Державний університет телекомунікацій
Київський національний університет імені Тараса Шевченка
Національний авіаційний університет
Військовий інститут телекомунікацій та інформатизації
Національний університет “Львівська політехніка”
Вінницький Національний технічний університет
Національна академія оборони України
Академія Служби безпеки України
Інститут спеціального зв’язку та захисту інформації
Університет Бульсько-Бяла
Вроцлавський технічний університет

II МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ НАУКИ І ТЕХНІКИ»

ЗБІРНИК ТЕЗ

20 грудня 2015 року

м. Київ

State University of Telecommunications
Taras Shevchenko National University of Kyiv
National Aviation University
Military Institute of Telecommunications and Information
Lviv Polytechnic National University
Vinnytsia National Technical University
National Defence Academy of Ukraine
Academy of Security Service of Ukraine
Institute of Special Communication and Information Protection
University of Bielsko-Biala
Wrocław University of Technology

II INTERNATIONAL SCIENTIFIC-TECHNICAL CONFERENCE

«ACTUAL PROBLEMS OF SCIENCE AND TECHNOLOGY DEVELOPMENT»

BOOK OF ABSTRACTS

December 20, 2015

Kyiv

УДК 621.387:681.327

Актуальні проблеми розвитку науки і техніки: Матеріали другої міжнародної науково-технічної конференції. Збірник тез. — Київ : ДУТ, 2015. — 40 с.

Даний збірник містить тези учасників конференції, представлених на II Науково-технічній конференції "Актуальні проблеми розвитку науки і техніки", яка проводилась 20 грудня 2015 р. в Навчально-науковому інституті Захисту інформації Державного університету телекомунікацій, м. Київ.

Actual problems of science and technology: Proceedings of the second international scientific conference. Book of abstracts. - Kyiv: SUT, 2015. - 40p

This book contains abstracts of conference participants presented at II Scientific-technical conference «Actual problems of science and technology development », which was held on December. 20, 2015 in the Educational-scientific Institute of Information security of the State University of Telecommunications, c. Kyiv

Робочі мови конференції - українська, російська, англійська.

Секретарі конференції

Складаний П.М. ст. викладач кафедри Інформаційної та кібернетичної безпеки, Дежравний університет телекомунікацій.

Платоненко А.В. асистент кафедри Систем захисту інформації, Дежравний університет телекомунікацій.

Рабчун Д.І. асистент кафедри Управління інформаційної безпекою, Дежравний університет телекомунікацій.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Програмний комітет:

ШЕВЧЕНКО Віктор Леонідович *(д.т.н., проф. , Київ, Україна);*
БУРЯЧОК Володимир Леонідович *(д.т.н., с.н.с., Київ, Україна);*
РОЗОРІНОВ Георгій Миколайович *(д.т.н., проф., Київ, Україна);*
НАКОНЕЧНИЙ Володимир Сергійович *(д.т.н., с.н.с., Київ, Україна);*
СКЛАДАННИЙ Павло Миколайович (*ст. викладач, Київ, Україна);*
КОЗЕЛКОВ Сергій Вікторович *(д.т.н., проф., Київ, Україна);*
ПОЛОНЕВИЧ Андрій Петрович *(к.т.н., Київ, Україна);*
НЕВДАЧИНА Ольга Володимирівна *(к.т.н., Київ, Україна);*
ЖУРАКОВСЬКИЙ Богдан Юрійович *(д.т.н. проф, .Київ, Україна);*
ДРУЖИНІН Володимир Анатолійович*(д.т.н., проф., Київ, Україна);*
ТУПКАЛО Віталій Миколайович *(д.т.н., проф., Київ, Україна);*
ОКСІЮК Олекесандр Глебович *(д.т.н., доцент, Київ, Україна);*
ТОЛЮПА Сергій Васильович *(д.т.н., проф., Київ, Україна);*
САМОХВАЛОВ Юрій Якович *(д.т.н., проф., Київ, Україна);*
ЮДІН Олександр Констянтинович *(д.т.н., проф., Київ, Україна);*
КОРЧЕНКО Олександр Григорович *(д.т.н., проф., Київ, Україна);*
ЯРЕМЧУК Юрій Євгенович *(д.т.н., проф., Вінниця, Україна);*
КОЗЛОВСЬКИЙ Валерій Валерійович *(д.т.н., проф., Київ, Україна);*
СУБАЧ Ігор Юрійович *(д.т.н., доцент, Київ, Україна);*
ГОРБЕНКО Іван Дмитрович *(д.т.н., проф., Харків, Україна);*
ПАРКУЦЬ Любомир Тодорович *(д.т.н., проф., Львів, Україна);*
ДУДИКЕВИЧ Валерій Богданович *(д.т.н., проф., Львів, Україна);*
НАЗАРКЕВИЧ Марія Андріївна *(д.т.н., проф., Львів, Україна);*
ГРИЩУК Руслан Валентинович *(д.т.н., с.н.с., .Житомир, Україна);*
БАЙЕР Анджей *(д.т.н., проф., Польща);*
ТУРМАНІДЗЕ Рауль Сергійович*(д.т.н., проф., Грузія);*
КАРПІНСЬКИЙ Микола *(д.т.н., проф., Польща);*
СУРМАЧ Томас (*PhD, Польща.)*

ЗМІСТ

Жученко А.С.
доцент кафедры Транспортной связи
Штомпель Н.А.
доцент кафедры Транспортной связи
Украинский государственный университет железнодорожного транспорта
г. Харьков, Украина

МЕТОД ДЕКОДИРОВАНИЯ БЛОКОВЫХ КОДОВ НА ОСНОВЕ ПРОЦЕДУР ПРИРОДНЫХ ВЫЧИСЛЕНИЙ

Обеспечение заданной достоверности передачи информации в телекоммуникационных сетях требует применения методов помехоустойчивого кодирования, в том числе различных видов блоковых кодов. Для увеличения энергетической эффективности телекоммуникационных систем целесообразно использовать методы мягкого декодирования блоковых кодов [1, с. 201 – 203]. Рассмотрены основные этапы, принципы и особенности мягкого декодирования блоковых кодов на основе алгебраического и вероятностного подходов. Показано, что классические подходы к декодированию блоковых кодов не удовлетворяют требованиям, которые предъявляются к современным телекоммуникационным системам. Предложено формальное представление задачи мягкого декодирования блоковых кодов в виде задачи целочисленного нелинейного программирования. Обосновано применение процедур природных вычислений для решения данного вида оптимизационных задач [2, с. 8 – 10]. Представлены основные этапы разработанного метода декодирования блоковых кодов, в основе которого лежит использование информации о надежности принятых символов, структуры модифицированной проверочной матрицы и обобщенных процедур природных вычислений. Разработаны вычислительный алгоритм и программная реализация предложенного метода мягкого декодирования блоковых кодов. Проведена оценка характеристик существующих и предложенного методов мягкого декодирования блоковых кодов для различных математических моделей каналов связи. Представлены практические рекомендации по применению разработанного метода декодирования блоковых кодов в телекоммуникационных сетях различного назначения.

Литература:

1. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение: пер. с англ. [Текст] / Р. Морелос-Сарагоса. – Москва: Техносфера, 2005. – 320 с.

2. Карпенко, А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой [Текст]: учебное пособие / А.П. Карпенко. – Москва: издательство МГТУ им. Н. Э. Баумана, 2014. – 446 с.

Власенко Г.М.
завідувач кафедри Космічних систем та комплексів і супутникових телекомунікацій
Державний університет телекомунікацій
м. Київ, Україна
Махонін Є.І.
професор кафедри Космічних систем та комплексів і супутникових телекомунікацій
Державний університет телекомунікацій
м. Київ, Україна

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАВІГАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УКРАЇНИ

Для визначення координат на території України широко використовуються приймачі сигналів глобальних навігаційних супутникових систем (ГНСС) GPS і ГЛОНАСС. Але точність визначення координат за допомогою цих ГНСС не повністю задовольняє багатьох споживачів супутникової навігаційної інформації [1].

Вирішити проблему підвищення якості координатних визначень на території України можна шляхом створення наземного функціонального доповнення до ГНСС – мережі перманентних (референтних) станцій. В місцях з відомими координатами, встановлені опорні (базові) станції, оснащені приймачами GPS і ГЛОНАСС. За вимірами цих приймачів формуються диференціальні поправки, які передаються споживачам через Інтернет або радіо і дозволяють значно поліпшити точність визначення координат в зоні обслуговування мережі.

Тепер на території України розгорнута система координатно-часового та навігаційного забезпечення України (СКНЗУ), яка забезпечує точне позиціонування. З цього питання вирішуються правові аспекти, здійснюється міжнародне співробітництво, але є не вирішені питання. На даний момент СКНЗУ працює в тестовому режимі. Розглядається питання роздачі диференціальних поправок споживачам через супутник зв'язку та використання алгоритмів обробки цих поправок в пристроях споживачів.

Література:

1. Системи супутникової навігації в Україні: використання і перспективи розвитку – К.: НКАУ, 2009,- 48 с. – Укр. та англ. мовами.

Некряч О.В.
Аспірант кафедри Телекомунікаційних систем
Державний університет телекомунікацій
м. Київ, Україна

АНАЛІЗ ВЗАЄМОЗАЛЕЖНОСТІ ПОДІЙ В СКЛАДНИХ ДИНАМІЧНИХ СИСТЕМАХ.

Враховуючи наявність взаємозв'язків між елементами мережі, зміна стану одного з них, з певною імовірністю, призводить до зміни параметрів інших елементів мережі. В реальних умовах ці взаємозв'язки є складними та не завжди очевидними, тому у складі системи управління необхідно мати інструмент автоматичного визначення наявність взаємозалежностей між контрольованими параметрами і локалізації причин тих чи інших процесів [2, с.3].

Взаємозалежність між контрольованими параметрами може бути визначена на основі аналізу імовірнісних характеристик цих параметрів. Так, проаналізувавши наявність взаємної інформації між двома параметрами можна встановити наявність кореляційної взаємозалежності між ними.

Зменшення невизначеності однієї випадкової величини завдяки отриманню значень іншої змінної називається "взаємною інформацією". Міра залежності між двома змінними обчислюється таким чином [3, с.7]:

$$I(X, Y) = H(X) - H(X|Y) = \sum_{x,y}^{k,l} P(X_k, Y_l) \log \frac{P(X_k, Y_l)}{P(X_k)\,P(Y_l)} \qquad (1.1)$$

Взаємна інформація максимальна і дорівнює безумовній ентропії, коли між X і Y є однозначна залежність.

