**Державна служба України з надзвичайних ситуацій**

**Львівський державний університет безпеки життєдіяльності**

**Національний університет "Львівська політехніка"**

**Politechnika Krakowska (Polska)**

**Національний технічний університет "Київський політехнічний інститут"**

**Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)**

# ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СУСПІЛЬСТВІ

**ТЕЗИ ДОПОВІДЕЙ**

**ІІ-ої Міжнародної науково-технічної конференції**

**24-25 листопада 2016 р.**

**Організатори конференції:**

Львівський державний університет безпеки життєдіяльності

Національний університет "Львівська політехніка"

Politechnika Krakowska (Polska)

Національний технічний університет "Київський політехнічний інститут"

Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)

У збірнику опубліковано матеріали конференції, присвячені проблемам інформаційної безпеки в сучасному суспільстві, зокрема управлінню інформаційною безпекою, безпеці інформаційно-комунікаційних систем, технічному захисту інформації.

**Поштова адреса оргкомітету:**
м. Львів, 79000, вул. Клепарівська, 35, кафедра управління інформаційною безпекою, кім. № 415

**Відповідальний за випуск – професор Самотий В. В.**

**Комп'ютерне макетування та верстка – доцент Лагун А. Е.**

**Матеріали подано у авторській редакції**

## ПРОГРАМНИЙ КОМІТЕТ

### ГОЛОВА

**Козяр М.М.** – ректор Львівського державного університету безпеки життєдіяльності, доктор педагогічних наук, професор, Член-кореспондент НАПН України, Заслужений працівник освіти України, генерал-лейтенант служби цивільного захисту

### ЗАСТУПНИК ГОЛОВИ

**Самотий В. В.** – завідувач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, д.т.н., професор

### ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ

**Бурячок В.Л. –** завідувач кафедри безпеки інформаційних технологій Державного університету телекомунікацій, доктор технічних наук, професор

**Горбенко І.Д.** – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, доктор технічних наук, професор

**Грицюк Ю.І.** – професор кафедри програмного забезпечення, НУ "Львівська політехніка", доктор технічних наук, професор

**Дудикевич В.Б.** – завідувач кафедри захисту інформації НУ "Львівська політехніка", доктор технічних наук, професор

**Корченко О.Г.** – завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, доктор технічних наук, професор

**Кузнецов О.О.** – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Н. Каразіна, доктор технічних наук, професор

**Максимович В.М.** – завідувач кафедри безпеки інформаційних технологій НУ "Львівська політехніка", доктор технічних наук, професор

**Мачуський Є.А.** – завідувач кафедри фізико-технічних засобів захисту інформації Національного технічного університету України "Київський політехнічний інститут", доктор технічних наук, професор

**Мельник А.О.** – завідувач кафедри електронних обчислювальних машин НУ "Львівська політехніка", доктор технічних наук, професор

**Мороз Л.В.** – професор. кафедри безпеки інформаційних технологій НУ "Львівська політехніка", доктор технічних наук, доцент

**Пархуць Л.Т**. – професор кафедри захисту інформації НУ "Львівська політехніка", доктор технічних наук, професор

**Рак Т. Є.** – проректор з науково-дослідної роботи Львівського державного університету безпеки життєдіяльності, доктор технічних наук, доцент, полковник служби цивільного захисту

**Ренкас А.Г**. – начальник інституту цивільного захисту Львівського державного університету безпеки життєдіяльності, кандидат технічних, доцент

**Саченко А.О. –** завідувач кафедри інформаційно-обчислювальних систем і управління Тернопільського Національного економічного університету, доктор технічних наук, професор

**Хорошко В.О.** – професор кафедри безпеки інформаційних технологій Національного авіаційного університету, доктор технічних наук, професор

**Шевчук В.О.** – завідувач кафедри міжнародних економічних відносин Львівської комерційної академії, доктор економічних наук, професор

**Яремчук Ю.Є.** – директор Центру інформаційних технологій і захисту інформації Вінницького Національного технічного університету, доктор технічних наук, професор

**Karpiński M.** – prof. ATH, Katedra Matematyki i Informatyki, dr hab. inż., Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)

**Khoma V.** – prof. PO, Katedra Systemow Sterowania i Systemow Decyzyjnych, dr hab. inż., Politechnika Opolska (Polska)

**Kirenko I.** – Phd, Project Leader at Philips Research (Nederland)

**Kovela S.** - PhD MBA PGCE CITP Senior Lecturer Accounting, Finance and Informatics, Kingston University London (United Kingdom)

**Petrov O. –** prof. AGH, Katedra Informatyki Stosowanej, dr hab. inż., Akademia Gorniczo-Hutnicza im. Stanisława Staszica, Kraków (Polska)

**Shakya S. –** Professor and Asst. Dean at Institute of Engineering, Tribhuvan University (Nepal)

**Yurish S.** – Professor, Technical University of Catalonia (UPC, Barcelona, Spain)

**Zając M.** – prof. nadzw. PK, Katedra Informatyki i Technik Informacyjnych, dr hab. inż., Politechnika Krakowska (Polska)

## ГОЛОВА ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

**Лагун А. Е.** – заступник завідувача кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

## ЗАСТУПНИК ГОЛОВИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

**Кухарська Н. П.** – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат фізико-математичних наук, доцент

## ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

**Гриник Р. О.** – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, старший лейтенант служби цивільного захисту

**Дзелендзяк У. Ю.** – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

**Мандрона М. М.** – старший викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

**Полотай О. І.** – старший викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

**Процько І.О.** – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

# ЗМІСТ

# ІНФОРМАЦІЙНА БЕЗПЕКА В ЕЛЕКТРОННОМУ НАВЧАННІ НА ПІДСТАВІ ХМАРНОГО ХОСТИНГУ MOODLECLOUD

*Віктор Артеменко*

Львівський торговельно-економічний університет, м. Львів, Україна

**The levels of cloud computing and project of move to "cloud" LMS Moodle are considered. Approaches to information security of cloud hosting. Their essence is based on principle: the security of the cloud – is the responsibility of the provider, the security in the cloud – is the responsibility of the client.**

**Keywords: information security, e-learning, cloud computing, learning management system Moodle.**

У сучасних умовах на ринках електронного (дистанційного) навчання все більшої популярності набувають хмарні обчислення (cloud computing) або хмарні технології. Суть цих понять – у наданні користувачам віддаленого доступу до послуг, обчислювальних ресурсів і додатків (у тому числі до операційних систем й інфраструктури) через інтернет. Розвиток аналізованої сфери хостингу (хостинг-послуга з розміщення обладнання клієнта на території провайдера із забезпеченням підключення його до каналів зв'язку з високою пропускною спроможністю) було обумовлено потребою в програмному забезпеченні та цифрових послугах, якими можна було б управляти зсередини, але які були б при цьому більш економічними та ефективними. Ці веб-інструменти, відомі також як хмарні сервіси, можна розділити на три основні категорії або рівні [1].

Нижчий рівень іноді називають "*Інфраструктура як послуга*" (IaaS, infrastructure as a service). На цьому рівні зовнішні користувачі отримують базові обчислювальні ресурси – наприклад, процесори та пристрої для зберігання інформації – і використовують їх для створення власних операційних систем і додатків. Одним з прикладів такого підходу є Amazon Elastic Compute Cloud (Amazon EC2). Тому будь-який навчальний заклад може застосовувати цю інфраструктуру за допомогою встановлення на віртуальних машинах Лінукс-серверів і за потреб нарощувати обчислювальні потужності.

Наступним рівнем є "*Платформа як послуга*" (PaaS, platform as a service). Тут користувачі мають можливість встановлювати власні додатки на платформі, що надається провайдером цієї послуги. Як приклад можна вказати на сервіс Google Apps Engine, що дозволяє розробникам створювати і встановлювати додатки на мові Python, Java або PHP.

Вищий рівень називається "*Програмне забезпечення як послуга*" (SaaS, software as a service). Саме цей рівень становить найбільший інтерес для певних навчальних закладів і користувачів електронного (дистанційного) навчання. При цьому в "хмарі" зберігаються не тільки дані, але й пов'язані з ними додатки, а користувачеві для роботи потрібно тільки веб-браузер. Кращим прикладом цього підходу є Google Apps Education Edition, де на базі хмарних обчислень надаються студентам і викладачам навчальних закладів інструменти, необхідні для ефективного спілкування та спільної роботи.

Інший підхід до використання хмарного хостингу, який починає поширюватися в електронному навчанні, це переміщення в "хмару" систем управління навчанням (LMS, Learning Management Systems). Зокрема творці LMS Moodle, найпопулярнішої системи управління навчанням, оголосили про запуск хмарного хостинга для освітніх закладів [2].

Варто зазначити, що передача підтримки LMS Moodle зовнішньому провайдеру має сенс для тих навчальних закладів, які спрямовані на більш економічне та ефективне використання дорогої комп'ютерної техніки та програмного забезпечення з урахуванням витрат, необхідних для навчання та підвищення кваліфікації викладачів і обслуговуючого LMS Moodle персоналу. Тому здається сумнівним, що в майбутньому навчальні заклади захочуть встановлювати і супроводжувати LMS самостійно на своїх внутрішніх ресурсах,

якщо хмарні провайдери зможуть надати доступ до безпечних, доступних і дешевшим аналогам традиційних LMS.

Основним ризиком, який пов'язаний з використанням хмарного хостингу, вважається іформаційна безпека. Європейський досвід свідчить про те, що необхідно враховувати відмінності між безпекою хмари (security OF the cloud) і безпекою в хмарі (security IN the cloud) [3]. Звичайно ж, провайдер вже подбав про безпеку самої хмари. Однак у деяких клієнтів існує помилкова точка зору про те, що передавши дані в хмару, вони передають відповідальність за захист даних та виконання нормативних вимог щодо інформаційної безпеки. Таким чином, безпека самої хмари є відповідальністю провайдера, а безпека в хмарі є відповідальністю клієнта. Тобто клієнт MoodleCloud сам займається розподілом і контролем доступу, управлінням оновленнями та іншими необхідними процесами щодо інформаційної безпеки.

Ми маємо на меті розглянути хмарний проект, який спрямований на переміщення у "хмару" LMS Moodle, та базові підходи щодо забезпечення інформаційної безпеки цього хмарного хостингу [4].

На рисунку представлена головна сторінка хмарного навчального середовища, яке ми створили для апробації вищевказаного підходу до інформаційної безпеки у MoodleCloud.

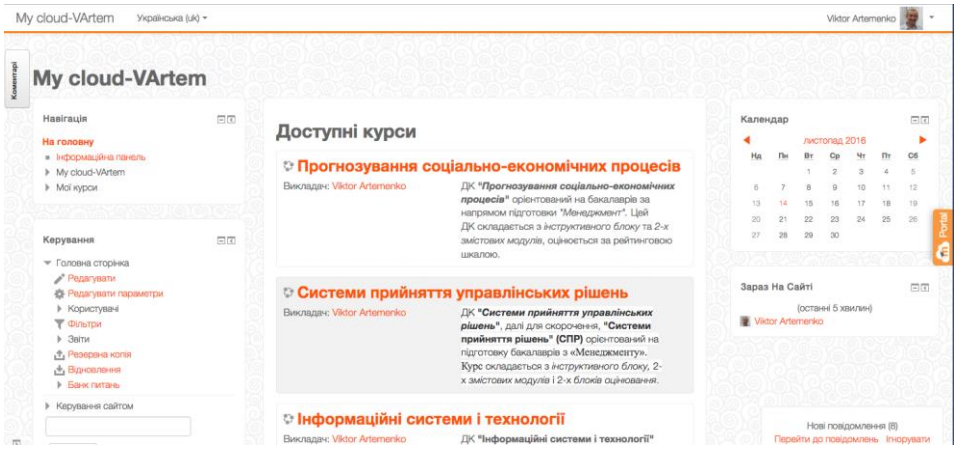



Рисунок. Головна сторінка хмарного навчального середовища My cloud-VArtem.

У хмарному хостингу My cloud-VArtem інформаційна безпека грунтується на політиці рольового розмежування доступу до ключових елементів цього навчального середовища. Тобто права доступу суб'єктів My cloud-VArtem формуються відповідно до їх повноважень та обов'язків (ролей). Оскільки My cloud-VArtem є повною версією Moodle з мінімальними обмеженнями, то рольове розмежування доступу виконувалося на засадах інформаційної безпеки цієї LMS [5].

## Література


1. Облачные вычисления в образовании / Институт ЮНЕСКО по информационным технологиям в образовании. Аналитическая записка. [Электронный ресурс]. – Режим доступа: https://moodle.org/pluginfile.php/1969005/mod_page/content/16/Oblachnyie%20vychiskenia%20v%20obrazovanii.pdf.
2. Moodle запускает бесплатно Облако Хостинг для преподавателей. [Электронный ресурс]. – Режим доступа: https://campustechnology.com/articles/2015/07/06/moodle-launches-free-cloud-hosting-for-educators.aspx?admgarea=news.
3. Облачная безопасность – взгляд из Европы. [Электронный ресурс]. – Режим доступа:
4. http://cloudzone.ru/articles/analytics/51.html.
5. Авторський сайт хмарного навчального середовища MoodleCloud. [Електронний ресурс]. – Режим доступу: https://artemvb15.moodlecloud.com/.
6. Артеменко В.Б. Дистанційні технології та курси: створення і використання в освітній діяльності : монографія / В.Б. Артеменко, Л.В. Ноздріна, О.Б. Зачко; [за заг. ред. В.Б. Артеменка]. – Львів : Вид-во ЛКА, 2008. – 297 с.

# ПОРІВНЯННЯ МЕРЕЖЕВИХ СИМУЛЯТОРІВ OPNET І NS-2

*Анатолій Балик*

Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

**Summary. Network simulator – is a software that predicts the behavior of a computer network. In this research we will review the following network simulators: Ns-2, Opnet. And review their possibilities, structure, advantages and disadvantages. The goal of this article is to help scientists to make their choice of network simulator.**

**Keywords: OPNET, NS-2, NS-3, network simulator.**

**Вступ.** У зв'язку з повсюдним поширенням інтернету з плином часу розмір і складність мереж значно зростає. Це відбувається у зв'язку зі значним збільшенням числа додатків, які вимагають високої пропускної здатності мереж, таких як VoIP і потокове відео, також для виконання вимог підвищення безпеки [1]. Однією з головних проблем, які пов'язані зі структурою мереж, є можливість передбачити, як вплинуть зміни в структурі на функціонування мереж. Для вирішення цієї проблеми було розроблено ряд інструментів. Було б ідеально, якщо б існував практичний метод відтворення структури мережі, оскільки це давало б найточніші результати. На жаль, через кількість обладнання і, отже, витрати, пов'язані з цим, це не практично. Тому такі інструменти, як мережеві симулятори, часто використовують у дослідженнях. У цих тезах ми проаналізували кілька мережевих симуляторів: Opnet і NS-2. У секції 3 подано інформацію, що стосується порівнянь у роботі мережевих симуляторів, яку здійснено у ряді наукових праць. У кінці тез зроблено висновки.

**1.OPNET**

OPNET (Optimized Network Engineering Tool) є комплексним та багатофункціональним інструментом для симуляції, призначений для побудови, моделювання та оцінювання зв'язків, проектування мережі (топологій з конкретними пристроями), конфігурації мережевих вузлів, передачі пакетів через мережу, і використання усіх мережевих протоколів. У жовтні 2012 року OPNET став частиною Riverbed. Він був розроблений Массачусетським технологічним інститутом (MIT). OPNET є комерційним продуктом, але освітні ліцензії знаходяться у вільному доступі за умови, що результати дослідницької роботи повертаються розробникам. OPNET складається з чотирьох різних редакторів:

1) редактор мережі: інструмент для проектування топології мереж;
2) редактор вузлів: інструмент для встановлення параметрів потоків даних;
3) редактор процесів: інструмент для опису логічних потоків і поведінки;
4) редактор параметрів: дозволяє встановити параметри, такі як формат пакетів, функції ймовірності тощо, які використовуються у вузлі модулів та вузлі процесів як вхідні параметри.

OPNET має графічне середовище для проектування топології мережі, що дає можливість імітувати реальну мережу, ефективно збирати дані про мережу та зручно відображати результати. Програмне забезпечення OPNET може перевіряти і ефективно обробляти різні методи вторгнення (атак). Це програмне забезпечення було використано у багатьох науково-дослідних роботах, його результати вважаються достатньо точними та надійними.

**2.Ns-2**

Ns-2 – це програмне забезпечення з відкритим вихідним кодом Симулятор розроблений у Каліфорнійському університеті в Берклі. Він доступний на платформах UNIX, Free BSD і ОС Windows. NS-2 зараз є частиною проекту VINT (Virtual Inter-Network Test bed). Ns-2 призначений для імітації невеликих мереж і базується на трьох

мовах: TCL для сценаріїв моделювання, OTCL визначає параметри симуляції, C ++ для реалізації планувальників задач. NS-2 дозволяє отримувати результати досліджень у таких форматах: trace файли загального формату, trace файли NAM формату, персоналізовані trace файли. Превагами NS-2 є те, що сценарії симуляцій можуть бути легко виконані, результати отримуються швидко, підтримка багатьох платформ і протоколів.

Основним недоліком є те, що буває достатньо складно змоделювати сучасну мережу в реальному часі, також є проблеми з масштабованістю. Ns-2 є одним з найпопулярніших симуляторів, які використовуються в наукових роботах. Однак розвиток Ns-2 зупинився і на даний час переважна більшість дослідників використовує новішу версію Ns-3. У Ns-3 реалізовано більш розвинену підтримку IP мереж у порівнянні з Ns-2. Наприклад, Ns-2 не надає повної підтримки IPv4 або IPv6, у Ns-3 вона присутня. Ns-3 також надає можливість більш зручного управління багатьма мережевими інтерфейсами та дозволяє створювати більш реалістичні симуляції реальних комп'ютерів, які використовують sockets-подібну API. Іншою перевагою Ns-3 є те, що він розроблений лише на мові C ++.

**3.Огляд праць з порівняння мережевих симуляторів**

Ранні дослідження реалістичності результатів мережевих симуляторів були проведені Pawlikowski, який наводить огляд публікацій про мережеві симулятори [1]. Lucio дослідив придатність мережевих симуляторів на основі результатів експериментів, здійснених на OPNET modeler і Ns-2 [2]. На додаток було зібрано дані з аналогічної реальної мережі з метою порівняння. В експерименті використовували постійну швидкість передачі в бітах (CBR) і FTP (file transfer protocol) для кожної симуляції на обох симуляторах. Незважаючи на точні результати з CBR трафіком, результати FTP з Ns-2 були недостатньо точними. Це було пов'язано зі спрощеною моделлю, що використовувалася для пересилання пакетів. Проте, було встановлено, що OPNET дав точніші результати після більш точного налаштування параметрів симуляції.

Rathod порівняв 3 мережевих симулятори: Ns-2, OPNET і QualNet та симуляцію в реальній мережі, у результаті було отримано значні відмінності. Причиною цього стало те, що у реальній мережі відбувалося блокування викликів сокету, що було неможливо відтворити за допомогою симуляторів [3].

*Висновки*

У цих тезах ми оглянули ряд наукових праць на тематику порівняння мережевих симуляторів. Описали мережеві симулятори: Ns-2 (Ns -3) та OPNET, які найчастіше зустрічаються у сучасних наукових працях. Обидва симулятори мають широкі можливості та інструментарій та придатні для отримання достатньо точних результатів у моделюванні мереж. На нашу думку, OPNET зручніший у використанні та дозволяє дослідникам швидше освоїти техніку мережевих симуляцій. Ми плануємо продовжити роботу у напрямі моделювання мереж за допомогою мережевих симуляторів, зокрема, здійснити симуляції DDoS атак та технік захисту від них за допомогою симуляторів та у реальних мережах.

## Література


1. Pawlikowski K. On credibility of simulation studies of telecommunication networks / K. Pawlikowski, H.-D.J. Jeong, J.S.R. Lee // IEEE Communications. – 2002. – Vol. 40, № 1. – P. 132-139.
2. Opnet modeler and ns-2 – comparing the accuracy of network simulators for packet-level analysis using a network testbed / G.F. Lucio, M. Paredes-Farrera, E. Jammeh [et al.] // WSEAS Transactions on Computers. – 2003. – Vol. 2, № 3. – P. 700-707.
3. Rathod P. Bridging the gap between the reality and simulations: An Ethernet case Study / P. Rathod, S. Perur, R. Rangarajan // IEEE 9th International Conference on Information Technology (ICIT'06). – Bhubaneswar, Mumbai, India, 2006. – P. 52-55.

## СТАТИСТИЧНЕ ТЕСТУВАННЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

*Кирило Безпалий*

Вінницький національний технічний університет, м. Вінниця, Україна

**In this work is considered the method of statistical evaluation of practical stability cryptographic algorithms.**

На сьогодні одним з кращих пакетів для статистичного тестування криптографічних схем/протоколів є пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite), який був розроблений в 1999 році в рамках проекту AES (Advanced Encryption Standart). Віні включає в себе набір з 15 статистичних тестів, які на сьогодні найкращим чином відповідають висунутим вимогам щодо статистичного тестування криптографічних схем/протоколів.

