системному підході до побудови та організації системи інформаційної безпеки.

В свою чергу система інформаційної безпеки підприємства представляє собою комплекс організаційно-управлінських, режимних, технічних, профілактичних и пропагандистських заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.

Інформаційна безпека підприємства повинна оцінюватись з урахуванням умов, обмежень і критеріїв усіх основних учасників його діяльності, а саме: держави, підприємств-конкурентів, споживачів [2].

Серед існуючих засобів забезпечення інформаційної безпеки підприємства можна виокремити наступні:

1) Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо.

2) Організаційні засоби. Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства.

3) Інформаційні засоби. Передусім це друкована і відеопродукція з питань збереження конфіденційної інформації.

4) Фінансові засоби. Без достатніх фінансових коштів не можливе функціонування системи інформаційної безпеки підприємства, питання лиш в тому, щоб використати їх цілеспрямовано та з високою віддачею.

5) Правові засоби. Підприємство повинне у своїй діяльності керуватися не лише виданими вищестоящими органами влади законами та підзаконними актами, але й розробляти власні документи з питань забезпечення інформаційної безпеки підприємства.

6) Кадрові засоби. Підприємство повинне бути забезпечене кадрами, що займаються питаннями інформаційної безпеки.

7) Інтелектуальні засоби. Залучення до роботи кваліфікованих спеціалістів, наукових робітників, що дозволяє модернізувати систему безпеки підприємства.

Одночасне впровадження усіх цих засобів неможливе. Воно проходить в кілька етапів:

I етап. Прийняття рішення на створення системи інформаційної безпеки та виділення фінансових коштів.

II етап. Формування кадрових і організаційних засобів.

III етап. Розробка системи правових засобів.

IV етап. Залучення технічних, інформаційних та інтелектуальних засобів.

Відповідно можна виділити технічні, інформаційні, фінансові, правові, інтелектуальні методи, сутність яких полягає в наступному:

1. технічні - спостереження, контроль, ідентифікація;

2. інформаційні - складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо;

3. фінансові - матеріальне стимулювання працівників, що мають досягнення в забезпеченні інформаційної безпеки підприємства;

4. правові - судовий захист законних прав і інтересів, сприяння діям правоохоронних органів;

5. кадрові - підбір, навчання кадрів, що забезпечують інформаційну безпеку підприємства;

6. інтелектуальні - патентування, ноу-хау тощо.

Слід також відзначити, що важливим елементом організації інформаційної безпеки є поділ заходів на групи. У теорії та практиці виділяють такі три групи: активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні (охоронні) засоби (наприклад, встановлення екранів проти несанкціонованого витоку інформації тощо); комплекс засобів підтримки - органічне поєднання попередньо вказаних груп щодо моделювання потенційних (невідомих раніше практиці) загроз.

Ураховуючи міжгалузеву сутність теорії організації інформаційної безпеки в умовах формування глобальної кіберцивілізації, в ній поєднуються методи пізнання традиційних фундаментальних наук: соціології та фізики, які концентруються у такій науці, як кібернетика. Це зумовлено безпосередньо предметом теорії: людино-машинними (соціо-технічними) системами, провідними з яких є комп'ютеризовані інформаційні системи, в тому числі телекомунікаційні.

Через наявність людського фактору як провідного теорія організації інформаційної безпеки як система знань має предметний гіперзв'язок з такими фундаментальними гуманітарними науками, як соціологія, соціальна психологія, правознавство тощо.

У даному аспекті визначається також напрям теорії щодо оцінки, характеристики зловмисників, які посягають на безпеку інформаційної системи [3].

Таким чином, інформаційна безпека на підприємстві це комплексне поняття, що містить в собі достатньо різнопланові аспекти. Воно включає в себе засоби фізичної перешкоди доступу зловмисників до захищеної інформації, керування доступом за допомогою регулювання ресурсів інформаційних систем та технологій, криптографічне закриття інформації, використання антивірусних програм, файерволів та інших засобів протидії шкідливим атакам[1].

Список використаних джерел

1. Ортинський В.Л. Економічна безпека підприємств, організацій та установ : навч. посібник [для студ. вищих навч. закладів] /[В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін.] ─ К.:Правова єдність ,2009. ─ 544 с.

2. Братель О. Поняття та зміст доктрини інформаційної безпеки //Право України. - 2006. - № 5. - С.36-40

3. Бут В.В. Проблеми безпеки в інформаційній сфері - сутність понять та їх термінологічне тлумачення //Науковий вісник Національної академії внутрішніх справ України. - 2003. - № 5. - С. 225-232.

Акімов.А.О.
Державний університет телекомунікацій

Забезпечення інформаційної безпеки у сучасному світі

Актуальність даної статті полягає в тому, що на сучасному етапі основними реальними і потенційними загрозами інформаційній безпеці є прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожує сталому і безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Зросли зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також через Інтернет.

Мета статті - проаналізувати інформаційну безпеку в контексті проблем національної безпеки.

Завдання статті: дослідити співвідношення понять "національна безпека" і "інформаційна безпека", розглянути сутність інформаційного протиборства в сучасному світі.

Як відомо, вперше в політичному лексиконі поняття "національна безпека" було використано в посланні президента Т. Рузвельта Конгресу США в 1904 р., де він обгрунтував приєднання зони Панамського каналу до національних інтересів Сполучених Штатів Америки. Даний факт слугував поштовхом в науковому осмисленні національних інтересів в контексті національної безпеки. Тому невипадково деякі з дослідників-юристів підкреслюють політичне походження даного поняття, "що, з одного боку, обумовлює його нерозривний зв'язок з державною діяльністю і державною політикою, а з іншого - створює певні труднощі при правовому регулюванні пов'язаних з нею питань через декларативність та нестабільнісь деяких її аспектів".

Уперше поняття "національна безпека" та "національні інтереси" на законодавчому рівні були визначені в "Концепції (основах державної політики) національної безпеки України", яка була прийнята Верховною Радою України. У ній визначається, що захист національної безпеки є однією з найважливіших функцій держави. У цьому контексті інформаційна безпека, як невід'ємна складова національної безпеки, потребує свого забезпечення на державному рівні, оскільки протягом усієї історії розвитку людства інформація розглядалася як важливий військовий, політичний, економічний і соціальний фактори, що значною мірою обумовлює розвиток держави, суспільства і особистості в конкретних історичних умовах.

На думку українського ученого Б.Корміч, "національна безпека представляє собою стан захищеності гарантованих законодавством розумів життєдіяльності держави, суспільства та окремої особини від внутрішніх та зовнішніх загроз. Підтримання національної безпеки

Є важливим напрямком державної діяльності, що актуалізується в залежності від наявності та ступеня відповідних загроз".

Український дослідник Ю. Максименко пропонує визначати національну безпеку як результат управління реальними або потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави.

У цілому, до основних проблем, які несуть ризики й загрози національній безпеці України, експерти відносять такі явища, властиві багатьом державам, як: боротьба за енергоресурси, техногенні катастрофи, міжнаціональні й міжконфесійні конфлікти, тероризм, наркоторгівля, організована злочинність і корупція, нелегальна міграція, торгівля людьми, демографічні проблеми тощо. Особливу загрозу становлять тенденції консолідації національних і міжнародних злочинних угруповань, об'єднання кримінальної злочинності з націоналістичними й екстремістськими угрупованнями.

Активізація терористичної діяльності, яка все більше набуває глобального характеру, посилює небезпеку для будь-якої окремо взятої країни і пов'язується переважно з міжнаціональними й міжконфесійними конфліктами й сепаратистськими рухами. Терористичні організації перетворилися на інструмент досягнення певних політичних цілей і, дуже часто, високоприбуткового злочинного бізнесу. Повсякчасна загроза міжнародного тероризму трансформувалася в один з основних викликів світовій цивілізації.

Перехід ряду держав в постіндустріальну фазу суспільного розвитку сприяє швидкому розвитку комунікативних технологій, що підсилює потребу в боротьбі за здобуття якісної інформації. Новий вигляд безпеки - інформаційна безпека. Її відмінність від інших складових національної безпеки в нематеріальності. Таким чином, на державному рівні виникає потреба в додаткових матеріальних витратах з боку компетентних органів влади в її перевірці. Як відзначають дослідники, "інформаційна складова не може існувати поза цілями загальної національної безпеки, так само як і національна безпека не буде всеохоплюючою без інформаційної безпеки".

Інформаційна сфера є в даний час системоутворюючою сферою життя суспільства. З цієї причини вона активно впливає на стан політичної, економічної сфери, а також інших складових національної безпеки. У політичній сфері все більшої значущості набуває інформаційно-психологічна дія з метою формування стосунків в суспільстві, його реакції на процеси, що відбуваються. у економічній сфері зростає уразливість економічних структур від невірогідності,запізнювання і незаконного використання економічної інформації. У сфері духовного життя виникає небезпека розвитку в суспільстві за допомогою електронних засобів масової інформації агресивної споживчої ідеології, поширення ідей насильства і нетерпимості та інших негативних дій на свідомість і психіку людини.

Як показує практика останніх років, чим вище активність громадян, організацій або держав в кіберпросторі, тим перед суспільством гостріше встають проблеми забезпечення своєї інформаційної безпеки. І сьогодні є всі підстави вважати, що національна безпека країн залежатиме від забезпечення інформаційної безпеки. По мірі ж інтенсифікації технічного прогресу і посилення "електронної співпраці" держав, ця залежність постійно зростатиме.

Як вважає військовий експерт С. Гріняєв, сьогодні істотна доля всіх суперечностей між державами перенесена в інформаційну сферу. Дана обставина привела до трансформації підходів до поняття "військової сили". На зміну "грубій силі" зброї приходить "м'яка сила" переконання і психологічної маніпуляції. Реалізація цього принципу вимагає перегляду підходів до формування військової стратегії нової епохи. Домінуюча роль інформації і інформаційних технологій, а також орієнтація на парирування принципово нових загроз інформаційної епохи, змусили керівництво деяких західних країн, і перш за все США, активніше упроваджувати нові концепції будівництва збройних сил.

Б. Корміч вважає за необхідне пов'язати національну безпеку та її інформаційну складову з функціонуванням держави, що створює ресурс захисту безпеки, і з розвитком системи міжнародного співробітництва задля створення безпечних умов для кожної держави.

Особливе місце в системі інформаційної безпеки займає інформаційне протиборство. Його особливість в тому, що воно ведеться державними органами інформаційної безпеки з формуваннями, що мають різне суспільне (державне) положення (фізичні особи, юридичні особи, суб'єкти міжнародного права) і які зловмисно створюють інформаційні загрози життєво важливим інтересам особи і суспільству. Ця обставина обумовлює значущість його цілей і ширший арсенал засобів, які використовуються для їх досягнення. У зміст інформаційного протиборства, окрім інформаційного забезпечення і інформаційного захисту, входить комплекс заходів інформаційної протидії, спрямованих на блокування інформації, яка цікавить різного роду зловмисників, і доведення до них помилкових відомостей.

Як відзначає С. Пірумов, "інформаційний простір практично став театром військових дій, де кожна з протиборчих сторін прагне отримати і як можна довше утримувати перевагу, а у разі потреби - розгромити противника. Стає очевидним, що сторона, яка не розуміє або недооцінює вказану обставину, приречена виявитися на узбіччі стовпового шляху цивілізаційного розвитку".

Інформаційно-психологічні методи дії стають усе більш масштабними і політично результативними, і тому все частіше використовуються державами для досягнення своїх політичних цілей замість так званих "гарячих" воєн. У світовій практиці міждержавних відносин створюються умови не лише для послідовної трансформації озброєного протистояння в інформаційне протиборство, але і для перетворення її на самостійний напрям зовнішньої політики розвинених держав. Так, С Гріняєв вважає, що цілі національної політики США досягатимуться шляхом ведення стратегічного інформаційного протиборства з використанням атакуючої інформаційної зброї. І тому все частіше останнім часом розглядаються не апаратно-програмні засоби дії на інформаційні системи і інформаційний ресурс противника, а засоби і методи маніпулювання інформацією. Це підтверджує аналіз робіт з даної тематики - в закордонній пресі останніми роками різко зросло число робіт по засобах і методах маніпулювання свідомістю (зокрема, по методах нейролінгвістичного програмування, гіпнозу та іншим методам дії), дослідженнях психології особи та ін. З'явилися ряд нових понять, наприклад - "реальна віртуальність", коли освітлення деякої події в пресі набуває більшої важливості, ніж ця подія.

Таким чином, інформаційне протиборство є сукупністю таких взаємин, в рамках яких одні суб'єкти шляхом активної дії на інформаційну сферу інших суб'єктів прагнуть отримати перевагу над іншою стороною на користь досягнення своїх політичних цілей.

Література:

1. Рішення всеукраїнської науково-практичної конференції "Стан та вдосконалення безпеки інформаційно-телекомунікаційних систем (Коблево, 15-17 вересня 2009 р. [Електронний ресурс]. - Режим доступу: Http://www. afa. biz. ua/news).
2. Варфоломеев М. Проблема национальной безопасности в современном политическом процессе / М. Варфоломеев // Власть. -2008. - № 4. - С. 38.
3. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. … док. юрид. наук: Спеціальність 12.00.07 - теорія управління; адміністративне право і процес; фінансове право; інформаційне право / Б. А. Кормич. - Харків, 2004. - С. 14.
4. Постанова Верховної Ради України "Про Концепцію (основи державної політики) національної безпеки України" від 16 січня 1997 р. № 3/97 ВР // Голос України. - 1997. - 4 лютого. - С 5.
5. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба [Електронний ресурс]. - Режим доступу: Http://www. nbu. gov. ua/infan/arxiv/arxiv0/2007/01/28).
6. Кормич Б. А. Указ. праця. - С 15.
7. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки: автореф. дис. … канд. юрид. наук: спец. 12.00.01 - теорія та історія держави і права, історія політичних і правових учень / Ю. Є. Максименко. - Київ, 2007. - С 9.
8. Горбулін В. Національна безпека України: загрози і виклики / В. Горбулін // Безпека та нерозповсюдження. - Вип. 3 (15). - К, 2006. - С 54.
9. Галамба М. Указ. праця.

Бурячок В.Л.
доктор технічних наук, старший науковий співробітник
Державний університет телекомунікацій

ІНФОРМАЦІЙНА БЕЗПЕКА У КОНТЕКСТІ ЗАХИСТУ ДЕРЖАВИ ВІД СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ

Розвиток подій на міжнародній арені наприкінці XX – початку XXI сторіччя свідчить, що незважаючи на потужні зусилля світової спільноти щодо врегулювання міждержавних протиріч мирним шляхом кількість і гострота збройних конфліктів сучасності з року в рік фактично не знижуються. Більш того, останнім часом вони охоплюють не тільки традиційні сфери збройної боротьби – зокрема землю, море і повітря, а й поступово просуваються у такі новітні сфери, як **простори інформаційний** (*глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку інформації про конфліктуючі сторони та їх навколишнє оточення в інтересах підтримки прийняття рішень по створенню оптимального, для досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах обстановки*) **та кібернетичний** (*комунікаційне середовище, утворене системою зв'язків між об'єктами інформаційної інфраструктури – інформаційним ресурсом, системами і мережами усіх форм власності, що керуються автоматизованими системами управління й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протилежної сторони*) (рис.1).

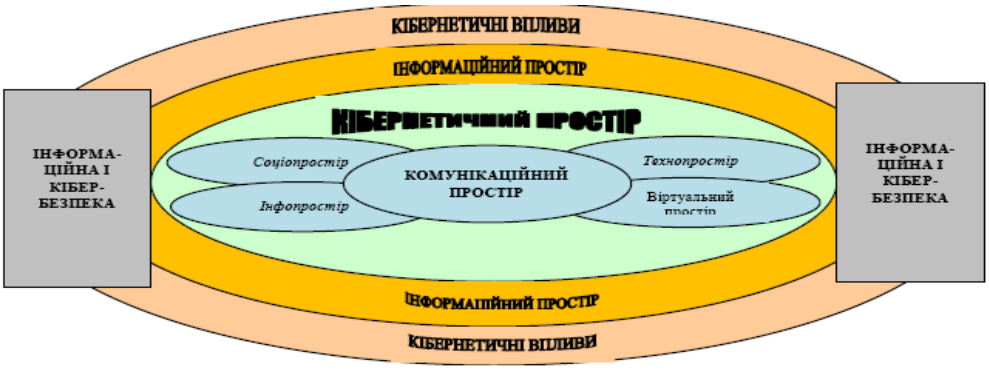


Рис.1. Інформаційний та кіберпростори – головні субстанції сучасного інформаційного суспільства

Неконтрольоване поширення інформаційного і кіберпросторів та їх необмежене застосування протягом останніх десятиліть більшістю провідних держав світу (рис.2), зокрема США, Японією, Францією, Великою Британією, Росією, Китаєм й багатьма іншими призвело до суттєвої уразливості **інформаційної сфери** (*сфери функціонування суб'єктів, що беруть участь в інформаційній взаємодії, інформації, призначеної для використання цими суб'єктами, а також технологій, що забезпечують цю взаємодію з точки зору обробки, зберігання й обміну інформацією між суб'єктами*) цих країн. Спектр ведення цими країнами операцій у кіберпросторі полягає у вирішенні таких прикладних завдань:

Рис.2. Приклади об'єктів, які відносяться до рівнів кіберпростору

виявлення – пасивний або активний моніторинг інформаційного й електромагнітного середовища для виявлення загроз ІР і каналам передачі даних;

переривання доступу протиборчої сторони до інформаційного ресурсу (ІР) – обмеження поінформованості супротивника в бойових умовах і захист власних ІР від можливого використання або впливу з боку супротивника;

порушення працездатності й зниження інформаційного потенціалу протиборчої сторони – втручання в працездатність інформаційно-комунікаційного встаткування протиборчої сторони для зниження його бойової стійкості й керованості (електронне придушення, мережні комп'ютерні атаки й т.п.);

знищення – гарантоване знищення електронної апаратури протиборчої сторони з використанням зброї спрямованої енергії або традиційної зброї кінетичної дії;

захист власних мереж на програмному (антивіруси, файєрволи) та апаратному (підвищення завадозахищеності, протидія електромагнітним імпульсам) рівнях;

моніторинг і аналіз – збір інформації про стан кібернетичного й електромагнітного середовищ в інтересах ведення наступальних і оборонних кібероперацій;

реагування – відповідні дії оборонного (зниження ефективності операцій супротивника) і наступального (нанесення відповідного удару) характеру;

вплив – перекручування сприйняття інформації людьми або суспільними інститутами, а також перекручування інформації, що циркулює в машинних і змішаних (машина-людина, людина-машина) системах для переорієнтації їхніх дій у власних цілях.