Виходячи з наведеної вище інформації, можна описати базовий алгоритм автоматичного виявлення взаємозалежностей між контрольованими параметрами:

1) Отримання значень контрольованих параметрів $(X_k, Y_l,$ *де* $k,l \in 0,1\ldots n)$; 2) Визначення імовірнісних характеристик кожного із значень $(P(X_k), P(Y_l), P(X_k, Y_l))$; 3) Визначення взаємної інформації між параметрами $(I(X, Y))$; 4) Визначення комбінацій параметрів із найбільшим значенням взаємної інформації.

Наведений метод дозволяє автоматизувати процес виявлення взаємозалежностей між контрольованими параметрами телекомунікаційної мережі. Та може бути використаний як окремий блоку аналізу даних у системі моніторингу та як складова частина системи виявлення першопричини інцидентів в мережевій інфраструктурі.

Література:

1) Hyong S. Kim, Root cause analysis in large and complex networks. University of Lisboan. 2008. –66
2) Thomas M. Cover, Joy A. Thomas., Elements Of Information Theory. Second Edition. Canada. 2006. – 774

Дорогий Я.Ю.
доцент кафедри автоматики і управління в технічних системах
Національний технічний університет України «Київський політехнічний інститут»
Дорога-Іванюк О.О.
асистент кафедри автоматики і управління в технічних системах
Національний технічний університет України «Київський політехнічний інститут»
м. Київ, Україна

КРИТЕРІЙ ОПТИМАЛЬНОСТІ ПОБУДОВИ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ

Оскільки в критичних ІТ-інфраструктурах [1] зосереджені потужні і досить дорогі ресурси, виникає проблема їх ефективного використання. Це стає можливим за рахунок розподілу, управління і диспетчерування ресурсів і навантаженням на основі комплексу відповідних математичних моделей і методів. Формалізація проблеми ефективного використання ресурсів привела до задач нечіткого програмування [2] з широким вибором критеріїв оптимізації і врахуванням критичності, ресурсних, часових, технологічних та інших обмежень.

Для формування критерію оптимальності створення і подальшого функціонування критичної ІТ-інфраструктури пропонується використати наступну множину параметрів:

- надійність – показник надійності критичної ІТ-інфраструктури в період експлуатації;
- живучість – можливість виконувати свої функції при втраті ресурсів, підсистем і т. ін.;
- забезпеченість – показник максимальної кількості процесів та сервісів, що обслуговуються;
- відновлюваність – тривалість відновлення готовності до експлуатації;
- економічність – витрати різноманітних ресурсів на забезпечення функціонування критичної ІТ-інфраструктури;
- безпечність – показник неможливості виконання несанкціонованих дій, спрямованих на порушення роботи критичної ІТ-інфраструктури чи її частин;
- строк життя;
- ефективність – поєднання вище згаданих параметрів в кожному окремому випадку під визначену задачу.

При формуванні вимог критерію управління критичною ІТ-інфраструктурою необхідно також враховувати особливості розв'язання задачі. Слід зазначити, що визначення всієї множини параметрів не можна повністю звести до системи формалізованих процедур, бо деякі з них вимагають якісного аналізу. Для такого аналізу слід використати метод структуризації, який дозволяє поділити задачу на підзадачі, визначитись за допомогою експертів або без низ з методами розв'язання цих підзадач, обмеженнями використання цих розв'язків та методами поєднання розв'язків.

Література:

1. *Дорогий Я.Ю.* Критична інфраструктура: вразливості, загрози, ризики / *Я.Ю.Дорогий, В.В.Мохор, І.О.Козлюк, В.В.Цуркан* // Тези доповідей. ІІ міжнародна науково-практична конференція «Інформаційні технології та взаємодії», 3-5 листопада. – Київ, 2015. – с. 46-47.

Liu B. *Theory and Practice of Uncertain Programming* / B.Liu. – UTLAB. – 2009. - http://orsc.edu.cn/liu/up.pdf.

Жданова Ю.Д.
Доцент каф. Інформаційної та кібернетичної безпеки
Березюк А.С.
Студент навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ВИДИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ДЛЯ АВТЕНТИФІКАЦІЇ

У більшості сучасних інформаційно-комунікаційних системах (ІКС) при наданні різного виду послуг використовується електронний цифровий підпис (ЕЦП) для ідентифікації особи, яка підписала електронний документ. Метою застосування систем ЕЦП є автентифікація інформації – захист учасників інформаційного обміну від нав'язування хибної інформації, встановлення факту модифікації інформації, яка передається або зберігається, й отримання гарантії її справжності, а також вирішення питання про авторство повідомлень. В ІКС використовуються наступні види ЕЦП:

Простий ЕЦП – використовується для підтвердження авторства і організації документообігу на підприємстві, але не дає документу юридичну значимість і не забезпечує незмінність після його підписання.

Некваліфікований ЕЦП – використовується для внутрішнього документообігу, а також для обміну електронними документами між декількома організаціями. У другому випадку, компанії повинні укласти між собою угоду, що встановлюють правила визнання і використання ЕЦП. У створенні такого підпису використовуються засоби криптографічного захисту, які забезпечують інформаційну безпеку при взаємодії.

Кваліфікований ЕЦП – має всі характеристики некваліфікованого ЕЦП, проте може бути отриманий тільки в акредитованому засвідчувальному центрі. Використовується для здачі звітності в контролюючі органи державної влади і для участі в електронних торгах.

Засоби криптографічного захисту, необхідні для роботи з кваліфікованим ЕЦП, повинні бути сертифіковані акредитованим засвідчувальним центром. В результаті кваліфікований ЕЦП стає повноцінною заміною (аналогом) власноручного підпису та забезпечує виконання вимог щодо забезпечення безпеки інформації обмеженого доступу.

Література:

1. Закон України «Про електронний цифровий підпис» від 22.05.2003 №852-IV (зі змінами та доповненнями).
2. Гулак Г.Н., Мухачев В.А., Хорошко В.А., Основы криптографической защиты информации. – К.: Изд. ГУИКТ, 2009.

Жданова Ю.Д.
Доцент каф. Інформаційної та кібернетичної безпеки
Бровченко Є.В.
Студент навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ДЕЯКІ ТИПИ АТАК НА СИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

У криптосистемах з відкритим ключем, на відміну від криптосистем з секретним ключем, вже не один ключ, а два – відкритий, який доступний для всіх і секретний. Розглянемо криптографічну стійкість криптосистем з відкритим ключем на прикладі двох найвідоміших систем Діффі-Хеллмана і RSA, яка набула актуальності в світлі результатів про поліноміальні квантові алгоритми обчислення дискретного логарифма і факторизації чисел.

В [1] запропоновано ймовірнісний квантовий алгоритм факторизації, що дозволяє розкласти число N за час $O((\log N)^3)$. У 2001 році, його працездатність була продемонстрована групою фахівців IBM. Число 15 було розкладено на множники 3 і 5 за допомогою квантового комп'ютера з 7 кубітами. Здатність виконати факторизацию числа за поліноміальний час може поставити під загрозу надійність більшості криптосистем з відкритим ключем, заснованих на складності проблеми факторизації чисел.

В [2] запропоновано новий спосіб атаки на системи з відкритим ключем. Точно вимірюючи кількість часу, необхідного для операцій із закритими ключами, зловмисник може знайти постійний показник ступеня у схемі Діффі-Хеллмана, факторизовані ключі в RSA, а також зламати і інші криптосистеми.

Один із способів захисту від цього типу атак – забезпечення одного й того самого часу роботи алгоритму на будь-якому шифротексті. Однак, подібний спосіб істотно знижує продуктивність. Замість цього, більшість реалізацій RSA використовують інший метод, відомий як «*криптографічне осліплення*». Замість обчислення $y^d (mod\ N)$ абонент А спочатку вибирає випадкове число r і обчислює $(r^e y)^d (mod\ N)$. В результаті обчислень виходить число $rm (mod\ N)$ і, домножуючи його на $1/r$, отримуємо вихідне повідомлення. Для кожного шифротекста число r вибирається знову. Таким чином, після застосування цієї техніки час розшифрування не залежить від шифротекста і часовий аналіз втрачає сенс.

Список літератури

1. http://en.wikipedia.org/wiki/Shor%27s_algorithm
2. Paul C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. Lecture Notes in Computer Science (vol. 1 109), pages 104-113. Springer, 1996. http://citeseer.ist.psu.edu/kocher96timing.html

Tomasz Surmacz
Institute of Computer Engineering, Control and Robotics,
Wroclaw University of Technology
ul. Janiszewskiego 11-17, 50-372 Wroclaw, Poland
email: tsurmacz@ict.pwr.wroc.pl

MEASUREMENT OF KEY PERFORMANCE FACTORS IN USENET NEWS SYSTEMS

Abstract

Usenet news is a worldwide network of servers providing discussion forums with topics ranging from scientific research to hobbies, entertainment or politics. The paper describes methods of measuring the flow of articles, delays introduced by message transmission and other data, as well as problems of detecting anomalies and dealing with the m in order to assure a smooth operation of the whole system.

1 Introduction

Discussion forums are one of the key elements of modern electronic communications. A worldwide network of servers called ”Usenet news” is one of the oldest, but still a popular system, allowing computer users all over the world to share their opinions on various topics. There are several thousand groups (such as ”comp.software.measurement”) organised in hierarchies (e.g. ”comp.*”, ”sci.*”, ”rec.*”, etc.) Articles are sent by users to a nearest news server of the local Internet Service Provider (ISP) and are automatically distributed throughout the whole web of cooperating news servers though the usage of NNTP protocol [2, 1]. An article sent from any of the servers flows through the whole network from one server to another (via a link called a *newsfeed*), leaving exactly one copy at each cooperating server. Appropriate mechanisms exist to prevent transmission loops when multiple connections exist and old articles (usually older than one month) are expired from servers to make space for new ones.

Problems associated with running a news server [3] include: * maintaining redundant links to other news servers, in order to provide reliable incoming news flow and to allow propagation of locally posted articles to the world; * monitoring those links for a possible network congestion and detecting failures or unannounced configuration changes at remote sites; * monitoring data flow statistics for traffic exceeding some predefined thresholds (meaning usually some Denial of Service (DoS) attack or a misconfigured server somewhere in the net).