Слід відзначити, що окрім NIST STS існує ряд інших програмних пакетів призначених для статистичного тестування, але вони зазвичай мають малий набір тестів, не є стандартизованими щодо представлення даних для порівняння та не завжди доступними для використання.

Розглянемо критерії прийняття рішення щодо проходження послідовністю заданого тесту.

На сьогодні для прийняття рішення щодо проходження послідовністю ВЧ чи ПВЧ статистичного тесту використовуються такі три основних підходи.

Нехай, задана двійкова послідовність $S = \{S_1, S_2, ..., S_n\}$, $S_i \in \{0,1\}$ довжиною $n$ біт. Необхідно прийняти рішення, проходить дана послідовність статистичний тест чи ні. Можливі такі підходи до вирішення цієї задачі:

1. Критерій прийняття рішення на основі встановлення порогового рівня. Даний підхід оснований на обчисленні по заданій послідовності $S$ статистики тесту $c(S)$ з її подальшим порівнянням з деяким пороговим значенням $c_n(S)$. За цим критерієм вважається, що двійкова послідовність $S$ не проходить статистичний тест кожен раз, коли статистика тесту $c(S)$ приймає значення менше, ніж порогів рівень $c_n(S)$.

Однак такий підхід не є достатньо надійним. Як показали практичні дослідження, використання такого критерію часто приводить до помилкового рішення.

2. Критерій прийняття рішення на основі заданого довірчого інтервалу. За цим критерієм вважається, що двійкова послідовність $S$ не проходить статистичний тест, якщо значення статистичного тесту $c(S)$ знаходиться поза межами довірчого інтервалу значень статистики, обчисленого для заданого рівня значимості $\alpha$.

Даний критерій є більш надійним в порівнянні з першим. Але необхідно завжди враховувати, що різним рівням значимості будуть відповідати різні довірчі інтервали.

3. Критерій прийняття рішення на основі обчислення для статистики тесту $c(S)$ відповідного значення імовірності $P$. За цим критерієм статистика тесту розглядається, як реалізація випадкової величини, яка підкоряється відомому закону розподілу. Статистика тесту будується так, щоб її більші значення вказували на який-небудь дефект випадковості послідовності. При цьому значення імовірності $P$ є імовірність того, що статистика тесту прийме значення більше, чим те що спостерігається при дослідженні щодо припущення випадковості послідовності. Таким чином малі значення $P$ ($P < 0{,}05$ або $P < 0{,}01$) інтерпретуються як доказ того, що послідовність не випадкова. Таки чином за цим критерієм для фіксованого рівня значимості $\alpha$, двійкова послідовність $S$ не проходить статистичний тест, якщо значення імовірності $P < \alpha$. Значення $\alpha$ рекомендується вибирати з інтервалу $[0{,}001; 0{,}01]$.

Використання даного підходу має додаткові переваги в порівнянні з попередніми, які полягають в тому, що одноразово обчислене значення $P$ може порівнюватись з довільно обраним рівнем значимості $\alpha$ без проведення додаткових обчислень.

В основу найбільш потужних бібліотек тестування ПВЧ, до яких можна віднести пакет DIEHARD, Crypt-SX та пакет NIST STS, покладено саме третій критерій прийняття рішення.

Розглянемо принцип та особливості тестування ПВЧ пакетом NIST STS.

Пакет NIST STS включає в себе 15 статистичних тестів, які розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини, які породжуються ВЧ чи ПВЧ. Всі тести направлені на виявлення різних дефектів випадковості. Основним принципом тестування є перевірка нульової гіпотези $H_0$, яка полягає в тому, що послідовність яка тестується є випадковою. Альтернативною гіпотезою $H_0$ є гіпотеза того, що послідовність яка тестується не випадкова. За результатами застосування кожного з тестів нульова гіпотеза або приймається, або відхиляється. Висновок про те, чи буде задана послідовність випадковою або ні, приймається за сукупності всіх тестів.

Порядок проведення тестування окремої послідовності $S$ виглядає таким чином:

Висувається гіпотеза $H_0$ - припущення того, що двійкова послідовність $S$ є випадковою.

Обчислюється статистика тесту $c(S)$ по послідовності $S$.

Обчислюється значення імовірності $P = f(c(S)), \quad P \in [0,1]$ за допомогою використання спеціальної функції і статистики тесту.

Значення імовірності $P$ порівнюється з рівнем значимості $\alpha$, $\alpha \in [0,001;0,01]$. Якщо $P \geq \alpha$, то гіпотеза $H_0$ приймається. В інакшому випадку приймається альтернативна гіпотеза.

При виконанні 15 тестів, в залежності від вхідних параметрів отримуємо приблизно 189 значень імовірності $P$, які можна розглядати як результат роботи окремих тестів. Нижче приводиться опис всіх тестів з кількістю обчислювань значень імовірностей $P$ в тесті, фізичного змісту статистики тесту і дефекту, на виявлення якого направлений тест

## Література


1. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. – National Institute of Standards and Technology, 2010. – 131 с.
2. Barker E. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) / E. Barker, J. Kelsey., 2007. – 133 с.
3. Good Practice in (Pseudo) Random Number Generation for Bioinformatics Applications [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://www0.cs.ucl.ac.uk/staff/d.jones/GoodPracticeRNG.pdf.
4. Dieharder: A Random Number Test Suite [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://www.phy.duke.edu/~rgb/General/dieharder.php.
5. Security requirements for Cryptographic Modules. FIPS 140-1, 1994.
6. Randomness Testing of the Advanced Encryption Candidate Algorithms, 1999. – (NIST).
7. Statistical test suite Crypt-SX [Електронний ресурс] – Режим доступу до ресурсу: http://www.isrc.qut.edu.au/cryptx.

# МОЖЛИВОСТІ ВЗЛОМУ ТА ЗАХИСТУ В СИСТЕМІ КЕРУВАННЯ БАЗАМИ ДАНИХ MS SQL SERVER

*Олександр Белей*

Львівський інститут ДВНЗ «Університет банківської справи», м. Львів, Україна

**The article deals with information security database and the embodiments of the attack on the MS SQL database. As a result of the attack potential intruder can gain access not only to the stored data in the database, but also full control over the database server.**

**Keywords: database, management system, information, access, authentication, password, command, procedure, accounts, administrator, user**

Сьогодні бази даних є основою будь-якої великої інформаційної системи, що зберігає і обробляє великі масиви даних. Оскільки в базах даних зберігається критична для ведення бізнесу інформація, то першочерговим завданням адміністраторів баз даних є підтримка конфіденційності, цілісності та доступності цих даних.

В системі керування базами даних (СКБД) MS SQL є кілька службових баз даних, що створюються в процесі її установки (master, tempdb, model, msdb, pubs). Найбільш важлива з них - master. Вона забезпечує підтримку основних функцій сервера, в ній зберігаються всі системні налаштування сервера, облікові записи користувачів, ролі, відомості про бази даних і - найважливіше для нас - збережені процедури. Процедура - це набір скомпільованих команд T-SQL, що доступні безпосередньо SQL-сервера. Команди розміщуються в збереженій процедурі і виконуються як одне ціле або підпрограма. Збережені процедури знаходяться на сервері СКБД і використовуються, коли необхідно часто виконувати повторювані в певному порядку запити до сервера MS SQL.

В MS SQL є два варіанти аутентифікації. Перший варіант – аутентифікація засобами Windows, другий - аутентифікація засобами самої СУБД (в тому випадку якщо при установці MS SQL був обраний змішаний режим аутентифікації). У першому варіанті аутентифікація користувача проводиться засобами операційної системи, і вхід здійснюється з використанням облікових даних користувача ОС Windows. Варто відзначити, що при установці MS SQL всім користувачам операційної системи, що входять до групи "Адміністратори", автоматично призначається роль "Адміністратор бази даних". У другому випадку аутентифікацію проводить СКБД, використовуючи власну базу облікових записів користувачів. При установці MS SQL стандартно створюється обліковий запис "sa" з роллю "Адміністратор бази даних".

Розглянемо можливий сценарій атаки на сервер з встановленим MS SQL Server 2005. Потенційному порушнику необхідно отримати доступ до MS SQL з роллю "Адміністратор бази даних", а це може легко статися якщо: пароль облікового запису "sa" порожній або може бути легко підібраний; неправильно призначені ролі користувачів в самій СКБД; пароль деякого облікового запису, що входить до групи "Адміністратори" може бути легко підібраний або визначений.

Потім потенційний порушник може запустити розширену збережену процедуру xp_cmdshell, вказавши їй як параметр команду операційної системи, яка створює користувача і включає його в групу "Адміністратори", щоб отримати повний доступ до сервера, на якому встановлена СКБД. Для цього необхідно запустити SQL Server Enterprise Manager, що входить до складу MS SQL Server. Далі в Enterprise Manager потрібно створити нове підключенню до SQL-сервера, і, після встановлення зв'язку зі сервером, створити нове представлення (view) для бази даних master (рис. 1).

У вікні, яке призначене для вводу SQL-запитів, можна ввести і виконати команди для створення нового користувача операційної системи з правами адміністратора:

- EXEC xp_cmdshell “net user test_user test_password / add” - викликає збережену процедуру xp_cmdshell і передає її як параметр команди операційної системи, що створює в системі нового користувача test_user з паролем test_password;

- EXEC xp_cmdshell “net localgroup Administrators test_user / add” - дана команда додає користувача test_user в локальну групу "Адміністратори".

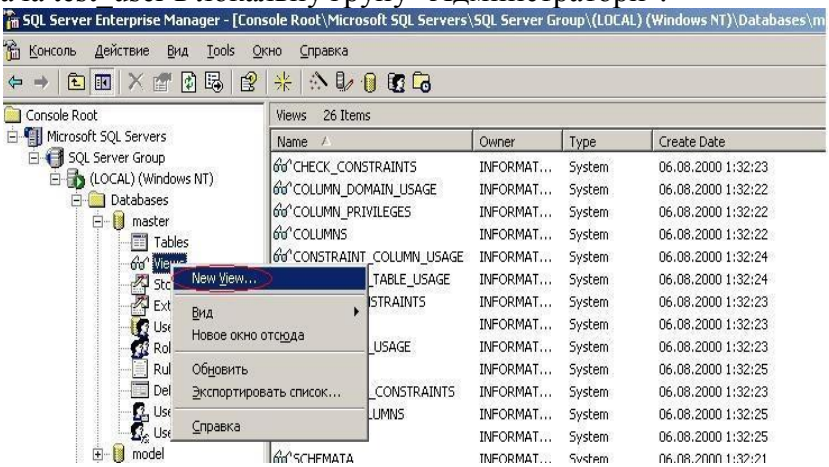



Рис.1. Створення нового представлення

На рисунках 1 і 2 нами показано основні етапи здійснення атаки з використанням стандартних засобів ОС Windows і СКБД MS SQL. Якщо сервер, на якому встановлена СУБД MS SQL, виконує також і інші функції (контролер домену, послуги корпоративної пошти, зберігання архіву документів), потенційний збиток від проникнення на даний сервер за допомогою атаки на MS SQL істотно збільшується.

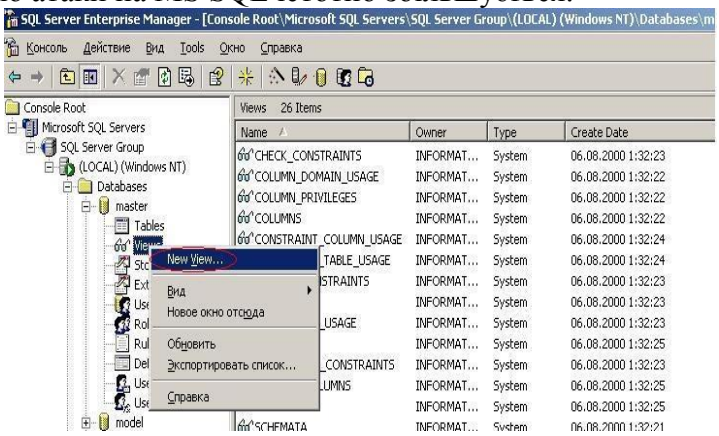



Рис. 2. Виклик розширеної збереженої процедури "xp_cmdshell"

Для усунення описаної уразливості і зниження ризику від проникнення порушника на сервер з встановленою СКБД MS SQL ми рекомендуємо: чітко розмежувати виробниче і тестове середовище; виключити можливість суміщення різних мережевих сервісів на сервері зі встановленою СКБД MS SQL; використовувати складні паролі для адміністративних облікових записів як операційної системи, так і СКБД; видалити з користувачів MS SQL групу "Адміністратори" операційної системи і чітко прописати, які облікові записи операційної системи мають доступ до баз даних; уникати надання доступу до розширених збережених процедур для користувачів СКБД; використовувати привілейовані облікові записи СКБД тільки для виконання адміністративних завдань; запускати процес MS SQL Server з правами облікового запису непривелейованого користувача; протоколювати системні події MS SQL Server, що дозволить спростити процес стеження за діями потенційного порушника; обмежити за допомогою брандмауера доступ до портів MS SQL для користувачів, які не використовують цей сервіс.

## Література

1. М. Каба. MySQL и Perl – СПб.: Питер, 2001.
2. Бен Форта SQL за 10 минут – М: Вильямс, 2015.

# ЗАСТОСУВАННЯ ДОДАТКОВОГО ЗАШУМЛЕННЯ В АЛГОРИТМІ RSA ДЛЯ ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ

*Юрій Борзов, Ігор Малець*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**An RSA algorithm modification with bit operations and adding an extra noise operator to remove borderlines on encrypted images, and decrease of calculating power while encryption and decryption of images is proposed.**

Розвиток інформаційних систем призвів до значного зростання об'ємів інформації, яка передається телекомунікаційними каналами. Нерідко основним інформаційним пакетом в телекомунікаційних сеансах виступають цифрові зображення. Відповідно виникає проблема захисту інформації від несанкціонованого доступу для забезпечення конфіденційності при передаванні цих зображень комунікаційними каналами.

На даний час одним із основних засобів захисту цифрових зображень в комунікаційних сеансах є використання криптографічних алгоритмів, зокрема асиметричної системи RSA. Алгоритм при застосуванні великих значень ключів шифрування забезпечує високий рівень захисту інформації, що призвело до того, що алгоритм RSA практично є промисловим стандартом. Однак використання таких ключів ставить додаткові вимоги до розрядності операційного середовища, оскільки в процедурах шифрування/дешифрування виникає необхідність оперувати великими простими числами.

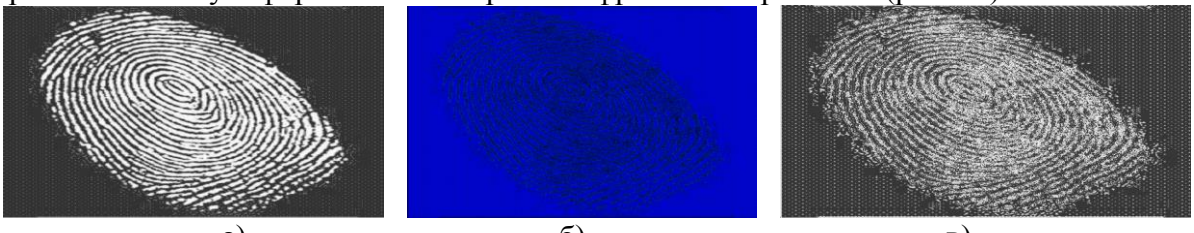
Для шифрування-дешифрування цифрових зображень алгоритмом RSA виникає проблема збереження контурів (флуктуації функції інтенсивності) на зашифрованому зображенні, що несе в собі додаткову інформативність.

Однією з важливих характеристик зображення є наявність у зображенні контурів об'єктів. Контури – це ті області зображення, де виникають різкі зміни інтенсивності[1].

Математично ідеальний контур – це розрив просторової функції інтенсивності в площині зображення. Тому задача виділення контурів об'єкта на зображенні полягає у визначенні різких змін інтенсивності. Застосування алгоритму RSA при шифруванні зображень призводить до стрибків значення інтенсивності, оскільки шифрування відбувається шляхом піднесення до степеня за модулем деякого натурального числа.

Для мінімізації часових витрат при використанні алгоритму RSA намагаються число *e* (відкрита експонента) вибирати невеликим, що значно зменшує обчислювальні витрати та забезпечує не вихід за межі розрядної сітки, що надає можливості використовувати мобільні пристрої з невеликим обчислювальним ресурсом.

Проблема використання алгоритму RSA для захисту зображень полягає у тому, що при малих значення числа *e* на зашифрованому зображенні зберігаються контури об'єкта (рис.1.б). Застосовуючи методи цифрової обробки зображення, можна отримати практично повну інформативність про зашифроване зображення (рис.1.в).



а) б) в)

Рис. 1. Приклад застосування матричного оператора Собеля:
а – початкове зображення; б – зашифроване зображення; б – реконструйоване зображення

Для вирішення даної проблеми пропонується використання побітових операцій в алгоритмі RSA з додатковим зашумленням в програмній реалізації [2].

Алгоритмічно шифрування за одним рядком матриці напівтонового зображення з привнесенням додаткового зашумлення можна представити так:

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне $d$, що виконується конгруенція

$$ed \equiv 1(\text{mod } \varphi(N)). \quad (1)$$

2. Будується число $A$

$$A = (e << k) + (d << l) + (e << l) + (d << k), \quad (2)$$

де $k < 16$ , $l < 16$ – натуральні числа, $k \neq l$, << – операція логічного зсуву вліво.

3. В кожному рядку виконується логічний зсув вліво значення інтенсивності $i$-го пікселa, $i = 1, 2, \ldots, m$, $m$ – число елементів у рядку, за наступним правилом: виконується логічний зсув вліво значення інтенсивності пікселa на величину $i \bmod n$, $n<16$.

$$c_{i,j} = c_{i,j} << i \bmod n, \quad n < 16. \quad (3)$$

4. Будується число $B$ відніманням від отриманого значення інтенсивності пікселa числа $(A + e)$.

5. Закодованим значенням інтенсивності $i$-го пікселa, $i = 1, 2, \ldots, m$, $m$ – число елементів у рядку, вибирається число

$$C \equiv \mathrm{B}^{\mathrm{e}} (\text{mod } N) + f(i^2) . \quad (4)$$

Дешифрування проводиться в порядку, протилежному до шифрування після отримання числа

$$(C - f(i^2))^d \equiv (B^e)^d (\text{mod } N), \quad (5)$$

виконанням протилежних операції до змісту пунктів 4) – 1).

На рис. 2 наведено результати шифрування напівтонового однобайтового зображення розміром 667 х 332 пікселів. На зашифрованому зображенні контури не спостерігаються, причому відбувається гармонізація зашифрованого зображення, що може слугувати додатковим елементом захисту

Рис. 1. Вихідне зображення

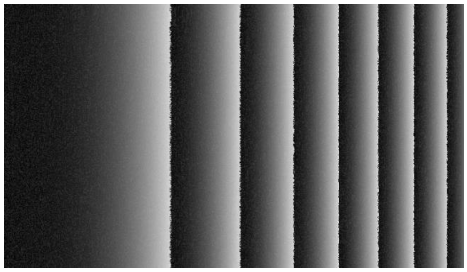


Рис. 2. Зашифроване зображення

Використання оператора зашумлення в сумісному використанні побітових операцій та алгоритму RSA дозволяє понизити мінімальні значення простих чисел, які використовуються в алгоритмі і при яких контури об’єктів на зашифрованому зображенні відсутні, що може бути використане при створенні стійких методів інформаційного захисту зображень.

## Література


1. Сойфер В. А. Компьютерная обработка изображений, Ч. 1 / В. А. Сойфер // Соровский образовательный журнал. – 1996. – № 2. – с. 118-124.
2. Ковальчук А. Використання побітових операцій і додаткового зашумлення в алгоритмі RSA при шифруванні-дешифруванні зображень / А.Ковальчук, Д. Пелешко, Ю. Борзов// Вісник НУ ЛП “Комп’ютерні науки та інформаційні технології”.– 2012.– №744.– С. 132–136.

## НАЛАШТУВАННЯ ЗАХИЩЕНОГО ПОШТОВОГО СЕРВЕРА

*Тарас Брич, Богдан Сухомлінов*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**This work present importance of adding security layers into emailing systems and shows those systems from different points of view: for end-users, system administrators and for hackers. It consists with short introduce of how emailing works in general, ways to configure simple, but secured multiuser mailing server and how to reduce and block inner and outer spam.**

У даній роботі запропоновано необхідні засоби захисту електронної кореспонденції на всіх етапах її обробки – формування, надсилання, отримання та зберігання листів на поштових серверах. Розглянуто також такий аспект ефективного ведення електронного листування як зменшення вхідного, і, що важливіше, вихідного спаму – небажаних листів, що містять рекламу, посилання на ресурси зловмисників з метою викрадення особистих даних, проведення фінансових махінацій, зараження комп'ютера користувача вірусами, тощо.

Насамперед, потрібно встановити як саме працює система електронного листування. Головна ідея системи електронного листування полягає в забезпеченні успішного доставлення повідомлення незважаючи на зовнішні фактори (відмова маршрутизації, недоступність поштового сервера, тощо). Якщо сильно узагальнити, дана система поділяється на програми-клієнта (MUA), що створює, та читає листи, поштового сервера (MTA), що далі листи зберігає, отримує та надсилає, та інших поштових серверів, що беруть участь у пересиланні листів (MX).