Щоб запобігти **сторонньому кібернетичному впливу** – *деструктивним діям, що зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ та ІТС (рис.3*) вони були змушені контролювати і в подальшому регулювати взаємовідносини у цих сферах. Нормами поведінки та базовими принципами, що мають бути забезпечені при цьому є:

1) норми поведінки в кіберпросторі:

– ***дотримання основних свобод.*** Держави мають поважати свободи слова та зібрань, що так само актуальні для он-лайну, як і для офф-лайну;

– ***повага до власності.*** Держави у своїх ініціативах мають поважати право на інтелектуальну власність, включно з патентами, торговими таємницями, товарними знаками та авторськими правами;

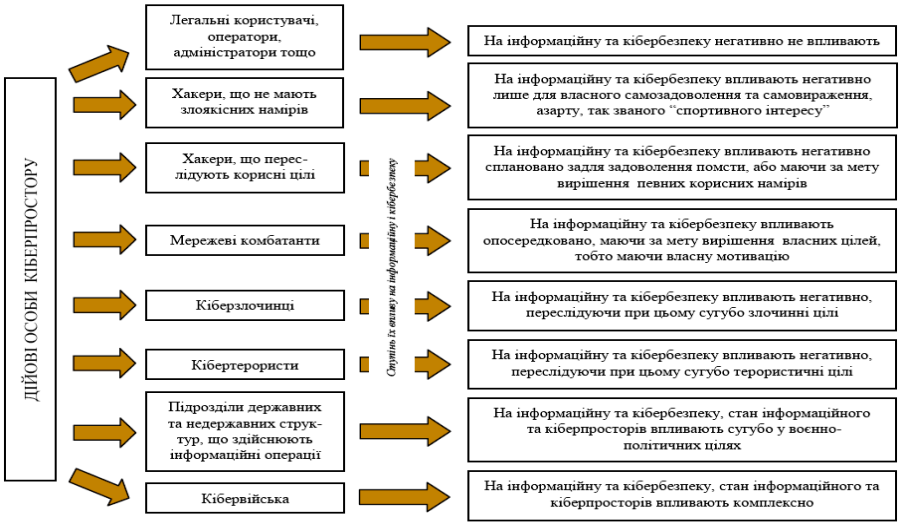


Рис.3. Дійові особи кіберпростору

– ***цінність приватного життя***. Громадяни-користувачі інтернету мають бути захищені від довільного/незаконного втручання у їхнє приватне життя;

– ***захист від злочинів***. Держави мають виявляти та переслідувати кіберзлочинців, створювати таке законодавство та практики, що не дозволять зловмисникам переховуватися на їх території, а також сприяти співробітництву з міжнародними структурами, що переслідують таких злочинців;

– ***право на самозахист***. Відповідно до Статуту ООН держави мають право на самозахист, що може бути застосований у відповідь на агресивні дії у кіберпросторі;

– ***глобальна сумісність***. Держави мають вживати заходів, що сприятимуть максимальній сумісності та зручності використання мережі інтернет, а також її доступності якнайбільшій кількості громадян;

– ***мережева стабільність***. Держави мають поважати свободу потоків інформації у національних мережах та не втручатися в роботу тієї інфраструктури, що відноситься до такої, що тісно пов'язана з міжнародною функціональністю мережі;

– ***надійний доступ***. Держави не мають штучно заважати доступу громадян до мережі інтернет чи мережевих технологій;

– ***багатостороннє управління***. Управління мережею інтернет не має обмежуватися виключно урядами, а повинне здійснюватися й іншими стейкхолдерами;

– ***особлива увага до кібербезпеки***. Держави мають визнавати свою відповідальність за безпечність на надійність роботи власних сегментів мережі інтернет та відповідної інфраструктури.

2) базові принципи формування політики щодо кіберпростору:

«фундаментальні свободи» (можливість шукати, отримувати та передавати інформацію та ідеї через будь-які засоби зв'язку та незважаючи на кордони);

«прайвесі» (усвідомлення користувачами кіберпрстору загроз їх персональній інформації та можливость вчинення проти них кіберзлочинів);

«вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, адже вони лише створюють видимість безпеки. Кіберпростір має бути місцем інновацій і співпраці держави та бізнесу задля більшої безпеки).

Як результат це призвело до того, що процеси пошуку, збору і добування інформації у відкритих, відносно відкритих і закритих електронних джерелах, заходи із забезпечення конфіденційності, цілісності та доступності власного IP, а також заходи щодо протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз стали для цих країн особливо актуальними. Зважаючи на це та враховуючи постійно зростаючий потенціал використання мережі Internet зазначені країни почали активно модернізувати власні сектори безпеки й, передусім, **безпеки кібернетичної** – *стану захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам* (рис.4).

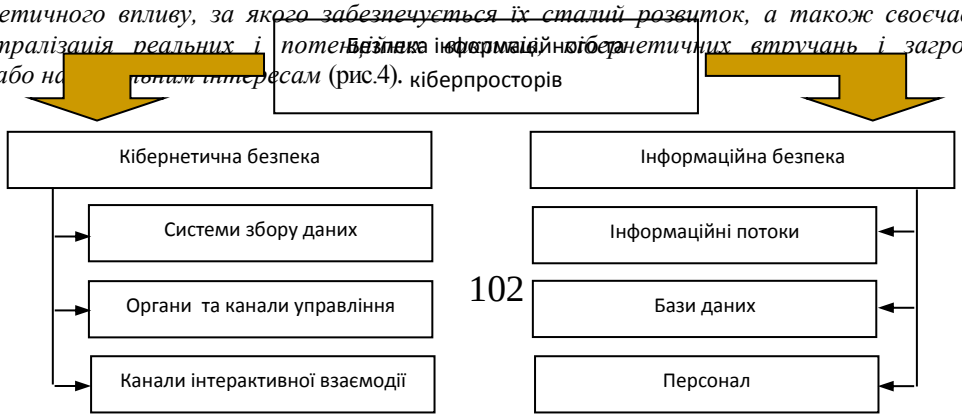


Рис. 4. Об'єкти впливу інформаційної та кібербезпеки

Характерними ознаками кібербезпеки при цьому є *сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань (хакерів, крекерів та/або розвідувальних організацій) розгортаються навколо ІР й які спрямовані на досягнення і утримання потенціальними супротивниками переваги у протидії новим загрозам безпеці для об'єктів їх критично-важливої інфраструктури* (рис.5).

Рис.5. Дійові особи кіберпростору

Такі дії спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої фізичної, інформаційної та кіберінфраструктури, кількість секторів та принцип групування яких різниться в залежності від країни. Вплив на ці сектори може призвести до:

– виникнення надзвичайної ситуації або масових заворушень;

– блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки;

– блокування роботи державних органів, органів місцевого самоврядування;

– блокування діяльності військових формувань, органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю;

– порушення безпечного функціонування банківської та/або фінансової системи держави;

– розголошення державної таємниці тощо.

Віддаючи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази зазначені країни у практику збройної боротьби впровадили концепцію **інформаційного протиборства** (рис.6) – *закономірного об'єктивного процесу у стосунках між протиборчими сторонами, спрямованого на досягнення ними цілей власної державної політики в мирний та воєнний час, за рахунок комплексного впливу на систему державного і військового управління супротивної сторони та її військово-політичне керівництво, а також захисту своїх інформаційних об'єктів від подібного впливу* та **кіберборотьби** – *комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані ІТ системи противника й захисту від такого впливу власних інформаційно-обчислювальних ресурсів шляхом використання спеціально розроблених програмно-апаратних засобів, а також проведення ряду спеціалізованих навчань*.

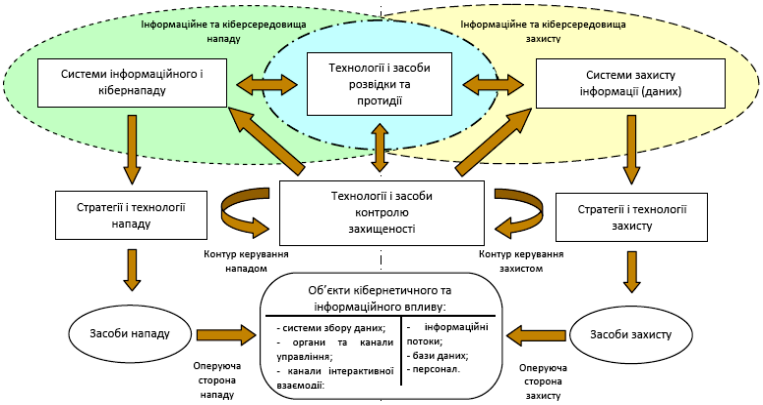


Рис.6. Концептуальна схема інформаційного протиборства

Їх наслідком у найближчій перспективі можуть стати так звані **кібернетичні війни** (табл.1) – *активне протистояння між державами, політичними групами, соціальними утвореннями, приватними і комерційними установами та іншими державними і позадержавними суб'єктами, метою якого є заподіяння шкоди один одному в ІТ сфері за рахунок проведення як оборонних (захист власних ІТ систем від деструктивного впливу), так і наступальних дій (встановлення контролю над ІТ системами супротивника або взагалі їх знищення).* Їх головні завдання полягатимуть у:

– здійсненні протиборчими сторонами заходів з розвідки інформаційно-телекомунікаційних систем один одного та руйнуванні їх інфраструктури;

– блокуванні або виведенні з ладу автоматизованих систем управління супротивника як цивільного, так і військового призначення;

– добуванні стратегічної та іншої, цінної для протиборчих сторін відкритої і конфіденційної інформації;

– порушенні цілісності і доступності інформації потенціального супротивника та спостережності процесів тощо.

Таблиця 1

Складові інформаційного протиборства та його окремі завдання

Складові	Завдання
Розвідка	Виявлення державної інформаційної інфраструктури противника, пунктів управління (ПУ), вузлів зв'язку, проведення спеціальних розвідувально-диверсійних операцій зі знищення інформаційної інфраструктури противника
РЕБ	Придушення радіомовлення, телебачення та телефонних систем противника, державних систем зв'язку і телекомунікацій, вузлів зв'язку системи управління військами, радіодезінформація. Створення інформаційного вакууму в радіопросторі противника
Інформаційно-психологічна війна	Проведення інформаційно-психологічного впливу: засобами залистування, радіо-, гучномовлення, тощо з метою підриву бойового духу противника, ослаблення його наступального пориву, деморалізації особового складу, розпалення паніки і пораженських настроїв. Спеціальні дії, щодо посадових осіб, що приймають рішення, державних органів управління, військового керівництва, операторів, персоналу, що обслуговує інформаційні системи. Дезінформування
Кібервіна	Здобуття, знищення та викривлення інформаційних масивів, програмного забезпечення в комп'ютерних системах різного призначення, удари по Інтернет – зоні противника (сервера компаній та державних установ). Знищення сайтів противника. Створення спеціальних пропагандистських сайтів. Розміщення інформаційних матеріалів в Internet-виданнях

Основними методами, які застосовуватимуться протиборчими сторонами в ході таких дій можуть бути (табл.2):

1) на тактичному рівні – **кібератаки**, здійснювані на фізичні (інфраструктуру кіберпростору: використовувані кабелі, маршрутизатори, комутатори тощо), семантичні (неопрацьовані дані, що циркулюють у кіберпросторі та які використовує машина або людина), а також синтаксичні (стандарти і протоколи передачі даних між фізичним та семантичним шарами на кшталт *TCP/IP*, на якому тримається весь *Internet*) шари кіберпростору. У цьому випадку, згідно з, під кібератакою будемо розуміти *сукупність узгоджених за метою, змістом і часом дій або заходів – так званих кіберакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації, а також порушення роботи його ІТ систем*;

2) на стратегічному та спеціальному рівнях – **кібероперації**. За аналогією з методами і способами ведення звичайної війни та згідно з – *це сукупність узгоджених за часом, глибиною і завданнями відносно короткочасних кібератак, спрямованих на певну кількість об'єктів впливу протиборчої сторони з метою одержання несанкціонованого доступу до їх ІР, порушення роботи їх ІТ систем або взагалі повного виведення обраних об'єктів з ладу.*

Таблиця 2

Основні методи проведення кібератак, стратегічних та спеціальних кібероперацій

Складові	Завдання
Розвідка	Виявлення державної інформаційної інфраструктури противника, пунктів управління (ПУ), вузлів зв'язку, проведення спеціальних розвідувально-диверсійних операцій зі знищення інформаційної інфраструктури противника
РЕБ	Придушення радіомовлення, телебачення та телефонних систем противника, державних систем зв'язку і телекомунікацій, вузлів зв'язку системи управління військами, радіорозвідка. Створення інформаційного вакууму в радіопросторі противника
Інформаційно-психологічна війна	Проведення інформаційно-психологічного впливу: засобами залякування, радіо-, гучномовлення, тощо з метою підриву бойового духу противника, ослаблення його наступального пориву, деморалізації особового складу, розпалення паніки і поразницьких настроїв. Спеціальні дії, щодо посадових осіб, що приймають рішення, державних органів управління, військового керівництва, операторів, персоналу, що обслуговує інформаційні системи. Дезінформування
Кіберзброя	Здобуття, знищення та викривлення інформаційних масивів, програмного забезпечення в комп'ютерних системах різного призначення, удари по Інтернет – зоні противника (сервера компаній та державних установ). Знищення сайтів противника. Створення спеціальних пропагандистських сайтів. Розміщення інформаційних матеріалів в Internet-виданнях

Кібератаки та кібероперації можуть проводитись за допомогою *спеціальних атакових і оборонних засобів ураження, що* становлять зміст поняття кібернетична зброя (далі – **кіберзброя**) і *дають можливість цілеспрямовано змінювати, знищувати, копіювати і блокувати інформацію, долати системи захисту, обмежувати доступ законних користувачів, порушувати функціонування носіїв інформації для дезорганізації роботи технічних засобів IT систем і мереж тощо*. Основними компонентами, використання яких сприятиме формуванню їх атакових і оборонних можливостей мають бути:

засоби доставки (*Weapon Delivery Vehicle*);

компоненти подолання системи безпеки (*Security Breaching Component*);

корисне навантаження – злоякісний програмний код (*Payload – Malicious Activity Code*).

Нині, як стверджує директор Лондонського міжнародного інституту стратегічних досліджень Джон Чіпмен, ймовірність застосування оборонної й атакової кіберзброї у збройних конфліктах сучасності надзвичайно зросла, але вона й досі залишається "... серйозно недооціненою …" загрозою міжнародній безпеці. Її наявність може відіграти вирішальну роль у розпал бою, сформувавши умови для знищення або блокування IT систем і мереж потенціальних протиборчих сторін тощо. Одними із доволі показових прикладів такому слід вважати:

1) події в Естонії та Грузії у 2007 та 2008 роках. Причому, якщо напад на Естонію згідно оцінок фахівців був малоефективним за рахунок швидкого та адекватного реагування на широкий діапазон атак – від спама до DDoS та ним подібних, то Грузія фактично втратила контроль над власним доменом і була змушена перевести певну кількість державних порталів на закордонні сервери;

2) спрямовані атаки, спричинені програмними засобами Stuxnet і Hydraq, які стали двома самими помітними кібер-подіями 2010 року. Причому, наприклад, результатом дії вірусу Win32/Stuxnet стало гальмування ядерної програми Ірану. Цьому сприяло виявлення вірусом програмованих логічних контролерів (ПЛК) у автоматизованій системі управління технологічними процесами станції (Supervisory Control And Data Acquisition), а також можливість використання (для впровадження особливого коду у "залізо" ПЕОМ АЕС) чотирьох, невідомих раніше уразливостей "нульової доби" ("zero-day") у діючих версіях ОС Windows та двох дійсних сертифікатів від компаній Realtek і JMicron;

3) події навколо сайту Wikileaks у тому ж таки 2010 році, на сторінках якого була опублікована величезна кількість грифованих документів, що стосувались воєн, які ведуть США в Афганістані й Іраку, а також понад 250 тисяч документів переписки американських дипломатів. Ані західні, ані вітчизняні фахівці виявилась неспроможними надати однозначну оцінку цьому факту. Частина з них й нині вважає Wikileaks проектом прихованої операції ЦРУ, що спрямована на загальну дестабілізацію обстановки у світі. Інші навпаки – характеризують діяльність сайту Wikileaks як удар власне по Європі й пряму загрозу західній демократії.

Саме ці та подібні ним приклади, спричинені:

недосконалістю нормативно-правової бази, на основі якої заборонялося б застосовувати інформаційну і кіберзброю та проводити інформаційні і кібероперації, а також встановлювалася б відповідальність протиборчих сторін за здійснення злочинів у IT сфері;

формуванням окремими державами власних доктрин і стратегій наступальних та підривних дій в інформаційному і кіберпросторах;

створенням та застосуванням спеціальних сил і засобів негативного впливу на критично важливу інформаційну і кіберінфраструктуру;

проникненням IT технологій у всі сфери державного й громадського життя, побудовою на їхній основі систем державного і військового управління;

розвитком державних проектів і програм у сфері інформатизації (електронний документообіг, міжвідомча електронна взаємодія, універсальні електронні карти, надання державних послуг в електронній формі), спрямованих на формування інформаційного суспільства, тощо, - показали усьому світу, що можливості **кіберзброї** можуть бути досить вражаючими, а протидія її негативному впливу може виявитися вкрай складним завданням для сторін, що захищаються.