Usually, when a server failure occurs, such as an overflown news spool (and no free disk space) or a dried news feed (and lack of new articles at all), it is already too late to start finding the reasons, unless some reference data has been gathered during the normal operation of the news server.

2 Subject of measurements

Several quantities can be measured in a running news server system to build a current view of a running system. As articles are constantly being received from

incoming feeds and are resent to other news servers, each incoming article can be logged with additional data such as:

S – article size in bytes;

F – the news server from which the article was received;

P – Path the article took from the originating server (i.e. recorded track of all the servers that carried the article);

Tp – time and date the article was originally posted;

Tr – time and date the article was received;

Te – time and date the article should be expired from the system.

N – newsgroup name (or a list of newsgroup names) in which the article appeared;

All these values are worth considering only when summarized or compared over some period of time, e.g. gathered as hourly or daily statistics. Also, much more interesting then the plain sum of the article sizes are the results of processing data selected by other factors, e.g. number of articles in some hierarchy or a total volume of articles sent to a particular server.

From the maintenance point of view, the most interesting values are: the average article delay, measured as a difference between *Tr* and *Tp*; Incoming flows – volume and count of incoming articles per site (newsfeed) or per hierarchy; Outgoing flows – acceptance rate and volume of outgoing newsfeeds.

Measuring article delays can help detecting backlogs of data accumulating at remote ends of incoming newsfeeds. If such backlogs exist, they usually mean an insufficient bandwidth of the underlying network or some other efficiency problems between the two communicating news servers. Solving that usually requires redesigning the structure of incoming newsfeeds.

Keeping daily statistics about incoming flows can help identifying problems when there is a sudden change of volume or number of articles. A sudden increase of data usually means some news system abuse, such as posting binary data in some of the groups (e.g. ripped CDs or pirated copies of movies), increased level of SPAM, or a Denial of Service (DoS) attacks.

3 Measurement methods

Delay between sending an article at some remote news server and receiving it locally can be calculated by comparing *Tr* and *Tp*. However, the value of *Tp* depends on the clock accuracy of a remote server which was used to post the article (and sometimes even a client computer which posted an article) and cannot be always trusted to be correct. Although most servers nowadays use NTP protocol to synchronize their local clocks, care has to be taken to allow for potential clock skews and timezone misconfigurations.

Delays can be calculated in two different ways: online – by monitoring *Tp* and *Tr* logged by news server as new articles are being received, or offline – by analysing a so-called *history* file (containing article IDs and their *Tr* values) and finding each article in disk spool area to get the *Tp* value from article headers

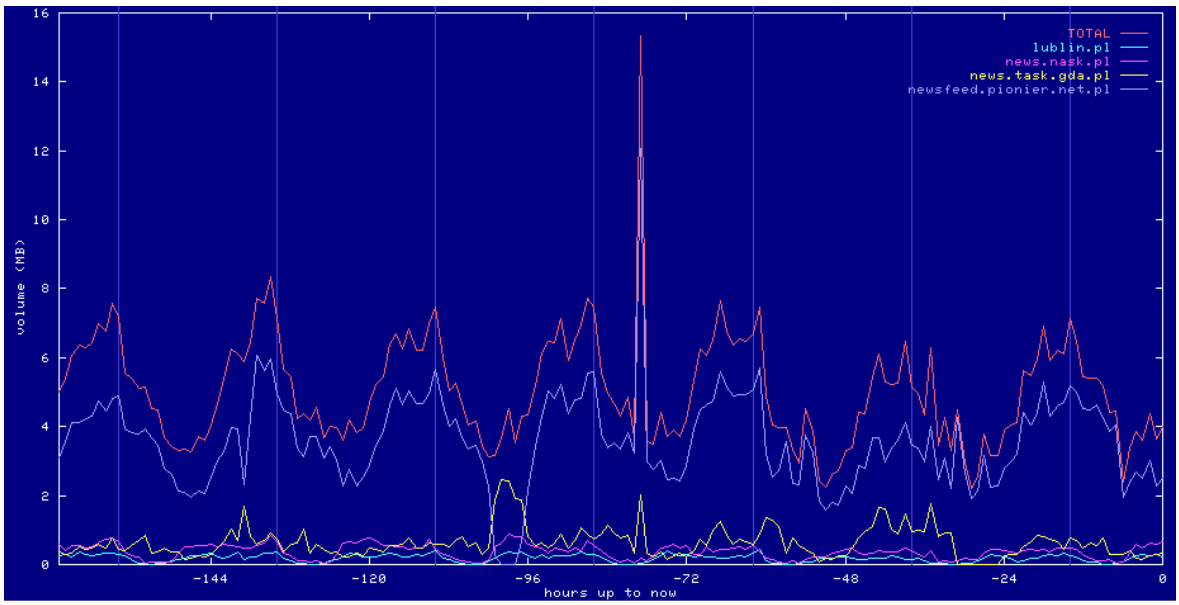

Figure 1: Incoming flow of articles split by newsfeed

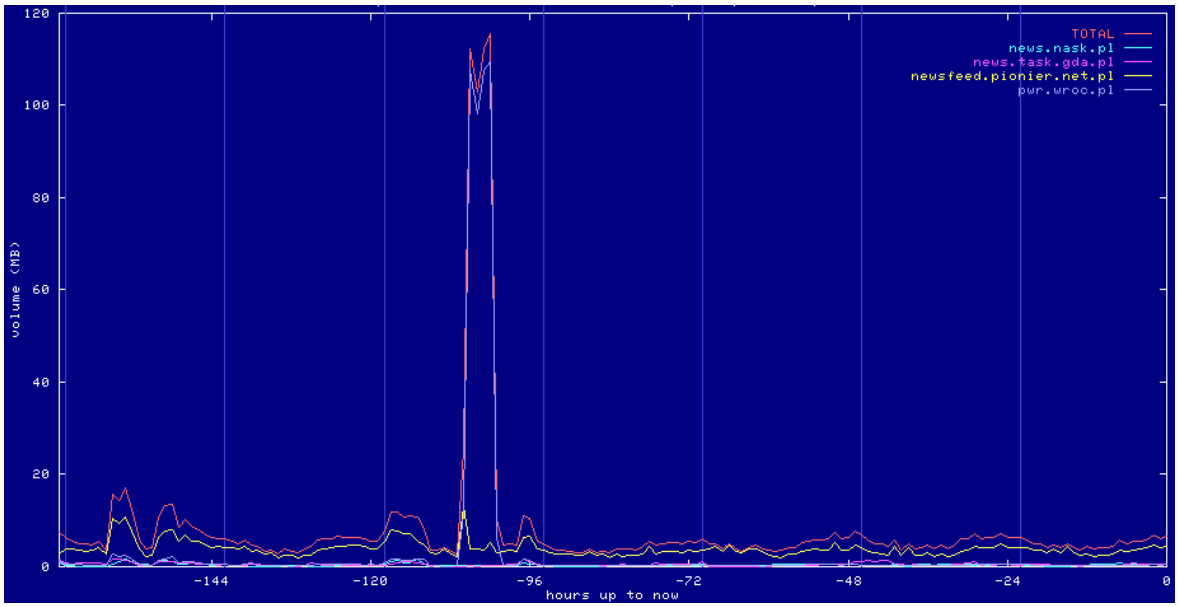

Figure 2: Incoming flow anomalies

.

For measuring input and output data flows, a simple one-time setup is usually required. As new articles come, the news server writes a special log file, recording all the required information: the article size (*S*), newsgroup name (*N*), time received (*Tr*), and incoming feed name (*F*). Then a separate process can analise this data periodically, creating hourly and daily summaries of system state.

Incoming volume and count of articles can be split by incoming newsfeed name, showing how many articles come from each neighbouring news server. Fig. 1 shows sample of such data. At around -100 hours (counted from plot generation time) one can observe that newsfeed.pionier.net.pl stops sending articles, but at the same time more of them comes from news.task.gda.pl, meaning a temporary

problem at ”pionier” and a proper operation of redundant links. At -78 hours there is a peak in volume of articles received from ”pionier”. When compared to another plot showing article count for that time (not shown here) with no anomalies at all, one can draw a conclusion, that there must have been some large articles posted at that time (e.g. binary postings) and if disk space gets exhausted, appropriate log files can be checked to see to which news groups or hierarchies these articles were sent to.

Input flow anomalies are shown in Fig. 2. A sudden volume increase at -110 hours appears from one of the newsfeeds which may be interpreted as a temporary news system abuse or a sudden increase of spam. This are often accompanied by a following stream of cancel messages to delete this spam from all news servers. The analysis of this particular log however shows another important factor of the system setup – that there is still a lot of bandwidth reserve for news servers operation under normal conditions.

Analysis of flow data can also help reconfiguring incoming and outgoing data streams to utilize the bandwidth of the underlying network links in a best way.

Let’s consider two news servers A1 and A2 (see Fig. 3) located in the same metropolitan area network ($N1$), thus connected through 622 Mbps or 1 Gbps links, and two other servers B1 and B2 located in another city (network $N2$) connected with city A/network $N1$ through a lower speed 2-64 Mbps line. To maintain a basic reliability in case of any server failure it is wise to create two links between A and B, e.g. A1-B1 and A2-B2, as well as local links between A1-A2 and B1-B2. Full news feed of 200 GB/24h means an average bandwidth of around 20 Mbps which is quite a lot for a typical Frame-Relay network used for long distance links. Thus, each article from city A should be sent to city B only once (either through A1-B1 link or through A2-B2). Articles should be propagated locally in the fastest possible way, in order to prevent sending the same article twice over the slow long distance link – whether in the same direction or going back from B2 to A2 after being sent from A1 to B1.