MTA Поштовий сервер, сервер електронної пошти – це серверна програма, яка передає повідомлення від одного комп'ютера до іншого. Найпоширеніші: Exim, Postfix.

MX Сервер що отримує, та пересилає повідомлення. Потрібний для швидкої маршрутизації, а також використовується в якості буферу, де зберігаються та повторно надсилаються повідомлення при недоступності потрібного MTA.

MUA Поштовий клієнт, клієнт електронної пошти – комп'ютерна програма, яка встановлюється на комп'ютері користувача і призначена для одержання, написання, відправлення та зберігання повідомлень електронної пошти одного або декількох користувачів (у випадку, наприклад, кількох облікових записів на одному комп'ютері) або декількох облікових записів одного користувача.

Загальна схема "життя" листа виглядає наступним чином.

Користувач, використовуючи поштовий клієнт (MUA) створює та надсилає листа. MUA з'єднується з поштовим сервером (MTA), та здійснює запит на виконання двох операцій – надіслати листа отримувачу, а також зберегти цього листа в каталозі "Надіслані". MTA визначає адресу поштового сервера отримувача, та здійснює спробу надіслати листа. Якщо операція успішна, лист передається отримувачу. Якщо операція надсилання зазнала невдачі – лист передається на резервні поштові сервери (MX). Після чого отримувач може відкрити листа за допомогою свого MUA.

Всі операції надсилання та отримання листів відбуваються по протоколу SMTP. Протокол – це спосіб, за яким різні за своїм призначенням програми взаємодіють одна з одною (зазвичай через глобальну мережу Інтернет).

Всі операції пов'язані з доступом користувача до листів на поштовому сервері відбуваються за протоколами POP3 та IMAP. Протокол POP3 вважається застарілим і не рекомендується до використання, хоча й підтримується більшістю MTA та MUA.

Захист електронних листів відбувається по різному на різних етапах "життя" листа. Найперше безпечне зберігання листів на сервері забезпечується засобами операційної системи; політик безпеки сервера; криптостійкістю паролів (користувачів, адміністраторів, баз даних); коректним чином налаштованого фаєрволу – програми, що

блокує доступ до сервера “ззовні”; при потребі – антивірусом; програмами анти-брутфорсу (Fail2ban) – тобто програмами що унеможливлюють злам паролів користувачів через їх перебір; стійкістю до ddos – тобто здатністю сервера протидіяти атаками типу “відмова в обслуговувані”, коли зловмисними навмисне генерують трафік імітуючи величезний потік користувачів на сервер.

На рівні надсилання та отримання листів, захист здійснюється засобами MTA. Сюди входить коректне налаштування конфігурації програми поштового сервера; введення в дію необхідних правил фільтрації листів, правил надсилання та пересилання, правил отримання і допущення листів на сервер; захист бази даних користувачів, їх паролів, рівнів доступу, тощо. Додатково, до MTA встановлюють антивірусне програмне забезпечення (Clamav), а також спам-фільтри (SpamAssassin).

На рівні пересилання листів захист відбувається за допомогою системи DNS.

До́менна систе́ма іме́н (англ. Domain Name System, DNS) – ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу.

На даному етапі здійснюється перевірка одразу двох речей. По-перше , перевірка чи дійсно сервер-адресат є насправді тим сервером що потрібно. Використовується MX та PTR (зворотня зона) записи – записи що однозначно ідентифікують поштовий сервер як легітимний. По-друге, записи SPF – достовірність адресанта. Таким чином унеможливлюється перехоплення листів, надсилання їх на сервери зловмисників, чи надсилання листів з таких серверів з підміною адреси відправлення.

Також, варто розглянути рівень користувача – а саме налаштування поштового клієнта та загальні правила безпечного користування поштою.

Нарешті, для всебічного і повного осмислення захисту поштової кореспонденції потрібно провести пентести – тести на проникнення. Іншими словами, спробувати здійснити зловмисні дії, використовуючи весь доступний зловмисникам функціонал. Атака на паролі користувачів, атака на достовірність даних, атака на “відмову в обслуговуванні”, зараження комп’ютера користувача вірусом для подальшого надсилання з даного комп’ютера спам-повідомлень, проведення масованих розсилок спаму – це лиш невелика частина можливих векторів проведення атак збоку зловмисників.

## Література


1. https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%B8%D1%81%D1%8C_MX
2. https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BF%D0%BE%D1%88%D1%82%D0%B0
3. https://uk.wikipedia.org/wiki/IMAP
4. https://uk.wikipedia.org/wiki/POP3
5. https://ru.wikipedia.org/wiki/SMTP
6. https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BA%D0%BB%D1%96%D1%94%D0%BD%D1%82
7. https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80
8. https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%B8%D1%81%D1%8C_MX
9. https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%96%D0%BC%D0%B5%D0%BD
10. https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%B8%D1%81%D1%8C_MX
11. https://ru.wikipedia.org/wiki/PTR
12. https://support.google.com/a/answer/33786?hl=ru
13. https://support.google.com/a/answer/173535
14. https://ru.wikipedia.org/wiki/DomainKeys_Identified_Mail
15. https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D1%8B%D0%B9_%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D1%81_DNS

# СЕЛФІМАНІЯ, КІБЕРБУЛІНГ, ШАРЕНТІНГ:НОВІ ВИКЛИКИ КІБЕРПРОСТОРУ

*Олег Вацлавик*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The problem of cyber bullying, selfiemania and sharenting as a threat to the personal security of little considered in the scientific literature. But it studied due to its urgency. The most frequent users of the Internet space are becoming teens. That can lead to negative consequences, since they are the most vulnerable from the psychological point of view. One of the main problems is the lack of security in the network against such cyberattacks. Cyber bullying is a threat to personal security in view of the fact that the aggressor ignores all the rules of propriety and may even degrade the victim in a virtual space. The process of cyber bullying little studied, so that you can give tips to protect your personal information from identity theft.**

**Keywords: security, cyberbulling, aggression, self-defense, information.**

Повсюдне і швидке поширення Інтернету не тільки дає сучасній людині найширші можливості роботи з інформацією, але й ставить перед нею нові завдання, несе в собі незнайомі загрози і небезпеки. Не звертаючи уваги на це, ми опиняємося втягнутими в масовий кіберповедінчастий флешмоб. Схильність до зайвої відкритості в кіберпросторі набуває абсолютно химерних форм: одні користувачі популярних фотосервісів фіксують кожен момент свого життя і публікують сотні однотипних фотографій, інші - із захватом стежать за цим. Як наслідок, самооцінка визначається кількістю «лайків», а життя підпорядковується конкурентній боротьбі і спробам бути завжди в тренді. Сучасні ризики інтернет-користування виводять на перший план такі феномени як кіберексбіціонізм і кібервуайерізм.

Все більшого поширення в мережі отримують сьогодні такі явища як селфіманія, кібербулінг і шарентінг.

Селфіманія - патологічне прагнення до фотографування себе і викладання фото в соціальні мережі. Американські психіатри зараховують селфіманію до психічних розладів обсесивно-компульсивного ряду, для яких характерне нав'язливе бажання здійснювати ті чи інші дії. Разом з тим, виявляються риси істероїдного психотичного розладу, що виражаються в постійному прагненні до визнання з боку оточуючих і діяльності, що дозволяє перебувати в центрі уваги; надмірної стурбованості фізичною привабливістю (МКХ-10). Незважаючи на епідемію Селфі, яка захоплює соціальні мережі Інтернету, вітчизняні фахівці поки не схильні розглядати це явище з точки зору патології.

Кібербулінг складається з англійського слова bullying ( від bully - забіяка, задирака, грубіян, ґвалтівник ) і cyber (приставка, яка зв’язана з комп'ютерними та цифровими технологіями, особливо, з всесвітньою глобальною мережею Інтернет та т.п. ). Це схоже на хуліганство і переслідування в Мережі з використанням повідомлень, зображень, аудіо- та відеофайлів образливого характеру, з метою наклепу, залякування чи погрози. Як і в повсякденному житті, ініціаторами Кібербулінгу зазвичай стають невпевнені в собі, закомплексовані люди , які не можуть самоствердитися ніяким іншим способом, окрім як уявної переваги над більш слабким суперником. Надзвичайно важливо приділяти увагу кіберсоціалізації підростаючого покоління, оскільки найбільшого поширення набуло саме у підлітковому середовищі.

Oversharenting або просто sharenting - це нова тенденція, широко поширена на Заході, яка отримує розвиток у нашій країні. Вперше цей термін був застосований Steven Leckart в статті The Wall Street Journal "The Facebook-Free Baby", де описується тяга батьків до надмірного розміщення в соціальних мережах фотографій своїх дітей. При

цьому автор додає, що є велика різниця між розміщенням фотографії вашої дитини, яка щойно навчилась повзати чи сидіти, і тенденцією демонстрування фото кожного моменту дитячого життя, включаючи брудні підгузки та інші не найестетичніші подробиці. Таким чином, батьки не визнають за дитиною право на особистий простір і не замислюються про наслідки такої відкритості. Дотримуючись принципів моралі та етикету, ми розглядаємо вищезгадані явища як вкрай негативні форми задоволення, на перший погляд, нейтральних потреб (у визнанні, самопізнанні, самоствердженні і т.п. ), які спровоковані низькою культурою поведінки в кіберпросторі. Розглядаючи кіберсоціалізацію людини як «процес якісних змін структури самосвідомості особистості і мотиваційної сфери індивідуума, що відбувається під впливом і в результаті використання людиною сучасних інформаційно-комунікаційних, комп'ютерних, електронних, цифрових, мультимедіа та інтернет-технологій в контексті засвоєння і відтворення їм культури в рамках персональної життєдіяльності» (Плешаков В.А.), ми заявляємо про необхідність якісного інформаційно-консультаційного супроводу користувачів кіберпростору різного віку, для досягнення цілей безпечної, успішної і мобільної кіберсоціалізації.

Кібербулінг та селфіманію можна розглядати як явище свідоме і несвідоме.

Несвідоме найчастіше відбувається в стані афекту або великої кількості емоцій. В основному воно відбувається, коли об'єкт чи суб'єкт міняються ролями. Це можна розглядати як захисну реакцію агресивного і негативного впливу на людей. Такі атаки раптові і завдають більшої психологічної шкоди, викликають зниження самооцінки, появу внутрішньої агресії, замкнутості й інші серйозні проблеми, що особливо небезпечні для дітей і підлітків. Анонімність кібербулінгу дозволяє їм почувати себе захищеними, вони можуть використовувати фото і відеоматеріали, фрагменти особистих листувань, тобто все те,що максимально зачіпає і принижує жертву. Безперервне селфі можна трактувати як відхід від роботи над собою - в лінь, пересичені розваги, даремне дозвілля. Невміння себе зайняти, відсутність інтересу до навколишнього світу, концентрація тільки на задоволеннях і бажанні бути крутим, ні до чого доброго не приводять. Вихід з «селфіманії» - це свідоме життя з розумним співвідношенням праці і відпочинку.

Інформаційно-комунікативні технології змінили світ та безумовно мають вплив на людську психологію. Тому дуже важливо, щоб батьки, вихователі, вчителі, держава об'єднались проти кібер-атак, які знищують особистість, змінюють світогляд. Кожен на своєму рівні повинен приділяти увагу збереженню моралі і духовності суспільства.

## Література


1. Анохин С.М., Анохина Н.Ф. КИБЕРБУЛЛИНГ УЧИТЕЛЯ: ПОСТАНОВКА ПРОБЛЕМЫ // Современные проблемы науки и образования. – 2014. – № 6.;
2. Кон, И.С. Что такое кибербуллинг и как с ним бороться? / И.С. Кон // Семья и школа. – 2006. – № 11. – 15 с.
3. Бочавер А.А., Хломов К.Д. Кибербуллинг: травля в пространстве современных технологий // журнал Высшей школы экономики. – 2014. - № 3. – С. 177-191
4. .Зинцова А.С. Социальная профилактика кибербуллинга// Вестник Нижегородского ун-та им. Н.И. Лобачевского. – 2014. - № 3. – С. 122-128.
5. Мусихин А.И. Кибербуллинг // Педагогическое образование на Алтае. 2013. № 1.С. 76-83.
6. Черкасенко О.С. Травля в социальных сетях // Наука и Мир. 2015. Т. 2. № 8 (24).С. 107-108.

## ОСНОВНІ БЕЗПЕКОВІ ПРОБЛЕМИ КІБЕРПРОСТОРУ УКРАЇНИ

*Валерія Войтович, Ростислав Гриник*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In this work, the main task is to consider the basic problems of providing Ukraine in cyberspace and propose solutions to improve the security of cyberspace and in our country.**

**Keywords: Cyberspace, information security, cybersecurity.**

На сьогоднішній день в умовах створення глобального інформаційного суспільства, інформаційна безпека країни, не виключенням є і Україна, починає відігравати одну з основних ролей у забезпеченні державної безпеки загалом. Насамперед це відображається у тому, що Україна є європейською державою і не може обминати всі проблеми й небезпеки, створені інформаційним суспільством. І це не дивно, адже інформація є безпосередньо головним елементом кіберпростору, а саме того віртуального простору, де кожен з нас, що найменше, є учасником, щодня.

У даній роботі розглядаються основні проблеми захисту кіберпростору. Поява кіберпростору призвела до значимих змін у суспільстві, функціонуванні держави, принципах роботи економіки, а також в соціальних взаємозв'язках. Більшість науковців, як вітчизняних так і закордонних, вважають, що кіберпростір – це середовище, що взаємодіє з комп'ютерною технікою, зокрема, мережею та системами, у рамках яких створюються, відбуваються, змінюються та припиняються правові відносини. Однією з основних джерел загроз інформаційній безпеці України можна вважати соціальні мережі, які можуть використовуватись окремими країнами, організаціями чи особами для пропаганди власних ідей та внесенні деструктивних чинників у соціум. Важливо виділити, що на сьогоднішній час існує велика кількість ускладнень, що перешкоджає формуванню належного захисту кіберпростору, до них можна віднести:

- Відсутність державного і приватного сектору стандартів кібернетичної безпеки на основі визнаних міжнародних стандартів;
- Відсутні системні міжнародні нормативно-правові документи, які точно давали б визначення кіберпростору та всім елементам та чинникам котрі впливають на безпеку кіберсередовища;
- Розвиток новітніх інформаційних технологій на низькому рівні, особливо зазначимо, що розвиток виробництва конкурентоспроможного національно-інформаційного продукту, а саме сьогоднішніх засобів й систем захисту інформаційних ресурсів;
- Рівень фінансового забезпечення державних структур наразі обмежений, адже саме ці системи функціонують в управлінні державою, забезпечують потреби захисту і безпеки держави.

Розглянувши вище перечисленні проблеми, я пропоную наступні етапи вирішення завдання, щодо забезпечення безпечного кіберпростору України.

В першу чергу, варто розпочати з суттєвого доопрацювання понятійного апарату сфери забезпечення кіберпростору, адже на сьогодні не існує жодних офіційних трактувань даної термінології, що змушує кожну країну самостійно виробляти підходи у цій сфері. Безумовно, потрібно, щоб для законодавства поняття "кіберпростір", "кібератака", "кібербезпека", а також низка інших пов'язаних з ними термінів стали на рівень вивченості і розуміння про що йдеться.

Наступним це є реформування нормативно-правових документів, що мають за основу визначення сучасних загроз кібернетичній безпеці України, а також механізмів реагування на них. Створення рамкового акту, що містить основні юридичні визначення і принципи використання норм права. Це дозволить вирішити саме політичну частину проблеми.

Для України важливим є те, що застосування інформаційних технологій дає можливість підвищити якість підготовки і прийняття важливих рішень влади. Основним завданням розвитку інформаційних технологій в Україні є сприяння кожній людині широкого використання сучасних інформаційно-комунікативних технологій (ІКТ), можливість створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, реалізовуючи свій потенціал, повною мірою підвищувати якість свого життя. Розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів, являється одним з найвагоміших напрямів державної політики. Передбачається розвиток інформаційних технологій, насамперед у тих ділянках, де минулорічні розробки відповідають світовому рівню. Це стосується, зокрема, нейромережних технологій, створення засобів інтелектуалізації широкого призначення.

Наразі в Україні на низькому рівні є фінансове забезпечення державних систем, що взаємодіють працюють у кіберпросторі з різними типами інформації і не тільки. Для підвищення потрібно сприяти розробці інноваційної продукції, що може бути використана для посилення кібернетичної безпеки держави. Також, оптимізація системи підготовки кадрів у сфері кіберпростору для потреб органів системи безпеки та оборони України. Важливим є активна робота державних безпекових інституцій щодо інформування населення про різні загрози кібернетичного характеру. Постійно має бути присутнім підвищення кваліфікації військовослужбовців, державних службовців та працівників, які працюють у даній структурі. Додатком до цього повинна існувати підтримка багатосторонніх навчань з протидії кібератакам на державні ресурси та інформаційний світ нашої держави, а також ініціювання нових навчань у цій інфраструктурі.

**Висновок**. На сьогодні існує ряд основних проблем, через які унеможливлюється створення ефективної системи протистояння загрозам у кіберпросторі. Такими проблемами є: понятійна невизначеність, відсутність правого забезпечення, залежність України від іноземних інноваційних продуктів, складнощі у політичній структурі, економічні негаразди в країні. Створення національної системи кібербезпеки вимагає введення нової системи організації та навчання для інформаційної боротьби, що матимуть деякі органи, у секторах безпеки і оборони України. Необхідно запроваджувати в Україні найліпші здобутки закордонних країн, які є на першому місці з питань кібепростору.

## Література


1. 1. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management. 2. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
2. 2. ISO/IEC TR 18044:2004. Information technology - Security techniques - Information security incident management.
3. 3. ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice.
4. 4. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. - Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р.
5. 5. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах" №2594-IV від 31.05.2006.
6. 6. Указ Президента України “ДОКТРИНА інформаційної безпеки України" № 514/2014 від 6.06.2014.
7. 7. Сташевський З.П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / З.П. Сташевський, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2012. – Вип. 22.10. – С. 79-96.

# ДОСЛІДЖЕННЯ БЕЗПЕКИ ПРОТОКОЛУ ZigBee МЕТОДОМ ПЕРЕВІРКИ МОДЕЛІ

*Степан Войтусік, Олег Горячий*

Національний університет «Львівська політехіка», м. Львів, Україна

**Application of Model Checking method for verifying the accuracy of authentication protocol widely used for program products verification. Method Model Checking, software product implemented SPIN, has used to study security authentication protocol ZigBee, which is part of the cyber-physical systems (CFS). The effectiveness of this method in a case verification of this protocol is discussed.**

**Keywords: Model Checking, ZigBee, cyber-physical systems, SPIN.**

Вибуховий розвиток кібер-фізичних систем (КФС) за останні десятиріччя виявив усі ризики, яким вони піддаються під час експлуатації, та при цьому показав важливість розробки і використання захищених алгоритмів передачі інформації. Захист інформації є складовою частиною безпеки КФС в цілому [1-3]. Під захистом інформації розуміють насамперед забезпечення її цілісності, доступності, конфіденційності, автентичності, неспростовності і надійності. При цьому особливістю каналів передачі інформації, присутніх в КФС, є їх різноманітність. В КФС можуть бути застосовані як швидкі канали передачі великих масивів даних, таких як відео, звук, на великі відстані (інтернет, локальні мережі), так і повільніші канали, що використовуються для передачі невеликих об'ємів даних (WiFi, Bluetooth, ZigBee) на коротші відстані. І у всіх протоколах вбудована автентифікація об'єктів і даних. Тому проблема перевірки безпеки щойно розроблених, чи тих, що вже використовуються, має велике значення. При цьому необхідно відмітити, що в роботах [4,5] авторами було показано неможливість алгоритмічно вирішити задачу верифікації протоколів автентифікації у загальному вигляді. Тому всі методи верифікації, розглянуті в [6,7] безумовно мають обмежені можливості.

Із наведених в [6,7] засобів перевірки протоколів автентифікації ми вибрали **SPIN** (Simple Promela Interpreter), розроблений в дослідницькому центрі **Bell Labs,** насамперед, за його гнучкість, наявність можливості отримання алгоритму атаки та солідну теоретичну базу. На сьогоднішній день це є, мабуть, найбільш популярний open source – ний продукт, що використовує метод *Model Checking* [8-11], і який інтенсивно розвивається та використовується для перевірки програм на наявність у них логічних помилок [11]. В 2001 р. SPIN був нагороджений Міжнародною Асоціацією ACM (Association for Computing Machinery) премією ACM Software System Award.

Даний програмний пакет може використовуватись у двох режимах: як симулятор і як верифікатор. При цьому на вхід програми подається модель досліджуваного алгоритму. Модель будується на мові Promela (Process or Protocol Meta Language), яка дає можливість описати розподілені асинхронні процеси, як систему переходів зі скінченною кількістю станів, яка, в свою чергу, моделює реальний алгоритм, програму чи протокол, що потребує верифікації.

В режимі симуляції SPIN виводить одну конкретну траєкторію виконання програми, яка виникає в результаті роботи протоколу, що моделюється. Але для доведення заданих властивостей моделі цього не достатньо. Для цього використовується інший режим роботи пакету SPIN – верифікація. У режимі верифікації програма намагається знайти помилковий шлях поведінки моделі, так званий контр приклад, який спростовує певну наперед задану її властивість. Для цього програма перебирає всі можливі шляхи некоректної поведінки, які є результатом синхронного добутку моделі переходів системи, що аналізується, і автомата Б'юхі [3].