Це може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони. Головним чином це пояснюється появою нових комунікаційних можливостей та постійно зростаючим інформаційним ресурсом, які останнім часом значно розширюють кількість потенціально-можливих джерел для такого виду розвідки, як **розвідка інформаційно-телекомунікаційних систем** (рис.7) - *комплексу заходів, спрямованих на систематичний і цілеспрямований пошук та добування з ІТС розвідувальної інформації про існуючого і вірогідного противника (конкурента), її вивчення та обробку, а також формування на цій підставі уявлення про реальні та/або потенціально можливі джерела кібернетичного впливу на власний інформаційний і кіберпростори.* Головними способами ведення розвідки ІТС є:

розвідка систем телекомунікацій – *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про об'єкти розвідки із систем передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень, звуків і повідомлень будь-якого роду, а також їх подальшого вивчення та обробки*;

мережна розвідка – *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про ІТС об'єкта розвідки, їх ресурси, засоби захисту, пристрої та ПЗ, що в них використовується, їх уразливі місця та межі проникнення, а також подальшого вивчення цих даних та їх обробки*;

кібернетична розвідка – *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про об'єкти розвідки за допомогою засобів ЕОТ і ПЗ із ресурсів ІТС з їх подальшим накопиченням, наступною верифікацією та аналітичною обробкою, оцінювання на підставі отриманої інформації можливих загроз (ризиків) власному кіберпростору, виявлення їх ознак та прогнозування їх можливого прояву, а також планування та, у разі потреби, здійснення впливу на кіберпростір ворогуючої сторони.*

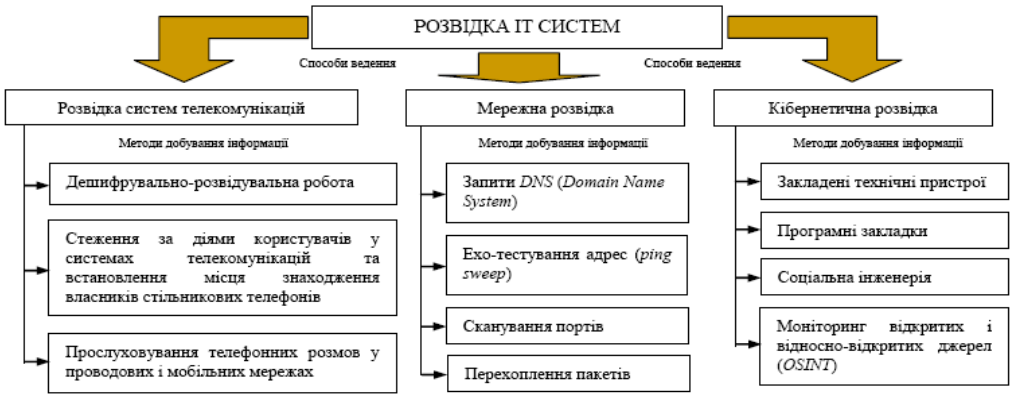


Рис. 7. Способи та методи ведення розвідки ІТ систем

Впродовж останніх років Україна, як і більшість інших країн світу, робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає:

Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV;

Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»;

Укази Президента України, зокрема про: Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;

окремі положення Кримінального Кодексу України, окремі Постанови Кабінету Міністрів та Рішення РНБОУ.

При цьому ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007-2015 роки» у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України», яким має бути запроваджено низку термінів, пов'язаних із кібербезпекою.

Практичними кроками щодо реалізації існуючої нормативно-правової бази стало створення у 2007 році в складі Державної служби спеціального зв'язку та захисту інформації України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім цього Указом Президента України "Про виклики та загрози національній безпеці України у 2011 році" від 10 грудня 2010 року №1119/2010

ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України "Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України" від 25 січня 2012 року №34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Усвідомлюючи ступінь та динаміку поширення комп'ютерних інцидентів теренами України у липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю і торгівлею людьми. Середня інтенсивність загальної злочинності на 100 тис. населення, що фіксувалася в регіонах України протягом 2001-2011 років зазначеними вище структурними підрозділами МО, МВС, СБ та ДССЗЗІ України подана на рис. 8.

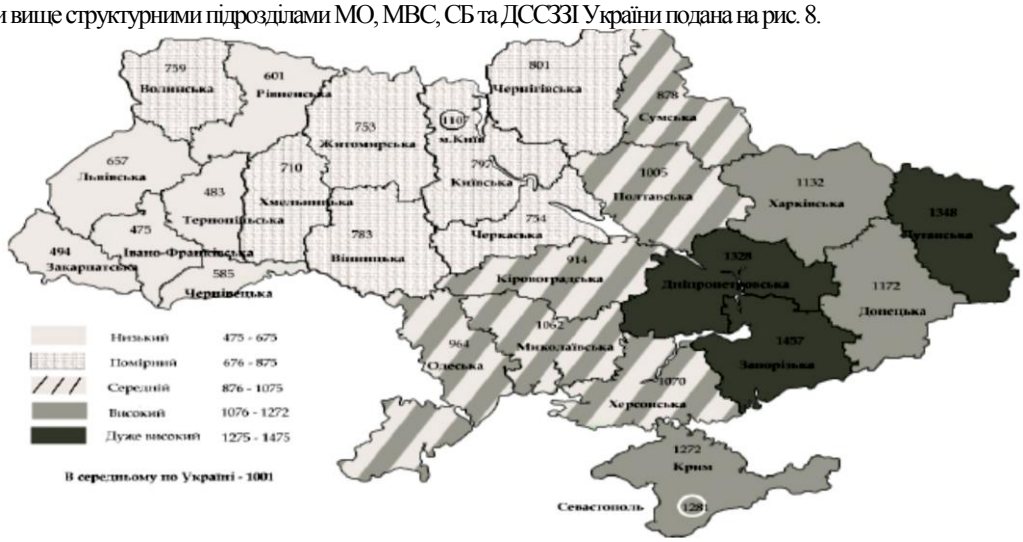


Рис.8. Інтенсивність кіберзлочинності в регіонах України протягом 2001-2011 років

На ефективність діяльності спеціальних структурних підрозділів ДССЗЗІ, СБ, МВС, СЗР та МО України у цій діяльності значною мірою впливає:

складність структури ІКТ та національного кіберпростору;

ускладненість щодо розмежування воєнних і цивільних об'єктів критичної інфраструктури держави у кіберпросторі;

можливість недержавних суб'єктів та неавторизованих користувачів виступити у ролі гравців в кіберпросторі та проблематичність щодо їх виявлення;

наявність якісних відмінних рис кіберзброї від зброї звичайної;

можливість прихованого проведення протиборчими сторонами кібератак і кібероперацій у кіберпросторах один одного;

відсутність у вітчизняному законодавстві визначень перш за все таких термінів як "кібербезпека", "кібервійна", "кіберзахист" тощо.

Наведені дані свідчать про наявність кореляційного зв'язку між рівнем кіберзлочинності, географією розповсюдженості споживачів послуг Інтернет та Інтернет-злочинністю, а отже, і про наявність взаємно обумовлюючих кримінологічно значущих зв'язків між ними. Пояснення такої ситуації можна знайти в тому, що мережа Інтернет, будучі носієм масового постачальника інформації, перетворилась в один із домінуючих інструментів інформаційно-технічного, морально-правового та психологічного впливу на населення і майже всі сфери соціального буття. Зважаючи на певні труднощі з якими фахівці з кіберзахисту від ДССЗЗІ, СБ та МВС України стикаються в процесі роботи та неможливість самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному і кіберпросторах, з плином часу постала гостра потреба у пошуку ними шляхів співробітництва з аналогічними організаціями світового суспільства. Фактично програмним документом для нашої держави на підтвердження такому став вислів Першого заступника Секретаря РНБО України, Співголови Спільної робочої групи Україна – НАТО з питань воєнної реформи, згідно якому "… суттєво підвищити рівень безпеки кіберпростору…" сучасного інформаційного суспільства можна лише "… завдяки тісній міждержавній співпраці, використовуючи для цього всі наявні можливості і механізми, які є в розпорядженні кожної з країн …". При цьому одним із головних напрямків такої діяльності на його думку має стати нарощування темпів співпраці передусім з організацією НАТО.

Вагомим поштовхом для активізації зусиль у цьому напрямку стало прийняття організацією НАТО програмного документу під назвою "Рамки для співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами", який було розповсюджено у Штаб-квартирі Альянсу 2 квітня 2009 року. У документі наголошується, що головним елементом політики НАТО у сфері кіберзахисту є принцип, згідно якого держави-члени Альянсу несуть пряму відповідальність за захист власних національних комунікацій та інформаційних систем. При цьому НАТО повинна мати спроможність для підтримки союзників, які стали жертвою кібератак міжнаціонального значення. Окрім цього в документі зазначається, що головні цілі співробітництва НАТО з державами-партнерами у сфері кіберзахисту перш за все полягають у покращенні спроможності НАТО та держав-партнерів у сфері захисту критичних комунікаційних та інформаційних інфраструктур проти кібератак, наданні допомоги у відновленні нормального функціонування відповідної інфраструктури після кібератак, а також у створенні основ для заходів з підтримки у випадках кібератак. Відповідно до основних положень документу країни-партнери закликаються до вжиття необхідних заходів з метою гармонізації національного законодавства у сфері кібернетичної безпеки з відповідними міжнародними нормами (зокрема, такими як Конвенція Ради Європи з питань кіберзлочинності) шляхом дотримання таких головних принципів:

1) співпраця між НАТО та країною-партнером має бути взаємовигідною у тому сенсі, що Альянс може надати країні-партнеру інформацію та підтримку у сфері кібербезпеки за умови дотримання останньою аналогічних умов взаємодії;

2) НАТО може надати країні-партнеру як експертну допомогу, так і свої технічні можливості для захисту від кібернетичних атак;

3) країни-партнери можуть звертатися з пропозицією щодо співпраці у сфері кіберзахисту та отримання підтримки з боку НАТО у випадках кібератак національного значення;

4) НАТО і партнери повинні уникати дублювання зусиль, що вживаються у рамках інших міжнародних організацій, які залучаються до захисту ІС від кібератак;

5) наявність Угоди про безпеку між НАТО та країною-партнером визначатиме обсяги допомоги та інформаційного обміну. Разом з цим, інформація, яка стосується захисту критичної інфраструктури національних комунікаційних та інформаційних систем, буде позначена та передана належним чином лише у разі потреби ознайомлення з нею.

Документ визначає також сфери співробітництва НАТО з державами-партнерами у сфері кіберзахисту, а саме: узагальнений обмін інформацією щодо політики та доктрин; обговорення технічних засобів захисту комунікаційної та інформаційної інфраструктури (може бути передбачений на більш змістовному рівні співробітництва). Окремо у документі наголошується про те, що:

по-перше, країни-партнери можуть звертатися з пропозиціями щодо проведення консультацій з питань кібернетичного захисту у форматі "28+1" або "28+n";

по-друге, процес планування та оцінки сил, а також Річні національні програми мають слугувати головними інструментами щодо прив'язки співробітництва з державами-партнерами у питаннях кіберзахисту з їхніми індивідуальними потребами та обставинами (загальна кількість Цілей партнерства у рамках ППОС, схвалених для України – 96, з них: на Збройні Сили України покладено 70 Цілей партнерства, на МВС України – 8, на МЗС України – 6, на СБУ – 11 та на Мінфін України – 1);

по-третє, потенціал Центру передового досвіду із захисту від кібернетичних загроз в Таллінні (Естонія), Центру передового досвіду із боротьби проти тероризму в Анкарі (Туреччина), Програми НАТО "Наука заради миру та безпеки" та Комітету з планування цивільного зв'язку може використовуватися країнами-партнерами у плані підготовки відповідного персоналу. Виходячи з такого провідні фахівці світу прогнозують, що збільшення доходів у сфері кібербезпеки у різних регіонах земної кулі може сягнути до 2018 року понад 4 500 мільйонів доларів (рис. 9).

Тим не менш нині існує ціла низка проблем, які заважають блоку НАТО та країнам ЄС створити дієздатну систему протидії внутрішнім і зовнішнім загрозам власному інформаційному і кіберпросторам. Найсуттєвішими з них є:

відсутність єдиної системи реагування на кібератаки. Можливість скритного (прихованого) проведення протиборчими сторонами кібератак та кібероперацій у кіберпросторах один одного;

відсутність єдиних стандартів у сфері кібербезпеки та чіткого уніфікованого категорійного апарату, які б регламентували діяльність певних відомств, правоохоронних і силових структур у сфері кіберзахисту;

низький рівень обміну інформацією про кіберінциденти між державами, а також держав з власним приватним бізнесом. Можливість недержавних суб'єктів та неавторизованих користувачів виступити у ролі гравців в кіберпросторі та проблематичність щодо їх виявлення;

декларативність багатьох положень у національних стратегіях кібербезпеки, недостатній рівень координації діяльності між наднаціональними та національними органами, що призводить до дублювання їх задач;

значна диспропорція рівня готовності країн-членів НАТО та країн ЄС до протидії кіберзагрозам на національному рівні, недостатній рівень фінансування ними науково-дослідних проектів з цих питань.

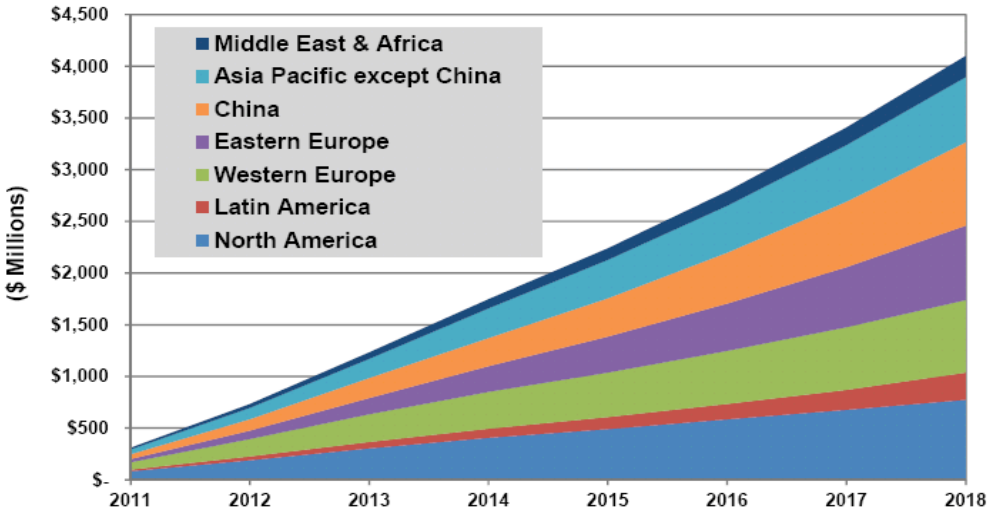


Рис. 9. Зростання доходів у сфері кібербезпеки з 2011 по 2018 роки

На додачу до визначених наднаціональних проблем Україні притаманні власні, що не були вирішені протягом понад 20 років незалежності. Найвагомішими з них є:

складність структури ІКТ та національного кіберпростору;

ускладненість щодо розмежування воєнних і цивільних об'єктів критичної інфраструктури держави у кіберпросторі;

значна уразливість інфосфери України через надмірно широке впровадження до неї західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;

деградація науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інфосфері та низький рівень конкурентоспроможності в ній;

непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення кваліфікованими фахівцями з цих питань;

відсутність у вітчизняному законодавстві визначень перш за все таких термінів, як "кібервійна", "кіберзахист" та "кібербезпека" (на відміну від інформаційної безпеки, сутність якої викладена у ст. 17 Конституції України), "комп'ютерна злочинність" і "комп'ютерний тероризм" (певним чином знайшли відображення у законі України "Про основи національної безпеки" та доктрині ІБ України, а також у статті 1.1.5 проекту Річної національної програми України);

відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати і координувати діяльність зазначених вище правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпросторам України та керувати проведенням комплексних навчань з проблеми забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань "Cyber Storm", які проводяться в США та/або "Cyber Europe", що проводяться у ЄС тощо.

Такий стан справ фактично є каталізатором для ініціювання втручань в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами її критично важливої інформаційної і кіберінфраструктури, виникнення техногенних катастроф тощо. Саме тому найбільш пріоритетним напрямом керівництво України вважає нині реформування власної інформаційної безпеки за рахунок створення дієвої системи кібербезпеки, розбудова якої вимагає вирішення різних завдань як соціального і техногенного, так і передусім організаційного характеру. Найбільш актуальними серед них нині є: чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподілу повноважень між ними, забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів, розробка та впровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки, а також запровадження дієвих стимулів для залучення до такого роду діяльності фахівців високого рівня кваліфікації. Для цього необхідно:

по-перше, розробити національну стратегію кібернетичної безпеки, яка має чітко визначити мету, завдання та пріоритети такої діяльності, а також структури, відповідальні за реалізацію заходів щодо протидії сторонньому кібервпливу;

по-друге, реалізувати в межах окремої цільової програми структурно-функціональну модель формування державної системи кібернетичної безпеки, варіант якої подано на рис. 10.