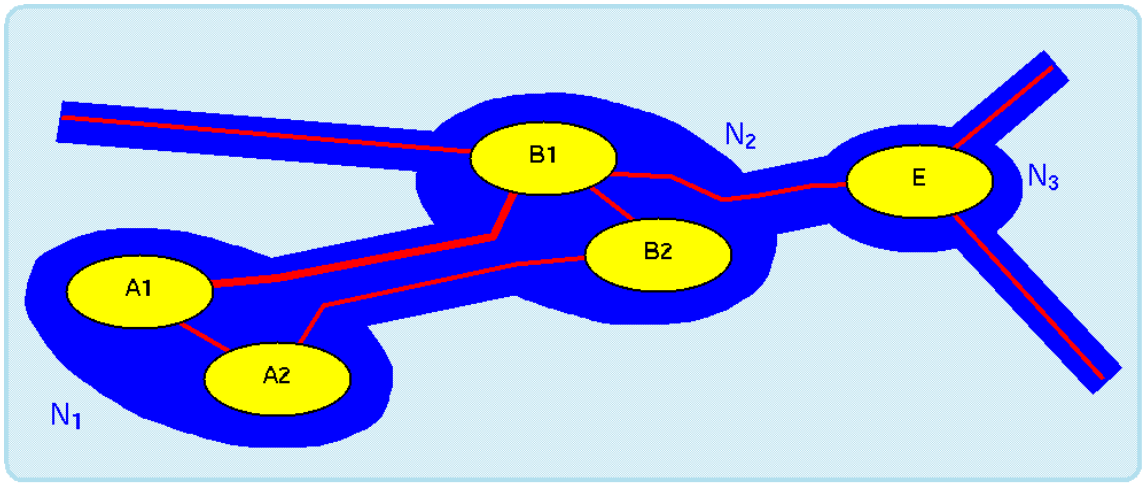

Figure 3: Sample usenet news server network

To prevent network bandwidth waste, an incoming news volume per server should be monitored as we ll as outgoing news volume and rejection rate to other servers. E.g. if high volume of news coming from B1 to A1 is accompanied by a 90-100% acceptance rate of artic le s sent from A1 to A2, the bandwidth is utilized properly (based on unique Message-Ids of incoming articles, A2 will refuse to accept these messages again from other sources in the handshake phase of an article transmission). However, p o or acceptance rate between A1 and A2 as well as high volume of data on B 2-A2 links means that the same articles travel multiple times through slow long-distance links and some feed reconfiguration is needed.

4 Conclusions

The flow data in numerical form can be used to automatically raise alarms when some predefined thresholds are exceeded, e.g. resulting in disk space problems or bandwidth exhaustion. However, except some trivial examples, such fixed thresholds are usually hard to set, as they dep end on many factors, such as the available network bandwidth, acceptable delays, desired reliability, allowed link redundancy, and sometimes even local policies for exchanging news – so for a better view of the running system a visualisation of gathered data is preferred. Such graphical data can be presented through WWW service, helping system administrators to maintain a proper operation of the Usenet News system.

Constant monitoring is needed to maintain the Usenet News system running in a smooth way. Measuring the right type of data and its proper analysis are the key to identifying and solving potential problems. Analysis of existing article flows can be used to redesign server network top ology and techniques such as deploying some minor delays in article sending can help optimising usage of available network bandwidth.

References

[1] J. Elie. Network News Transfer Protocol (NNTP) Additions to LIST Command. RFC 6048 (Proposed Standard), November 2010.

[2] C. Feather. Network News Transfer Protocol (NNTP). RFC, October 2006. Updated by RFC 6048.

[3] Tim O'Reilly and Grace Todino. *Managing UUCP and Usenet*. O'Reilly & Associates, Inc., March 1988.

Мякухин Ю. В.,
Наконечный В.С., д.т.н., с.н.с.,
Сайко В.Г., д.т.н., професор
Государственный университет телекоммуникаций
г. Киев, Украина

ПРОБЛЕМЫ ПРОЕКТИРОВАНИЯ ПЕРСПЕКТИВНЫХ КОМПЛЕКСОВ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В докладе рассматриваются наиболее значимые проблемы, касающиеся физической защиты особо важных объектов (ОВО) Украины, связанные с проектированием эффективного автоматизированного комплекса технических средств охраны (АКТСО) с целью его дальнейшего внедрения на заданном объекте. Затрагиваемые в докладе вопросы в теоретическом и практическом плане изучены не достаточно. На результативность их решения влияет [1]:

1) отсутствие нормативно технической документации и соответствующих стандартов, руководящих документов и методик, регламентирующих:
   - порядок внедрения в эксплуатацию АКТСО на объектах;
   - технические требования, предъявляемые к АКТСО во время эксплуатации;
   - методик испытаний АКТСО на степень пригодности их к эксплуатации на объектах;
2) отсутствие в Украине испытательных полигонов, на которых могли бы испытываться в максимально приближенной обстановке и условиях к реальному объекту охраны АКТСО и элементы ТСО;
3) несовершенство математических методов и моделей оптимального выбора и структуры ТСО, которые выполняли бы поставленные цели и задачи на ОВО Украины.

В связи с этим, предлагается выполнить следующие первоочередные мероприятия:

1.Разработать методики выбора рациональных и оптимальных типов ТСО и проверки подлинности указанных значений технических характеристик.

2.Создать экспериментальный полигон, на котором бы исследовались объектовые ТСО в разных условиях воздействия внешней среды с целью разработки комплексов математических моделей, методов и методик, которые смогли бы адекватно заменять реально существующие изделия.

Литература

1. Мякухин Ю.В. Применение модифицированного метода парных сравнений для решения задач выбора технических средств охраны для сложных объектов энергетики // Моделювання та інформаційні технології: Зб. н. пр.: Спеціальний випуск. Матеріали міжнародної наукової конференції “SIMULATION – 2010”. 12 – 14 травня 2010 р. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ. 2010. – том.2. – С. 274 – 278.

Ткаченко О.М.
доцент кафедри Телекомунікаційних систем
Державний університет телекомунікацій
м. Київ, Україна
Перепелиця Н.Л.
старший викладач кафедри Телекомунікаційних систем
Державний університет телекомунікацій
м. Київ, Україна

ВИЗНАЧЕННЯ УМОВ ПРАЦЕЗДАТНОСТІ КАНАЛУ

Нехай стан каналу характеризується значеннями контрольованих характеристик $x_1, x_2 \ldots, x_n$. Зміну працездатності каналу можна представити як зміну цільової функції, яка має вигляд

$$S = f(x_1, x_2 \ldots, x_n).$$

Для прогнозування стану каналу скористаємося методом градієнтного прогнозування [1, с.14].

Характеристики каналу змінюють свої значення в часі, які можна представити у вигляді $x_i = \varphi_i(t)$. У моменти часу $t_1, t_2 \ldots, t_m$, де $t_1 < t_2 < \ldots < t_m$, значення працездатності S змінюватиметься і набуватиме значень $x_1, x_2, \ldots, x_n$, тобто маємо множину $\{S\}$, яка визначає простір D.

$$S_1 = f(x_{11}, \ldots, x_{1n})$$
$$\vdots$$
$$S_m = f(x_{m1}, \ldots, x_{mn})$$

Оскільки значення працездатності S залежить від аргументів $x_1, x_2 \ldots, x_n$, то S можна розглядати як вектор в багатовимірному просторі. Кінець багатовимірного вектора знаходиться в просторі, обмеженому гіперповерхнею. Положення гіперповерхні в просторі визначається максимальними значеннями вибраних характеристик. Гіперповерхня розділяє простір на дві області: область допустимих досліджуваних характеристик каналу, яка відповідає стійкій роботі каналу і його придатності для передачі дискретних повідомлень; і область допустимих значень, яка представляє придатність каналу обумовлену низькою достовірністю передачі повідомлення.

Література

1. Сокол Ш. Прогнозирование состояний дискретного канала – Л.: ЛЭИС, 1985. – 17 с.

2. Захаров Г. П., Архипов М. Н. Проектирование и техническая эксплуатация сетей передачи данных. – М.: Радио и связь, 1989. – 360 с.

3. Райцис Я. Н., Соколов В. А. Специальные системы связи. Введение в системотехническое проектирование: Учебное пособие. – М.: МИС, 1991. – 81 с.

4. Журавин А. И., Родионов А. В. Управление сетями связи: Учебное пособие. − Л.: ВИКИ им. А.Ф. Можайского, 1989. – 50 с.

Отрох С.І.
к.т.н., професор кафедри Телекомунікаційних систем
Ярош В.О.
аспірант кафедри Телекомунікаційних систем
Державний університет телекомунікацій
М. Київ, Україна

ТРАНСФОРМАЦІЯ ІСНУЮЧИХ МЕРЕЖ ДО ТЕХНОЛОГІЙ SDN

Основною метою розробки нових мережевих технологій Software Defined Network (SDN, програмно-конфігуровані мережі) є прагнення спростити основні мережеві компоненти, а саме маршрутизатори та комутатори, знизити їх вартість та збільшити пропускну здатність мережі. Ще однією із важливих цілей розробки SDN є можливість централізованого управління мережевим трафіком.

Технологія SDN передбачає розподіл функцій управління мережею і функцій передачі даних. Така архітектура дозволяє виділити з мережевого обладнання рівень управління і зробити його програмованим (програмно-управляємим або програмно-конфігурованим). При цьому базова інфраструктура передачі даних також відділяється від мережевих сервісів і додатків. Основним елементом архітектури SDN є протокол OpenFlow, за допомогою якого виконується взаємодія між рівнем управління і базовою мережевою інфраструктурою.

Мережеві пристрої можно поділити на «спадкові» (традиційні комутатори і маршрутизатори), OpenFlow-засоби (комутатори з підтримкою рівня перенаправлення, де керування знаходиться на зовнішньому компоненті) і гібридні.

Трансформацію існуючих мереж до технологій SDN потрібно проводити в декілька етапів. Під час цих процесів в мережу потрібно вводити OpenFlow-засоби, які будуть працювати разом з наявними пристроями. Мережеві операції будуть здійснюватись як і традиційними пристроями управління, так і контролерами і конфігураторами OpenFlow.

Для реалізації процесу міграції можна запропонувати наступні способи:

– розгортання мережі з початкового етапу (вводяться OpenFlow контролери, необхідності підтримувати «спадкові» пристрої немає);

– змішане розгортання мережі (нові OpenFlow-засоби розгортаються спільно з традиційними комутаторами і маршрутизаторами, а також взаємодіють зі «спадковими» пристроями);

– гібридне розгортання мережі.

Після міграції існуючої мережі на платформу SDN, початкова система керування мережею (пристрої керування, комутатори і маршрутизатори) видаляється.

Отже, мережі SDN відкривають більше можливостей для промисловості і бізнесу, дозволяючи вирішувати задачі підвищення пропускної здатності каналів, спрощення керування мережею, перерозподіл навантаження, підвищення маштабованості.

Власенко В.О.
аспірант кафедри Інфокомунікацій
Державний університет телекомунікацій
м. Київ, Україна

СТАНДАРТ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G ЯК СКЛАДОВА МЕРЕЖ МАЙБУТНЬОГО

На сьогодні мобільна індустрія розвивається досить високими темпами. До 2020 року планується побудова та впровадження мереж передачі мобільного зв'язку 5-го покоління (5G), які перевернуть уяву про бездротові мережеві технології, що передбачає з'єднання смартфонів, різних електронних пристроїв та різноманітних електронних пристроїв між собою. Для цього необхідно розширити проникнення мобільного зв'язку за рахунок розвитку волоконно-оптичних технологій передачі даних.