Для формалізації поведінки досліджуваної системи використовують модель Кріпке, яка складається із множини станів, множини переходів між станами і функції, що помічає

кожен стан набором властивостей, істинних в даному стані [3]. При цьому, звісно, існує проблема трансляції досліджуваної програми в модель, пов'язана із недостатньою/надлишковою деталізацією кроків програми, що у свою чергу може призвести до виключення деяких важливих станів, які існують в системі, або в протилежному випадку - до появи надлишкових станів, які, навпаки, ніколи не будуть проявлятись. Теоретичним базисом пакету SPIN є метод, що базується на використанні темпоральних логік (LTL - лінійна темпоральна логіка і CTL - деревоподібна темпоральна логіка або логіка розгалуженого часу), які специфікують моделі Кріпке.

Результати перевірки алгоритму автентифікації Нідхема – Шредера, для якого вже відома атака Лоу [12], показали ефективність даного пакету. Наведений в [12] приклад, демонструє атаку «людина по середині», знайдену Лоу в 1995 р., тобто через 17 років після його формулювання. Проведені дослідження безпеки протоколу ZigBee програмою SPIN продемонстрували її ефективність у пошуку вразливостей протоколів автентифікації. Враховуючи даний та інші результати перевірки протоколів системою SPIN, її можна рекомендувати для використання при верифікації програмних продуктів, що реалізують існуючі алгоритми автентифікації.

## Література


1. Мельник А.О. Багаторівнева базова платформа кіберфізичних систем. Кіберфізичні системи: досягнення та виклики. Матеріали Першого наукового семінару. 25-26 червня, 2015. Львів. С.5-15.
2. Горбенко І.Д., Горбенко Ю.І. // Прикладна криптологія: Теорія. Практика. Застосування. – Харків: «Форт», 2013. -880 с.
3. Дудикевич В.Б., Максимович В.М., Горпенюк А.Я., Пархуць Л.Т., Микитин Г.В., Мороз Л.В., ВойтусікС.С. // Концепція побудови кіберфізичних систем. Кіберфізичні системи: досягнення та виклики. Матеріали Першого наукового семінару. 25-26 червня, 2015. Львів. С.129-131.
4. Durgin N., Lincoln P., Mitchell J., Scedrov A. Undecidability of bounced security
5. protocols // Proc. of the FLOC'99 Workshop on Formal Methods and Security Protocols
6. (FMSP'99), 1999.
7. Durgin, N., Lincoln, P., Mitchell, J., Scedrov, A.: Multiset rewriting and the complexity of bounded security protocols. Journal of Computer Security 12(2), 247– 311 (2004).
8. Котенко И.В., Резник С.А., Шоров А.В. Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств. // Труды СПИИРАН. 2009. Вып. 8. С.292-310.
9. Лепендин А.А., Уберт А.В. Метод верификации моделей в приложении к анализу протоколов аутентификации. Известия Алтайского государственного университета. // Управление, вычислительная техника и информатика. Выпуск№ 1 (73) / том 2 / 2012. С.84-86.
10. И.В. Шошмина, Ю.Г. Карпов. // Введение в язык Promela и систему комплексной верификации Spin. // БХВ-Петербург, 2009. 66 с.
11. Holzmann G. "Spin Model Checker. The Primer and Reference Manual" Addison-Wesley, 2003, 608 стр.
12. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. Пер. с англ. /Под ред. Смелянского. - М.: МЦНМО, 2002. – 416с.
13. Карпов Ю.Г. Model checking. Верификация параллельных и распределенных программных систем. // БХВ-Петербург, 2009, 520 с.
14. Lowe G. " Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR" Lecture Notes In Computer Science; v. 1055, Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems table of contents, стр. 147 – 166, 1996.
15. Dolev D., Klawe M., Rodeh M. "An O(n log n) Unidirectional Distributed Algorithm for Extrema Finding in a Circle" Journal of Algorithms, 3, стр. 245-260, 1982.
16. Mohsen Pourpouneh, Rasoul Ramezanian. A Short Introduction to Two Approaches in Formal Verification of Security Protocols Model Checking and Theorem Proving. /The ISC Int'l Journal of Information Security. January 2016, Volume 8, Number 1 (pp. 1-22).

# ВИКОРИСТАННЯ ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ ДЛЯ ЗАХИСТУ ЕЛЕКТРОННИХ ВІДОМОСТЕЙ

*Олег Горячий, Степан Войтусік*

Національний університет «Львівська політехніка», м. Львів, Україна

**Research of program-technical complex of Certificate Authority IIT CA-1.3 was conducted in this paper, its features and main components were studied. A scheme of secured https connection between the client and the server using CA was offered, the possibility of practical implementation of this scheme for Lviv Polytechnic National University teacher's site protection was demonstrated. The configuration of the test site was made, programs for the end user and registration administrator were developed using this program-technical complex to organize the scheme in practice.**

**Keywords: Certificate Authority, certificate, private keys, web-server, user, electronic signature, protocol https, protocol LDAP, library, web-service.**

В Україні та в світі високими темпами розвивається електронний документообіг. Завдяки використанню електронного цифрового підпису (ЕЦП) як фізичними, так і юридичними особами у сфері бізнесу чи для взаємодії із державними структурами, наприклад заповнення податкової звітності, підвищується надійність, зручність використання, безпека електронного документообігу, зменшуються фінансові витрати та підвищується швидкість опрацювання документів та проведення будь-яких комерційних операцій. Поруч із використанням ЕЦП часто застосовується і криптографічний захист інформації для забезпечення конфіденційності [1].

У цей же час виникає проблема організації безпечної взаємодії між суб'єктами цієї діяльності (обмін та керування ключами). Ця проблема вирішується залученням довірчої третьої сторони – центру сертифікації ключів (ЦСК), що видає і підписує сертифікати [2]. Сертифікат – це цифровий документ, що підтверджує відповідність між відкритим (публічним ключем) та інформацією, що ідентифікує власника цього ключа. Сертифікати публічних ключів користувачів можуть публікуватись на загальнодоступних ресурсах ЦСК.

Даний механізм можна застосувати крім підписування та направленого шифрування документів, також і для ідентифікації та автентифікації користувачів. Зокрема, існує механізм, що дозволяє організувати захищений зв'язок між веб-сервером та його клієнтами через протокол HTTPS (SSL/TLS) із використанням власних сертифікатів (та приватних ключів) як клієнтів, так і сервера. Кожен учасник взаємодії генерує для себе пару ключів (відкритий та закритий), реєструється як користувач ЦСК та отримує сертифікат власного публічного ключа. Сертифікат, сформований на доменне ім'я сайту, разом із його приватним ключем та кореневим сертифікатом ЦСК імпортується у веб-сервер. Сертифікати клієнтів, їх приватні ключі та кореневий сертифікат ЦСК відповідно інсталюються на робочих станціях, що будуть використовуватись як клієнти веб-сервера. Варто сказати, що доступ до приватних ключів можна додатково захищати паролем. Під час спроби клієнта встановити з'єднання із сервером завдяки процесу, що називається TLS Handshake Protocol, відбувається автентифікація як клієнта, так і сервера, вироблення спільного ключа сесії, що потім використовується для встановлення захищеного тунелю та подальшої передачі між ними лише зашифрованих даних.

Як приклад практичної реалізації даного механізму розглянемо механізм автентифікації користувачів для доступу до сайту електронних відомостей викладачів НУ "Львівська політехніка". На даний момент цей ресурс доступний лише із внутрішньо університетської мережі та використовує парольну автентифікацію користувачів. Викладачі не мають можливості заповнювати чи переглядати електронні відомості, якщо вони не мають доступу до університетської мережі, наприклад із своїх домашніх

комп'ютерів через мережу Інтернет. Застосувавши розглянуту вище схему, можна об'єднати парольну автентифікацію викладачів, перевірку їх персональних сертифікатів та шифрування трафіку між клієнтом та сервером, що підвищить безпеку даного ресурсу в марежі Інтернет. Це питання є досить актуальним із огляду на важливість інформації, що там міститься, та недопустимість її несанкціонованої модифікації.

Розглянемо процес впровадження даного механізму. Для генерації ключів, створення сертифікатів для користувачів, їх обслуговування можна використати наявний на кафедрі Безпеки інформаційних технологій університету програмно-апаратний комплекс ЦСК, розроблений Інститутом інформаційних технологій (ІІТ) [2]. Даний комплекс серед всього іншого містить програму «ІІТ Користувач ЦСК-1.3», що дозволяє користувачам генерувати ключі та працювати із ними (підписувати та шифрувати дані). Ключі генеруються у захищений паролем файл у файловій системі комп'ютера, на з'ємний диск (флешку), або ж навіть у електронний ключ (наприклад, Кристал-1). Адміністратор ЦСК може формувати сертифікати, використовуючи програму «ІІТ ЦСК-1.3. Адміністратор реєстрації». Обидва ці процеси вимагають втручання оператора, вимагають від них певного рівня знань та вмінь роботи із програмою, займають досить великий час, оскільки вимагають від операторів введення та перевірки всіх необхідних параметрів та даних про користувачів. На щастя, в програмно-апаратний комплекс ЦСК входить бібліотека користувача ЦСК «Підпис (ОС Microsoft Windows)» [3], що дозволяє розробляти програми, зокрема на мові C#, що використовують певні функції ПЗ «ІІТ Користувач ЦСК-1.3». Також існує можливість використати у своїй програмі веб-сервіс віддаленого адміністратора реєстрації, що дозволить автоматизувати також процес реєстрації користувачів ЦСК та формування їм сертифікатів.

На рис. 1 зображено запропоновану схему організації захисту сайту електронних відомостей викладачів.

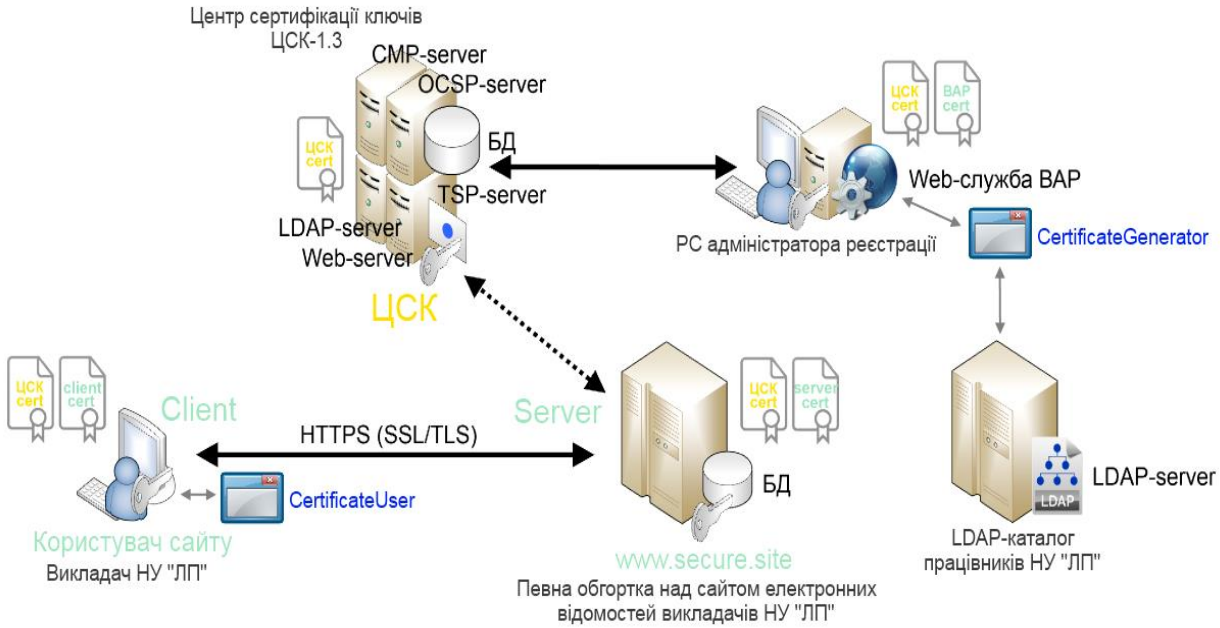



Рис. 1. Запропонована схема захисту сайту електронних відомостей

Отже, для практичної тестової реалізації даної схеми були виконані наступні кроки:

1. Згенеровано пару ключів на сервері та, використовуючи ПЗ ІІТ, сформовано відповідний сертифікат для тестового сайту «www.secure.site». Імпортовано сформований сертифікат у веб-сервер IIS, виконано прив'язку його до сайту та налаштовано використання https протоколу. Імпортовано кореневий сертифікат ЦСК.
2. Із використанням бібліотеки користувача ЦСК розроблено програму «CertificateGenerator» на мові C#, що дозволяє автоматизувати процес генерації ключів та формування сертифікатів для викладачів НУ «ЛП». Дані про викладачів отримуються із LDAP-каталогу університету.
3. Із використанням бібліотеки користувача ЦСК розроблено програму «CertificateUser» на мові C#, що дозволяє зчитувати особистий ключ користувача, змінювати пароль його захисту, автоматизувати процес інсталяції/деінсталяції сертифікатів та приватних ключів у системі для їх подальшого використання.

Виконуваний файл програми «CertificateUser» можна розміщувати на одному носії (флешці) із приватним ключем викладача. Флешка належить викладачу, особистий ключ захищений його паролем. Після того, як сертифікати користувача інстальовані в системі у сховище сертифікатів, їх можна використовувати для ідентифікації та автентифікації користувача з допомогою звичайного браузера. Після завершення роботи програми, сертифікати користувача видаляються із системи. Слід зауважити, що дана програма не прив'язана лише до автентифікації користувача, хоча це її основна особливість, проте її можна в подальшому розширити функціями шифрування та підписування файлів, обміну захищеними повідомленнями тощо.

## Література


1. Горбенко І.Д., Горбенко Ю.І. / Прикладна криптологія: Теорія. Практика. Застосування. – Харків: «Форт», 2013. - 880 с.
2. Горбенко Ю.І., Горбенко І.Д. / Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика.: Монографія. – Харків: «Форт», 2010. - 608 с.
3. Програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК «Підпис (ОС Microsoft Windows)». Опис програми. Настанова програміста. Настанова системного програміста. – Харків: ІІТ, 2013. -175 с.

# КЛАСИФІКАЦІЯ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ЗБРОЇ

*Ростислав Гриник, Богдан Буній*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In recent years have increasingly used such terms like influence information, information warfare, information weapons. This article examined the basic concepts you kind of information classifications of weapons and impact on society as a whole.**

**Keywords: information, warfare, weapons, influence**

У сучасному світі стрімко розвиваються новітні технології. Еволюція технологій прискорюється у геометричній прогресії, а отже стає все важче захистити інформацію і тому її цінність виростає в декілька разів. Недаремно відомий політичний діяч Вінстон Черчіль одного разу сказав: «Хто володіє інформацією, той володіє світом». Цей прогрес зачепив фактично всі сфери розвитку суспільства. Однак у міру впровадження інформаційних технологій у різні сфери суспільного життя виникають серйозні проблеми, пов'язані із забезпеченням справного функціонування елементів інформаційної інфраструктури.

На сьогоднішній день рівень розвитку військової майстерності відрізняється від минулих років все більшим посиленням інформаційного протиборства. Аналізуючи сучасні військово-аналітичні публікації, робимо висновок, що в даний момент засоби інформаційного протиборства розвиваються найбільш стрімко та динамічно.

Оглянувши доступний матеріал, можна дійти до висновку, що інформаційна зброя поділяється на два основних класи:

- інформаційно-психологічна, що впливає на морально-психологічній стан людини;
- інформаційно-технічна зброя, що на інформаційно-технічну інфраструктуру об'єкта;

Під інформаційно-психологічною зброєю слід розуміти сукупність засобів, форм, способів, методів і технологій, що використовуються для латентного (утаємниченого) викривлення інформаційного забезпечення (потоку даних) цивільних та воєнних мас супротивника з метою ураження індивідуальної і масової свідомості [1]. І в кінцевому випадку для подальшого несвідомого для особи контролю над нею. Тобто, не зважаючи на те, що при цьому застосовуються науково-технічні, психологічні, принципи, головною мішенню інформаційно-психологічної зброї виступає людський розум.

Інформаційно-технічна зброя передбачає вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонування (зупинка роботи, несанкціонований доступ до інформації та її перекручування (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини [1].

Інформаційну зброю від відомих нам звичайних засобів ураження відрізняє:

- скритність – можливість досягнення бажаної мети без видимої роботи спецслужб, заворушень чи оголошення війни;
- масштабність – незважаючи на кордони, суверенітет держав чи національність, створюється можливість наносити колосальні збитки та непоправиму шкоду, суспільству чи державі, в деяких випадках навіть без кровопролиття;
- універсальність – можливість неодноразово та в різний спосіб застосовувати методи впливу без застосування як військових, так і цивільних структур країни. А також можливість створення конфліктів в

середині держави для знищення противника з середини, та в успішній поразці противника ще до початку воєнного конфлікту.

Інформаційна зброя з часу свого зародження приймала багато форм, однією з найбільш досконаліших на сьогоднішній час є електромагнітна зброя [2]. Даний вид зброї є одним з найбільш ефективних засобів ведення інформаційного конфлікту, оскільки виведення з ладу інформаційних потоків обумовлено їх високою важливістю для опонента як засобу зв'язку. Масове застосування цієї зброї може порушити функціонування інформаційно-телекомунікаційної інфраструктури цивільних та військових систем життєзабезпечення. У зв'язку з чим вдасться паралізувати практично повністю військові системи управління і життєво важливі системи виробництва супротивника, що значно знизить його боєготовність і ефективність проведення бойових операцій.

Даний аналіз інформаційної зброї свідчить як про надзвичайну небезпечність і різноманітність її видів, так і про небезпечність і різноманітність каналів її впливу – від засобів масової інформації до засобів впливу на свідомість і підсвідомість людей, що вкрай небезпечно у зв'язку з практично повною відсутністю засобів контролю цих процесів. Саме в цьому полягає головна небезпека викликів і загроз у XXI столітті.

## Література


1. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): монографія. – К.: НАОУ, 2003. -320 с.
2. Панарин И.Н., Панарина Л.Г. Информационная война и мир.- М.: ОЛМА-ПРЕСС, 2003.- 384 с.

# ОПТИМАЛЬНІСТЬ НЕ УСІЧЕНОЇ ПОСЛІДОВНОЇ ПРОЦЕДУРИ ВАЛЬДА В ЗАДАЧАХ ПЕРЕВІРКИ ДВОХ ПРОСТИХ ПРОГНОЗІВ НСД В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

*Валерій Дудикевич[1], Іван Опірський[1], Петро Гаранюк[1], Олексій Вавpічен[2]*

1. Національний університет «Львівська політехніка», м. Львів, Україна
2. Національна академія Державної прикордонної служби України ім. Б. Хмельницького, м. Хмельницький, Україна

**The paper is mathematically valid and withdrawn expression that describes sequential rule Wald. As part of the assumptions and research derived the optimal expression of testing two simple prediction, which in turn allows you to further development addressing unauthorized access prediction.**

**Keywords: unauthorized access, state information systems, Wald procedure, forecast, forecasting, optimal sequential rule.**

Прогнозування НСД на інформаційні мережі держави (ІМД) без сумніву повинно ґрунтуватись на вивченні тенденцій, що спостерігаються в зміні її поточного стану під дією НСД. В теорії автоматичного контролю передбачається, що цей стан може бути представлено сукупністю значень деяких контрольних параметрів. Тоді, очевидно, причиною, що викликає зміни стану ІМД, повинні бути зміни значень саме цих параметрів. Таким чином прогнозування НСД в ІМД повинно базуватись на прогнозуванні значень складових контрольних параметрів. Це може здійснюватись на базі математичного апарату екстраполяції процесів, що описує закономірності змін в параметрах. В свою чергу використання апарату екстраполяції потребує певної формалізації процесів змін контрольних параметрів, тобто потребує створення певної математичної моделі процесів вимірювання параметрів ІМД під впливом НСД.

Розглянемо не усічену послідовну перевірку двох альтернативних прогнозів при незалежних, можливо, неоднорідних спостереженнях при дотримані умови $R_n^N(T_n) = \min\left\{R_n^0(T_n), R_{nї}^V(T_n)\right\}, n = \overline{1, N-1},$ для виконання якого в даному випадку достатньо виконати умову $g_{ij}(n)P_i(\tau^0 > n) \to 0, n \to \infty, N \to \infty$, відповідно з теоремою 1 [1] оптимальне не усічене правило може бути отримано з усіченого шляхом граничного переходу $N \to \infty$. Тому оптимальна неусічена процедура має вигляд

$$u_n^0(\Lambda_n) = \begin{cases} 1, \Lambda_n \geq B_n, \\ 0, \Lambda_n \leq A_n, \\ u_ї, \Lambda_n \in (A_n, B_n), n \geq 1, \end{cases} \quad (1)$$

де пороги $A_n$ $B_n$ знаходяться з рівнянь $G_{n0}(\Lambda_n) = G_{nП}(\Lambda_n), G_{n1}(\Lambda_n) = G_{nП}(\Lambda_n),$ в яких $G_{nП}(\Lambda_n) = \lim_{N\to\infty} G^N{}_{nП}(\Lambda_n)$.