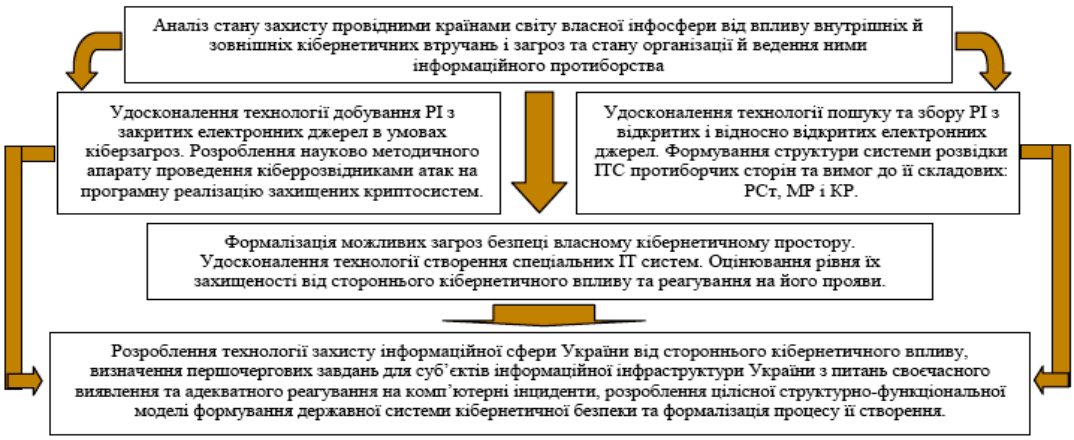


Рис. 10. Структурно-функціональна модель формування системи кібернетичної безпеки

Зважаючи на досвід іноземних країн та особливості українських реалій, вирішення цих завдань неможливе без створення (рис.11):

Рис. 11. Пропозиції до організаційної структури системи кібербезпеки України

1) міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки;

2) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їхні інформаційні системи;

3) органів власної інформаційної і кібербезпеки державних установ (відомств) та комерційних структур, які мають тісно взаємодіяти зі вказаними вище центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів.

Стислий аналіз стану боротьби за володіння світовим ІР дає можливість зробити такі висновки.

1) Сучасний етап розвитку суспільства характеризується зростанням ролі інформаційної сфери, що уявляє собою сукупність інформації, відповідної інфраструктури, а також суб'єктів, які збирають, накопичують, обробляють формують, поширюють інформацію.

2) Інформаційна сфера як системотворчий фактор життя суспільства активно впливає на стан політичної, економічної, національної, оборонної й інших складових безпеки України. Це потребує адекватного стану інформаційної безпеки та її важливої складової – захисту інформації.

3) Провідні держави світу у результаті вироблення і реалізації єдиної науково-технічної політики щодо захисту власних ІР та ІТ інфраструктури від деструктивного кібернетичного впливу свою головну увагу зосередили на міжвідомчих і міждержавних аспектах такої діяльності.

4) Україна, як суверенна та незалежна держава, знаходиться нині на початкових етапах складного шляху щодо створення власної системи кібернетичної безпеки, як складової її воєнної безпеки в інформаційній сфері. Будь-які спроби осмислити проблеми інформаційної та кібербезпеки впираються у відсутність єдиної термінологічної бази. У зв'язку із цим, необхідно чітке розмежування понять кіберпростору й інформаційного простору, кібербезпеки й, з іншого боку, інформаційної та інформаційно-психологічної безпеки, а також будь-яких інших видів діяльності, кінцевою метою яких є вплив на людину, групи людей або суспільство в цілому за рахунок інформаційно-комунікаційних технологій.

5) Застосування проти нашої держави розвиненими країнами світу, що мають необхідний промисловий та інтелектуальний потенціал, низки кібератак і кібероперацій вже зараз може призвести до серйозних проблем, пов’язаних із забезпеченням безперебійного функціонування головних елементів її інфраструктури, цілісності та конфіденційності інформації, а також її збереження, тобто всього того, з чим вже зіштовхнулась більшість розвинених країн Заходу.

6) Одним із найбільш ефективних засобів профілактики, протидії та боротьби з найрізноманітнішими комп’ютерними втручаннями і загрозами, поступово перетворюючись із діяльності щодо своєчасного викриття ознак підготовки імовірного противника до збройного нападу в діяльність, орієнтовану на досягнення та/або утримання над ним певної інформаційної переваги провідними державами світу нині визнана розвідка ІТС. Значне підвищення її результативності у сучасних умовах може бути здійснено ними шляхом активізації зусиль за напрямом розвідки систем телекомунікацій, мережної і кіберрозвідок.

7) Позитивний результат від виконання завдань кібербезпеки на місцевих рівнях може бути досягнутий за рахунок створення, наприклад, універсального програмно-апаратного “кіберполігону” з тестування засобів захисту власних ІТ систем і мереж від стороннього кібернетичного впливу, програмно-апаратного комплексу обґрунтування раціональних за показником “захищеність – вартість” способів кібернетичного захисту закритих інформаційних та криптосистем, а також автоматизації усіх, супутні цьому процесівя

\

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications /2007/cgdc-2007-r.pdf
2. Новейшая военная энциклопедия. Сила и гордость новой России. / редкол. А.П. Поркин [и др.]. – М.: РИПОЛ классик, 2007. – 1664 с.
3. І.О. Ляшенко, В. А. Кириленко. Кібернетичні операції - майбутня форма збройної боротьби. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/znpnapv_vtn/2010_53/ 10liofzb.pdf
4. Бурячок В.Л., Гулак Г.М.,Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі //Наука і оборона. – 2011. №3. – С.35–42
5. В.Ф. Комарович, И.Б. Саенко. Компьютерные информационные войны. Концепция и реалии. [Електронний ресурс]. – Режим доступу: http://www.cprspb.ru/bibl/opv/komarovich.doc
6. Мир вступил в эпоху сетевых войн и конфликтов. [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-100408112419
7. Мир вступает в эпоху глобальной кибервойны. [Електронний ресурс]. – Режим доступу: http://www.newsland.ru/news/detail/id/668325/
8. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа / Пер. с англ. В.Смирнова. –М.:КРОН-ПРЕСС, 1999. – 816 с.
9. П. Павел. Сетевая разведка. [Електронний ресурс]. – Режим доступу: http://www.warning.dp.ua/comp11.htm
10. Бурячок В.Л. До питання організації та проведення розвідки у кібернетичному просторі. / Бурячок В.Л., Гулак Г.М., Хорошко В.О. // Наука і оборона. – 2011. - №2. – С. 19-23.
11. Ющук Е.Л. Интернет-разведка. Руководство к действию. – М.: Изд-во “Вершина”, 2007. – 256 с.
12. Доронин А.И. Бизнес-разведка. – М.: Изд-во “Ось-89”, 2003. – 384 с.
13. Тараскин М.М. Взгляды высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн. [Електронний ресурс] / М.М. Тараскин, С.А. Чешуин. – Режим доступу: http://nic-nauka.ru/material/171/
14. Мир вступил в эпоху сетевых войн и конфликтов. [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-100408112419
15. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

Куклов В.М., Василенко В.В., Гринкевич Г.О.
Державний університет телекомунікацій

SDN як платформа підвищення безпеки в телекомунікаційних мережах

В доповіді обґрунтовано доцільність використання концепції SDN в сучасних системах передачі даних з метою аналізу пропускної здатності мережі на предмет проведення атак на відмову доступу.

Сучасне мережеве обладнання дозволяє виявляти атаки даного типу базуючись на пропрієтарному програмному забезпеченні, що в ньому встановлено, та на статично, або динамічно обновлюваних чорних списках адрес атакуючих.

Такий підхід має свою ефективність, яка в сучасних реаліях не дозволяє виявляти цілеспрямовані, але значно розподілені елементи атакуючої групи. Концепція SDN дозволяє впроваджувати керування апаратною частиною мережевого обладнання в реальному часі, використовуючи програмне забезпечення, що керує мережевим обладнанням віддалено. Таким чином, досягається гнучкість управління мережевим обладнанням, що дозволяє створювати нові комплекси прийняття рішень по управлінню трафіком, аналізу мережевого оточення, використовуючи складні алгоритми аналізу та прийняття рішень.

SDN враховує той факт, що статична архітектура звичайних мереж погано підходить для динамічних обчислень і забезпечення потреб сучасних центрів обробки даних. Ключові обчислювальні тенденції випливають в потребу нової мережевої парадигми:

- Зміна характеру трафіку: додатки, які зазвичай отримують до географічно розподілених баз даних і серверів через загальнодоступні і приватні хмари вимагають надзвичайно гнучкого управління трафіком і доступу до пропускної спроможності на вимогу.
- "Консьюмерізація IT": Bring Your Own Device (BYOD) тенденція потребує мереж, які є гнучкими і безпечними.

SDN мережі надають величезні можливості з точки зору менеджменту та рероутінга потоків. З допомогою їх ми в змозі гнучко і ефективно використовувати різні рішення в боротьбі з різного роду атаками, а також вирішувати питання аутентифікації, авторизації, шифрування важливого трафіку. З точки зору ресурсів, надання сервісів якимось DATA-центрами абсолютно не важливо, традиційна у вас мережа або SDN мережа. Специфіка останньої в тому, що вона більш низькорівнева - саме на етапі комутацій у неї є велика гнучкість рішеннях з безпеки, маршрутизації, включаючи динамічну.

д.т.н. Субач І.Ю.
Військовий інститут телекомунікацій та інформатизацій
Державного університету телекомунікацій

ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК

Розвиток інформаційних технологій протягом останнього десятиліття активно вплинув на воєнну сферу, фундаментально змінив зміст війн нового покоління, форми та способи їх ведення, а також змусив переглянути питання організації управління військами під час підготовки і ведення бойових дій. Основну загрозу об'єктам інформаційної інфраструктури воєнної сфери – інформаційно-телекомунікаційним (інформаційним, телекомунікаційним) системам являють кібернетичні атаки. Під кібернетичною атакою розуміють сукупність декількох короткочасних узгоджених за метою і часом заходів інформаційно-технічного впливу в кібернетичному просторі, направлених на деструктивні зміни визначеного об'єкту інформаційної інфраструктури. Кібернетична атака проводиться з метою порушення порядку функціонування (блокування роботи та/або виведення з ладу) інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (мереж), використання інформаційних ресурсів, змін властивостей інформації, отримання контролю над системою, копіювання, модифікації, вилучення, пошкодження, впровадження або знищення даних, створення умов для зміни поведінки їх користувачів.

Одним із важливих засобів захисту від кібернетичних атак є системи виявлення атак (СВА) – програмні або апаратні засоби, які призначені для виявлення фактів неавторизованого доступу у комп'ютерну систему або мережу або несанкціонованого керування ними. Проте, незважаючи на той факт, що у теперішній час питанням побудови СВА присвячено велику кількість наукових робіт, головне питання – ефективне застосування СВА для побудови системи кібернетичного захисту, залишається не вирішеним.

У свою чергу, це обумовлює актуальність подальших досліджень, які полягають у підвищенні ефективності застосування СВА на основі розробки та впровадження нових методів виявлення кібернетичних атак.

Аналіз останніх досліджень і публікацій показує, що методи виявлення атак у сучасних СВА недостатньо повно опрацьовані з точки зору стійкості, адаптованості та верифікації, а також достатньо складно оцінити їхні властивості такі, як обчислювальна складність, коректність, завершуємість та ін.

У свою чергу, аналіз відомих на сьогоднішній день СВА з відкритим кодом за прийнятими критеріями показує, що жодна з них у повній мірі не відповідає ним, зокрема завдяки відсутньої адаптації до невідомих типів атак та неможливості аналізувати поведінку інформаційної системи (ІС) на всіх рівнях одночасно.

Таким чином, проведений аналіз методів і СВА дозволяє зробити висновок про відсутність у теперішній час СВА, яка б була адаптивною до невідомих атак. Незважаючи на те, що існує велика кількість методів виявлення аномалій, їхня слабка стійкість, неверифікація, велика кількість хибних спрацьовувань, вузька спеціалізація та дослідницький характер, не дозволяють широко використовувати їх в ІС.

Для усунення даних недоліків, є доцільним проведення низки наукових досліджень щодо розробки адаптивної СВА, в основу функціонування якої необхідно покласти методи, які б при низькій (близькій до лінійної) обчислювальній складності, стійкості та верифікації мали б низькій рівень хибних спрацьовувань.

Тому, прспективними напрямками подальших наукових досліджень у галузі розробки систем виявлення кібернетичних атак можна вважати:

розробку моделей ідентифікації атак (у тому числі, на основі теорії нечітких множин та нечіткого логічного виводу);

розробку методів збору, узгодження, очищення, верифікації вхідних даних та завантаження їх у централізоване Сховище Даних СВА;

розробку методів і методик добування та формування знань у базі знань СВА;

розробку моделей та методів та візуального аналізу даних.

д.т.н., проф. Оксіюк О.Г.
КНУ ім. Т.Шевченка,
к.т.н. Прус Р.Б.
КНУ ім. Т.Шевченка,

ПОШУК ОПТИМАЛЬНОГО РІШЕННЯ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗ ВРАХУВАННЯМ ДІЙ НАПАДУ

Постійне зростання потоків інформації та її вартості сприяє збільшенню інтенсивності атак. Це викликає необхідність прийняття адекватних заходів з боку захисту інформації. Проте націленість атак з часом може змінюватись, супроводжуючись перерозподілом ресурсів нападу між об'єктами. Подібна ситуація виникає, зокрема, при проведенні розвідки, коли зловмисник не має відомостей про об'єкти і в результаті розвідки має можливість спрямувати свої зусилля у вигідному для себе напрямку. Перерозподіл ресурсів нападу викликає відповідну реакцію захисту, змушуючи перерозподіляти власні інвестиції.

Оптимальне рішення про розподіл інвестицій між об'єктами захисту інформації у запропонованій моделі відповідає сідловій точці цільової функції, яка визначає завдану шкоду від реалізації загроз при протистоянні двох сторін:

$$i(x,y)=\sum_{k=1}^{I} i_k(x,y)=\sum_{k=1}^{I} g_k p_k f_k(x_k,y_k)\,, \qquad (1)$$

де $k=\overline{1,l}$ – номер об'єкта; x_k і y_k – інвестиції нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$, $x_k \geq 0$, $\sum_{k=1}^{l} y_k = Y$, $y_k \geq 0$; g_k – відносна цінність інформації на об'єкті, $\sum_{k=1}^{l} g_k = 1$; p_k – імовірність реалізації загрози на об'єкті; $f_k(x_k, y_k)$ – уразливість k-го об'єкта, яка залежить від співвідношення інвестицій нападу і захисту.

При динамічному управлінні розподіл ресурсів проводиться з затримкою – після того, як визначено націленість атак, що забезпечує досягнення оптимальних показників в ситуаціях, які постійно змінюються. Тому для підвищення ефективності використання запропонованої моделі необхідне застосування надійної системи моніторингу інцидентів інформаційної безпеки та механізму сповіщення про атаки. Моніторинг інцидентів, що включає збір, обробку, передачу та аналіз інформації про систему, стає ключовим елементом при обогрунтуванні рішень в задачах інформаційної безпеки.

Запропонована модель динамічного управління інвестиціями у захист інформації за рахунок врахування дій суперника дає змогу оцінити наслідки прийнятих рішень, прогнозувати рівень очікуваних втрат та вчасно і опертивно реагувати на інциденти інформаційної безпеки і запобігати атакам зловмисників.

Павлов І.М.
Державний університет телекомунікацій

ОЦІНКИ ЕФЕКТИВНОСТІ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми. Під час аналізу процесів захисту інформації на етапі ескізного проектування, коли розробник моделює ворожу для системи захисту обстановку передусім мають бути сформульовані правила гри, тобто система умов, яка визначає можливі варіанти дій протилежних сторін (гравців), послідовність ходів, обсяг інформації кожного гравця про поведінку іншого і про функцію виграшу. Можливі варіанти способів дій витікають безпосередньо з аналізу конфліктної ситуації. Однією з перспективних математичних теорій, яка може надати інструменти для розв'язання таких ситуацій є математична теорія ігор. Правильно вибрати математичний апарат для моделювання таких процесів в системах захисту інформації є головною проблемою будь-якого дослідження.

У зв'язку з цим, аналіз підходів оцінки ефективності математичних моделей при проектуванні систем захисту інформації та обгрунтування класифікації таких підходів, є *актуальними науковими завданнями*.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені, неповні, а у деяких випадках суперечливі.

Так, використання математичного аналізу [1] дає змогу обгрунтувати лише часткові данні класифікації моделей теорії ігор такі як, кількість зацікавлених сторін та кількість коаліцій дій гравців. Математичні моделі аналізу [2] розкривають тільки моделі за результатами гри, за характером та об'ємом інформації, в залежності та кількості можливих стратегій. Джерело [3] розкриває моделі за кількістю коаліцій дій гравців, за виграшем гри, за характером отримання інформації, за кількістю стратегій. Автори [4] розкривають тільки класичні кооперативні ігри не вдаючись до їх місця у загальній теорії ігор. Автори [5] у загалі надають приклади безкінцевих антагоністичних ігор не розкриваючи класифікації математичних підходів теорії ігор. Автор [6] розкриваючи моделі статистичних та динамічних ігор і будуючи математичні перетворення в інтересах моделювання нападів на інформацію зовсім не визначив місце і роль математичних моделей теорії ігор в аналізі систем захисту інформації. Надаючи обгрунтування доцільності застосування теорії ігор для моделювання процесів нападу на інформацію автор [7] пропонує такі перетворення тільки для 2-х гравців, що є частковим прикладом коаліційної гри, а не питання розгляду роботи системи захисту інформації у цілому. Особливо це важливо при розгляді питань аналізу систем захисту інформації під час проектування.

Для проведення аналізу процесів прийняття рішення розробнику необхідно мати чітку уяву місця своїх досліджень в предметній області. Пропонуючи основні результати досліджень в області захисту інформації необхідно відштовхуватися від зрозумілих посилань на місце аналітичних моделей прийняття рішень в процесі моделювання роботи систем захисту інформації.