В мережі 5G мільярди людей та машин матимуть змогу передавати інформацію зі швидкістю до 100 Гбіт/с.

Сьогодні значний обмін даними між мобільними пристроями відбувається за рахунок використання мереж LTE. Коли у 2G (GSM) і 3G (UMTS) телефонні мережі і мережі передачі даних розглядаються окремо, то в мережах 4G обмін даними і телефонні розмови здійснюється за рахунок пересилання IP-пакетів, використовуючи технології передачі голосу по мережі LTE (Voice over LTE). Стандарт LTE використовує тільки одну мережу – Інтернет, тоді як 5G має можливість охопити всі мережеві платформи.

Приведемо різні фактори які впливають на розвиток мереж майбутнього.

Фактор даних – передбачає оптимізацію мереж у зв'язку з гігантським об'ємом оброблюваної інформації, що зробить легким доступ до послуг, швидким та якісним незалежно від місцеперебування користувача. Кожна людина отримає свою унікальну адресу, за допомогою якої зможе авторизуватися в будь-якій точці світу і отримувати всі потрібні йому послуги.

Екологічний фактор впливу передбачає, що мережа майбутнього буде безпечна для навколишнього середовища. Її архітектура повинна бути побудована таким чином, щоб мінімізувати вплив на екосистему, скоротити споживання матеріалів і енергії, а також зменшити викиди парникових газів.

Соціально-економічний фактор свідчить про те, що проблеми у світовій економіці, а саме втрата платоспроможності населення спричинять зниження використання послуг. Тому слід переглянути витрати на забезпечення циклу послуг у бік їх зниження та уніфікації надання доступу населенню до ресурсів FN, а широкосмуговий доступ, послугує розвитку економіки.

5G дозволить операторам зв'язку підвищити доходи і рентабельність шляхом надання повного діапазону послуг і додатків. Також, вони зможуть досягти економії за рахунок інтеграції існуючих мереж, що спричинить скорочення експлуатаційних витрат. Таким чином FN сприятиме розширенню можливості доступу в Інтернет, подоланню цифрового розриву і збільшенню ступеня проникнення цифрового зв'язку до світової спільноти.

Примаченко В.І.
аспірант кафедри Комутаційних систем
Державний університет телекомунікацій
м. Київ, Україна

МАТРИЦЯ РОЗПОДІЛУ ЧАСТОТНОГО РЕСУРСУ

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 [1, с. 533].

Тому, використання програм комп'ютерної математики [2, с. 5] при автоматизації розрахунку зони радіопокриття БС дозволяє значно спростити і підвищити точність планування мережі.

Мета дослідження полягає в розробці програми автоматизації розрахунку зони радіопокриття базової станції при попередньому плануванні мережі в MathCad.

Приведений алгоритм 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 [3, с. 22, 4, с. 143].

Література

1. Галкин В. А. Цифровая мобильная радиосвязь. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2007. - 432 с.
2. В. П. Дьяконов VisSim+Mathcad+MATLAB. Визуальное математическое моделирование. - М.: СОЛОН-Пресс, 2004. - 384 с.
3. Гринкевич Г.О., Макаренко А.О. Розробка імітаційної моделі та алгоритмів функціонування MIMO-системи / Г. О. Гринкевич // Зв'язок. - 2012. - №2. - С. 22-24.
4. Примаченко В.І. Аналіз сучасного стану розвитку широкосмугової безпроводової передачі даних в Україні // Збірник тез міжнародної науково-технічної конференції "Сучасні інформаційно-телекомунікаційні технології: Том ІІІ. Розвиток інформаційних технологій". - К.: ДУТ, 2015. - С. 143.

Сабадаш В.А.
аспірант кафедри обчислювальної техніки
Державний університет телекомунікацій
м. Київ, Україна

АКТУАЛЬНІСТЬ СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Зі швидким розвитком технологій, прогрес сучасних технологій кожен рік прискорюється, а це породжує той факт, що одним з основних цінних ресурсів являється час. Саме тому пропонується створення та впровадження системи підтримки прийняття рішень (СППР) у сфері інформаційних технологій. Функціонування та мета СППР вказується нижче у даному тезісі.

Система підтримки прийняття рішень являє собою систему підтримки прийняття рішень, яка дозволяє використовувати методи штучного інтелекту (ШІ). Використовуючи технології ШІ в інформаційних системах дає змогу автоматизації процесу тощо.

В ідеалі, система підтримки прийняття рішень, повинна бути як консультант для користувача, а саме для людини. Допомагаючи у прийнятті рішень збираючи та аналізуючи докази, а також ідентифікація та діагностика проблеми, слідом пропозиції дій та оцінка запропонованих дій.

Метою ШІ вбудованого в інтелектуальну систему підтримки прийняття рішення являється забезпечення завдань, які повинні бути виконані за допомогою комп’ютера, в той час, як емуляція проводиться близька до можливостей людини.

СППР основана на експертних системах, які кодують когнітивні поведінки людей експертів, використовуючи правила предикативної логіки. Такий метод кращий, адже демонстрував кращу роботу ніж живі люди при певних обставинах.

Точність та сталість СППР можна порівняти з експертами людьми, коли параметри рішення заздалегідь відомі, проте можуть виникати певні проблеми, якщо відбуваються невизначені чи непередбачені обставини.

Деякі дослідження щодо ШІ зосереджені на наданні системі реагувати на новинки та невизначеності, це більш гнучкий шлях для використання в системах підтримки прийняття рішення.

Ряд методів ШІ, наприклад, які засновані на «міркуванні», також використовуються для системи підтримки прийняття рішень для кращого виконання операцій в умовах невизначеності.

Література:

1. «Intelligent decision support system» - мережа інтернет

Dorogyy Y.Y., Vasylenko D.A.
NTUU "KPI, Faculty of Informatics and Computer Technology

SPIKING NEURAL NETWORKS FOR PATTERNS RECOGNITION

A spiking neural network model can be used to identify patterns. The network is a two layered structure consisting of integrate-and-fire and active dendrite neurons.[2]

Neurological research shows that the biological neurons store information in the timing of spikes. Spiking neural networks belong to the third generation of neural networks and use spikes to represent information flow. As they use pulse coding for information processing, they are much faster than rate.

Spiking neurons can be used for spatial and temporal patterns analysis. They provided a biologically plausible learning algorithm for realizing radial basis functions, which are quite powerful in function approximation and pattern classification.[2]

The following spiking neural network model is used for pattern recognition. It is an active dendrite and dynamic synapse model. In this model, a neuron receives input via spike through a set of synapses and dendrites. The total post-synaptic current for the synapse i, with weight w^i attached to a dendrite is given by:

$$T_d^i \frac{dI_d^i(t)}{dt} = -I_d^i\ t\ + R_d^i w^i \delta(t - t_f^i)$$

Here t_f^i is the set of pre-synaptic spike times filtered as Dirac δ pulses. The time constant T_d^i and resistance R_d^i defines the active property of the dendrites as the function of synaptic weights and are defined as:

$$T_d^i = T_{max} - \ w_i\ \ T_{max} - T_{min}\ ,\ w_i\ \ \leq 1$$

From the above equation we can see that for height weights, T_d^i is closer to T_{min}, whereas for low weights, T_d^i is closer to T_{max}. Thus, as the time constraint is low for stronger synapses, we have an earlier and stepper increase of soma potential as compared to weaker synapses. The resistance R_d^i is given by:

$$R_d^i = \frac{T_d^i \theta}{R_m}\ \ \frac{T_m}{T_d^i}^{\ \frac{T_m}{T_m - T_d^i}}$$

Here θ is the neuron's firing threshold, R_m is the soma resistance, and T_m is the soma time constant. The above equation for R_d^i ensures that the maximum value of the membrane potential change is proportional to the neuron's firing threshold θ[1].

A two layered spiking neural network can be used to identify patterns, for example characters in a character set. Spike timing dependency plasticity can be used to train the network. The network should be trained until no significant weight change is observed. Using the given model, spiking neural network was used to recognize character. It managed its task successfully and thus, image recognition can also be possible using the explained model.

References

1. Ankur Gupta, Lyle N. Long "Character recognition using Spiking neural networks.
2. Israel Tabarez, Neil Hernandez, Miguel Gonzalez "Pattern recognition with Spiking neural networks"

Мушта С.С.
аспірант кафедри Вищої математики
Прилєпов Є.В.
аспірант кафедри Інформаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ NGN В УКРАЇНІ

Серйозною термінологічною проблемою, пов'язаною з NGN, є підміна поняття NGN. Окремі компанії, намагаючись прикритися цим модним словом, пропонують послуги та механізми ISDN або Ethernet по традиційних TDM-мережах, аргументуючи це тим, що ця служба дозволяє передавати мовлення і дані.

Окрім того, до основних проблем, які гальмуватимуть впровадження NGN-мереж на вітчизняному ринку, слід віднести:

1. недостатню зрілість послуг, особливо бізнес-послуг;
2. повільне нарощування пропускної здатності транспортної пакетної мережі NGN;
3. забезпечення сумісності мережних компонентів різних виробників у комплексних рішеннях;
4. нестача фахівців високої кваліфікації в основних компаній-операторів.

Проте ключова організаційна проблема щодо NGN полягає у відсутності проблемно-орієнтованої нормативно-правової бази, що є одним з основних факторів, які стримують упровадження NGN-рішень в Україні. Проблеми регулювання ринку NGN стосуються аспектів ліцензування операторської діяльності, побудови мереж, приєднання до інших мереж, нумерації тощо.

Сьогодні практично всі великі постачальники телекомунікаційних рішень пропонують комплекси NGN-обладнання, у першу чергу різні версії програмних комутаторів. Серед основних постачальників платформ на базі SoftSwitch — Alcatel, Lucent, Nortel, Ericsson, Siemens, Huawey, Italtel, VerasNetworks і CiscoSystems. Однак слід зазначити, що всі корпоративні платформи підтримують власні технології, несумісні між собою ні за функціями, ні за інтерфейсами. Це звичайна проблема нових технологій, особливо складних і багаторівневих, для яких важко апріорно виявити оптимальні варіанти реалізації. Так відбулося і з NGN для яких «декларація про наміри» не була вчасно підтримана розробкою відкритих стандартів на міжрівневі й зовнішні інтерфейси. Самі виробники, зацікавлені в продажах комплексних рішень і прив'язці клієнтів до своїх технологій, спочатку не виявляли ініціативи в розробці таких стандартів.