Таким чином, при довільній залежності втрат від номера кроку спостереження і неоднаково розподілених спостережень оптимальна не усічена процедура перевірки двох простих прогнозів полягає в порівнянні відношення правдоподібності (ВП) з двома змінними (що залежать від n) порогами.

Припустимо тепер, що спостереження однорідні $(p_{in}(x_n) = p_i(x_n))$, а функція втрат має вигляд

$$g_{ij}(n) = \varphi_{ij} + c_{ij}n, i, j = 0,1, \quad (2)$$

де $c_i$ вартість затримки у винесенні рішення на один крок при $\theta = i; \varphi_{ij}$ – втрати при прийнятті $j$-го рішення в $i$-й ситуації $(\theta = i)$, що не залежить від $n$. Для виконання

умови $\rho^{\mathbf{0}} \equiv \rho(\delta_{\mathbf{0}}) = \lim_{N\to\infty} \rho_N(u_{\mathbf{0}}^N)$, достатньо виконання умови $nP_i(\tau^0 > n) \to 0, n \to \infty, i = 0,1.$ Останні виконуються у випадку кінцевого середнього ризику (СР) $\rho^0 = \rho(\tau^0)$.

Припустимо, що оптимальні пороги не залежать від $n(A_n = A, B_n = B)$. Тоді підставляючи (2) в

$$G_{nj}(\Lambda_n) = \chi\Lambda_n g_{1j}(n) + g_{0j}(n)$$

$$G_{n\ddot{I}}^N(\Lambda_n) = \sum_{\nu=1}^{N-n}\sum_{j=0}^{1}\{\chi\Lambda_n g_{1j}(n+\nu)P_{1j}^{(\nu)}(\Lambda_n, n, N) + g_{0j}(n+\nu)P_{0j}^{(\nu)}(\Lambda_n, n, N)\}, n = \overline{1, N-1};$$

отримаємо:

$$G_{n\ddot{I}}(\Lambda_n) = \tilde{G}_{\ddot{I}}(\Lambda_n) + n(c_0 + c_1\chi\Lambda_n);\ G_{nj}(\Lambda_n) = \tilde{G}_j(\Lambda_n) + n(c_0 + c_1\chi\Lambda_n),$$

де

$$\tilde{G}_j(\Lambda_n) = \chi\Lambda_n\varphi_{1j} + \varphi_{0j}; \qquad (3)$$

$$\tilde{G}_{\ddot{I}}(\Lambda_n) = \sum_{\nu=1}^{\infty}\sum_{j=0}^{1}\ [\ \chi\Lambda_n(\varphi_{1j} + c_1\nu)P_{1j}^{(\nu)}(\Lambda_n) + (\varphi_{0j} + c_0\nu)P_{0j}^{(\nu)}(\Lambda_n)\ ], n = 1,2,...; \qquad (4)$$

$$P_{ij}^{(\nu)}(\Lambda_n) = \int_{\{X_{n+1}^{\ddot{I}}\}} P_{ij}^{(\nu-1)}(\Lambda_{n+1})p_i(x_{n+1})dx_{n+1}, \nu \geq 2;\ P_{ij}^{(1)}(\Lambda_n) = \int_{\{X_{n+1}^{j}\}} p_i(x_{n+1})dx_{n+1}; \qquad (5)$$

$$X_{n+1}^{\ddot{I}} = \{x_{n+1} : \Lambda`(x_{n+1}) \in (A/\Lambda_n, B/\Lambda_n)\};\quad X_{n+1}^{0} = \{x_{n+1} : \Lambda`(x_{n+1}) \leq (A/\Lambda_n)\};$$

$$X_{n+1}^{1} = \{x_{n+1} : \Lambda`(x_{n+1}) \geq B/\Lambda_n\};$$

не залежать $n$. Оптимальні пороги $A$ і $B$ при цьому знаходяться з рівнянь

$$G_j(\Lambda) = \tilde{G}_{\ddot{I}}(\Lambda), j = 0,1, \qquad (6)$$

і дійсно виявляються постійними. Відповідно, при лінійній залежності втрат від номера кроку спостереження і однаково розподілених спостережень оптимальна послідовна процедура, базується на порівнянні ВП з двома постійними порогами. В перше ця процедура була запропонована і досліджена А.Вальдом [2]. Тому в подальшому будемо називати двопорогову послідовну неусічену процедуру

$$u_n^*(\Lambda_n) = \begin{cases} 1,\ \Lambda_n \geq B, \\ 0, \Lambda_n \leq A, \\ u_{\ddot{I}}\ , \Lambda_n \in (A,B), n \geq 1, \end{cases} \qquad (7)$$

процедурою Вальда.

Пороги $A,B$, що входять в (7) залежать від відношень між коефіцієнтами $\varphi_{ij}, c_i, i, j = 0,1,$ апріорної ймовірності $P_1$ і степені різноманітності прогнозів (щільностей $p_1(x), p_0(x)$). Знайдені пороги з рівняння (6) в реальному вигляді представляють собою проблему.

## Література


1. Опірський І.Р. Оптимізація послідовних процесів прийняття рішень при умовно екстремальній постановці задачі/Опірський І.Р.// СНУ ім. В.Даля: Інформаційна безпека. – №4(16), 2014. –С.120-127;
2. Орлов А. И. Теория принятия решений: учебник. — М.: Экзамен, 2006. — 573 с.
3. Siegmund D. Sequential Analysis. Tests and confidence intervals.–N.Y.: Springer veriage, 2005.–270p.

# МІЖНАРОДНИЙ КІБЕРТЕРОРИЗМ І ОСОБЛИВОСТІ ЙОГО ПРОЯВУ

*Олексій Косиєв, Ростислав Гриник*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The current state and development of international cyber especially its manifestation. The key aspects of international cooperation in the fight against cybercrime. The basic problems of international cooperation in this field.**

**Keywords: cyberspace, cybercrime, cyberterrorism, information security**

Визначити поняття «комп'ютерний тероризм» – доволі складне завдання, оскільки нелегко встановити чітку межу для відмінності його від інформаційної війни і інформаційного криміналу. Ще одна складність полягає в тому, що необхідно виділити специфіку саме цієї форми тероризму. Саме поняття «кібертероризм» утворено злиттям двох слів: «кібер» («кіберпростір») і «тероризм». Виходячи з основного поняття тероризму і поєднання його з віртуальним простором, можна зробити висновок, що кібертероризм – це комплексне поняття, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту.

Одним із способів кібертероризму є політично мотивована атака на інформацію. Вона полягає в безпосередньому управлінні соціумом за допомогою превентивного залякування. Це проявляється в загрозі насильства, підтримці стану постійного страху з метою досягнення певних політичних чи інших цілей, примусі до певних дій, залученні уваги до особистості кібертерориста або терористичної організації, яку він представляє.

Ряд країн, таких як США, Великобританія, Канада, Австралія та інші використовують глобальну систему радіоелектронної розвідки «Ешелон», яка використовується і для попередження проявів міжнародного тероризму [1]. Але незважаючи на «ешелонування», терористи можуть скоординувати свою діяльність і вдало провести акт тероризму. Цьому може бути кілька пояснень:

- терористи використовували для взаємодії неелектронні засоби телекомунікацій;
- терористи маскували свої повідомлення за допомогою криптографічних або стенографічних методів;
- алгоритм, закладений в систему «Ешелон», неефективний, або ця система попередньо була виведена з ладу.

Терористи підтримують свою діяльність іншими злочинами, вчиненими через Інтернет, наприклад, отримують доступ до баз кредитних карт або здійснюють різні форми прибуткового шахрайства. Інформаційні технології також полегшують безліч дій терористів і міжнародних злочинних груп – від фінансування до створення необхідних документів. За допомогою комп'ютерних технологій організовані злочинні групи здатні створити підроблені документи, що засвідчують особу, документи, що свідчать про ведення будь-якої діяльності, яка є прикриттям для їх операцій. Використання інформаційних технологій злочинцями і терористами відбувалося одночасно із зростанням їх легального використання міжнародною спільнотою. Можливість швидкого впровадження нових технологій в терористичні і злочинні організації обумовлюється і тим, що сучасні злочинні організації існують у вигляді мереж, із осередками діяльності. Вони мають кваліфікованих технічних фахівців в своїх структурах або наймають їх ззовні.

Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові

інформаційної інфраструктури, що здійснюються угрупованнями або окремими особами [2]. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати мережевий інформаційний обмін, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності.

Проведення кібератак забезпечує високу ступінь анонімності і вимагає більшого часу реагування. Вироблення методів антитерористичної боротьби лежить перш за все в області протидії звичайному тероризму [3]. Здійснення атаки через інформаційні системи взагалі може виявитися не розпізнаною як акт тероризму, а буде сприйнято, наприклад, як випадковий збій системи. Таким чином, загроза кібертероризму в даний час є дуже серйозною проблемою. Актуальність цього питання буде зростати в міру розвитку і поширення інформаційно-телекомунікаційних технологій. Немає спільної думки з приводу визначення об'єкта актів тероризму. Причому думка коливається від міждержавної спрямованості, коли об'єктом стають не тільки окремі міжнародні організації, а й цілі держави, народи, конкретні особи (політичний або державний діяч) або випадкові люди. Дії кібертерористів можуть бути спрямовані як на цивільні, так і військові об'єкти. На думку американських експертів, найбільш уразливими точками інфраструктури є енергетика, телекомунікації, авіаційні диспетчерські, фінансові електронні та урядові інформаційні системи, а також автоматизовані системи управління військами і зброєю[1].

Загроза кібертероризму вже не перший рік широко обговорюється в сучасному суспільстві на різних рівнях, породжуючи безліч суперечок, міфів і спекуляцій. Неадекватна оцінка ризиків, пов'язаних із здійсненням цієї загрози, призводить як до недооцінки, так і до переоцінки її серйозності. В результаті поряд з «страхітливими» описами глобальних катастроф, нерідко зустрічається і повне ігнорування цієї проблеми. Поняття кібертероризму часто використовується для політичних спекуляцій. Реальне ж положення справ, залишається не настільки страхітливим, проте, не вселяє і приводів для оптимізму.

## Література


1. Goben F. Op. cit. – P. 57-72; Scbwartau W. Information Warfare: Chaos on the Electronic Superhighway. – NY, 1994.
2. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. - СПб.: БХВ - Петербург; Арліт 2002.
3. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : [моногр.] / Голубєв В. О. – Запоріжжя : Гуманіт. ін-т «Запоріз. ін-т держ. і муніцип. упр.», 2003.

# ОБҐРУНТУВАННЯ ПОТРЕБИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

*Юрій Грицюк, Ольга Сівець*

Національний університет «Львівська політехніка», м. Львів, Україна

**The paper features examination of the ground of necessity of introduction of the protection system of the informative resources (IR) of the enterprise, what would provide continuity of business processes of the enterprise, firmness of its functioning and prevention of potential losses of the enterprise from realization of informative attacks.**

**Вступ.** Стрімкий розвиток ІТ призвів до різкого нагромадження інформаційних ресурсів (ІР) підприємства [1]. Ці ресурси постійно піддаються різним інформаційним атакам з боку конкурентів, зловмисників чи просто хакерів [5, 8]. Наслідками таких атак можуть стати розголошення конфіденційної або спотворення цілісної інформації, нав'язування керівництву підприємства помилкової інформації, порушення доступу до інформації, а також відмови і збої роботи програмно-технічних систем [2, 6].

Для вирішення поточних завдань захисту ІР підприємства впроваджується комплексна система захисту інформації (КСЗІ) [4]. Відповідно до принципу розумної достатності [3], КСЗІ має проектуватися так, щоб здійснювалася протидія тільки тим загрозам, що мають істотне значення для замовника ІР підприємства. Системи захисту ІР також мають нейтралізувати чи послабити інформаційні атаки конкурентів або зменшити наслідки їх прояву. При цьому потенційні втрати підприємства від можливих реалізацій загроз не мають перевищувати гранично допустимих значень. Для виконання цих суперечливих завдань на стадії технічного проектування розробляється модель системи захисту ІР підприємства та визначається сукупність компонент функціонального профілю КСЗІ для реалізації необхідної множини засобів і механізмів захисту.

**Визначення витрат на захист інформаційних ресурсів.** Для найбільш ефективного використання інформації в той чи інший період її життєвого циклу (ЖЦ), протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до неї, при якому ефект від її використання досягав би максимальної величини з урахуванням позитивних і негативних наслідків [4]. Встановлення певних обмежень на доступ до інформації протягом деякого періоду її ЖЦ є одним із способів ефективного управління об'єктами інформаційної безпеки з боку ІТ-служби, спрямованого на досягнення максимального ефекту від впровадження КСЗІ на підприємстві [7].

Для встановлення обмеженого доступу до ІР підприємства потрібно вирішити такі основні завдання:

- оцінити наявну інформацію за ступенем прояву різних загроз і визначити: можливі збитки власника у разі її вільного використання; необхідні витрат на її захист при встановленні обмеженого доступу до інформації; упущеної вигоди при вільному та обмеженому доступі до інформації;
- ранжувати інформацію та визначити величину збитків, витрат і вигод з тим, щоб отримати єдину систему оцінок, які характеризують інтегральний ефект від вільного та обмеженого доступу до інформації.

Для вирішення цих завдань необхідно вибрати такий режим доступу до інформації, який би протягом періоду її активного ЖЦ забезпечував максимальний ефект від використання. Можливість прояву зловмисників у динаміці ЖЦ інформації оцінюється суб'єктивною ймовірністю. Для визначення потенційних збитків від витоку інформації, упущених вигод від обмеженого її використання та необхідних витрат на захист ІР застосовується суб'єктивне оцінювання інформації експертами, що добре розуміють її цінність, а також взаємозв'язок з вказаними чинниками [4, 7].

На підставі порівняння експертних оцінок окремих чинників (збитку, витрат і вигод) з урахуванням різних можливостей їх прояву обчислюється значення інтегрального показника вибраного режиму доступу до інформації за формулою

$$W(t) = U(t) \cdot p_t - V(t) \cdot q_t - Z(t),\ t = \overline{1,T},$$

де: $T$ – тривалість ЖЦ інформації; потенційно можлива величина збитку $U(t)$ та величина вигод $V(t)$ при вільному використанні інформації в $t$-ий період її ЖЦ; ймовірність прояву потенційного збитку ($p$) і прояву упущених вигод ($p$) в $t$-ий період ЖЦ інформації; $Z(t)$ – величина необхідних витрат на захист інформації в $t$-ий період її ЖЦ.

У випадку, якщо розраховане значення інтегрального показника виявиться більшим від нуля, то доцільно внести цю інформацію до переліку відомостей з обмеженим доступом. Приналежність інформації до ІР підприємства, що підлягають захисту від несанкціонованих і ненавмисних дій, вважається тоді, коли величина заподіяного збитку внаслідок реалізації загроз перевищує величину витрат на її захист. Однак, як зазначалося вище, секретність чи конфіденційність інформації – категорія економічна, тому з плином часу вимагає перегляду.

Для наочної демонстрації залежності параметрів і характеристик ІР підприємства, що визначають умови їх захисту, може слугувати графічна модель, наведена на рисунку. В цій моделі показано якісний взаємозв'язок таких параметрів системи захисту ІР підприємства: їх цінність, необхідний рівень захисту, тривалість забезпечення конфіденційності. Модель також враховує економічні характеристики впровадження таких захисних заходів, як витрати на забезпечення потрібного рівня захисту інформації та можливі втрати (збитки) унаслідок недосконалості системи її захисту.

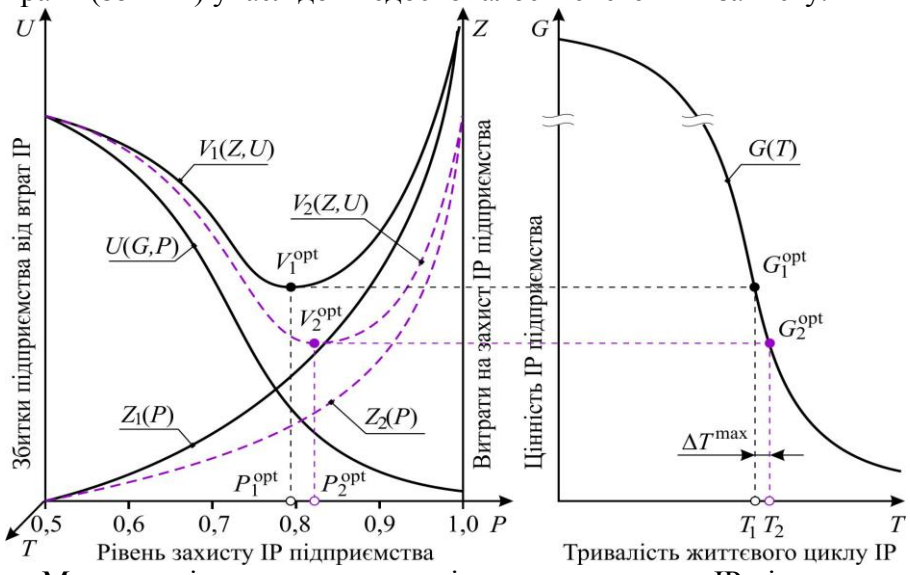



Рис. Модель оцінювання параметрів системи захисту ІР підприємства

На рисунку введено такі позначення: $G$ – цінність ІР підприємства – об'єкта конфіденційності (наприклад, науково-технічного звіту чи проектно-конструкторської документації, що містить опис нової технології); $G(T)$ – характеристика старіння інформації – зменшення цінності ІР підприємства з плином часу; $P$ – рівень (ймовірність) забезпечення захисту інформації (практично $0{,}5 \le P < 1{,}0$, оскільки абсолютно надійний її захист неможливий); $Z_1(P)$ – допустимі витрати на захист інформації як функція від необхідного рівня її захисту. Ці витрати зростають при підвищенні вимог до рівня захисту інформації. Прагнення досягти дуже високого рівня захисту інформації зазвичай призводить до різкого зростання витрат, які можуть перевищити цінність самої інформації, що захищається. Можливі втрати (збитки) власника інформації $U(G,P)$, понесені унаслідок неналежного рівня її захисту, є функцією від цінності самої інформації $G(T)$ та наявного рівня її захисту $P$. У нульовому наближенні ці втрати апроксимуються добутком цінності інформації $G(T)$ на ймовірність її витоку $H$, тобто $G(T) \cdot H$. Ймовірність

витоку інформації знаходиться в зворотній залежності до досягнутого рівня її захисту, $H = (1 - P)$. При такому допущенні $U(G,P) = G(T)\cdot(1 - P)$.

З рисунку видно, що сума $Z_1(P) + U(G,P)$ визначає витрати $V(Z,U)$, пов'язані із забезпеченням конфіденційності інформації. При цьому оптимальний рівень захисту інформації $V^{opt}(Z, U)$ відповідає мінімуму суми витрат на захист $Z_1(P)$ і можливих втрат $U(G,P)$ унаслідок неповноти захисту інформації. Прагнення перевищити його призведе до різкого зростання витрат $Z_1(P)$ на забезпечення захисту інформації; зниження ж рівня захисту призведе до збільшення можливих втрат $U(G,P)$ унаслідок недосконалості системи захисту ІР.

Якщо прийняти, що $\Delta T = T_2 - T_1$ – часовий інтервал, впродовж якого конфіденційність інформації може бути економічно виправданою, то його максимальне значення становить $\Delta T^{max} = \Delta T(G(T), V^{opt}(Z, U))$. При цьому, як показано на рисунку, величина витрат на захист інформації $Z_1(P)$ в сумі з можливими збитками від її втрати $U(G,P)$ менша від вартості самої інформації $G(T)$ з урахуванням її знецінення. Для спрощення викладення матеріалу, нехтуємо залежністю $Z(P,T)$, тобто зростанням сумарних витрат на захист ІР підприємства з плином часу. Це можна легко побачити, подавши ліву частину рисунка в тривимірних координатах, а саме $PT0U$.

З викладеного вище матеріалу видно, що значення величини досягнутого рівня захисту інформації $Z(P)$ залежить як мінімум від двох параметрів: $R_{pi}$ – використовуваних ресурсів (зокрема, матеріальних витрат на забезпечення захисту) і $E_{pim}$ – ефективності механізму захисту інформації (використання цих ресурсів). Тому в рамках математичної моделі $Z(P) = f(R_{pi}, E_{pim})$ можлива така постановка оптимізаційної задачі.

Фактично $E_{pim}$ – показник досконалості створеної та наявної системи захисту ІР підприємства. При дещо якіснішому проектуванні КСЗІ та практичній реалізації необхідної множини засобів і механізмів захисту, тобто максимально ефективному залученні всіх наявних ресурсів, один і той же рівень забезпечення захисту інформації може бути досягнутий при менших матеріальних витратах. На рисунку це переконливо демонструє крива $Z_2(P)$. При цьому відповідно оптимальний рівень захисту інформації $P_2^{opt}$ може бути вищим порівняно з $P_1^{opt}$, а економічно виправдана тривалість конфіденційності інформації $\Delta T$ – більшою, тобто $T_2 = T_1 + \Delta T$.