Таким чином, *метою доповіді є* надання системного аналізу підходам оцінки ефективності математичних моделей прийняття рішень при проектуванні систем захисту інформації. В доповіді вперше представлено повний аналіз моделей теорії ігор у вигляді струнокої класифікації, у якій була зроблена спроба проаналізувати різні підходи в побудові математичних моделей протиборства гравців як у вигляді окремих протилежних стратегій – як частковий випадок, так і побудови системи математичних моделей прийняття рішень на застосування різних підходів моделювання роботи процесу захисту інформації. Представлені математичні моделі, як правило, повинні використовуватися в різних інтерпретаціях в залежності від поставлених цілей та задач досліджень роботи систем захисту інформації.

Література:

1. Оуен. Г. Теория игр / Г. Оуен. – М.: 1971. – Мир. – 230. с.
2. Вентцель Е.С. Элементы теории игр / Е.С. Вентцель. – М.: 1961. – Физматгиз. – Вип. 32. – 72 с.
3. Петросян Л.А. Теория игр / Л.А. Петросян, Н.А. Зенкевич, Е.А. Семина. – М.: 1998. – Вища школа. – 304 с.
4. Дюбин Г.Н. Введение в прикладную теорию игр / Г.Н. Дюбин, В.Г. Суздаль. – М.: 1981. – Наука. – 336 с.
5. Воробьев Н.Н. Бесконечные антагонистические игры / под ред. Н.Н. Воробьева. – М.: 1993. – Вища школа. – 505 с.
6. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень / Р.В. Грищук. – Монографія. – Житомир. – 2010. – 280 с.
7. Павлов І.М. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації / І.М. Павлов, С.В. Толюпа. "Сучасний захист інформації". – К.: 2014. − № 2. − С.59 − 68.

Толюпа С.В., Яремчук Ю.Є.
Державний університет телекомунікацій

ОСОБЛИВОСТІ РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ АСИМЕТРИЧНОГО ШИФРУВАННЯ

В асиметричних криптографічних системах шифрування інформації [1] використовуються різні ключі: відкритий ключ – для зашифрування даних, а секретний – для дешифрування. Відкритий ключ публікується для використання усіма користувачами системи, що бажають зашифрувати і відправити дані одержувачу. Секретний ключ використовується одержувачем для дешифрування даних, він не може бути визначений з відкритого ключа зашифрування, принаймні на це необхідний неприйнятно великий час.

Найбільш відомими асиметричними криптоалгоритмами є RSA [2] та Ель-Гамаля [3]. Стійкість методів асиметричного шифрування базується на складності вирішення математичних задач для великих чисел, однак необхідність виконувати обчислення з великими числами створює певні обчислювальні проблеми і санкціонованому користувачу, що використовує метод.

У цьому зв'язку в роботі [4] було запропоновано метод асиметричного шифрування інформації, що базується на математичному апараті рекурентних U_k –послідовностей, який у порівнянні з відомими аналогами забезпечує спрощення обчислень при достатньому рівні криптографічної стійкості. У роботі [5] представлено алгоритми та особливості програмної реалізації цього методу.

Однак представлений у роботі [4] метод асиметричного шифрування має потенційні можливості для підвищення крипостійкості, тому в роботі [6] запропоновано метод асиметричного шифрування на основі математичного апарату рекурентних V_k^+ –послідовностей, який, у порівнянні з методом шифрування на основі U_k –послідовностей забезпечує вищу криптографічну стійкість, оскільки під час шифрування/дешифрування відкрите/зашифроване повідомлення поєднується з результатом обчислень елементу V_k^+ –послідовностей, обчисленого за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальним залишається розроблення алгоритмів та визначення особливостей програмної реалізації представленого у [6] методу асиметричного шифрування на основі V_k –послідовностей.

Розроблення алгоритмів та програм реалізації методу асиметричного шифрування на основі V_k –послідовностей.

Розглянемо особливості розробки програмної реалізації процедур шифрування та дешифрування інформації згідно представленого у [6] методу асиметричного шифрування інформації.

Шифрування інформації в відбувається над блоками відкритого повідомлення M, яке розбивається на окремі частини M_j, що визначається розміром модуля – параметру p.

Параметр p вибирається як випадкове число, розрядність якого кратна розрядності машинної одиниці інформації і залежить від можливостей комп'ютера, на якому реалізується програма шифрування інформації. Для сучасних комп'ютерів цю розрядність слід вибирати 1024, 2048 або 4096 розряди.

Вибір параметру p здійснюється в програмному модулі завдання та вибору параметрів, де окрім нього задається параметр k та вибираються коефіцієнти рекурентного співвідношення g_i, $i = \overline{1,k}$.

Коефіцієнти g_i, $i=\overline{1,k}$, вибираються як випадкові числа. Оскільки параметр p є модулем при обчисленнях та визначає верхню границю усіх чисел, що використовуються в алгоритмах шифрування, вибір параметрів g_i, $i=\overline{1,k}$, здійснюється в діапазоні [, p_.

Для вибору параметрів алгоритмів шифрування/дешифрування використаємо звичайні генератори випадкових чисел. Для генерування параметрів g_i, $i=\overline{1,k}$, може використовуватись один з відомих генераторів випадкових чисел, наприклад, лінійний конгруентний генератор.

В алгоритмах шифрування/дешифрування інформації генератор випадкових чисел потрібен і для вибору секретних ключів a та b. Для вибору секретних ключів рекомендується використовувати більш випадкові генератори.

Одним з найбільших під час програмної реалізації є модуль реалізації математичного апарату рекурентних V_k –послідовностей, для якого виділено спеціальний клас його реалізації.

Для кожної операції класу Vk розроблено модульні тести, що перевіряють правильність реалізованих операцій. Загалом тести містять у собі порівняння елементів послідовності отримані у результаті використання певної операції та у результаті використання прямої формули.

Розглянемо основні особливості щодо реалізації модулів виконання криптографічних операцій та відповідних їм модульних тестів, які будуть підтверджувати правильність реалізації алгоритмів.

Реалізація алгоритмів методів асиметричного шифрування на основі V_k та U_k –послідовностей [4, 6] є схожою. Кожна сторона генерує велике просте число A та B, яке зберігається у відповідних параметрах кожного модуля. Також є параметри, у яких зберігаються послідовності _vka та _vkb відповідно для кожної сторони. Вираховується A-й та B-й елемент послідовності. Процес шифрування складається з того, що формується відкритий ключ внаслідок отримання елементу з індексом A+B, і послідовність додається за модулем 2, внаслідок чого отримується шифртекст. Процес дешифрування виглядає ідентично, тільки виконується додавання елементів послідовності B та A, після чого шифротекст додається за модулем 2 з отриманим ключем. Модульні тести для методів на основі V_k та U_k –послідовностей аналогічні.

Висновки.

Таким чином здійснено розробку програм реалізації представленого у [6] методу асиметричного шифрування інформації на основі V_k –послідовностей. Розроблено алгоритми програмної реалізації процедур шифрування та дешифрування інформації для цього методу. Розглянуто основні особливості щодо реалізації модулів виконання криптографічних операцій та відповідних їм модульних тестів. Найбільш докладно розглянуто програмний модуль реалізації математичного апарату рекурентних V_k –послідовностей, для якого виділено спеціальний клас його реалізації, описано параметри та операції цього класу.

ЛІТЕРАТУРА

1. Menezes, A.J. Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.

2. Rivest, R.L. A method for obtaining digital signatures and public-key cryptosystems [Текст] / R.L. Rivest, A. Shamir, and L.M. Adleman // Communications of the ACM. – 1978. – Volume 21, Issue 2. – P. 120–126.

3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms [Текст] / T. ElGamal // IEEE Intern. Symp. Informat. Theory. – 1985. – V.IT–31. №4. – P. 469–472.

4. Яремчук, Ю.Є. Метод асиметричного шифрування інформації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасна спеціальна техніка. – №4, 2012. – С. 79–87.

5. Яремчук, Ю.Є. Особливості розроблення програмних засобів реалізації протоколів асиметричного шифрування інформації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Вісник Тернопільського національного технічного університету. – №1, 2013. – С. 174–182.

6. Яремчук Ю.Є. Особливості розроблення програмних засобів для асиметричного шифрування на основі рекурентних vk-послідовностей. . “Сучасний захист інформації”. – К.: 2014. − № 3. − С.59 − 68.

Толюпа С.В., Головко А.А.
Державний університет телекомунікацій

ВИКОРИСТАННЯ ШИРОКОСЕКТОРНИХ НИЗЬКОПРОФІЛЬНИХ АНТЕН ПРИ ОРГАНІЗАЦІЇ МЕРЕЖ РАДІОЗВ'ЯЗКУ ТА РАДІОРОЗВІДКИ

Системи рухомого радіозв'язку динамічно удосконалюються у всіх країнах світу й на сьогоднішній день продовжують залишатися одним з найбільш перспективних сегментів телекомунікаційної галузі. Застосування цифрових способів передачі й обробки інформації є одною з головних тенденцій розвитку сучасних систем рухомого радіозв'язку. Саме тому перспективи розвитку мобільних інфокомунікаційних систем в різноманітних сферах пов'язані перш за все з активним використанням цифрових технологій.

При плануванні стільникових мереж зв'язку виникає безліч проблем, пов'язаних з ефективним використанням радіочастотного спектру і забезпеченням внутрішньосистемної електро-магнітної сумісності (ЕМС) в процесі реалізації повторення частот і що включають: раціональний вибір місцеположення базових станцій (БС), що використовують однакові частотні групи; визначення мінімальної відстані між БС залежно від умов розповсюдження радіохвиль; вибір типів антен, визначення висоти їх розташування і орієнтації діаграм направленості (ДНА) і т.д.

Одним з методів вирішення даних проблем є застосування на БС антен із змінною ДНА, які дозволяють отримати значний виграш в зниженні рівня внутрішньосистемних радіоперешкод, а значить підвищити щільність трафіку, а також збільшити зону і якість обслуговування БС. Суть цього методу полягає у використанні низькопрофільних антен, що формують в ідеалі індивідуальні ДНА у напрямку кожної обслуговуваної абонентської станції (АС) або їх групи.

В значній мірі можливості перспективних систем радіозв'язку (СРР) визначаються технічними параметрами антенних систем БС: коефіцієнтом підсилення; діаграмою направленості; рівнем бічних пелюсток, які у свою чергу залежать від амплітудно-фазового розподілу поля на апертурі антени, конструкції і розмірів випромінюючих елементів і т.д. Такі параметри систем рухомого зв'язку, як робоча частота, кількість каналів, що використовуються, допустиме відношення сигнал/шум, зона обслуговування і деякі інші, які є суттєвими для низько профільних антен (НПА).

Перевагами НПА є:

- сумування сигналів як при передачі, так і при прийомі, що збільшує відношення сигнал/шум - зниження впливу завмирань сигналів за рахунок рознесеного прийому (передачі);
- вибіркове придушення завад і забезпечення просторової фільтрації сигналів і завад;
- збільшення пропускної спроможності мережі за рахунок просторового ущільнення каналів.

В перспективних СРР вказані властивості НПА можуть забезпечити обслуговування зон з високою щільністю абонентів, широку зону впевненого прийому і високу пропускну спроможність мережі.

Проте використання НПА в мережах рухомого зв'язку передбачає ряд вимог до цих систем:

1) НПА повинні забезпечити достатнє підсилення корисних сигналів від абонентів мережі. Коефіцієнт підсилення антен характеризує здатність збільшення відношення сигнал/шум на вході приймача.

2) НПА повинні забезпечити виграш за рахунок рознесеного прийому. Реалізація цієї переваги вимагає розміщення елементів антен на відстані декількох довжин хвиль, що залежить у свою чергу від виду діаграми направленості кожної окремої НПА, висоти антени БС і місцевих перешкод;

3) НПА повинні забезпечити ущільнення каналів, що дозволить значно збільшити швидкість передачі в СРР. При ущільненні каналів потрібна наявність багатоелементних антен на обох кінцях радіолінії.

Таким чином, всі перераховані вимоги до НПА направлені на підвищення ефективності використання частотного спектру в перспективних стільникових СРР.

Враховуючи нинішнє політичне положення нашої країни: проведення військових операцій на сході, забезпечення надійним зв'язком мирного населення, виникає завдання щодо забезпечення необхідних зони покриття при організації радіозв'язку, що постійно потребує в сфері антенної техніки нових технічних рішень для її вирішення.

Як відомо антенний пристрій є невід'ємним елементом всіх сьогоденних базових станцій систем радіозв'язку та є складовою частиною її антенно-фідерного пристрою. Безпосередня роль антенного пристрою, щодо забезпечення необхідної зони покриття, полягає у формуванні заданої характеристики направленості (ХН) поля випромінювання в двох основних взаємно-ортогональних площинах: азимутальній та меридіальній, а також у забезпеченні необхідного коефіцієнту підсилення. В залежності від особливостей побудови мереж радіозв'язку, висуваються жорсткі вимоги саме до антени базової станції з формування поля випромінювання, насамперед, в азимутальній площині від ненаправленого до секторного як з вертикальною так і з горизонтальною поляризацією випромінюючого поля.

Аналіз перспектив застосування антенних технологій в системах рухомого зв'язку показує, що побудова стільникових СРР, використовуючи переваги НПА дозволить впровадити ефективніші методи повторного використання частот, поліпшити просторово-часові характеристики сигналів при прийомі і передачі і успішно боротися з завадами, що підвищить ефективність використання частотного спектру і місткість стільникових мереж при заданій якості обслуговування.

Отже, застосування НПА в якості випромінюючого елемента двохелементної дугової решітки надає змогу створити компактний антенний пристрій, застосування якого розширить можливість традиційних НПА з плоским

екраном в плані формування широкосекторних ДН в азимутальній площині. На відміну від симетричного вібратору розташованого над трубою, як єдиного АП, що може бути застосований в нижній частині дециметрового діапазоні довжин хвиль для формування широкосекторних ДН, практична реалізація запропонованої конструкції можлива в усьому дециметровому діапазоні довжин хвиль.

Список літератури

1. *Бузов А.Л. Антенно-фидерные устройства систем сухопутной подвижной связи / Бузов А.Л., Казанский Л.С.; под ред. А.Л. Бузова. М.: Радио и связь, 1997. - 150 с.*

2. *Ломан В.И. Микрополосковые антенные устройства / Ломан В.И., Ильинов М.Д.. – М.: Зарубежная радиоэлектроника. – № 10, 1981. – С. 99 – 115 с.*

3. *Ільїнов М.Д., Толюпа С.В., Шацький І.О. Широкосекторна низькопрофільна антена. // Науково- технічний журнал "Сучасний захист інформації".– 2012. - №3. – С. 78-83.*

4. *Резников Г.Б. Антенны летательных аппаратов / Резников Г.Б. – М. : Сов. радио, 1967. – 415 с.*

5. *Ільїнов М.Д, Мацаєнко А.Н., Шацький І.О. Антена базової станції з секторною діаграмою направленості в азимутальній площині // Зб. наук. праць ВІТІ НТУУ. -К.: «КПІ», 2010. - № 1.*

6. *Mimo and smart antennas for 3G and 4G wireless systems: Practical Aspects and Deployment Considerations, May 2010. – 135 p.*

Субач .Ю., Лойко А.О.
Державний університет телекомунікацій

КРИПТОГРАФІЧНИЙ МОДУЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ УДОСКОНАЛЕНОГО АЛГОРИТМУ ШИФРУВАННЯ CLEFIA

Інформація − це одна з найцінніших речей у сучасному житті. Поява глобальних комп'ютерних мереж зробило простим отримання доступу до інформації як для окремих людей, такі для великих організацій. Але легкість і швидкість доступу до даних за допомогою комп'ютерних мереж, таких як Інтернет, також зробили значними наступні загрози безпеки даних за відсутності заходів їх захисту:

- не авторизований доступ до інформації;
- не авторизоване зміна інформації;
- не авторизований доступ до мереж та інших сервісів;
- інші мережеві атаки, такі як повтор перехоплених раніше транзакцій і атаки типу "відмова в обслуговуванні";
- використання застарілих та не ефективних алгоритмів шифрування.

Для боротьби з цими загрозами необхідна така наука як криптографія. Криптографія − це наука про забезпечення безпеки даних. Вона займається пошуками рішень чотирьох важливих проблем безпеки − конфіденційності, аутентифікації, цілісності та контролю учасників взаємодії. Основні напрямки використання криптографічних методів − передача конфіденційної інформації каналами зв'язку (наприклад, електронною поштою), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

На даний час існує безліч криптоалгоритмів, деякі з них розроблені «в надрах спецслужб» або науковими інститутами, а деякі розроблені приватними особами, та не зважаючи на це серед них є досить вдалі і широко використовувані.

Результатом масового використання сучасних інформаційних технологій є необхідність масового використання криптографічних методів, а, отже, і необхідність поширення досліджень і розробок в даній галузі. Знання основ криптографії стає суттєво необхідним та важливим для вчених та інженерів, що займаються розробкою сучасних засобів захисту інформації, експлуатацією і проектуванням інформаційних та телекомунікаційних систем.

У наш час завдання вдосконалення методів шифрування в обчислювальних системах є особливо ***актуальним*** саме тому, що значно збільшилася сфера використання комп'ютерних мереж. Сьогодні за допомогою комп'ютерних мереж передаються великі обсяги інформації різного характеру (військового, державного, особистого і комерційного), що не дає змоги стороннім особам получити доступу до неї, але водночас, виникнення сучасних надпотужних комп'ютерів, поява технологій нейронних і мережевих розрахунків робить можливим дискредитацію систем шифрування, які ще нещодавно вважалися цілком безпечними.

Метою доповіді є підвищення ефективності криптографічного захисту інформаційних ресурсів шляхом розробки криптографічного модуля на основі удосконаленого алгоритму шифрування Clefia.