Тобто основна технологічна проблема NGN — це складність реалізації системи експлуатаційного управління при конвергенції різних технологій в рамках однієї мережі. За підвищення ефективності й гнучкості використання мережних ресурсів у результаті міграції існуючих мереж до NGN оператори «розплачуються» неймовірним ускладненням механізмів, для адекватної підтримки яких потрібні найсучасніші інформаційні технології. Наприклад, сьогодні умова доступності організовується: у телефонії софтсвічем, у передачі даних — сервером, хоча вже існують рішення для спільного надання цих послуг. Надалі розвиток софтсвічів убік єдиної платформи приведе до того, що «суперсофтсвіч» майбутнього забезпечить на рівні комутації принцип виконання умов NGN.

Література:

1.Гольдштейн Б.С., Кучерявий А.Е. Сети связи пост-NGN// СПб.:БХВ-Петербург, 2014.—160 с.: ил

2.Гольдштейн Б.С., Орлов О.П., Ошев А.Т., Соколов Н.А. Модернизация сетей доступа в эпоху NGN// Вестник связи.-2003.-№6.

3.Шнепс-Шнеппе М.А. Архитектура OSA/Parlay как реализация NGN// Вестник связи.-2003.-№9.

Мушта С.С.
аспірант кафедри Вищої математики
Сабадаш В.А.
аспірант кафедри Обчислювальної техніки
Державний університет телекомунікацій
м. Київ, Україна

РЕКОМЕНДАЦІЇ ЩОДО ПОБУДОВИ МЕРЕЖ NGN НА ОСНОВІ ІСНУЮЧИХ МЕРЕЖ ЗВ'ЯЗКУ

NGN – це мережна архітектура, яка повинна бути реалізована перш за все на базі об'єднання різних мереж. Революційні перетворення мереж і відповідний інтерес до цих перетворень, відносяться до об'єднання мобільних і фіксованих мереж.

Отже, NGN характеризується незалежністю сервісних функцій мережі від використовуваних в ній транспортних технологій. Така мережа повинна забезпечувати абонентів можливістю безперешкодного отримання послуг різних провайдерів і підтримувати "мобільність" абонента, забезпечуючи йому постійний доступ до послуг незалежно від його місцезнаходження.

Для впровадження NGN на існуючі мережі зв'язку існує декілька сценаріїв, але їх аналіз дозволив зробити висновок, що найефективнішим рішенням є радикальна зміна структури мережі.

Модернізацію існуючої мережі слід починати з транзитного рівня мережі, при цьому для впровадження мереж NGN рекомендується дотримуватися наступного порядку дій:

1.Установка транзитних вузлів комутації Softswitch + UMG на транзитному/міжміському рівні мережі. Введення вдосконаленого HLR (Smart HLR) для зберігання абонентської бази мережі.

2. Відведення мовного трафіку по IP-мережі (замість розширення пропускної здатності каналів транспортної мережі TDM). Надання базових мовних послуг класів 4 і 5 по IP-мережі з керуванням від Softswitch.

3. Реконструкція місцевого рівня мережі із заміною місцевих АТС на медіа-шлюзи доступу високої ємності,розвиток оптичних мереж доступу на основі медіа-шлюзи малої і середньої ємності, впровадження широкосмугових інтерфейсів доступу xDSL. Початок впровадження мультимедійних рішень IMS на основі MSAN.

4. Розвиток обслуговуючих платформ.

5. Інтеграція з мобільного мережею FMC.

Література:

4. Гольдштеин А.Б. Устройства управления мультисервисными сетями: Softswitch.

5. Абонентский доступ к сетям NGN. Электронная версия на сайте http://www.comquest.ru/sol/iskratel/sa_ngn/

Жданова Ю.Д.,
Доцент каф. Інформаційної та кібернетичної безпеки
Шевченко С.М.
Доцент каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

МАРКОВСЬКИ МЕРЕЖІ СИСТЕМ МАСОВОГО ОБСЛУГОВУВАННЯ

Математичні моделі систем, які призначені для обслуговування заявок, що надходять через випадкові проміжки часу, де тривалість обслуговування в загальному випадку також випадкова, називають системами масового обслуговування (СМО).

Марковська мережа СМО утворюється скінченним числом N однакових за типом марковських СМО. Їх робота задається матрицею $P = p_{ij}, i, j = \overline{1,N}$, де p_{ij} – ймовірність переходу обслуженої вимоги від системи i до системи j.

Зіставимо мережі СМО граф, вершинами якого є окремі СМО, а ребрам відповідають переходи між системами (вузлами мережі). Припустимо, що граф не має петель, тобто для будь-якого i $p_{ii} = 0$. Кожна i-та СМО визначається також інтенсивностями вхідного $\lambda_i\ x$ та вихідного $\mu_i\ x$ потоків вимог. Будемо вважати, що інтенсивності $\lambda_i\ x$, $\mu_i\ x$ залежать від стану всіх вузлів мережі, тобто $x = x_i, i = \overline{1,N}$. Звідси випливає основне припущення про роботу марковської мережі СМО – інтенсивності вхідного $\lambda_i\ x$ та вихідного $\mu_i\ x$ потоків вимог є вектор-функціями $\lambda\ x = \lambda_i\ x, i = \overline{1,N}$, $\mu\ x = \mu_i\ x, i = \overline{1,N}$ від векторного аргументу $x = x_i, i = \overline{1,N}$.

Розглянемо, наприклад, мережу СМО типу $M/M/\infty^N$, яка утворюється N однаковими СМО типу $M/M/\infty$ з необмеженим числом обслуговуючих пристроїв у системі. Для такої СМО вектор-функції $\lambda\ x$, $\mu\ x$, що задають інтенсивності вхідного та вихідного потоків вимог відповідно, мають вигляд $\lambda\ x = \lambda = \lambda_i, i = \overline{1,N}$, $\mu\ x = x_i \mu_i, i = \overline{1,N}$.

Процес вимог $\nu\ t$ визначає число вимог, що обслуговуються в системі в момент часу t. При $\lambda > \mu$ нормований процес вимог $X^\varepsilon\ t = \varepsilon\nu\ t/\varepsilon^2 - \varepsilon^{-1}\ \rho_0 + \lambda - \mu\ t$ при $\varepsilon \to 0$ збігається до дифузійного процесу $X^0\ t$ з нульовим середнім значенням і дисперсією $\varepsilon^2 = \lambda + \mu$.

Література:

1. Анисимов В.В., Лебедев Е.А. Стохастические сети обслуживания. Марковские модели. – Киев: Лыбидь, 1992. – 205 с.

Дорогий Я.Ю.,
Колісніченко В.Ю.,
Національний технічний університет України «Київський Політехнічний Інститут»
м. Київ, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ТРЕНУВАННЯ СПАЙКОВИХ НЕЙРОННИХ МЕРЕЖ

Спайкові нейронні мережі відрізняються від звичайних нейронних мереж, тому не можна використовувати класичні методи для їх тренування (наприклад backpropagation). Тематика спайкових мереж досить нова, тому не існує консенсусу як найкраще навчати мережі. У доповіді розглядаються методи тренування спайкових нейронних мереж для вирішення задач машинного навчання.

Різноманіття методів навчання спайкових мереж можна розділити на два типи: методи, побудовані на основі зворотного поширення помилки та методи, засновані на біологічних законах (правилах).

Традиційні алгоритми для навчання штучних мереж можна адаптувати для навчання спайкових мереж, використовуючи часове кодування (temporal coding). Одним з таких методів є SpikeProp. Він використровує SRM модель нейрона для передачі інформації під час імпульсів [1, с 35]. Також існують алгоритми, які використовують моделі нейронів QIF та Theta [2, с 26]. Методи FreqProp та Remote Supervised Method (ReSuMe) беруть ідеї з біологічних нейронних мереж [3, с 46].

Навчання спайкових мереж можна робити за допомогою законів, відкритих в області нейронаук. Найчастіше імітують Spike-timing-dependent plasticity (узагальнення правила Хебба) - процес встановлення ваг (сил зв'язку) між нейронами. Ще один алгоритм використовують для навчання мереж - Local Hebbian delay-learning [1, с 33].

При використання різних методів навчання потрібно зважати на те, які задачі ставлються. Потрібно зважати на швидкість навчання спайкової нейронної мережі та на втрату точності (порівняно зі звичайними ANN) для задач розпізнавання та класифікації. Одна із цілей поставлена на спайкові мережі — це імітування роботи біологічних нейронних мереж, тому й методи їх навчання повинні бути схожі.

Література:

1. Developing a supervised training algorithm for limited precision feed-forward spiking neural networks / Evangelos Stromatias. – 2011.
2. The Next Generation Neural Networks: Deep Learning and Spiking Neural Networks / Erdem Basegmez**.** – 2014.
3. Learning in large-scale spiking neural networks / Trevor Bekolay. - 2011.

Мушта С.С.
Аспірант кафедри Вищої математики
Державний університет телекомунікацій
м.Київ, Україна

ОСОБЛИВОСТІ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ САМООРГАНІЗУЮЧИХСЯ МЕРЕЖ

Як відомо інформаційно телекомунікаційна мережа складається з вузлів комутації і каналів зв'язку між ними. головною вимогою, що висувається до інформаційних телекомунікаційних мереж, є виконання нею основної функції– забезпечення абонентів мережі потенційною можливістю доступу до розподілених інформаційних ресурсів, об'єднаних у ІТМ. Всі інші вимоги – продуктивність, надійність, точність, сумісність, керованість, живучість, розширюваність і масштабованість – зв'язані з якістю виконання цієї основної задачі [1]. У сучасних умовах на ІТМ впливають внутрішні і зовнішні фактори, тому задача забезпечення стійкого функціонування ІТМ є актуальною. Ця задача досліджувалась і досліджується у багатьох наукових працях [1–3]. Основна увага в них приділяється вирішенню задач побудови резервованих інформаційно-керуючих систем, відмовостійких керуючих обчислювальних систем, адаптивних систем управління. В [4] ведене поняття функціональної стійкості складних динамічних об'єктів, що можуть описуватися системою диференціальних рівнянь. Однак для складних організаційних систем даний апарат неприйнятний. В теорії надійності [2] обчислення показників надійності опирається в основному на приведенні структури до послідовних і паралельних з'єднань. Це також не прийнятно для складних організаційних систем з безліччю перехресних зв'язків і взаємовпливом станів окремих елементів на інші елементи.