## Література


1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. – Доступний з http://nbuv.gov.ua/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf
2. Бармута Андрей. Утечка информации в корпоративной сети: угроза виртуальная, защита реальная. – Доступный с http://www.itsec.ru/articles2/in-ch-sec/ytechka-informacii-v-korporativnoi-seti-ygroza-virtyalnaya-zashita-realnaya
3. Грицюк Ю.І. Обґрунтування принципу розумної достатності функціонування КСЗІ на підприємстві // Захист інформації і безпека інформаційних систем : матер. IV-ої Міжнар. наук.-техн. конф., м. Львів, 04–05 червня 2015 р. – Львів : Вид-во НУ "Львівська політехніка". – 2015. – С. 39-40.
4. Грибунин В.Г., Чудовский В.В. Комплексные системы защиты информации на предприятии. – М. : Изд. центр "Академия", 2009. – 416 с.
5. Корпоративная информационная безопасность: виды IT-угроз. – Доступный с http://www.razumny.ru/stat/it-ugrozy.html
6. Кунинець А.І., Грицюк Ю.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.
7. Мальцев А. Методика оценки состояния инженерно-технической защищенности объектов // Технологии защиты. – 2010. – № 4. – С. 15-21.
8. Утечка информации – угроза корпоративной безопасности. – Доступный с http://www.staffcop.ru/articles/Information_leakage.php

# АНАЛІЗ СТОХАСТИЧНИХ ТА ДИНАМІЧНИХ МОДЕЛЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

*Валерій Дудикевич, Іван Опірський*

Національний університет «Львівська політехніка», м. Львів, Україна

**Presented and developed systematic modeling problems schemes of unauthorized access (UA) on information and its protection. The analysis and study of stochastic and dynamic models of security policies at UA in information networks state.**

**Keywords: unauthorized access, stochastic models of protection, dynamic models of protection, security model, Lukin-Volokity model, "cost-security" model, Kobozyevoyi-Khoroshko model, Poisson model, Ignatova V.O. model**

Теоретичне підгрунтя для створення сучасних СПЗ виступають політика безпеки й моделі безпеки, які відображають процеси НСД на інформацію та регулюють механізми її захисту. Під політикою безпеки розуміють інтегральну і, як правило, якісну характеристику, що описує властивості, принципи та правила захищеності інформації в ІМД в загальному просторі загроз. Модель безпеки являє собою формалізоване (математичне, аморетмічне, схемотехнічне тощо) подання обраної політики безпеки. Головним призначенням моделей безпеки є вибір та обґрунтування базисних принципів архітектури, що визначають механізми реалізації засобів захисту інформації, підтвердження властивостей (наприклад, рівня захищеності інформації) системи, яка розробляється шляхом формального доведення дотримання політики безпеки, складання формальної специфікації політики безпеки новостворювальної СПЗ, тощо. Узагальнивши відомі підходи, подамо систематичну схему проблеми моделювання процесів НСД (стан нападу) на інформацію та її захисту (рис. 1), виходячи з неї, дослідимо та проаналізуємо існуючі моделі.

Як видно з рис.1 систематика досліджувальної проблеми визначає, власне, і сучасну технологію моделювання процесів нападу на інформацію та її захисту.

Для моделювання процесів НСД з інформацією в ІМД широкого використання набули теоретичні моделі безпеки.

Так основною теоретичного підходу є методи теорії підтримки та прийняття рішень, теорії графів, теорії ймовірностей та напівмаркованих процесів тощо. Розроблені на їх базі відповідні моделі (рис. 1) в основному відкривають можливість отримання якісних оцінок рівня захищеності інформації.

Синтез теоретичного та емпіричного підходів (див. рис. 1) ґрунтується на групі математичних методів, які відносяться до них.

Детально проаналізуємо лише ті стохастичні та динамічні моделі, які отримані найбільше розповсюдження.

Аналізом та дослідженням загальних моделей несанкціонованого доступу в інформаційних мережах держави займались відомі вчені та науковці світу. Так, наприклад, у наукових працях, авторами яких є: Воробйов А.А.[1], Мельников В.В.[2],Щербаков А.Ю, Дев'янін П.Н., Габович А.Г., Петренко С.А., Цирлов В.Л.,Браїловський М.М.[4], Габович А.Г., Горобець А.Ю., Махальський О.О. тощо прийнято дотримуватися такої класифікації відповідних політик й моделей безпеки:

- моделі дискретного доступу (модель Хартсона, модель Хартсона-Рузо-Ульмана; модель TAM; модель TAKE-GRANT тощо);
- моделі мандатного доступу (модель Бела-Лападулі, модель Low-WaterMark тощо);
- моделі математичного доступу;
- моделі рольового доступу (модель Лендвера і Мак-Ліна);
- автоматичні та теоретично-імовірністні моделі (Гогена-Медигера);

- моделі контролю цілісності (модель Біба, модель Кларка-Вілсона);
- модель захисту від загроз відмов в обслуговуванні (модель Мілена) тощо.

Зважаючи на вище наведену класифікацію відомих політик та моделей, на практиці вимагається можливість розкриття суті базових підходів, які покладено в їх основу. Крім того, за самої класифікації ускладнюється науково-технічний аналіз математичного базису моделей.

Існує й інший, альтернативний, підхід до класифікації моделей, якого дотримуютья переважно вітчизняні вчені – Кобозєва А.А., Андрєєв В.І., Козлов В.С., Хорошко В.А., [5], Козлова К.В., Пархуць Л.Т., Горбенко І.Д., Кавун С.В.[6]. В основу їх класифікації покладено теоретичний, емпіричний та теортико-емпіричний підходи.

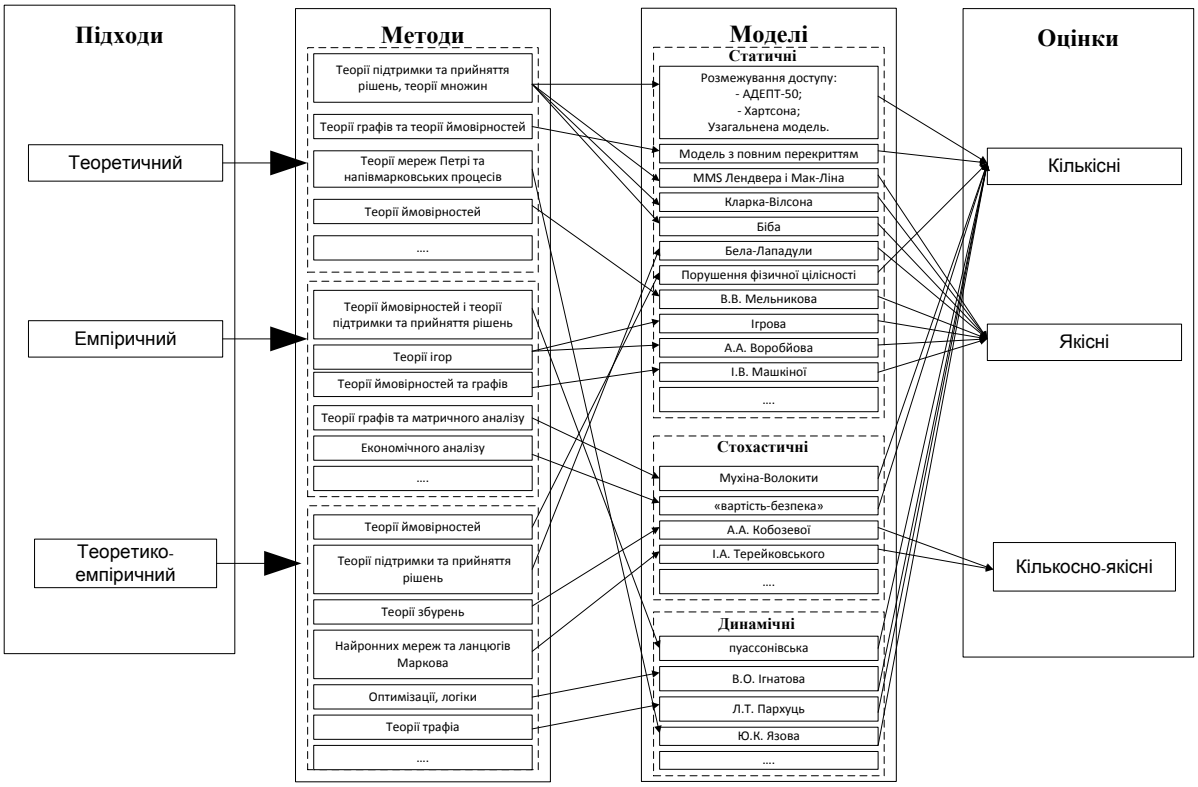



Рис.1. Схема проблем моделювання процесів НСД на інформацію та її захисту

## Література


1. Воробьев А.А. Оценивание защищённости автоматизированных систем на основе методов теории игр / Воробьеов А.А., Куликов Г.В., Некомнящих А.В. // Информационные технологии. – М: Новые технологии, 2007.-24с.
2. Цирлов В.Л. Основы информационной безопастности автоматизированных систем / Цирлов В.Л. – М: Феникс, 2008.–173с.
3. Браїловський М.М. Технічний захисту інформації на об'єктах інформаційної діяльності / Браїловський М.М., Головань С.М., Домарєв В.В.– К: Вид. ДУІКТ, 2007.–178с.
4. Габович А.Г. Методика оцінки рівня безпеки інформації / Габович А.Г., Горобець А.Ю., Хорошко В.О.// Вісник НУ «ЛП» – №55,2006. –с.46-53.
5. Кавун С.В. Математичне моделювання процесів побудови параметрів еліптичних кривих для криптографічних перетворень / І. Д. Горбенко, О. Є. Ілясова // Радіоелектронні і комп'ютерні системи. - 2006. - № 5. - С. 103–107.
6. Згуровський М.З. Основи системного аналізу/ Згуровський М.З., Панкратова Н.Д.– К:ВНV, 2007. –544с.

# ПРОБЛЕМИ ЗАХИСТУ ЛЮДИНИ ВІД НЕГАТИВНОГО ІНФОРМАЦІЙНО – ПСИХОЛОГІЧНОГО ВПЛИВУ

*Дмитро Дуржинський, Анатолій Шиян*

Вінницький національний технічний університет, м. Вінниця, Україна

**In this report was considered the problem of protection from negative information and psychological impact and possible ways to solve this problem by defining a sphere of human activity.**

Засоби масової інформації (ЗМІ) мають величезний вплив на особистість людини в даний період стрімкого розвитку інформаційних технологій.

Серед нерозв'язаних проблем, що стосуються внутрішнього та зовнішнього інформаційного простору України, залишається проблема негативного інформаційного впливів як з боку інших держав, так і у власному інформаційному середовищі, а також пошук механізмів державного регулювання захисту українських громадян від нав'язування їм негативної або суперечливої за своїм змістом інформації, різних видів маніпуляцій, навіювання загрозливих настроїв, психологічних атак тощо [1].

М. Г. Лашкіна у статті [2] розглядає «маніпуляцію» як вид психологічного впливу, майстерне виконання якого призводить до прихованого збудження в іншої людини намірів, які збігаються з її актуальними бажаннями; при цьому майстерність маніпулятора використовується для прихованого впровадження в психіку аудиторії цілей або установок, які не збігаються з тими, які є у нього на даний момент; цей вплив використовується для досягнення цілей шляхом прихованого залучення людини до виконання певних дій.

Одним із шляхів вирішення даної проблеми є визначення класу належності людини, використовуючи особливості дихотомічного способу визначення класу діяльності, який названо двокомпонентним абстрактним інформаційним автоматом (2AIA) [3]. За допомогою множини розроблених в [3] питань людину можна буде віднести до одного з класів належності, чим, на підприємстві, відокремити її від зовнішнього інформаційно-психологічного впливу.

## Література

1. Власенко О.В. Фактори негативних інформаційних впливів на громадян України [Електронний ресурс] // Державне управління: теорія та практика. – 2008. - № 2. – Режим доступу до журн. : http://www.nbuv.gov.ua/e-jourlals/dutp/2008-2/doc_pdf/vlsasenko.pdf
2. Лашкіна М.Г. Психологічний аспект комунікативної функції ЗМІ [Електронний ресурс]. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/Articles/KultNar/knp49_2_61-64.pdf
3. Shiyan, Anatoliy A., Technologies for HR-Managers: Typology for Person's Economic Behavior, Applications and Mechanism Design (May 1, 2011). – 373 p. – Режим доступу до ресурсу: http://ssrn.com/abstract=1827706 or http://dx.doi.org/10.2139/ssrn.1827706.

# СИСТЕМА ПРОТИПОЖЕЖНОГО ЗАХИСТУ ДЛЯ ЖИТЛОВИХ БУДИНКІВ

*Сергій Ємельяненко, Дмитро Гончаренко*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The paper presents the improvement of fire protection dwelling house using the fire protection system based on on-door speakerphone, which works as the apartment on-door speakerphone and additionally detects fires in apartments, informs inhabitants about fire, transmits alert to operational control of fire-rescue units and connects controller through telephone with the apartment in which the fire is.**

**Keywords: fire protection, on-door speakerphone, announcement, fire alarm, risk.**

Сьогодні одним з найдієвіших заходів для виявлення та оповіщення населення про пожежу є використання пожежних сповіщувачів, які дозволяють зменшити ризик загибелі населення [1], наприклад: в США щороку виникає 1,5 млн. пожеж, в Україні 60 тис. пожеж, а загибель однакова, близько 3-4 тис. жителів. Хоч ризик зіткнутися з пожежею у квартирі в Україні менший (7,8·10-4) ніж в США (1,8·10-3), а ризик загинути на пожежі у квартирі вищий (7,9·10-5), (1,3·10-5) відповідно. Використання пожежних сповіщувачів допоможе скоротити кількість загиблих та зменшити збитки від пожеж.

Згідно чинних законодавчих норм [2-3] пожежні сигналізації, в обов'язковому порядку встановлюються лише на підприємствах та у житлових будинках підвищеної поверховості та висотних з середнім та високим ступенем ризику. У малоповерхових та багатоповерхових житлових будинках з незначним ступенем ризику не вимагається влаштування пожежної сигналізації, лише за бажанням власника квартири.

**Метою роботи** є створення системи протипожежного захисту на базі домофона, яка б допомогла знизити рівень пожежних ризиків для мешканців одноквартирних та багатоквартирних будинків.

Запропонована система побудована у вигляді додаткових модулів до домофона та призначена для виявлення пожеж у квартирах, оповіщення про пожежу в будинку жителів, передачі сигналу про пожежу до підрозділу ДСНС та з'єднання телефонним зв'язком диспетчера з квартирою, у якій виникла пожежа. За відсутності пожежі домофон виконує функції системи контролю доступу до будинку

Система призначена для забезпечення контролю доступу до будинку у штатному режимі, а при виникненні пожежі – для її виявлення, оповіщення жителів та інформування про пожежу відповідної служби. Телефонне з'єднання диспетчера ОДС пожежно-рятувальної служби (Системи 112 чи пультом пожежного спостереження) з квартирою, в якій сталася пожежа, дає змогу уточнити інформацію про пожежу. Своєчасне інформування жителів будинку системою протипожежного захисту на базі домофона про місце виникнення пожежі, дозволяє швидше розпочати евакуацію і підвищити її безпеку. Система оповіщення проінформує інших жителів будинку про пожежу в ньому.

Робота системи протипожежного захисту на базі домофона за відсутності пожежі не відрізняється від роботи інших домофонів. При спрацюванні пожежного сповіщувача чи введення в дію ручного пожежного сповіщувача система протипожежного захисту на базі домофона діє як система пожежної сигналізації: здійснює оповіщення жителів та відповідної служби, автоматично відкриває вхідні двері під'їзду, а також встановлює телефонний зв'язок між оперативно-диспетчерською службою пожежно-рятувальних підрозділів (Системи 112 чи пунктом пожежного спостереження) та квартирою, в якій виникла пожежа, для з'ясування її обставин.

Система побудована у вигляді додаткових модулів до домофона та призначена для виявлення пожеж у квартирах, оповіщення про пожежу в будинку жителів, передачі сигналу про пожежу до підрозділу ДСНС та з'єднання телефонним зв'язком диспетчера з квартирою, у якій виникла пожежа (рис. 1).

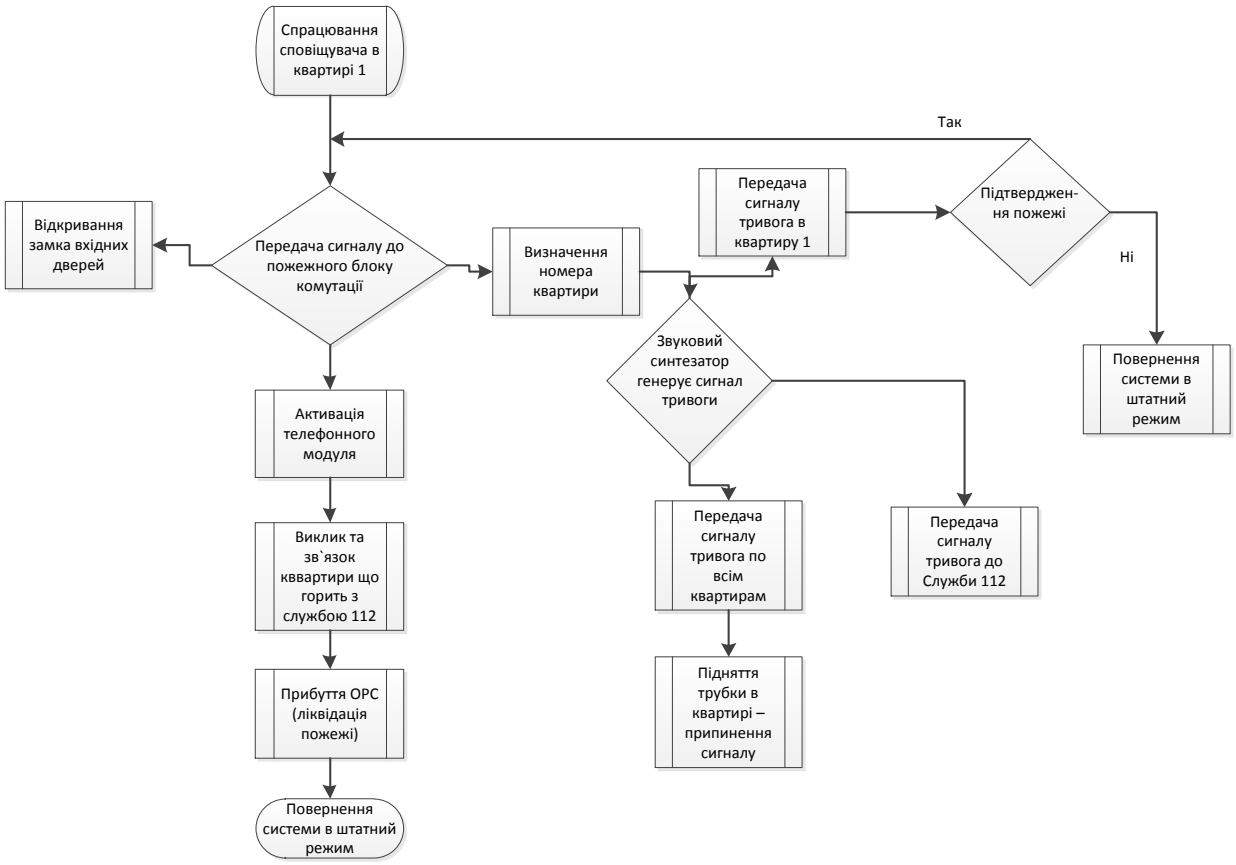



Рис. 1. Схема роботи системи протипожежного захисту на базі домофона

Своєчасне повідомлення мешканців системою протипожежного захисту на базі домофона та пожежно-рятувальні служби про пожежу сприятиме безпечній евакуації та прискорить прибуття підрозділів до місця пожежі, що дозволить знизити індивідуальні пожежні ризики у житлових будинках. За економічністю система потребує менших матеріальних витрат ніж монтаж системи адресної пожежної сигналізації по квартирах житлового будинку у зв'язку з тим, що використовує адресні лінії домофона, не потребує адресних пожежних сповіщувачів та пожежного приймально-контрольного пристрою.

## Література


1. Yung David Tin Lam Principles of fire risk assessment in buildings / David Tin Lam Yung // Toronto. : Yung & Associates Inc. Canada, 2008. С 90-92.
2. Інженерне обладнання будинків і споруд. Системи протипожежного захисту. ДБН В.2.5-56:2014 [Редакція від 13.11.2014].
3. Закон України 877-16 / Про основні засади державного нагляду (контролю) у сфері господарської діяльності. – [Чинний від 01.09.2015].

# РОЗРАХУНОК ІНТЕГРАЛЬНОЇ ХАРАКТЕРИСТИКИ КОНФІДЕНЦІЙНОЇ СОЦІАЛЬНОЇ МЕРЕЖІ ВЕЛИКОГО РОЗМІРУ

*Ігор Заступ, Анатолій Шиян*

Вінницький національний технічний університет, м. Вінниця, Україна

**We describe the confidential social network, which is modeled as large graph, in which the links are probably changed from certain node to another nodes. The number of links for certain node is influenced by two processes: the creation of new links and the destruction of existing links. Two stochastic ordinary equations for quantity of links are derived.**

**Keywords: privacy, social network, stochasticity, probability density.**

***Вступ та актуальність роботи.*** Сучасні конфіденційні соціальні мережі складаються із великої кількості окремих вузлів та зв'язків між ними. В цих мережах в якості вузлів виступають окремі суб'єкти (найчастіше окремі особи), які є носіями конфіденційної інформації. Зв'язки між агентами здійснюються за допомогою телекомунікаційних мереж – Інтернету, стільникового зв'язку тощо.