Під ефективністю будемо розуміти забезпечення криптостійкості до диференціального криптоаналізу та підвищення швидкості криптографічного перетворення даних в програмній реалізації.

Для досягнення поставленої мети необхідно буде вирішити ***наступні задачі***:

- провести аналіз існуючих симетричних алгоритмів шифрування даних;
- проаналізувати сучасні криптографічні модулі захисту інформації (ЗІ);
- розробити метод побудови алгоритмів шифрування;
- удосконалити криптографічний алгоритм Clefia;

– розробити криптографічний модуль ЗІ на основі удосконаленого алгоритму Clefia;
– провести експериментальне дослідження розробленого модуля ЗІ.

Оскільки задача захисту інформаційних ресурсів в інформаційному столітті є завжди актуальною, то реалізований алгоритм шифрування даних, в рамках даної дипломної роботи, і розроблений модуль захисту інформації, який реалізовує шифрування даних завдяки цьому алгоритму, знайдуть своє місце в комерційних організаціях, так як саме вони найбільш звертають увагу на забезпечення безпеки інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — М. : Горячая линия − Телеком, 2002. — 175 с.
2. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99 /
3. Иванов М. А. Стандарт криптографической защиты - AES (Advanced Encryption Standart). Конечные поля. Книга 1. / О. С. Зензин, М. А. Иванов. – М. : КУДИЦ-Образ, 2002. — 174 с.
4. Ященко В.В. Введение в криптографію / В.В. Ященко. — П.: Питер, 2001. — 288 с.
5. Shannon C.E. A Mathematical Theory of Communication. / C.E. Shannon. // Bell System Technical Journal. — 1948. — №27, pp. 379—423, 623—656.
6. Бабенко Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Бабенко Л.К., Ищукова Е.А. — М.: Гелиос АРВ — 2006.
7. Аграновский А. В. Практическая криптография. Алгоритмы и их программирование / Аграновский А. В., Хади Р. А. — СПб, СОЛОН-Пресс, — 2002.

Толюпа С.В., Софієнко І.І.
Державний університет телекомунікацій

МЕТОДИКА ОЦІНКИ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ

Реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей. Теорія нечітких мір, нечіткої логіки або *Fuzzy Logic* – новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу – введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі [1,2].

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості, кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість.

Розроблені моделі і методи вирішення задач нечіткого математичного програмування, які адекватні сучасним умовам функціонування об'єктів інформаційної діяльносі (ОІД), дозволяють підвищити наукову обґрунтованість, ефективність рішення, що формулюється та приймається при нечіткій вхідній інформації, збільшують аналітичну базу, надають можливість формалізації різних параметрів задачі та різноманітних цільових установок.

Існує декілька причин використання ТНМ. По-перше, нечіткі множини ідеально описують суб'єктну активність посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію. По-друге, нечіткі числа ідеально підходять для планування факторів у часі, коли їх майбутня оцінка ускладнена (розмита, не має достатніх імовірнісних умов). Таким чином, всі сценарії за тими чи іншими окремими факторами можуть бути зведені в один сценарій у формі трикутного числа, де відокремлюють три позиції: мінімально можливе, найбільш очікуване та максимально можливе значення фактору. По-третє, при використанні нечітких множин ми можемо в межах однієї моделі формалізувати особливості застосування ОІД [3].

Математичні моделі на основі Fuzzy-технологій набули широкого розповсюдження для вирішення задач в електроніці, кібернетиці, управлінні складними інтелектуальними системами. Більшість з таких завдань відносяться до класу експертно-аналітичних завдань (ЕАЗ) оцінки і прогнозу стану КСЗІ, вирішення яких повинне базуватися на методах системного аналізу, експертній методології і перспективних математичних методах обробки даних.

Запропоновано методику, яка ґрунтується на новій сукупності показників, принципах побудови математичної моделі (ММ) оцінки КСЗІ, визначення інтегральних показників на основі часткових. У той же час методика, що пропонується, використовує як окремі елементи положення всіх раніше відомих підходів та сумісна з ними.

Як результат, ММ оцінки КСЗІ, є оціночною та прогнозованою за цільовою спрямованістю; багаторівневою за

ієрархічною структурою; аналітичною за способом опису функціональних зв'язків; імовірнісною з точки зору врахування стохастичної невизначеності; комбінованою за способом урахування випадкових факторів (реалізовані детермінований та стохастичний підходи з урахуванням нестохастичної невизначеності); за характером вихідної інформації такою, що використовує методи обробки нечітких даних.

ЛІТЕРАТУРА

1. Алексеев А.В. Интерпретация и определение функций принадлежности нечетких множеств / А.В. Алексеев // Методы и системы принятия решений. - Рига: Риж. политехн. ин-т, 1979. - С. 42 - 50.
2. Бочарников В.П. Fuzzy - технология: Математические основы. Практика моделирования в экономике / В.П. Бочарников. - СПб.: "Наука" РАН, 2001. - 328 с.
3. Толюпа С.В., Борисов І.В. Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності. // Науково-технічний журнал "Сучасний захист інформації".– 2013. - №2. – С. 43-49.

Толюпа С.В., Боярский Ю.К.
Державний університет телекомунікацій

ПІДХОДИ МОДЕЛЮВАННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми. У багатьох ситуаціях проектування систем захисту інформації виникає необхідність розробки та прийняття рішень в умовах невизначеності. Невизначеність може мати різний характер. Так, невизначеними є сплановані дії хакерів, які скеровані на зменшення ефективності систем захисту; невизначеність може стосуватися ситуації ризику, в якій система управління інформаційної мережі, що приймає рішення по застосуванню системи захисту, здатна встановлювати не тільки усі можливі результати рішень, але й вірогідність можливих умов їх появи. Умови проектування впливають на прийняття рішень підсвідомо, незалежно від дій суб'єкта, що приймає рішення. Коли відомі всі наслідки можливих рішень, але невідома їх вірогідність, очевидно, що рішення приймають в умовах повної невизначеності. Основною перспективною теорією аналізу процесів прийняття рішень на етапі проектування систем захисту інформації є теорія ігор. Застосування теорії ігор в області моделювання процесів прийняття рішень має різні підходи, які в наступний час не систематизовані а інколи і вступають в протиріччя між собою.

У зв'язку з цим, аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації та обґрунтування класифікації таких підходів, *є актуальними науковими завданнями*.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені, неповні, а у деяких випадках суперечливі.

Так, використання математичного аналізу [1] дає змогу обґрунтувати лише часткові данні класифікації моделей теорії ігор такі як, кількість зацікавлених сторін та кількість коаліцій дій гравців. Математичні моделі аналізу [2] розкривають тільки моделі за результатами гри, за характером та об'ємом інформації, в залежності від кількості можливих стратегій. Джерело [3] розкриває моделі за кількістю коаліцій дій гравців, за виграшем гри, за характером отримання інформації, за кількістю стратегій. Автори [4] розкривають тільки класичні кооперативні ігри, не вдаючись до їх місця у загальній теорії ігор. Автори [5] у загалі надають приклади безкінцевих антагоністичних ігор не розкриваючи класифікації математичних підходів теорії ігор. Автор [6] розкриваючи моделі статистичних та динамічних ігор і будуючи математичні перетворення в інтересах моделювання нападів на інформацію, зовсім не визначив місце і роль математичних моделей теорії ігор в аналізі систем захисту інформації. Надаючи обґрунтування доцільності застосування теорії ігор для моделювання процесів нападу на інформацію автор [6] пропонує такі перетворення тільки для 2-х гравців, що є частковим прикладом коаліційної гри, а не питання розгляду роботи системи захисту інформації у цілому. Особливо це важливо при розгляді питань аналізу систем захисту інформації під час проектування.

Для проведення аналізу процесів прийняття рішення розробнику необхідно мати чітку уяву місця своїх досліджень в предметній області. Пропонуючи основні результати досліджень в області захисту інформації необхідно відштовхуватися від зрозумілих посилань на місце аналітичних моделей прийняття рішень в процесі моделювання роботи систем захисту інформації.

Таким чином, *метою доповіді є* надання системного аналізу підходам моделювання процесів прийняття рішень при проектуванні систем захисту інформації.

Висновок. Надані авторами підходи моделювання процесів прийняття рішень, під час проектування систем захисту інформації, у подальшому надають можливість розкрити ознаки класу ефективності математичних моделей прийняття рішень (які запропоновані авторами у наступній статті).

У цілому автори пропонують стрункy класифікацію математичних моделей теорії прийняття рішень при проектування систем захисту інформації, яку можливо застосовувати як під час проектування самих систем захисту інформації, так і процесів, які моделюються для оцінки ефективності систем захисту інформації у різних життєвих циклах роботи.

Література:

8. Оуен. Г. Теория игр / Г. Оуен. – М.: 1971. – Мир. – 230. с.
9. Вентцель Е.С. Элементы теории игр / Е.С. Вентцель. – М.: 1961. – Физматгиз. – Вип. 32. – 72 с.
10. Петросян Л.А. Теория игр / Л.А. Петросян, Н.А. Зенкевич, Е.А. Семина. – М.: 1998. – Вища школа. – 304 с.
11. Дюбин Г.Н. Введение в прикладную теорию игр / Г.Н. Дюбин, В.Г. Суздаль. – М.: 1981. – Наука. – 336 с.
12. Воробьев Н.Н. Бесконечные антагонистические игры / под ред. Н.Н. Воробьева. – М.: 1993. – Вища школа. – 505 с.
13. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень / Р.В. Грищук. – Монографія. – Житомир. – 2010. – 280 с.

Толюпа С.В. , Дружинин В.А.
Державний університет телекомунікацій

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ В ПРОЦЕССЕ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

В каждой информационной системе можно выделить самые слабые с точки зрения безопасности места. На них необходимо обратить внимание прежде всего. К таким местам, конечно, принадлежат хранилища данных, административная система, кабельная система, система доступа из внешних сетей. Злоумышленник, найдя доступ к хранилищу данных, сможет взять из него конфиденциальные данные, а зайдя в административную систему, он будет иметь доступ ко всем ресурсам системы. К кабельной системе благодаря ее разветвленности легко присоединиться, подслушать и проанализировать данные, которые передаются, или подменить их другими [1].

Обеспечение защиты информации в системах происходит в условиях случайного действия разных факторов, часть из которых является систематизированной в стандартах, а часть заранее неизвестны. Оценка эффективности систем защиты информации (СЗИ) должна обязательно учитывать как объективные обстоятельства, так и вероятностные факторы, а ее характеристики должны иметь вероятностный характер. Особенную важность на современном этапе развития информационных технологий (ИТ) имеет обоснование оптимальных значений показателей эффективности и целевое назначение системы.

Чем более конкретно сформулирована цель защиты информации, детально выясненные ресурсы, которые привлекаются для этого, а также определен комплекс ограничений, тем в большей степени можно ожидать получения желательного результата. Если цель обеспечения информационной безопасности простая и принципиально досягаемая, то оказывается достаточно сравнительно несложных по составу и структуре средств защиты информации.

Однако при расширении круга проблем обеспечения интегральной информационной безопасности, содержание целевого назначения системы на формализированном уровне будет иметь многомерный, векторный характер. При этом значимость свойств отдельных элементов средств защиты информации снижается, а на первый план выдвигаются общесистемные задачи - определения оптимальной структуры и режимов функционирования системы, организация взаимодействия между ее элементами, учет влияния внешней среды и т. др. При целеустремленном объединении элементов в систему последняя будет иметь специфические свойства, сначала не свойственные ни одной из ее составных частей. При комплексном подходе имеют первостепенное значение только те свойства элементов, которые определяют взаимодействие друг из друга и оказывают влияние на систему в целом, а также на достижение поставленной цели [2].

В силу того, что средства безопасности любой ИС имеют ограниченные возможности относительно противодействия угрозам, всегда существует достоверность нарушения защиты, даже если во время тестирования механизмы безопасности не были обойдены или блокированы. Для оценки этой достоверности должны проводиться дополнительные исследования. В методическом плане определения эффективности СЗИ должно заключаться в выработке мысли относительно пригодности способа действий персонала или приспособленности технических средств к достижению цели защиты информации на основе измерения соответствующих показателей, например, при функциональном тестировании.

Проектирование, организация и применение СЗИ ИС фактически связано с неизвестными событиями в будущем и потому всегда содержат элементы неопределенности. Кроме того, присутствующие и другие причины неоднозначности, такие как недостаточно полная информация для принятия решений управления или социальнопсихологические факторы.

Объективной характеристикой качества СЗИ - степенью ее приспособленности к достижению уровня безопасности, который требуется, в условиях реального действия случайных факторов, может служить вероятность, которая характеризует степень возможностей конкретной СЗИ при заданном комплексе условий. Другими словами - достоверность достижения цели операции или достоверность выполнения задачи ИС. Эта достоверность должна быть

установлена в основу комплекса показателей и критериев оценки эффективности СЗІ. Во время синтеза системы возникает проблема решения задачи с многокритериальным показателем. При этом рассматриваются показатели эффективности, какие назначенные при решении задачи сравнения разных структур СЗИ. Оценка оптимального уровня гарантий безопасности в определенной мере зависит от убытка, связанного с ошибкой в выборе конкретного значения показателя эффективности. Для получения численных оценок риска необходимо знать распределения ряда случайных величин. Это в определенной степени ограничивает количественное исследование уровней гарантий безопасности, которые предоставляются СЗИ, но во многих практических случаях такие оценки можно получить с помощью имитационного моделирования или по результатам активного аудита СЗИ.

Применение распределенных систем поддержки принятия решений (РСППР) в системах обеспечения безопасности позволит более качественно решать вопросы комплексной защиты информационных сетей [3]. Анализ основных требований, предъявляемых к РСППР позволяет сделать вывод о том, что РСППР является сложной человеко-машинной системой, характеризуемой большим числом территориально распределенных элементов и выполняемых ими функций, высокой степенью связности элементов, сложностью алгоритмов выбора тех или иных управляющих воздействий и большим объемом перерабатываемой при этом информации. Проектирование такой системы представляет собой сложный, трудоемкий процесс, который требует использования как определенного методологического аппарата, так и соответствующего методического обеспечения [4]. Одной из основных задач при создании РСППР является выбор ее структуры, поскольку от того, как организована система во многом зависит эффективность ее функционирования и обеспечение информационной безопасности. Поэтому при выборе структуры должны учитываться различные условия ее функционирования и степени угроз. Учитывая требования, предъявляемые к функционированию РСППР, задача выбора структуры сформулирована с учетом взаимосвязи его задач и узлов в процессе их решения. Для решения этой задачи предложено использовать агрегативно-декомпозиционный подход, который включает последовательную декомпозицию выполняемых системой целей, функций и задач и их агрегирование на соответствующих уровнях детализации структуры для генерирования вариантов построения системы в целом.

ЛИТЕРАТУРА

1. Ленков С.В. Методы и средства защиты информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. - К.: Техника, 2008. - Т. 1. - 465 с.
2. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защити информационных системах. // Науково-технічний журнал “Сучасний захист інформації”.– 2012. - №4. – С. 69-74.
3. С.В. Толюпа Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / О.М. Власов, С.В. Толюпа // Наукові записки Українського науково-дослідного інституту зв’язку. Наук.-вироб. зб. – 2011 - №3(19). – С. 38-45.
4. Саати Т. Принятие решений. Метод анализа иерархий. / Саати Т. – М.: Радио и связь, 1993. – 311 с.

Толюпа С.В., Уварова Г.А.
Державний університет телекомунікацій

ЗАСТОСУВАННЯ ТЕОРІЇ ДЕКОМПОЗИЦІЇ ДЛЯ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Проблема багатьох інфокомунікаційних систем (ІКС) зв’язку зводиться до того, що кількість параметрів, необхідних для опису поводження системи (розмірність системи), виявляється дуже великою і прийняти правильне рішення в таких мережах досить складно, враховуючи, що інформація про стан мережі може бути досить суперечливою. Збільшення розмірності сучасної технології представляється об’єктивною тенденцією, яку можна спостерігати в історичному зрізі протягом усього розвитку цифрових ІКС.

Гарантування безпеки інформації в мережах нового покоління взагалі та їх системах управління є складним комплексним завданням. У міжнародних стандартах проблеми захисту інформації вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі. Такий підхід відповідає комплексному характеру забезпечення безпеки інформаційних систем на всіх етапах їх життєвого циклу – від концептуальних схем та проектування до технічної експлуатації та використання. Окремими заходами досягти мети, як правило, не вдається й тому в кожному випадку потрібно розглядати всю систему в комплексі, причому захищеність усієї інфокомунікаційної системи (мережі) визначається рівнем захищеності її найбільш слабкої частини [1].

Бурхливий розвиток інфокомунікаційних систем у напрямку збільшення їх розміру та ускладнення, розширення спектру послуг, які надаються абонентам, росту кількості компаній, які займаються проектуванням, експлуатацією пов’язаних між собою мереж, що належать різним власникам, необхідність підвищення надійності роботи мережі, якості обслуговування, економічної ефективності та інших вимог, провідні фірми та корпорації світу прийшли до однозначного висновку – необхідності створення гнучкої та надійної системи управління й ними, що і дасть можливість повисити якість ефективності функціонування системи в цілому [2].

Внаслідок критичних ситуацій, які виникають в мережах, та неспроможності відвернути їх, почались пошуки нових принципів, методів та засобів управління ефективністю системи. Одним з варіантів вирішення цієї проблеми є застосування штучного інтелекту [3].

Від вибору критерію й системи показників якості (СПЯ) багато в чому залежить результат оцінки і його практична цінність. Загальноприйнятим підходом до розробки системи показників якості складних систем є формулювання безлічі локальних СПЯ, що відповідає сукупності властивостей ІКС, які впливають на виконання поставлених перед нею завдань. Глобальна СПЯ, що характеризує загальну, єдину задачу, яка стоїть перед інфокомунікаційною системою, реалізується шляхом з'єднання вихідних локальних систем показників якості.