Список використаної літератури

1. Додонов А.Г. Введение в теорию живучести вычислительных систем/ А.Г. Додонов, М.Г. Кузнецова, Е.С. Горбачик. – Ин-т пробл. регистрации информации. – К.: Наукова думка, 1990. – 184 с.

2. Кравченко Ю.В. Метод поетапного зменшення потужності бази матроіда в задачах побудови топології системи зв’язку і автоматизації управління військами/ Кравченко Ю.В., Микусь С.А.// Системи озброєння і військова техніка. – 2013. – № 4(36). – С. 74 – 78.

3. Королев А.В. Адаптивная маршрутизация в кор- поративных сетях/ А.В. Королев, Г.А. Кучук, А.А. Пашнев – Х.: ХВУ, 2003. – 224 с.

4. Обідін Д. М. Ознаки та критерії функціональної стійкості інтелектуалізованої системи автоматичного управління польотом літака./ Д.М. Обідін, О.В. Барабаш // Системи озброєння і військова техніка: Науковий журнал. – 2012. – № 1 (29). – С. 133 – 136

Усова А.І.
студентка ННІЗІ
Державний університет телекомунікацій
м. Київ, Україна

RELATIONAL DATABASE MANAGEMENT SYSTEM SECURITY

In order to store data in organized and secure way databases were designed. To operate database so called DBMS is used or database management system. There are two most popular DBMS solutions: relational database management system and object-oriented database management system. Both have their own strengths and weaknesses. Therefore, different approaches have to be applied in database protection [3, pg. 1395].

There are few aspects that has to be followed while Protecting RDBMS. Firstly, only administrator should have unique rights to prevent an unauthorized access and configuration change. Thus, configuration has to be considered as well in order to eliminate database's vulnerability. Lastly, penetrations can be hidden underneath the database itself. Hacker can use SQL or structured query language which can be forced into sending false queries [1, pg. 387].

Few possible solutions can be reviewed. Encrypting the data is the wide spread protection method [2, pg. 764]. Another method is designing and implementing Security Policies and Access Control Policies. Administrator should develop data model and then grant access permissions [1, pg. 387].

Regularly, for RDBMS security SQL GRANT and REVOKE statements are used. These statements allow database clients to selectively grant permission and revoke it if necessary [3, pg. 1401].

For the reasons of increased security needs new approaches are developed. However, for relational database management systems access control and cryptography is still the best methods that are used.

Literature:

1. Bidgoli, H. (2006). *Handbook of information security*. Hoboken, N.J.: John Wiley.
2. Khmelevsky,. (2008). nformation and data protection within a RDBMS. *Condensed Matter Physics*, *11*(4), 761. http://dx.doi.org/10.5488/cmp.11.4.761
3. Nozaki, M., & Tipton, H. (2006). *Information security management handbook on CD-ROM*. Boca Raton, FL: Auerbach Publications.

Романчук Б.М.
аспірант, М.Н.С.
Інститут газу Національної Академії Наук України
м. Київ, Україна

ЕНЕРГОЕФЕКТИВНІСТЬ ДЖЕРЕЛ ЕНЕРГІЇ

Для того, щоб отримати енергію, потрібно спочатку затратити енергію[1, с. 103]. У літературі це зветься EROEI (або ERoEI, англ. Energy returned on energy invested - співвідношення отриманої енергії до витраченої енергії; або EROI, energy return on investment - співвідношення отриманої енергії до витраченої). EROEI - це головний показник енергоекономічності[2, с.1].

Як яскравий приклад: раніше для отримання ста барелів нафти використовувався тільки один її барель. Але на сьогоднішній день всі запаси, які було легко розвідати і добути вже закінчилися. Через це EROEI для нафти вже не 100, а лише 10.

Звичайно можна займатись перетворенням одних форм палива на інші, але на кожне таке перетворення безповоротно витрачається енергія, яка містилася у вихідному паливі. Такий підхід може бути виправданий тільки в тих випадках, коли паливо змінює якісь свої фізичні властивості. Наприклад, отримання газу з твердого палива чи бензину з вугілля. Переробка ж таких не типових покладів, як бітумні піски і сланці здебільшого не рентабельна так як EROEI для них коливається в межах 1.5 - 5[3, с.5].

Біопаливом, як правило, можуть служити відходи виробництва продуктів харчування, або ж спеціально вирощені енергетичні культури. У випадку з відходами таке біопаливо є вторинним продуктом виробництва продуктів харчування і часто поліпшує його техніко-економічний баланс.

Біопаливо буде повноцінним відновлювальним джерелом енергії тільки в тому випадку коли його вирощування не завдаватиме шкоди земельним ділянкам. Важливим є щорічне відновлення землі з допомогою повноцінних добрив, що компенсують весь спектр органіки і мікроелементів в ґрунті.

Література:

1. Murphy, D.J. (2010). «Year in review EROI or energy return on (energy) invested». Annals of the New York Academy of Sciences 1185: 102–118. DOI:10.1111/j.1749-6632.2009.05282.x
2. Cutler, Cleveland Energy return on investment (EROI). The Encyclopedia of Earth
3. "Appendix VI – Fact Sheets" (PDF). Alberta Oil Sands Consultations Multistakeholder Committee Interim Report. Government of Alberta. 30 November 2006. p. 14. Retrieved 17 August 2007.

Тихонов Є. С.
аспірант кафедри Прикладного програмування
Державний університет телекомунікацій
м. Київ, Україна

ТЕНДЕНЦІЇ РОЗВИТКУ BIG DATA В НАШ ЧАС

Великі Дані (Big Data, ВД) - загальний термін, використовуваний для опису величезної кількості неструктурованих і частково структурованих даних, які створює компанія. Це дані, зберігання яких в реляційній базі даних для аналізу зайняло б занадто багато часу і коштувало б надто багато грошей [1]. Хоча Великі Дані не відносяться до якої-небудь конкретної величини, коли про них говорять, часто використовують терміни «петабайт» і «ексабайт» даних [2].

Значимість технології ВД в національній економіці буде підвищуватися в залежності від того, чи буде технологія ВД використовуватися для вирішення практичних завдань компаній.

Обсяги виробництва і в цьому секторі, як і раніше, будуть визначатися як числом працюючих, так і продуктивністю їх праці. Під працюючими тут і далі маються на увазі не фахівці в області IT або математики, а фахівці-предметники: лікарі, управлінці середнього і високого рівня, що працюють на заводах, фабриках, торговельних підприємствах оптової та роздрібної торгівлі, і широкий спектр фахівців самих різних спеціальностей. Вони повинні бути оснащені такими інструментами аналізу, з якими зможуть спілкуватися мовою своєї предметної області і отримувати відповіді, що інтерпретуються в поняттях їх предметної області.

В даний час можна відокремити дві тенденції ВД:

- освоєння і формування нових методик, вирішення практично значущих

завдань на основі доступних комплексів інструментальних засобів, або платформ;

- розвиток методів і технологій ВД, а також їх імплементація до складу

доступних платформ.

Обидві тенденції вимагають інтенсивної підготовки кадрів, які володіють відповідними знаннями, методиками та інструментами.

Література:

1) Preimesberger, Chris. Hadoop, Yahoo, ‘Big Data’ Brighten BI Future (англ.). EWeek (15 August 2011).

2) https://uk.wikipedia.org/wiki/Петабайт

Албул А.С.
аспирант кафедры 502
Национальный аэрокосмический университет им. Н. Е. Жуковского
г. Харьков, Украина

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СПУТНИКОВЫХ СИСТЕМ ВЫСОКОСКОРОСТНОЙ ПЕРЕДАЧИ ДАННЫХ

Системы телекоммуникаций в современном мире являются важнейшим элементом множества сфер деятельности человека. Возможность оперативно передавать информацию в любую точку планеты является обязательным условием успешного функционирования многих государственных и коммерческих субъектов. Спутниковые системы (СС) связи являются наиболее эффективными с точки зрения контроля за передаваемой информацией и территории покрытия. В настоящее время одной из мировых тенденций развития отрасли спутниковой связи является создание спутниковых систем высокоскоростной передачи (ВПД) данных в Ku- и Ka-диапазонах.

Новое поколение спутниковых систем, таких как OneWeb (который создали основатели Virgin Galactic, Qualcomm и O3b, проект возглавляет Greg Wyler) и SpaceX (Google/Fidelity, Elon Musk), ставит своей целью предоставить конкуретноспособные телекоммуникационные услуги, предназначенные для широкополосного соединения миллиардов людей по всему миру. За последние 12 лет общий объем инвестиций в спутниковые системы с высокоскоростной передачей данных превысил $ 13 млрд. Такой впечатляющий уровень инвестиций будет превзойден одними только OneWeb и SpaceX, которые оцениваются примерно в $ 2 млрд и $ 15 млрд соответственно. Указанные проекты также предполагают резкое увеличение в плане пропускной способности: OneWeb с помощью 649 спутников почти на 9100 Гбит/с Ku-диапазона; в то время как предполагаемая группировка из 4000 спутников SpaceX должна будет добавить до 40000 Гбит/с пропускной способности.

Учитывая особенности функционирования спутниковых систем (длительный процесс развертывания и жизненный цикл), предлагается при построении перспективных СС ВПД использовать agile (гибкий) подход, позволяющий оперативно реагировать на изменения структуры рынка, внешних условий и д.р.

[1]Толюпа С.В., [2]Прус Р.Б./
[1]доктор технічних наук, професор
[2]кандидат технічних наук
[1,2]Київський національний університет імені Т. Шевченка
м. Київ, Україна

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Однією з ключових проблем, які в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства постали перед усіма державами світу, є проблема захисту інформації, що обробляється в інформаційних системах, від викликів і загроз у кібернетичному просторі. Можливості кібернетичного простору, лавиноподібний процес розвитку та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для накопичення та використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур та дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і інформаційним системам [1].