Пропонується метод формування системи показників якості, відмінний від традиційного, тобто пропонується, ґрунтуючись на математичних методах теорії декомпозиції (факторизації, функціональної й параметричної декомпозиції), замість визначення локальних СПЯ (ЛСПЯ) низького рівня ієрархії й наступного їхнього об'єднання в глобальну СПЯ (ГСПК) розглядати завдання функціонування ІКС у цілому. При такому підході до оцінки ефективності інфокомунікаційної системи зростає розмірність завдання, яке розв'язується, оскільки формулюється не одна ГСПЯ, а сукупність ієрархічно зв'язаних ЛСПЯ, але зате забезпечується конструктивність рішення завдання й ураховуються реальні поточні ймовірнісні характеристики приватних показників ефективності (ППЕ). Повнота такої СПЯ ґрунтується на тім, що вихідними даними для її формулювання є вимоги, які запропоновані користувачем до ІКС, математично коректно декомпозовані в інтересах їхнього подальшого використання.

Аналіз різних методів формування узагальненого показника ефективності інформаційних систем показав, що найбільш повний облік особливостей рішення завдання оцінки ефективності функціонування інфокомунікаційної системи, а також природне рішення проблем нормалізації й згортки систем показників якості досягається при застосуванні методу ймовірнісної скаляризації.

Суть методу полягає у використанні в якості узагальненого показника ефективності спільної ймовірності виконання вимог, пропонованих користувачем до системи по своєчасній, достовірній, безпечній і економічній передачі повідомлень.

Оцінка оптимального рівня гарантій безпеки в певній мірі залежить від збитку, пов'язаного з помилкою у виборі конкретного значення показника ефективності. Для отримання чисельних оцінок ризику необхідно знати розподіли ряду випадкових величин. Це певною мірою обмежує кількісне дослідження рівнів гарантій безпеки, які надаються СЗІ, але в багатьох практичних випадках такі оцінки можна отримати за допомогою імітаційного моделювання або за наслідками активного аудиту СЗІ. Багаторівневій структурі системи показників ефективності СЗІ відповідає багаторівнева структура форм представлення відповідних показників, які змінюються від кількісної шкали для оцінки показників нижнього рівня до якісної - на верхніх.

Таким чином, поняття ефективність нерозривно пов'язане з результатами процесу функціонування інфокомунікаційної системи, опирається на систему показників якості процесу функціонування й вимоги до них. Узагальнений показник ефективності системи із урахуванням наявності взаємообумовлених випадкових факторів, що визначають її роботу, доцільно визначати на основі апарата умовних імовірностей у вигляді спільної ймовірності виконання всіх завдань, які розв'язуються у ході функціонування інфокомунікаційної системи та забезпечення її безпеки.

Вибір методу оцінки ефективності функціонування інформаційної системи і ліній зв'язку в кожному конкретному випадку визначається особливостями процесу ведення зв'язку, зовнішніми умовами, наявним обчислювальним ресурсом і необхідним часом. Застосування методів оцінки ефективності функціонування системи дозволяє оцінити внесок окремих підсистем у виконання завдань, поставлених перед системою в цілому, оптимізувати підхід до рішення завдань обґрунтування технічних вимог, розробки структури системи управління інфокомунікаційної системи, розподілу ресурсів між її підсистемами та забезпечення інформаційної безпеки.

Література

1. Власов О.М. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / О.М. Власов, С.В. Толюпа // Наукові записки Наукові записки УНДІЗ. Науково-вироб. зб. – 2011 - №3(19). – С. 38-45.

2. Толюпа С.В., Іванова О.М., Демченко І.О. Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних // Науково-технічний журнал "Сучасний захист інформації".– 2013. - №1. – С. 25-30.

3. Кувшинов О.В., Лівенцев С.П. Вибір параметрів багатопозиційних сигналів для підвищення ефективності системи передачі інформації / О.В. Кувшинов, С.П. Лівенцев // Зб. наук. праць ВІТІ НТУУ "КПІ". – 2004. – Вип. 5. – С. 87 – 93.

Ковтун О., Гончаренко М.
Державний університет телекомунікацій

МЕТОДИКА ОЦІНКИ ПЕРЕДАТОЧНОЇ ХАРАКТЕРИСТИКИ КАНАЛУ РАДІОЗВ'ЯЗКУ

Для досягнення високої завадостійкості та ємності мобільних стільникових інформаційних систем зв'язку передбачається використовувати багаторівневу модуляцію в поєднанні із застосуванням турбокодів при передачі інформації.

Сьогодні розроблені методики, що дозволяють оцінити ослаблення сигналів в таких системах. У основі методик лежать емпіричні моделі взаємодії переданого сигналу із забудовою траси поширення. Вони дозволяють визначити усереднене значення медіанної потужності сигналу, що приймається, використовуючи асимптотичні формули, отримані за результатами експериментальних вимірів, і забезпечують адекватність для певних умов поширення [1].

Проблема оцінки стану каналу та вірогідності помилок з метою адаптивного управління параметрами мобільної радіомережі в системах радіозв'язку з ортогональними піднесучими, що функціонують в складній завадовій обстановці, є надзвичайно актуальною. Окрім цього, розробка математичних моделей для прогнозування вірогідності помилки в системах з ортогональними несучими, які функціонують в частото-селективному каналі за наявності перешкод від сусідніх базових станцій, є одним з ключових моментів при розробці програмних комплексів для моделювання роботи *OFDMA* систем радіозв'язку на системному підрівні, що дозволяють отримати кількісні оцінки характеристик для різних сценаріїв розгортання мережі мобільного зв'язку.

Стратегічним напрямом при вирішенні задачі підвищення ефективності системи передачі інформації і забезпечення її безпеки в сучасних радіосистемах є перехід від систем з жорсткою структурою до адаптивних систем. В адаптивних системах алгоритми передачі і прийому сигналів можуть узгоджено змінюватися залежно від зміни зовнішніх умов. Алгоритми адаптації повинні дозволяти в умовах мінімальної апріорної інформації досягти оптимальних параметрів системи [2].

При проектуванні адаптивних систем радіозв'язку залежно від їх призначення вирішується завдання оптимізації одного з показників ефективності при встановлених обмеженнях на інші. В свою чергу, розробка і впровадження адаптивних методів інформаційного обміну вимагають створення ефективних процедур контролю та прогнозування стану дискретних каналів і якості передачі інформації. Для вирішення даного завдання необхідне залучення методів сучасної математичної статистики, зокрема перевірки статистичних гіпотез щодо параметра (групи параметрів), який характеризує стан каналу зв'язку [3].

Завадостійкість приймання *OFDM*-сигналу суттєво залежить від точності оцінювання передаточної характеристики каналу зв'язку. Вплив навмисних завад, окрім безпосереднього погіршення завадостійкості приймання сигналу, суттєво спотворює оцінку каналу зв'язку й погіршує його захищенність. Існуючі методи оцінки передаточної характеристики каналу зв'язку не дозволяють забезпечити прийнятну точність в умовах впливу навмисних завад, тому виникає необхідність удосконалення цих методів [4].

Запропонований метод полягає в тому, що оцінка передаточної характеристики каналу зв'язку здійснюється методом поелементного ділення з використанням алгоритму виявлення подавлених шумовими завадами в частині смуги пілот-несучих з подальшим виключенням їх впливу на одержання остаточної оцінки передаточної характеристики. Таким чином, запропонований метод контролю стану каналу зв'язку для OFDM-радіолінії при впливі шумових завад в частині смуги володіє більш високою ефективністю порівняно з відомим методом поелементного ділення при зменшенні відношення сигнал/завада порівняно з усередненим відношенням сигнал/шум в каналі.

ЛІТЕРАТУРА

1. Помехоустойчивость и эффективность систем передачи информации / А.Г. Зюко, А. И. Фалько, И. П. Панфилов и др.; под ред. А.Г. Зюко. – М.: Радио и связь, 1985. – 272 с.

2. Толюпа С.В. Метод контролю стану каналу сучасних та перспективних радіосистем. // Науково-технічний журнал "Сучасний захист інформації".– Спецвипуск - 2012. – с. 73-79.

3. Толюпа С.В. Вибор оптимальних значень параметрів OFDM-сигналу засобів радіозв'язку в залежності від стану каналу. // Збірник наукових праць "Компютерні технології друкарства". 2012 - №28. с 187-194.

4. Channel estimation techniques based on pilot arrangement in OFDM systems / S. Coleri, M. Ergen, A. Puri, A. Bahai // IEEE Trans. Broadcast. – 2002. – Vol. 48. – № 3. – P. 223–229.

Толюпа С.В., Хлапонін Ю.І.
Державний університет телекомунікацій

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Одним з головних завдань, які вирішуються при створенні та функціонуванні інфокомунікаційних систем спеціального призначення (ІКС СП) є забезпечення належного рівня безпеки інформації. Вирішення цього завдання покладається на систему захисту інформації (СЗІ), як невід'ємну складову ІКС.

Аналіз загроз безпеці інформації та методів захисту від них, проведений в [1] показав, що поряд з криптографічними методами захисту інформації одним з основних напрямків забезпечення безпеки інформації в інфокомунікаційних систем спеціального призначення є застосування методів підвищення прихованості передачі сигналів. Тому вдосконалення існуючих та розробка нових методів формування та обробки сигналів, спрямованих на підвищення прихованості та енергетичної ефективності є перспективним напрямком досліджень у галузі інформаційної безпеки.

В статті запропоновано рішення другого аспекту задачі, шляхом формування принципово нової, порівняно з ІКМ, структури цифрового сигналу. При перетворенні початкового сигналу (стандартного сигналу ІКМ) такі характеристики системи, як необхідна смуга частот, завадостійкість та інформаційна швидкість передачі, потрібно зберегти незмінними, такими ж, як і у відповідних структур ІКМ сигналів. Це дасть можливість застосовувати даний спосіб на діючих телекомунікаційних трасах стандарту Е1.

Сутність розробленого методу полягає в тому, що замість кожної *k*-розрядної кодової комбінації окремого канального інтервалу (КІ) формується лише один імпульс-символ, в якому цифрова інформація, на відміну від ІКМ, міститься не в розміщенні нульових і одиничних імпульсів на відповідних розрядних позиціях кодової комбінації, а в номері тієї квантованої часової позиції, на якій розміщується цей одиночний імпульс [5, 6]. Назвемо такий інформаційно-насичений імпульс, що містить інформацію про всю кодову комбінацію, позиційним код-імпульсом (ПКІ).

Всі реальні системи передачі мають обмежену смугу частот передачі Δf та обмежене значення пікової потужності P (обмежений динамічний діапазон). Для отримання енергетичного виграшу, не виходячи при цьому за межі відведених для тракту стандартної смуги частот і обмеженого динамічного діапазону, необхідно, щоб ПКІ мав тривалість $\tau_{ПКІ}$ і потужність $P_{ПКІ}$ такі ж самі, як у одиночного імпульсу ІКМ кодової комбінації:

$$\tau_{ПКІ} = \tau_{ІКМ}, P_{ПКІ} = P_{ІКМ}. \quad (2)$$

Всі подальші перетворення утвореного ПКІ повинні виконуватись при забезпеченні умови, що значення його енергії буде залишатись постійним.

Оскільки потужність і тривалість одиночних імпульсів ПКІ та ІКМ однакові, то $\alpha_{ПКІ} = \alpha_{ІКМ} = \alpha$. Тому для одиночних імпульсів ймовірність помилки $P_{\text{пом}}$, яка залежить від аргументу інтеграла ймовірності α, буде мати однакове значення для ПКІ і ІКМ. Тобто, потенційна завадостійкість ПКІ буде однаковою з ІКМ.

За наведеними в статті характеристиками потенційний енергетичний виграш для сигналів ПКІ порівняно з сигналами ІКМ буде:

$$\beta_E = \varphi_{\text{ПКІ}} \Big/ \varphi_{\text{ІКМ}} = \frac{1}{1 \cdot \alpha^2_{\text{ПКІ}}} \Big/ \frac{1}{4 \cdot \alpha^2_{\text{ІКМ}}} = 4{,}82. \quad (6)$$

Вираз (6) характеризує максимально можливе значення енергетичного виграшу в ПКІ-системі. Досягнення енергетичного виграшу не повинно призводити до зменшення швидкості роботи системи. Для того щоб швидкість передачі не була знижена, а залишилась незмінною, необхідно знайти потрібну кількість квантованих часових позицій для кожного ПКІ. При дотриманні умов виразу (2) для передачі замість однієї восьмирозрядної кодової комбінації лише одного ПКІ необхідно мати не 8, а $L = 2^8 = 256$ квантованих часових позицій, на одній з яких повинен розташовуватись ПКІ. Така кількість часових позицій в системі, яка використовує восьмирозрядні кодові комбінації (наприклад, ІКМ-30/32), відводиться для передачі цілого циклу, який складається з $N = 32$ кодових комбінацій. Тому на форматі одного циклу, що містить L квантованих часових позицій, необхідно сформувати ПКІ не одного, а всіх N каналів. Для того, щоб реалізувати цю можливість, необхідно виділити резерв часу тривалістю рівно один цикл $T_{\text{ц}}$.

Таким чином, сформовані за таким принципом ПКІ виявляються розташованими не послідовно канал за каналом, як кодові комбінації ІКМ, а в іншому порядку. Утворені ПКІ розміщуються на N паралельних виходах. Кожен на своєму виході та на відповідній квантованій часовій позиції.

Далі необхідно кожному ПКІ надати індивідуальну відрізнювальну ознаку, яка показувала б його канальний порядковий номер *i*. Імпульсними сигналами, що мають такі індивідуальні ознаки є різного роду ортогональні імпульсні псевдовипадкові послідовності (ПВП) [4, 8]. Кожний i-й ПКІ перетворюється у відповідну i-ту ПВП. При цьому буде відбуватися взаємне накладання ПВП різних каналів, а також можливе накладання ПВП одного каналу (рис. 3). Але це не призводить до порушення прийому сигналів, оскільки при використанні методів оптимального прийому, заснованих на обробці квазіортогональних ПВП за допомогою узгоджених фільтрів, буде здійснено незалежне відтворення кожного з сигналів, які накладалися. Сигнал відповідного узгодженого фільтру буде прийматися із загальної суміші усіх інших сигналів, які будуть сприйматися як адитивна інтерференція (шум). Принцип обробки сигналів такої системи на приймальному боці буде аналогічним асинхронно адресній системі зв'язку з кодовим розділенням каналів, яка описана в літературі [4].

Недоліком запропонованого методу є збільшення складності обладнання приймального та передавального трактів. Проте розвиток елементної бази робить цей недолік несуттєвим.

Для оцінки ефективності [9] розробленого методу було створено імітаційну модель в середовищі програмування *MatLab*. Результати моделювання показали, що при використанні ПВП, які повністю ортогональні між собою, енергетична ефективність системи передачі інформації підвищується в 2,2 рази, порівняно зі стандартною ІКМ-системою. При використанні реальних ПВП (які не є повністю ортогональними) енергетичний виграш складає близько 15-20%.

Висновки. Таким чином, використання розробленого методу підвищує енергетичну ефективність при передачі сигналів в інформаційно-телекомунікаційних системах спеціального призначення, що в свою чергу дозволяє покращити прихованість та завадозахищеність, а значить, й інформаційну безпеку взагалі. Перевагою отриманої внаслідок запропонованих перетворень структури сигналу є, також, набуття властивостей шумоподібності, що, в свою чергу, підвищує прихованість передачі інформації. Така малопотужна шумоподібна суміш групового сигналу може передаватися, не створюючи завад сусіднім радіоелектронним засобам, які працюють в тому ж діапазоні частот. При цьому, також, ускладнюється розкриття факту передачі засобами радіотехнічної розвідки.

ЛІТЕРАТУРА

1. Сташук О.В. Цілісність інформації в інформаційно-телекомунікаційних системах спеціального призначення: загрози та методи захисту / О.В. Сташук, М.М. Браіловський, О.В. Труш // Збірник наукових праць ВІТІ НТУУ „КПІ". - 2010. - Вип. 1. - С. 32-36.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр - Изд 2-е. - М.: Вильямс, 2003. - 1104 с.
3. Прокис Дж. Цифровая связь: пер. с англ. / Дж. Прокис; под ред. Д.Д. Кловского. - М.: Радио и связь, 2000. - 797 с.
4. Варакин Л.Е. Теория систем сигналов / Л.Е. Варакин. - М.: Советское радио, 1978. - 304 с.
5. Пат. № 42417А Україна, МПК 7 Н 03 К 5/00. Спосіб аналого-цифрового перетворення електричних сигналів і позиційний код-імпульсний аналого-цифровий перетворювач електричних сигналів; Сташук О. В., Сташук Л. Д., Сташук В. Д. - Промислова власність, 2001, бюл. № 9, від 15.10.2001р.
6. Пат. № 5071 Україна, МПК 7 G 06 F 1/00. Кодоперетворювач ІКМ-сигналів у позиційні код-імпульсні сигнали; Сташук О.В., Сташук Л.Д., Сташук В.Д. - Промислова власність, 2005, від 15.02.2005р.
7. Теплов Н.Л. Теория передачи сигналов по электрическим каналам связи / Н.Л. Теплов. - М.: Воениздат, 1976 - 424 с.
8. Волков Л.Н. Системы цифровой радиосвязи: базовые методы и характеристики: учеб. пособ. / Волков Л.Н., Немировский М.С., Шинаков Ю.С. - М.: Эко-Трендз, 2005. - 392 с.
9. Толюпа С.В., Лівенцев С.П., Браун В.О., Жиров Б.Г. Оцінка ефективності систем захисту інформації в інформаційно-телекомунікаційних системах // Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки. - 2007. - № 15. - С. 86-89.