Побудова в Україні інформаційного суспільства можлива за умови широкої інтеграції сучасних технологій автоматизованої обробки даних у всі сфери економіки, державного управління та суспільної діяльності. Це різко збільшує залежність реалізації окремих життєво важливих інтересів осіб, суспільства та держави від належного функціонування інформаційної системи (ІС), за допомогою яких й забезпечується така реалізація. Значно зростають ризики завдання значної шкоди національним інтересам із використанням впливів кібернетичного характеру, збільшується кількість кібернетичних загроз національній безпеці. Фахівці вважають, що "кіберзброя та кібератаки за своєю руйнівною потужністю наслідкам наближаються до зброї масового знищення" [2].

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Тому, розбудова дієвої системи кібернетичної безпеки – одне з найнагальніших завдань забезпечення національної безпеки України [3].

Якщо розглядати інформаційну модель майбутнього, то не можна не окреслити ті напрями державної політики, які доцільно вжити для прогнозованого розвитку інформаційних технологій та зниження уразливості стратегічних об'єктів підвищеної небезпеки в нашій країні.

По-перше, необхідно удосконалити нормативно-правову базу відносно національної та кібернетичної безпеки держави, в якій слід було б окреслити загальні підвалини розвитку національної державності і основні сфери життєдіяльності, спричинення шкоди яким загрожує національним інтересам. Однією з таких сфер безперечно є інформаційна сфера. Отже розроблення концепції забезпечення інформаційної безпеки, принципів та методів управління органами державної влади й приватного сектору у цій діяльності є пріоритетним.

По-друге, необхідно розробити методику стратегічного планування кібервійн і відповідно до неї змоделювати основні загрози в інформаційній сфері для України з виробленням варіантів їх унеможливлення або мінімізації впливу дії негативних наслідків.

По-третє, потребують значного доопрацювання законодавство України щодо легального здійснення заходів по інформаційній безпеці, і відповідно до цього вироблення правового механізму настання відповідальності за вчинення протиправних дій у кіберпросторі.

Серед найбільш актуальних загроз ІС сьогодення визначається нездатність України протистояти новітнім викликам національній безпеці, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. Головним завданням держави є вжиття заходів, що дадуть змогу протистояти протиправним діям у кібернетичному просторі, уникнути або зменшити негативні наслідки від реалізації кібернетичних загроз. Тому кібернетична безпека в умовах розвитку глобального інформаційного суспільства стає необхідною складовою національної безпеки будь-якої держави.

Література:

1. М. М. Алексєєв. Формалізація процесу забезпечення кібернетичної безпеки держави. Науково-технічний журнал “Сучасний захист інформації”.– 2014. - №4.

2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. «Інформаційна та кібербезпека: соціотехнічний аспект» // Навчальний посібник. – К.: Наш формат, 2015. – 288с.

3. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок.— К.: НАУ, 2013.— 432 с.

[1]Толюпа С.В., [2]Пархоменко І.І.
[1]доктор технічних наук, професор
[2]кандидат технічних наук, доцент
[1,2]Київський національний університет імені Т. Шевченка
м. Київ, Україна

ЗАСТОСУВАННЯ МЕТОДІВ ТЕОРІЇ ДЕКОМПОЗИЦІЇ ДЛЯ ФОРМУВАННЯ СИСТЕМИ ПОКАЗНИКІВ ЯКОСТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

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 систем телекомунікацій 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 інформаційної системи (ІС) визначається рівнем захищеності її найбільш слабкої частини [1].

Бурхливий розвиток ІС 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].

Завдання оцінки ефективності функціонування системи безпеки ІС можна розглядати як одне із приватних завдань сучасної теорії дослідження операцій. У загальному виді завдання оцінки ефективності такої системи можна сформулювати так: при заданих вихідних умовах необхідно визначити систему, що у порівнянні з еталонною є кращою в змісті обраного або заданого критерію.

Від вибору критерію й системи показників якості (СПЯ) багато в чому залежить результат оцінки та 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 інформаційною 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 ІС у цілому. При такому підході до оцінки ефективності ІС 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 ІС, математично коректно декомпозовані в інтересах їхнього подальшого використання.

Аналіз різних методів формування узагальненого показника ефективності безпеки інформаційних систем показав, що найбільш повний облік особливостей рішення завдання оцінки ефективності функціонування ІС, 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 [3].

Таким чином, поняття ефективність безпеки ІС нерозривно пов'язане з результатами процесу функціонування ІС, опирається на систему показників якості процесу функціонування й вимоги до них. Узагальнений показник ефективності безпеки ІС із урахуванням наявності взаємообумовлених випадкових факторів, що визначають її роботу, доцільно визначати на основі апарата умовних ймовірностей у вигляді спільної ймовірності виконання всіх завдань, які розв'язуються у ході функціонування ІС та забезпечення її 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.,** 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.

3. **Толюпа С.В.** Метод багатокритеріального аналізу ефективності функціонування та забезпечення інформаційної безпеки інфокомунікаційних систем. // Науково-технічний журнал „Захист інформації”. - 2012. - №3 (54). с. 80-86.

[1]Д.О. Третьяк
студент
[2]В.І. Вялкова
к.т.н., асистент кафедри кібербезпеки та захисту інформації
[1, 2] Київський національний університет імені Тараса Шевченка, м. Київ

БІОМЕТРИЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Актуальність. Забезпечення інформаційної безпеки є однією із першочергових задач у будь-якій сфері бізнесу. З розвитком інформаційних технологій праця людини стала легшою, але в той же час зловмисники отримали набагато більше можливостей вплинути на діяльність підприємства. В зв’язку цим розробляються все більше і більше засобів захисту даних та доступу до них. Одним із таких способів є біометричні системи захисту, які з кожним роком вдосконалюються та становляться все більш доступними. Вони перестають бути уділом лише державних структур, а становляться дієвим інструментом підвищення конкурентоспроможності бізнесу. Активне залучення біометричних технологій відбулося після серії терористичних актів 11 вересня 2001 року, коли стало зрозуміло, як важливо забезпечити надійних захист доступу до важливих об’єктів [1]

Мета доповіді. Сформулювати принцип дії біометричних систем захисту інформації та описати основні їх види. Спробувати дати подальший прогноз на сфери та напрямів застосування.

Біометричні технології є одним із найефективніших способів захисту доступу до інформації та важливих об’єктів. На відміну від паролів, Pin-кодів, матеріальних носіїв(карток, флешок та ін.) біометрія використовує унікальні параметри кожної людини які важко підробити: сітківка ока, малюнок вен, форма долоні, відбиток пальців. Якщо картку можна передати, пароль піддивитись, то біометричні ідентифікатори «невід’ємні» від людини і їх неможливо забути або позичити [2]. Широке розповсюдження біометричні технології отримали у криптографічній сфері, де доступ до розшифрування надається тільки після біометричної перевірки власника інформації.

Основними характеристиками будь-якої біометричної охоронної системи є два показники - FAR (False Acceptance Rate) і FRR (False Rejection Rate). Перше число характеризує ймовірність помилкового збігу

біометричних характеристик двох людей. Друге - ймовірність відмови доступу людині, що має допуск.

Біометрична технологія захисту даних полягає у порівнянні фізичних параметрів особи з його характеристиками, що містяться у базі даних. Біометричний захист складається з двох етапів: реєстрації та ідентифікації. Реєстрація полягає у наступному: система робить запис зразка біометричної характеристики(райдужки ока, відбитку пальця, голосу), потім перероблює його у цифровий шаблон, який і заноситься у базу даних. При ідентифікації проходить наступна послідовність дій:

- Запис – фізичний зразок запам'ятовується системою.
- Виділення – унікальна інформація береться із зразка і створюється біометричний шаблон.
- Порівняння – збережений шаблон порівнюється із шаблоном із бази даних.
- Збіг/ не збіг – система сама вирішує чи збігається біометричні шаблони і виносить рішення [3].

Функція перетворення даних про біометричний ідентифікатор – односпрямована. Відновити відбиток пальця, або малюнок з вен неможливо, користувачі можуть не хвилюватись про конфіденційність своїх даних.

Існують такі основні види біометричних систем:

1. За відбитком пальців.
2. За райдужною оболонкою ока.
3. За сітківкою ока.
4. За геометрією обличчя.
5. За геометрією рук.
6. За венозним малюнком руки.
7. За голосом [4].

Кожен з них має свої слабкі та сильні сторони. Порівнюються такі параметри як простота в використанні, стабільність ознаки у часі, унікальність, стійкість до підробки та ін.

Висновки. Біометричні автентифікація є одним із надійніших методів захисту доступу до інформації. ЇЇ перевагами є дуже мала можливість підробки та простота в використанні. З сьогоднішніми темпами розвитку в найближчому майбутньому біометричні технології стануть основним методом захисту доступу в корпоративних системах, так як ідентифікатори в таких системах невід'ємні і унікальні для кожної особи.

Список використаних джерел

1. Михайлов А. Комплексний підхід в біометричних рішеннях для захисту бізнесу // Директор по безпеці: наук.-техн. зб. – 2012. - №5. – с.35-40.

2. Сорокин К. Біометрична автентифікація користувача- ефективний інструмент мінімізації інсайдерських ризиків // Банковські технології: наук.-техн. зб. – 2012. - №5 – с. 52-53.

3. Біометричні технології // Інформаційний ресурс “Вікіпедія” [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Биометрические_технологии

4. Шаров В. Біометричні методи комп’ютерної безпеки / Шаров В. [Електронний ресурс]. – Режим доступу: http://www.bytemag.ru/articles/detail.php?ID=6719

Арделян В.В.

аспірант кафедри льотної експлуатації, аеродинаміки та динаміки польоту Кіровоградська льотна академія Національного авіаційного університету, м. Кіровоград, Україна

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ПІЛОТАЖНО-НАВІГАЦІЙНОГО КОМПЛЕКСУ ПОВІТРЯНОГО СУДНА НА ОСНОВІ ІНТЕЛЕКТУАЛІЗАЦІЇ

В даній доповіді обґрунтуванні основні положень концепції забезпечення функціональної стійкості процесів управління на основі інтелектуалізації навігаційного комплексу, а саме системи автоматичного управління літальним апаратом.

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 (структурної, програмної, тимчасової і т.д.) при їх проектуванні.

Разом з тим, такий підхід, що часто використовується в різних технічних системах, 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.

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.

В доповіді буде показано, що на основі проведених досліджень отримала подальший розвиток існуюча теорія функціональної стійкості складних технічних систем в контексті деталізації цієї властивості для інтелектуальної системи автоматичного управління літальним апаратом. Напрямком подальших досліджень в цій області може бути широке коло питань, присвячених моделям визначення показників функціональної стійкості перспективних систем автоматичного управління літальним апаратом.