ЗМІСТ

к.п.н. Шевченко С.М., к.т.н., доцент Жданова Ю.Д.
Основні аспекти технології ADSL як прогресивної технології передачі інформації……...…3
Левковець Г. С.
Законодавчі аспекти управління інформаційною безпекою передачі закритої інформації по відкритим каналам……..…….…….3
Довгаль А. В.
Забезпечення інформаційної безпеки України……4
к.в.н. Аносов А. О.
МЕТОДИКИ АНАЛІЗУ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ……...…….……..4
к.фіз-мат.н. Лукова-Чуйко Н.В.
МЕТОДИ ОЦІНКИ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАСТОСУВАННЯ FUZZY-ТЕХНОЛОГІЙ……...…….……4
к.т.н. Одіяненко О.В.
ОБГРУНТУВАННЯ ВИБОРУ РАЦІОНАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ІНЦЕДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……...……....5
к.т.н., доцент Гулак Г.М.,к.т.н., доцент Жданова Ю.Д.
КРИПТОГРАФИЧНО СТІЙКИ ГЕНЕРАТОРИ ПВЧ……...……5
к.п.н. Шевченко С.М., Кисіль О.В.
РОЗРОБКА КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ДОМАШНЬОЇ МЕРЕЖІ…….……..….5
к.т.н. Одіяненко О.В.
СЕРВІС ЧАСОВИХ МІТОК І АВТЕНТИФІКАЦІЯ ПОВІДОМЛЕНЬ.....5
к.п.н. Шевченко С.М. Березюк А.С.
ЗАСТОСУВАННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ КЕРУВАННІ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ…….....5
к.фіз-мат.н. Лукова-Чуйко Н.В.
ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ДЛЯ ФОРМАЛІЗАЦІЇ ЗАДАЧІ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ……...……6
к.т.н., доцент Гулак Г.М.,. к.в.н. Аносов А. О
НАПРЯМКИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИЩЕНОСТІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ……...……..6
Власенко В.О.
МЕХАНИЗМЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ IEEE 802.11…….6
Хлебалова М.В.
Проблематика криптографічних методів захисту інформації з відкритим ключем……...……6
Л.В. Пригорницька
АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ……...7
Стеблинський О. А.
Дослідження механізмів інформаційної безпеки в системах широкосмугового зв'язку Wimax і Wi-Fi……..7
Частокол М.М.
Захист від дистанційного впровадження комп'ютерних вірусів за допомогою ВЧ-нав'язування…….……..8
аспірант, Жебка В.В.
До питання оптимізації системи управління мережею при наявності невизначених факторів……...9

к.т.н. Труш О.В., Годієнко Д.О., Онопрієнко М.А.
ЦІЛІСНІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ……..……..……..…9
Доцент к.т.н. Лазаренко С.В., Цигак В.В.
Проблеми виявлення атак на захищені об'єкти інформаційної діяльності за допомогою лазерних мікрофонів……...……....10
Глєбова О.І., ст. викладач.
СУЧАСНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ..…11
Манько О.О., Ніколов К.О., Скубак О.М.
МОДЕЛЮВАННЯ ПЕРЕДАВАЛЬНИХ ХАРАКТЕРИСТИК САМОКЕРОВАНИХ ОБМЕЖУВАЧІВ ПОТУЖНОСТІ……...….12
Руденко Є. В., Пеньков В. І.
Дослідження методів та засобів захисту від НСД мереж стільникового зв'язку на основі стандарту GSM……...……..14
Хоботов Р.
Дослідження методів та засобів управління ресурсами захисту інформації….....…15
Зварич Є. О.
Технічні засоби захисту інформації……...……...16
Кононський О.Д.
Цільові атаки та кібершпигунство……...……....17
Пеньков В. І., Руденко Є. В.
Методи і засоби протидії злоякісному , шпигунському і завідомо фальшивому ПЗ……...….17
Киричок Р.В.
АТАКА НА ВІДМОВУ В ОБСЛУГОВУВАННІ: ТЕСТУВАННЯ НА СТІЙКІСТЬ СЕРВІСІВ……...……...18
Стребков – Саламатов
Дослідження методів та засобів захисту системи електронних платежів…….....18
Курінний С.В, Сосюра А.О.
ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ ЯК СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ……...19
Онопрієнко М.А. Гордієнко Д.О.
Кібернетичний тероризм та кібершпигунство на території України……21
Вовк В.О.
Безпека IP-телефонії: максимальний захист корпоративних IP-мереж……...…22
В. Ю. Однорог, О.В. Богомоленко
ВИКОРИСТАННЯ СМАРТ-КАРТ ЯК ЗАСОБІВ АУТЕНТИФІКАЦІЇ……..….23
А.А. Корченко
Формирование эвристических правил для систем обнаружения вторжений……...…….….23
Цигак В. В.
СИСТЕМИ КОНТРОЛЮ І КЕРУВАННЯ ДОСТУПОМ……....24
В.С. Наконечний, Н.В. Цьопа
МЕТОДИ ВИМІРУ РАДІОЛОКАЦІЙНИХ ОЗНАК ОБ'ЄКТІВ СПОСТЕРЕЖЕННЯ…… …25
О.В. Богомоленко, А.С. Старжинський.
ДОСЛІДЖЕННЯ ТРОЯНСЬКОЇ ПРОГРАМИ REGIN……...…….…26
Корченко О.Г., д.т.н., проф. Дрейс Ю.О., к.т.н.
ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ……...27
Тептя І.І, Білобородов М.Ю.
Стенографічний метода передачі даних, що використувую службові сигнали мережевого протоколу OSPF……...……....28
Ярош В., Ільницька М.
Технології захисту інформації у віртуальних приватних мережах……....28

І.Е. Похабова, д.т.н., проф. Беркман Любов Наумівна
Особливості векторного синтезу систем управління програмно-конфігурованої мережі..... .29
Крушець А.О.
НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО КОМП'ЮТЕРА ЗА ДОПОМОГОЮ ЛЕГАЛЬНОГО ПЗ……..……..…29
Крушець А.О., Сорокін Д.І.
СТІЙКІСТЬ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ОСОБИ – ЗА ГОЛОСОМ…….....30
СорокінД.І.
ВАГОМІ ДІРИ В ЗАХИСТІ ВЕБ-САЙТІВ ВІД CSRF-АТАК……...……..30
Фомін О. О.
БЕЗПЕКА МЕРЕЖЕВОГО ЦЕНТРУ ОБРОБКИДАНИХ……...…….…..31
Иванчук В.И.
Методика проектирования системы информационной безопасности в ИТ……...…….32
Кузьмич Олег Юрійович
Дослідження кіберзлочинності, пов'язаною з ризиком НСД до ІзОД……...……33
Фузік К. М.
Зниження впливу побічних електромагнітних випромінювань на комунікаційне обладнання……...……...…..34
Свередюк К.А.
АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……...…….…..34
Гнатченко А. В.
Дослідження методів забезпечення безпеки електронних документів……...….…….35
Федюк Б.С.
Дослідження методів та засобів захисту системи електронних платежів……...…….....36
Глущенко В.В.
Класифікація загроз інформаційній безпеці……...…….....37
Дмитренко Віталій Анатолійович
Технічні засоби захисту акустичної інформації……...……..38
Огірчак В.О.
Інциденти інформаційної безпеки, пов'язані з роботою персоналу та їх розслідування……..38
Думан М.О.
ОЦІНКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ……...……..41
Салюк М.
Впровадження системи управління захистом інформації електронних платіжних систем….42
Салюк М.
Загрози, пов'язані з використанням систем електронних платежів……..42
Поліщук К.А.
Процесний підхід до управління інформаційною безпекою……...….43
Чередніченко О.О.
Аудит інформаційної безпеки організації та систем……...…….…45
І.Г. Зотова, Д.С. Берестов
ВПРОВАДЖЕННЯ СЕРЕДОВИЩА АУТЕНТИФІКАЦІЇ……...…45
к.т.н., с.н.с. Голобородько М.Ю.
ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ……...45
Гвоздев А.Д.
Обоснование необходимости инноваций в сфере информационной безопасности…….46
Майстренко М.К
Основні методи дій кіберзлочинців в банківській сфері…….….47
Міщенко М.В.
КІБЕРЗЛОЧИННІСТЬ: ЗМІСТ ТА МЕТОДИ БОРОТЬБИ……...47
Мужанова Т.М, к.держ.упр.,доцент
Кадровий аспект забезпечення інформаційної безпеки держави……...……49

Рабчун Д. І.
Динамічні закономірності поведінки порушника інформаційної безпеки……..….52
Халапсіна О.А.
Організаційно-технічне забезпечення управління інформаційною безпекою установи…….53
Чудін Д.Д.
Основні етапи інформаційної атаки……...54
д.т.н., с.н.с. Шевченко В.Л.
Вплив тенденцій розвитку глобальної інформаційної інфраструктури на розвиток інформаційної інфраструктури силових відомств……...……55
к.т.н., с.н.с Щебланін Ю.М.
АНАЛІЗ СТРУКТУРИ СПЕЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ……..….57
к.в.н. Якименко Ю.М.
Напрями забезпечення безпеки інформації в організації……...……...…..58
Хропко Т.О.
Інформаційно-психологічний вплив як актуальна проблема інформаційної безпеки держави……..60
Карпенко Є.М.
Програмні засоби несанкціонованого одержання інформації……...…..60
Олександр М.П.
Системи захисту, з використанням систем відео спостереження……..…61
Пшоннік В.О.
Розробка метода захисту RFID технології…….….61
Боклан М.С.
Система управління доступом на об'єктах інформаційної діяльності…….…..…62
Боклан М.С.
Система управління доступом на об'єктах інформаційної діяльності…….…63
Рубан М.О.
Акустичні сейфи…….…..64
Г.В.Шевченко, О.В.Барабаш
МАТЕМАТИЧНА МОДЕЛЬ РОЗПОДІЛУ ОБСЯГУ АСИГНУВАНЬ НА РІЗНІ ЗАСОБИ РЕКЛАМИ В ІНТЕРНЕТ-МЕРЕЖІ……..…..….64
Иванюк Андрей Игоревич
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СИСТЕМЕ……..……..65
Вальченко О.І., Гунченко О.М.
БЕЗПЕКА ВИКОРИСТАННЯ РАДІОАКТИВНИХ МАТЕРІАЛІВ……..…….66
Гунченко О.М. к.т.н, доц., Вальченко О.І., к.т.н., доц.
НЕБЕЗПЕКИ СОЦІАЛЬНОГО ХАРАКТЕРУ – ФАКТОР НЕСТАБІЛЬНОСТІ ДЕРЖАВИ……...…….….67
Хропко Т.О.
Деструктивний інформаційно-психологічний вплив як актуальна загроза інформаційній безпеці держави……...……..…68
Спасітєлєва С.О. к.ф.-м.н.
Створення безпечних додатків платформи .NET з використанням Ms SQL Server 2014……68
Крицький Г.Г.
Розподіл обов`язків персоналу в системі управління інформаційною безпекою……...….70
ДОВГАНЬ О.Д., к.ю.н, с.н.с.
НАЦІОНАЛЬНИЙ ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ - ІНФОРМАЦІЙНА БЕЗПЕКИ: СПІВВІДНОШЕННЯ……...……...71
к.ф.-м.н., Мусієнко А.П., д.т.н., професор Барабаш О.В.
Самодіагностування телекомунікаційних мереж на основі гнучких структур перевірочних зв'язків……...……72

д.т.н., професор, Барабаш О.В., к.ф.-м.н.Мусієнко А.П.
Функціональна стійкість процесів управління на основі інтелектуалізації телекомунікаційної мережі……..……..73
канд. істор.наук, доцент КИРИЛЕНКО О. Г.
АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ПРОДУКЦІЇ НАУКОВИХ БІБЛІОТЕК……...……..….73
ПОЛІЩУК Р. В.
БЕЗПЕКА РЕСУРСІВ ВІДКРИТОГО ДОСТУПУ В БІБЛІОТЕЧНО-ІНФОРМАЦІЙНИХ УСТАНОВАХ: ПРАВОВІ АСПЕКТИ……..74
к.ф.н., доцент Омецінська О.Б., аспірант Сергієнко І.-В. О.
ВРАХУВАННЯ ФОРМИ МОДУЛЬОВАНОГО ІМПУЛЬСУПРИ РОЗРАХУНКУ ПРОПУСКНОЇ СПРОМОЖНОСТІ ВОЛОКОННО-ОПТИЧНОГО ЛІНІЙНОГО ТРАКТУ……75
Зоценко В.С., Барабаш О.В.
Застосування неорієнтованих графів для оцінки зв'язності телекомунікаційних мереж……..76
Онищенко В.В.
БЕЗПЕКА ІНФОРМАЦІЇ В ТРАНКІНГОВИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ СТАНДАРТА TETRA……..……..…77
Левицький В.О.
Необхідність інформаційних технологій в бізнесі…….77
Левицький В.О.
Користь аудиту інформаційної безпеки…….……78
д.т.н., с.н.с. Дружинін В.А.,Батрак Є.О.
СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ БАГАТОПОЗИЦІЙНИХ СИСТЕМ РАДІОЛОКАЦІЇ ІЗ ЗМІННОЮ ПРОСТОРОВОЮ КОНФІГУРАЦІЄЮ……....79
к.т.н. Цитрицька Л.М.
Знаходження мінімального остовного дерева за допомогою матриці інцидентності……..……79
Курінний С.В, Сосюра А.О.
ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ ЯК СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ……...80
СОЛОДКА О.М.
Інформаційна безпека людини в умовах інформаційного суспільства…….82
Чередніченко О.О.
Аудит інформаційної безпеки організації та систем…….……83
Чередніченко О.О.
Функціональний та процесний підходи до УІБ…….……...……...…84
Белоусов М.О., Ткач М.М., Почтарьов І.С.
Програма автоматизації розрахунку зони радіопокриття базової станції……..….84
Козовий В.Є., Волуйко І.В., Струк С.Є.
Вибір оптимального сценарію розвитку IPTV……....……..85
Могилевський В.Б., Малов О.І.
Проблеми реалізації технології «cloud computing» в телекомунікаційній мережі……..…85
Талабко О.Ю., Евтушенко В.К., Олійник О.Ю.
Розробка імітаційної моделі систем ідентифікації трафіку і управління чергами в тк мережі ……86
д.т.н.,професор Богданович В.Ю
Отработка стратегии и тактики гибридной войны XXI-го столетия на территории Украины…….……..87

аспірант Складанний П.М.
Технології обґрунтування прийняття рішень в інтелектуальній системі захисту інформації……..90
к.т.н. Семко В.В.
Концепція топологічного систуаційного аналізу та синтезу в "малому" управління об'єктом в умовах……...……...90
к.е.н., доцент Іщук Г.П.
Особливість оцінювання результатів АІБ промислових та фінансовихи організацій……...……..…92
к.е.н., доцент Г.П. Іщук
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ІНФОРМАЦІЙНО-ЕКОНОМІЧНОЇ ХАОТИЧНОСТІ……..…93
І. В. Мордас
НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ……..……96
Семко О.В.
Інформаційно-телекомунікаційна система видачі медичних довідок……...96
к.т.н., с.н.с. Курченко О. А., Храпач Г.С.
Аспекти забезпечення інформаційної безпеки на підприємстві……..…..97
Акімов А.О.
Забезпечення інформаційної безпеки у сучасному світі……...……..98
Бурячок В.Л. доктор технічних наук, старший науковий співробітник
ІНФОРМАЦІЙНА БЕЗПЕКА У КОНТЕКСТІ ЗАХИСТУ ДЕРЖАВИ ВІД СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ…….…….……100
Куклов В.М., Василенко В.В., Гринкевич Г.О.
SDN як платформа підвищення безпеки в телекомунікаційних мережах……..111
д.т.н. Субач І.Ю.
ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК……..…112
д.т.н., проф. Оксіюк О.Г.,к.т.н. Прус Р.Б.
ПОШУК ОПТИМАЛЬНОГО РІШЕННЯ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗ ВРАХУВАННЯМ ДІЙ НАПАДУ……..…..112
Павлов І.М.
ОЦІНКИ ЕФЕКТИВНОСТІ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ……..……113
Толюпа С.В., Яремчук Ю.Є.
ОСОБЛИВОСТІ РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ АСИМЕТРИЧНОГО ШИФРУВАННЯ…….114
Толюпа С.В., Головко А.А.
ВИКОРИСТАННЯ ШИРОКОСЕКТОРНИХ НИЗЬКОПРОФІЛЬНИХ АНТЕН ПРИ ОРГАНІЗАЦІЇ МЕРЕЖ РАДІОЗВ'ЯЗКУ ТА РАДІОРОЗВІДКИ……...…116
Субач І.Ю., Лойко А.О.
КРИПТОГРАФІЧНИЙ МОДУЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ УДОСКОНАЛЕНОГО АЛГОРИТМУ ШИФРУВАННЯ CLEFIA……...117
Толюпа С.В., Софієнко І.І.
МЕТОДИКА ОЦІНКИ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ……....118
Толюпа С.В., Боярский Ю.К.
ПІДХОДИ МОДЕЛЮВАННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ….……119
Толюпа С.В. , Дружинин В.А.
ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ В ПРОЦЕССЕ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТИ ИНФОРМАЦИОННЫХ СЕТЕЙ……120

Толюпа С.В., Уварова Г.А.
ЗАСТОСУВАННЯ ТЕОРІЇ ДЕКОМПОЗИЦІЇ ДЛЯ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ…..……....121
Ковтун О., Гончаренко М.
МЕТОДИКА ОЦІНКИ ПЕРЕДАТОЧНОЇ ХАРАКТЕРИСТИКИ КАНАЛУ РАДІОЗВ'ЯЗКУ……..123
Толюпа С.В., Хлапонін Ю.І.
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ……...……..124