Кількість вузлів для сучасних соціальних мереж, як правило, є величиною сталою. Задається вона часто кількістю агентів, окремих суб'єктів, ботів тощо. На відміну від вузлів, зв'язки між вузлами, як правило, є величиною змінною. Вони можуть виникати, деякий час існувати, а потім розриватися. В якості прикладу можна навести участь агента в окремих групах соціальних мереж (спільнотах, групах тощо).

Таким чином, сучасна соціальна мережа може бути представлена як стохастичний граф великого розміру, який включає в себе (незмінну, або ж порівняно повільно змінювану) велику кількість вузлів, зв'язки між якими мають випадкову (стохастичну) компоненту. Внаслідок цього дослідження кількісних характеристик великих стохастичних графів представляє собою актуальну наукову та важливу практичну задачу. Незважаючи на досягнуті результати, проблема моделювання інтегральних характеристик стохастичного графа великого розміру все ще залишається не вирішеною.

*Метою роботи* є побудова моделі для розрахунку інтегральних характеристик стохастичного графа великого розміру, який є моделлю конфіденційної соціальної мережі.

***Основні результати.*** В рамках масштабно-інваріантного підходу стохастичність можна врахувати в рамках через наявність стохастичної адитивної складової, внаслідок чого приходимо до двох основних моделей для динаміки кількості зв'язків заданого вузла:

$$\frac{dm}{dt} = \lambda \cdot m^a - m^b + \xi_{t\cdot} \cdot m^a \qquad (1)$$

$$\frac{dm}{dt} = m^a - \omega \cdot m^b + \eta_t \cdot m^b \qquad (2)$$

Тут $m$ є кількість зв'язків, які має розглядуваний вузол.

Для моделі (1) стаціонарне значення є $m_0 = \lambda^{1/(b-a)}$, а для моделі (2) стаціонарне значення є та $m_0 = \omega^{1/(a-b)}$. Функції $\xi_t$ і $\eta_t$ є стохастичні.

Моделі (1) та (2) є стохастичними диференціальними рівняннями із мультиплікативним шумом. Для простоти можемо вважати, що функції $\xi_t$ і $\eta_t$ є білим шумом із середнім значенням $\langle \xi_t \rangle = \langle \eta_t \rangle = 0$, а також із дисперсіями $\langle \xi_t^2 \rangle = \langle \eta_t^2 \rangle = \sigma_2$.

Властивостями моделей (1) та (2) є такі.

1. Для розглянутого прикладу асимптотика $P(m,t) \to P_s^{a,b}(m)$ справедлива незалежно від вигляду початкового розподілу $P(m,t=0)$.

2. Загальні властивості отриманих $P_s^{a,b}(m)$ є такими:

- При малій інтенсивності шуму $\sigma^2$ буде мати місце асимптотика $P_s^{a,b}(m) \to \delta(m - m_0)$, де $\delta(x)$ - сингулярна дельта - функція Дірака.
- З ростом $\sigma^2$ ширина $\Delta$ розподілів $P_s^{a,b}(m)$ збільшується.

3. Моделі (1) і (2) у наближенні білого шуму будуть добре описувати головний внесок в експериментально обмірювані $P_e(m)$, який зосереджений в околиці максимуму. «Хвости» розподілів $P_e(m)$ будуть формуватися з порівняно малої кількості об'єктів, тому в рамках моделі білого шуму в них не можна належним чином урахувати варіабельність вузлів графа великої розмірності (можна сказати, що в «хвостах» $P_e(m)$ проявляються «найбільш яскраві індивідуальності» серед вузлів графа).

4. Розглянутий клас моделей дозволяє формалізувати кількісний розрахунок таких параметрів графа великого розміру, які є інтегральними та характеризують його «в цілому». Це дає можливість розробити ряд нових критеріїв для загальних характеристик стохастичних графі великого розміру, що відкриває можливості для розробки нового класу їх характеристик.

5. Отриманий спосіб опису допускає поширення на нестаціонарні випадки, але дослідження може бути проведено, як правило, лише чисельними методами або ж шляхом комп'ютерного моделювання. Наприклад, введення «повільних» змінних $\tau$ (з характерним часом мінливості багато більше ніж $T_0 = [(1-a)c]^{-1} \cdot m_0^{1-a}$) дозволяє використати отримані результати шляхом введення залежностей виду $a(\tau), b(\tau), c(\tau), d(\tau), \sigma^2(\tau)$ тощо.

Отримана модель дозволяє безпосередньо провести її експериментальну верифікація, а також отримати на їхній основі прогноз поведінки числових значень параметрів, що характеризують стохастичний граф великого розміру.

***Висновки.*** Розроблена математична модель для розрахунку інтегрального показника для конфіденційної соціальної мережі великої розмірності, яка моделюється стохастичним графом. Результатом є розподіл вузлів графа за кількістю їх зв'язків із іншими вузлами. Отримані аналітичні формули для щільності ймовірності розподілу вузлів за кількістю зв'язків для випадку білого шуму та одного класу аналітичних залежностей для інтенсивностей створення та руйнування зв'язків у графі. Ці ймовірності можуть бути експериментально знайдені.

Отримані результати можуть бути застосовані для широкого кола соціальних мереж, у вузлах яких знаходяться суб'єкти інформаційної безпеки, які володіють конфіденційною інформацією.

Наприклад, для мережі мобільного зв'язку вузлами графа є соти, а зв'язками є зв'язки із абонентами. Стохастичність виникає внаслідок діяльності абонентів, яка виникає внаслідок їх не прогнозованого підключення до мережі, переміщення людей тощо. Для соціальних мереж, таких як ВКонтакті, Facebook, LinkedIn, Social Science Research Network, ArXiv тощо, веб-портали Coursera, eBay, Amazon тощо, вузлами слугують зареєстровані користувачі, а в якості зв'язків виступають їх месаджі, лайки тощо.

## Література


1. Злепко С.М., Шиян А.А., Павлов С.В., Хаїмзон І.І. Інформаційні технології для управління діяльністю людини. – Вінниця: ВНТУ, 2012. – 316 с.
2. Шиян А.А. Оптимізація діяльності агентів в інформаційних та телекомутаційних системах управління виробничими та організаційними структурами // Вісник Хмельницького національного університету. Технічні науки. – 2012. – № 4. – С.149-153.

# ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ВЕКТОРНИХ ЗОБРАЖЕНЬ

*Василь Карпінець, Юрій Яремчук*

Вінницький національний технічний університет, м. Вінниця, Україна

**The report observed the method of protecting the integrity of vector images digital watermarks with provision to reduce the influence of its embedding image quality. It analyzes the impact of watermark on quality vector images and sustainability of the proposed method is the most common malicious attacks aimed at the destruction or substitution of digital watermark, the results of which showed a sufficient level of stability**

Діяльність великої кількості підприємств та організацій пов'язана зі створенням та обробкою інформації у цифровому вигляді, левову частку якої складають цифрові зображення, зокрема векторного формату. Наприклад, векторні цифрові карти є основою системи державного земельного кадастру та картографічної промисловості. Зображення векторного формату використовуються промисловими підприємствами при проектуванні будь-якої техніки від портативної до авіатранспорту. При цьому на створення векторних зображень витрачається багато коштів та часу і часто вони є результатом наукових розробок та основою інноваційних технологій.

На сьогодні в Україні існує серйозна проблема захисту векторних зображень від несанкціонованого використання та їх зміни третіми особами. В багатьох зарубіжних країнах для вирішення такої проблеми використовують стеганографічні методи та засоби захисту цілісності інформації, що дозволяють визначати факт несанкціонованого використання чи модифікації векторних зображень. Для цього навіть прийняті відповідні закони, що дозволяють використовувати стеганографічні засоби для визначення правомірності використання цифрової інформації. На відміну від зарубіжних країн в Україні проблема захисту векторних зображень залишається не вирішеною.

Недоліком закордонних стеганографічних засобів та сервісів захисту цілісності інформації є їх висока ціна та необхідність адаптації для специфіки українського споживача. Для усунення зазначених недоліків пропонується розробка нового методу та сервісу захисту цілісності цифрових векторних зображень (ЦВЗ), що не потребує наявності оригіналу зображення при витягуванні ЦВЗ. При цьому запропоновані метод та сервіс забезпечать кращий рівень захисту, спрощену та швидшу процедуру підтвердження цілісності, а також у 2-2,5 рази нижчу вартість у порівнянні з зарубіжними аналогами.

Проведено аналіз існуючих на сьогодні стеганографічних методів вбудовування стійких ЦВЗ у векторні зображення з точки зору впливу ЦВЗ на якість векторних зображень та стійкості до зловмисних атак [1-3]. При цьому особливу увагу приділено аналізу методів, які для витягування ЦВЗ не потребують наявності оригіналу зображення чи самого ЦВЗ, що значно спрощує процедуру підтвердження авторства.

Також проведено дослідження можливості захисту цілісності векторних цифрових зображень без використання оригіналу зображення при її перевірці та із забезпеченням меншого рівня спотворень внаслідок вбудовування ЦВЗ.

Проведено аналіз можливості зменшення рівня спотворень векторних зображень внаслідок вбудовування ЦВЗ з точки зору вибору базового перетворення. Проведений аналіз частотних перетворень показав перевагу двовимірного дискретного косинус-перетворення (ДКП) над одновимірним з точки зору розподілу зміни коефіцієнтів на більшу кількість точок зображення і, відповідно, меншу зміну координат цих точок близько у 8 разів [4-5].

Запропоновано метод захисту цілісності векторних зображень ЦВЗ із забезпеченням зменшення впливу його вбудовування на якість зображення. Було проведено аналіз

впливу ЦВЗ на якість векторних зображень та стійкості запропонованого методу до найпоширеніших зловмисних атак, спрямованих на знищення чи підміну ЦВЗ, результати якого показали достатній рівень стійкості на рівні з відомими методами [6-7].

У порівнянні з існуючими методами захисту цілісності інформації метод, що пропонується, забезпечить спрощення процедури підтвердження цілісності. В методі для витягування ЦВЗ потрібно буде мати лише секретний ключ.

Переваги запропонованого двовимірного ДКП:

- до 4 разів зменшується вплив вбудовування бітів ЦВЗ на якість зображення (шляхом зміни коефіцієнтів ДКП на координати точок векторного зображення);
- забезпечується чітке розпізнавання бітів ЦВЗ;
- забезпечуватись достатній рівень стійкості до навмисних спотворень з метою знищення ЦВЗ (зловмисних атак);
- при вбудовуванні ЦВЗ проводиться зміна лише високочастотних коефіцієнтів ДКП, які найменше впливають на відхилення координат точок векторного зображення;
- використання особливого підходу до зміни коефіцієнтів дозволить змінювати їх на невелике значення, що зменшить вплив ЦВЗ на якість зображення;
- використовується певне граничне значення зміни коефіцієнтів, яке буде визначатися залежно від типу та розміру зображення та ЦВЗ, а також від вимог до якості зображення з вбудованим ЦВЗ;
- зменшення рівня спотворень до 2 разів у порівнянні з аналогами завдяки уникненню суттєвих відхилень окремих точок зображення при використанні методу відбору придатних коефіцієнтів ДКП.

Розробка Web-сервісу на основі розроблюваного методу дозволить користувачам вбудовувати ЦВЗ у свої векторні зображення прямо в Web-браузері, не використовуючи додаткового програмного забезпечення та робити це швидше ніж на власному комп'ютері за рахунок високопродуктивних серверів онлайн-сервісу.

## Література


1. Карпінець В. В., Яремчук Ю. Є. Аналіз впливу цифрових водяних знаків на якість векторних зображень // Сучасний захист інформації. – 2011. – №1. – С.72-82.
2. Карпінець В. В., Яремчук Ю. Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №2. – С.94 – 99
3. Карпінець В. В., Яремчук Ю. Є. Аналіз сучасних методів вирішення проблеми захисту авторського права векторних зображень / В.В. Карпінець, Ю.Є. Яремчук // Сучасна спеціальна техніка. – №3, 2013. – С. 102–113.
4. Карпінець В. В., Яремчук Ю. Є. Забезпечення захисту векторних зображень від атак спрямованих на видалення цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – №15 (204), Частина 1, 2013. – С. 62–68.
5. Карпінець В. В., Яремчук Ю. Є. Аналіз впливу параметрів відбору придатних матриць ДКП векторних зображень на спотворення та розмір ЦВЗ / В.В. Карпінець, Ю.Є. Яремчук // Інформаційна безпека. – №1, 2013. – С. 68–77.
6. V. Karpinets, Ju. Yaremchuk, M. Prokofjev. Матеріали конференції, Technical University of Gabrovo. International scientific conference UNITECH'12. / V. Karpinets, Ju. Yaremchuk, M. Prokofjev. // Proceedings. Volume I, 16–17 November 2012, Gabrovo. – Pp. 348 – 352.
7. Яремчук Ю. Є. Метод асиметричного шифрування інформації на основі рекурентних послідовностей / Ю. Є. Яремчук // Сучасна спеціальна техніка. – 2012. – №4. – С.79-87.

# ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ ОБРОБКИ ДЕРЖАВНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ В СИСТЕМАХ ПОЖЕЖНОЇ ОХОРОНИ

*Микола Карпінський[1], Віталій Чиж[2], Степан Балабан[2]*

1. Університет в Бєльську-Бялій і Державна вища професійна школа в Новому Сончі, м. Новий Сонч, Польща
2. Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

**It was proposed use of wireless sensor networks for identifying areas of origin or spread of fire. Clustering of information nodes was considered, method of determining the fire within range of the sensor network was described.**

**Keywords: wireless sensor network, attack, visualization, simplex, cluster model, computer visualization**

Бурхливий розвиток інформаційних технологій сприяє створенню досконалих засобів збору та опрацюванню великої кількості різноманітної інформації та створює умови їх використання у всіх галузях народного господарства. Серед таких засобів особливе місце займають безпроводові сенсорні мережі (БСМ). Протягом більше двадцяти років передові розробники засобів апаратного і програмного забезпечення БСМ пропонують безпроводові системи для служб надзвичайних ситуацій, зокрема для організації пожежної та охоронної сигналізації [1, 2]. Як правило, такі системи комплектують інтелектуальними безпроводовими інформаційними вузлами (ІВ), базовими вузлами (USB – або Ethernet - шлюз), диспетчерським пультом охорони (кінцевим пристроєм). Сучасні інформаційні вузли здатні збирати, опрацьовувати та передавати інформацію про наявність і концентрацію у навколишньому середовищі радіонуклідів, отруйних речовини, диму, підвищення температурного режиму тощо. Зібрана інформація з такої системи передається до базових вузлів. В якості базового вузла використовують USB – адаптер для систем до 200 ІВ. Ethernet – шлюз доцільно використовувати від 200 ІВ і більше.

БСМ, що експлуатуються службами надзвичайних ситуацій, виконують надзвичайно важливі господарські, соціальні та функції безпеки. Тому до надійності їх роботи та захищеності інформації, що в них циркулює, ставлять особливо високі вимоги. За даними дослідників [2] дезорганізація загрози роботи 25-ти ІВ мережі пожежної охорони лісу може знищити до 1 кв. км лісових насаджень, привести до пошкодження та виведення з ладу ліній електропередач та підстанцій електропостачання, а вивід з ладу шляхом атак на парметри сигналів порядку десяти тисяч інформаційних вузлів можу зумовити вигоряння лісу на площі до 400 кв. км. Збитки в даному випадку можуть прирівнюватися д загрози екологічній безпеці та катастрофи.

Засоби і методи атак на БСМ постійно вдосконалюються. Тому успішне використання БСМ вимагає постійного підвищення їх надійності, довговічності, швидкодії та рівня захищеності інформації. Вирішити дані проблеми важко без використання належних засобів для моделювання БСМ. Особливе місце серед засобів моделювання БСМ займає геометричне моделювання (ГМ). Таке моделювання дозволяє використовувати методи обчислювальної геометрії, зокрема, геометрії відстаней. Яка дозволяє із факту існування співвідношення між вимірюваними відстанями досліджувати внутрішні властивості геометричних фігур.

Основною фігурою для геометричного моделювання БСМ, до складу якої входять ІВ вузли з однаковими параметрами, авторами запропоновано використовувати рівносторонні трикутники зі стороною $l$ у вершинах якого розташовані сигнальні точки (СТ), які у змодельованій мережі представляють реальні інформаційні вузли. Оскільки, трикутники мало придатні для здійснення комп'ютерної візуалізації зміни параметрів сигналів ІВ, кожні два сусідні трикутники геометричної моделі БСМ об'єднують у чотири точкові симплекси [3].

Такі симплекси зручні для подальших досліджень, оскільки, при переміщені СТ, що розміщені у їх вершинах, симплекси можуть трансформуватися у відрізки прямої лінії, чотирикутники або трикутні піраміди.

При стабільній роботі ІВ у симплексі фіксується двомірний евклідовий простір із фізичними зв'язками (ФЗ) довжиною *l*. В залежності від того, яким чином встановлюють залежність між ФЗ і СТ у симплексі запропоновано два методи візуалізації сили сигналів ІВ: метод рухомих СТ і метод стаціонарних СТ [4].

Якщо змін зазнає параметр сигналу ІВ, СТ якого розміщена на кінці великої діагоналі ромба, або змін зазнали одночасно сигнали кількох ІВ, СТ яких належать одному симплексу, візуалізація трансформації симплекса ускладняється або стає неможливою. Для вирішення даної проблеми запропоновано використовувати симплексно-кластерну модель БСМ [4]. При цьому 18 СТ об'єднують у кластер, який складається з зовнішнього обвідного та внутрішнього шестикутника які об'єднані п'ятьма ФЗ з сусідніми СТ. інші шість СТ розташовані в серединах сторін зовнішнього обвідного шестикутника та зв'язані чотирма ФЗ з сусідніми СТ. останні шість СТ розміщені у вершинах зовнішнього обвідного шестикутника і зв'язані трьома ФЗ з сусідніми СТ.

Оскільки, в кластерній моделі кожен інформаційний вузол підтримує зв'язок з трьома-п'ятьма сусідніми інформаційними вузлами, інформація про його вихід з ладу може передаватися кількома інформаційними каналами зв'язку до базових вузлів (БВ). БВ, при необхідності, можуть об'єднуватися в кластерні системи з багатоканальною організацією зв'язків між собою і з сенсорами вищого рівня. Така схема моделювання БСМ, які використовують служби надзвичайних ситуацій, дозволяє оперативна одержувати інформацію про поширення фронту забруднення території небезпечними для життя речовинами, пожежі або іншого стихійного лиха.

Основні задачі кластерної БСМ полягають: після того як в межах кластера відбулось втручання зловмисника інформація про це може бути передана керуючому вузлу, після ідентифікації зловмисника кластер переходить в режим відслідковування зловмисника а саме повідомляє користувача про його місце знаходження при взаємодії з 1 чи 2 сенсорами буде повідомлятись його приблизне місце знаходження, а саме область в межах якої діє радіус сенсора який не перекривається іншими сенсорами або область перетину сенсорних радіусів при умові взаємодії з 2 сенсорами, якщо ж зловмисник потрапляє в середину кластера і встановлює зв'язок з 3 і більше сенсорами тоді з допомогою тріангуляції можна визначити місцезнаходження з точністю до 1 метра.

Під час моделювання було отримано підтвердження ефективності використання кластеризації, так як в результаті побудови різноманітних маршрутів та поширення інформації в межах кластера призводить до отримання більш достовірної інформації щодо ідентифікації відхилень в роботі БСМ, швидкої перебудуви кластера чи взагалі БСМ вразі виходу з ладу чи пошкодження ІВ.

## Література


1. A ZigBee-Based Wireless Sensor Network Node for Ultraviolet Detection of Flame / Pedro Cheong, Ka-Fai Chang, Ying-Hoi Lai, Sut-Kam Ho, Iam-Keong Sou, and Kam-Weng Tam // IEEE Transactions on Industrial Electronics. - IEEE , November 2011. - Volume: 58, Issue: 11. - P. 5271-5277.
2. Hyunsang Choi. Fast detection and visualization of network attacks on parallel coordinates: Journal Article / Hyunsang Choi, Heejo Lee, Hyogon Kim // Computers & Security. - July 2009. - Volume 28. - P.276–288. - ISSN 0167-4048.
3. Пат. 82896 Україна, МПК H04W 12/12. Спосіб симплексного моделювання: патент на корисну модель /Чиж В.М., Демчишин О.І., Карпінський М.П., Балабан С.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2012 13971 ; заявл. 07.12.12 ; опубл. 27.08.2013, Бюл. № 16. – 4 с.
4. Пат. 93269 Україна, МПК H04W 12/12. Спосіб кластерного моделювання бездротової сенсорної мережі /Чиж В.М., Карпінський М.П., Балабан С.М.; власник патенту Тернопільський національний технічний університет ім. Івана Пулюя (Україна), Академія технічно-гуманістична в Бєльску-Бялей (Польща). – № u 2014 03919 ; заявл. 14.04.14 ; опубл. 25.09.2014, Бюл. № 18. – 6 с.

# ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЛОКАЛІЗАЦІЇ ЗАКЛАДНИХ ПРИСТРОЇВ ПРИ ЗАСТОСУВАННІ НЕЛІНІЙНОЇ ЛОКАЦІЇ

*Віталій Катаєв*

Вінницький національний технічний університет, м. Вінниця, Україна

**Experimentally investigated the problem of localization of eavesdropping devices which located in shielded enclosures when using nonlinear locator. Results show that the using of same types of radiostable fabrics as shielding materials, can greatly complicate the detection of eavesdropping devices.**

**Keywords: information protect, bug devices, radio opaque fabrics**

Велику частину загроз для інформації становлять закладні пристрої або апаратні закладки. Найчастіше закладки слугують для перехоплення акустичної (мовної) та видової інформації, для цього можуть використовуватись портативні диктофони, провідні та радіо мікрофони та мініатюрні відеокамери і т.д. Виявлення закладних пристроїв зазвичай здійснюється з допомогою спеціальної пошукової апаратури. Причому цей спосіб повинен враховувати всі технічні характеристики та особливості роботи закладок, адже від принципу їх роботи буде залежати і метод, яким можна буде їх виявити [1].

Найбільш проблемними з точки зору виявлення являються портативні диктофони, адже дані пристрої під час своєї роботи не випромінюють ніяких сигналів, не підключаються до провідних ліній та працюють автономно. Тому виявити їх можна лише небагатьма пошуковими пристроями, такими як тепловізори та нелінійні локатори, при чому кожен з цих пристроїв мають свої недоліки. Наприклад, при використанні тепловізорів виникають значні обмеження, оскільки ступінь нагрівання об'єкта в якому знаходиться закладка залежить від багатьох факторів. Тому можливі випадки, коли локалізація закладного пристрою з допомогою тепловізора буде ускладнена або навіть неможлива [2]. Нелінійні локатори також мають свої проблеми - це і випадкові спрацювання на матеріали, які не є напівпровідниками, і неможливість виявлення закладок схованих у офісній та іншій техніці. Окрім цього, використання даних локаторів також може ускладнюватись і у випадку, якщо закладний пристрій має корпус виготовлений із екрануючих матеріалів, адже, це напряму буде впливати на сам принцип локалізації. Тому виникає необхідність дослідження даної проблеми більш детально.

В доповіді описані лабораторні виміри, які було проведено при розташуванні нелінійного елемента, який виступає у ролі складової апаратної закладки, у корпусах виконаних із різних типів екрануючих матеріалів в якості яких було використано радіонепрозорі тканини вітчизняного виробництва типу М1, М2, М3 та Н1, Н2, Н3. В якості нелінійного елемента використовувався напівпровідниковий діод, який розміщувався у діелектричному корпусі, що почергово огортався кожним із типів тканин. На відстані 0,15 м від корпусу розміщувався нелінійний локатор NR-μ. Локатор NR-μ являється індикаторним пристроєм і виявлення напівпровідникових матеріалів супроводжується загоранням лінійки світлодіодів, що знаходяться на корпусі пристрою. Тому при дослідженні впливу екрануючих матеріалів на процес локалізації нелінійних елементів, у якості вихідних даних будемо використовувати зображення індикаторних світлодіодів.

На рис. 1 представлені зображення індикаторної лінійки локатора при розміщенні напівпровідникового діоду у екранованих корпусах різних типів. Для аналізу впливу екрануючих матеріалів на можливість локалізації закладних пристроїв, будемо визначати кількість світлодіодів що світиться, тим самим ми визначимо, як змінюється ступінь впливу напівпровідникових елементів на поле локатора в якому вони знаходяться.

Як видно з рис. 1а при розташуванні діоду безпосередньо у полі локатора, засвічується шість індикаторних світлодіоди, тому вважатимемо це контрольним значенням відносно якого можна буде спостерігати вплив екрануючих матеріалів.

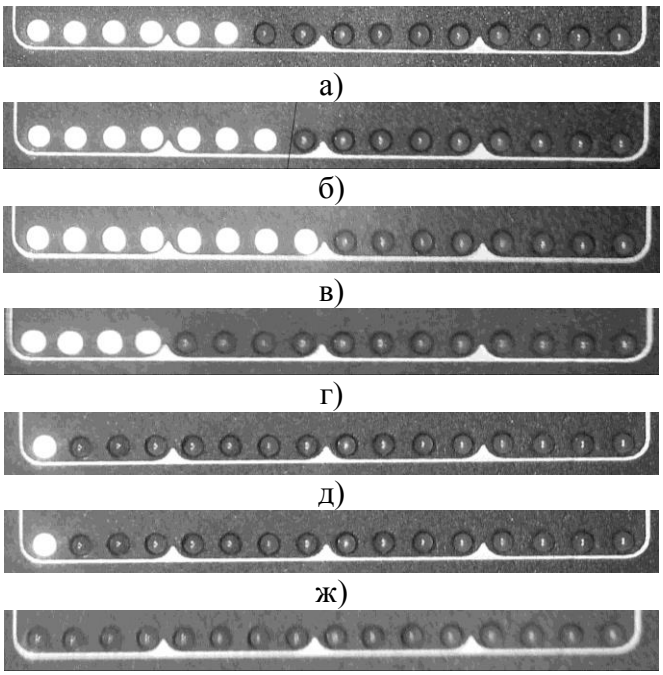



Рис. 1. Покази індикаторної лінійки локатора при розташуванні напівпровідникового діоду безпосередньо перед пристроєм а), у корпусі з тканини М1 б), у корпусі з тканини М2 в), у корпусі з тканини М3 г), у корпусі з тканини Н1 д), у корпусі з тканини Н2 ж) та у корпусі з тканини Н3 з)

При розміщенні напівпровідникового елементу у корпусах із тканин типу М ми спостерігаємо наступні результати, тканини М1 та М2 (рис.1 б,в) замість того, щоб зменшити вплив діода на поле локатора, навпаки його збільшують, і на пристрої засвідчується сім та вісім світлодіоди відповідно. Такий ефект можна пояснити недосконалістю установки, що використовується в дослідженні, а саме тим, що напівпровідниковий елемент розміщується в прямокутному корпусі, який обгортається екрануючою тканиною, і стінки корпуса в сумі з тканиною виконують роль спрямовуючої антени, а зміна діаграми направленості спричиняє зростання рівня сигналу. У випадку тканини М3 (рис.1 г) спостерігається зменшення впливу, про що сигналізують чотири світлодіоди. При розміщенні досліджуваного діода у корпусах із тканин типу Н ми спостерігаємо практично протилежні результати, адже у випадку використання тканин Н1 та Н2 (рис.1 д,ж) досліджуваний елемент індикується дуже слабо, оскільки світиться лише один світло діод, а при розміщенні діода у корпусі з тканини Н3 (рис.1 з) він взагалі перестає визначатись нелінійним локатором.

Таким чином в доповіді наведені результати дослідження, які показують, що якщо закладні пристрої будуть мати корпус виготовлений із використанням певних радіонепрозорих тканин то локалізація та виявлення цих закладок з допомогою нелінійних локаторів значно ускладниться, а в деяких випадках навіть буде неможливою. Тому застосування нелінійних локаторів необхідно проводити лише у комплексі з іншими заходами пошуку та локалізації, для підвищення ймовірності знаходження таких закладних пристроїв, як мініатюрні диктофони.

## Література

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации./ А.А. Хорев - М.: НПЦ «Аналитика», 2008. - 436 с.
2. Яремчук Ю.Є., Катаєв В.С., Гижко М.Ю. Можливості практичного застосування тепловізорів у питаннях захисту інформації. — "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" — 2016 — №1.- С.99-105.

# СТРУКТУРНО-АКУСТИЧНА МОДЕЛЬ СИСТЕМИ ПОВІТРЯ-СКЛЯНА ПЛАСТИНА-ПОВІТРЯ

*Галина Кеньо*

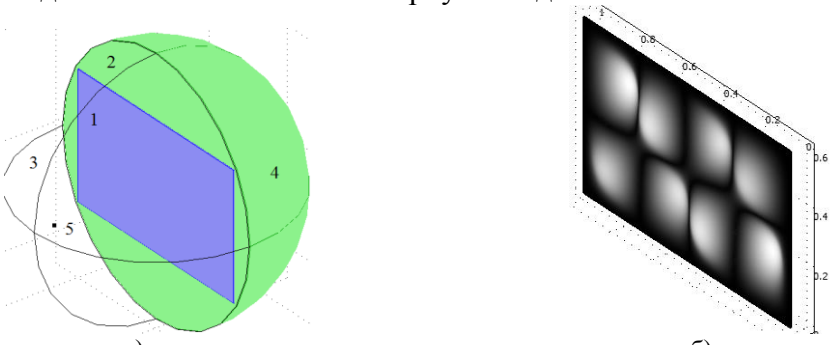
Національний університет «Львівська політехніка», м. Львів, Україна

**The paper is devoted to the research of transmission of an acoustics wave through a glass plate with the help of physical and technical modeling system COMSOL Multiphysics. Structural-Acoustics model of system "air-glass plate-air" was created. Glass plate's eigenfrequences and modes were calculated, the response of plate to external excitation, and resonance frequences modes was studied. The values of average vibration displacement of a glass plate that occurs under the influence of the incident sound wave were calculated.**

**Keywords: structural-acoustics interaction, response of plate to external excitation, resonance and eigenfrequences and modes.**

Проблема проходження звукових хвиль крізь тонкі перегородки найчастіше піднімається в будівельній акустиці у зв'язку з використанням щораз легших конструкцій, які недостатньо захищають від сторонніх шумів. Особливо це стосується резонансних частот, на яких вібрації набувають великих значень і призводять до значного зниження звукоізоляції [1,2]. У сфері технічного захисту інформації важливість взаємодії акустичних хвиль з будівельними конструкціями полягає в оцінюванні вібрацій та ізоляційних властивостей у всьому звуковому діапазоні (особливо в ділянці нижніх частот) з метою прогнозування виникнення та усунення акустичного та віброакустичного каналів витоку. Скляне вікно є найуразливішою конструкцією, через яку намагаються отримати конфіденційну інформацію, що зумовлює актуальність створення структурно-акустичної моделі системи «повітря-скляна пластина-повітря», застосування якої дозволяє досліджувати явища, що в ній відбуваються, а також отримувати важливі для фахівців дані про величини вібрацій та звукоізоляційні характеристики вікон.

Скляна пластина в моделі займає область 1 (рис.1а), і продовжується абсолютно жорсткою перегородкою 2. Ця конструкція розділяє два повітряні півпростори 3 і 4, в одному з яких розташоване джерело звуку 5. Обчислення відгуку скляної пластини на зовнішнє збудження проводилось шляхом моделювання акустичного поля в середовищі фізико-технічного моделювання COMSOL Multiphysics в діапазоні частот 50 – 500 Гц.




а) б)

Рис. 1. 3D-геометрія системи «повітря-скляна перегородка-повітря» (а): скляна пластина (1), відбиваюча поверхня (2), повітряні півпростори (3,4), джерело звуку (5) та власна мода (3 1) на частоті 437.5 Гц (б)

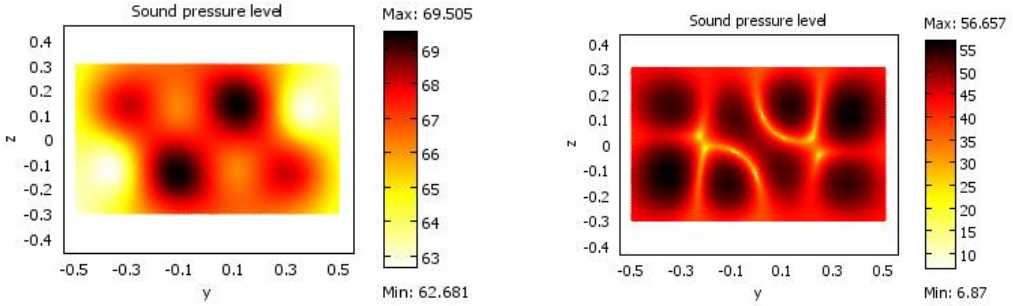
Джерело звуку породжує хвилі акустичного тиску. Перегородка, яка є продовженням жорстко закріпленої скляної пластини, відбиває хвилі без поглинання, повітряне середовище обмежене двома півсферами, на межах яких задавалась гранична умова випромінювання. Для зв'язку хвилі акустичного тиску зі склом у режимі напружено-деформованого твердого тіла на поверхнях скла встановлюється навантаження тиску**,** а для зв'язку частотного відгуку скла з проблемами акустики, використовується гранична умова нормального прискорення [3].

Обчислення, проведені на прикладі скляної пластини розміром 1?0,6?0,005 м$^3$, показали, що у досліджуваному діапазоні частот вона має 11 власних частот та мод (табл.1). Власна мода з індексом (3 1) на частоті 437.5 Гц подана на рис.1б.

Таблиця 1

| Індекс моди, ($m_1$, $m_2$) | Резонансна частота, ($f$) | Індекс моди, ($m_1$, $m_2$) | Резонансна частота, ($f$) | Індекс моди, ($m_1$, $m_2$) | Резонансна частота, ($f$) |
|---|---|---|---|---|---|
| 0 0 | 88.4 | 1 1 | 267.7 | 3 1 | 437.5 |
| 1 0 | 128.4 | 3 0 | 298.9 | 0 2 | 451.4 |
| 2 0 | 198.8 | 2 1 | 337.3 | 1 2 | 489.8 |
| 0 1 | 228.8 | 4 0 | 430.5 | | |

Для виявлення реакції скляної пластини на зовнішнє збудження, нами досліджувався рівень звукового тиску на поверхнях скляної пластини на власних (рис.2) і звичайних частотах.




а) б)

Рис.2. Рівень звукового тиску на поверхнях скляної пластини на власній частоті 437,5 Гц: зі сторони джерела звуку (а) та з протилежної сторони (б)

Дослідження показали, що на власних частотах внаслідок значних вібрацій на зовнішній поверхні формується область високого акустичного тиску, і звук інтенсивно перевипромінюється.

Для отримання даних, необхідних для кількісного оцінювання ймовірності перехоплення інформації, обчислювались спектри усередненої амплітуди зміщення та звукоізоляції пластини (рис.3).

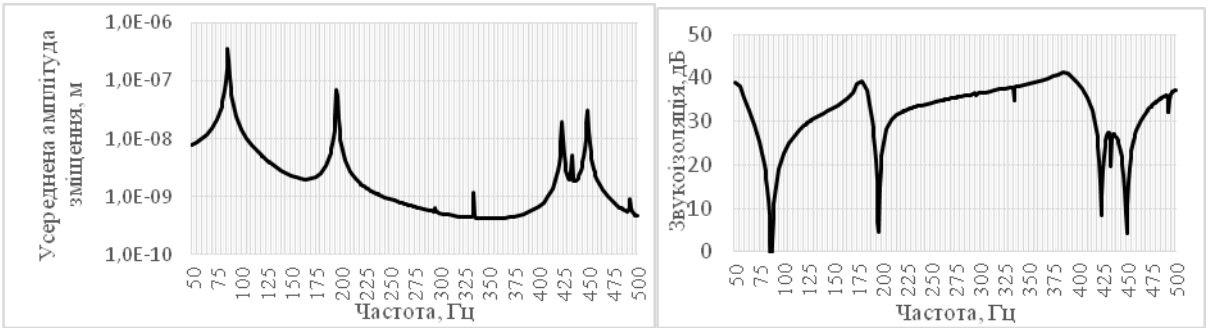



Рис.3. Спектр усередненого зміщення (а) та звукоізоляції скляної пластини

Таким чином, моделювання акустично-структурної взаємодії дає змогу визначити звукоізоляцію скляної пластини та частоти її акустичної прозорості, а також за відомих місця розташування та потужності джерела звуку оцінити ймовірність перехоплення інформації сучасними засобами акустичної розвідки.

## Література


1. Filippi, Paul J.T. Vibrations and acoustic radiation of thin structures : physical basis, theoretical analysis and numerical methods. – UK, ISTE Ltd, USA, John Wiley & Sons, Inc. 2008 – 288 p.
2. F. Fahy, P. Gardonio. Sound and Structural Vibration. Radiation, Transmission and Response. – Elsevier Ltd., 2007. – 633 p.
3. Acoustics Module User's Guide © COPYRIGHT 1994–2008 by COMSOL AB. Version: September 2008 COMSOL 3.5. – 272 p

# МЕТОД ІДЕНТИФІКАЦІЇ КРИТИЧНИХ ЗНАЧЕНЬ ХАРАКТЕРИСТИК ДЛЯ ВИЯВЛЕННЯ АГЕНТІВ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

*Євгеній Крайній, Лілія Нікіфорова*

Вінницький національний технічний університет, м. Вінниця, Україна

**The report is examined the existing model of identifying threats to information security agents using critical parameters; are defined early achievements and prospects of the development direction.**

**Keywords: threat, agent, access control, motivation, critical parameters.**

Для успішного функціонування будь-якого виробництва і будь-якої компанії, незалежно від послуг і товарів, які вона надає, необхідні ефективно працюючі і кваліфіковані кадри, які здатні зберегти конфіденційність, цілісність, доступність інформації, що пов'язана з їх діяльністю. Технічні та програмні засоби не здатні повною мірою захистити від витоку інформації, оскільки неможливо повністю виключити людський фактор.

Мотивація співробітників займає одне з центральних місць в управлінні персоналом, оскільки вона виступає безпосередньою причиною їхньої поведінки. Орієнтація працівників на досягнення цілей організації, по суті, є головним завданням керівництва персоналом. Тому, саме дослідження критичних кількісних характеристик респондентів дозволяє виявляти агентів загроз безпеки підприємства.

Кількісних показників виявлення агентів загроз інформаційної безпеки порівняно мало. Більшість показників опирається на психологічні характеристики особистості, які можуть бути вдало приховані під час дослідження.

У сучасних умовах проблемою мотивації є недосконаліть мотивації на підприємствах, недостатнє фінансування заходів, спрямованих на удосконалення мотивації персоналу, а також те, що на підприємствах не приділяють належної уваги мотивації.

Моделі [1,2] розрахунку рівня вмотивованості співробітників підприємства на основі модифікації соціометричних показників шляхом додаткового врахування кількісних показників із Internet та соціальних мереж дає можливість не лише кількісно оцінити рівень вмотивованості співробітників щодо збереження конфіденційності інформації, але й попередити виникнення можливих загроз зі сторони персоналу щодо забезпечення інформаційної безпеки на підприємстві.

Дана робота описує дослідження з метою виявлення агентів загроз конфіденційності інформації на підприємстві.

## Література

1. Нікіфорова Л. О. Метод розрахунку рівня вмотивованості співробітників щодо збереження конфіденційності інформації в задачах інформаційної безпеки / Л. О. Нікіфорова // Інформаційна безпека. – 2014. - №4(16). – С.175-182.
2. Нікіфорова Л. О. Узагальнена модель оцінки рівня вмотивованості агентів загроз в задачах забезпечення безпеки об'єктів на мікро та макрорівнях/ Л. О. Нікіфорова // Сучасний захист інформації. – 2015. – №4. – С.71–76.

## ЦИФРОВЕ ДИТИНСТВО: СОЦІАЛІЗАЦІЯ І БЕЗПЕКА

*Наталія Кухарська, Христина Задорожна*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In the thesis are considered the main types of children activity in the virtual Internet as a manifestation of online socialization. And also are defined the threats to security caused by the Network with its properties and functions of a social institution.**

**Keywords: Internet, social network, threat, children, information security.**

Соціальним мережам в Інтернеті вже більше 20 років: перша мережа Classmates з'явилася ще у 1995 році і, що цікаво, існує досі. Однак, справжній мережний бум, почався дещо пізніше і був спричинений появою таких соцмереж як LinkedIn, Myspace і Facebook. Саме, через шалену популярністю соціальних мереж нинішнє століття називають мережним. Так, лише у Facebook на сьогодні зареєстровано понад півтора мільярда людей. Згідно з правилами цієї соцмережі її користувачі повинні бути старші 13 років. Позаяк, ці обмеження не є перепоною для дітей, охочих зареєструватися у Facebook. З притаманним їхньому віку завзяттям вони проникають в усі закапелки мережі Інтернет, обходять встановлені заборони. Тим більше, що це зовсім не складно. Для того щоб завести свій профіль у соцмережі досить вказати номер мобільного телефону. Можливо, навіть у зв'язку з цим, дорослі доволі часто не знають, що їхнє малолітнє чадо є завсідником соцмереж.

Спектр базових потреб сучасної дитини доволі широкий. Крім життєво необхідних (фізіологічних і безпеки), важливе місце займають соціальні потреби (спілкування, любов, визнання), потреби, пов'язані з розвитком особистості (пізнання, розуміння, самореалізація).

Велику частину перелічених запитів діти задовольняють, використовуючи широкі можливості Інтернету. Причому, у Мережі це можна зробити набагато швидше, ніж у реальному житті. В Інтернеті підліток діє незалежно від батьків чи ще кого-небудь, що дає йому змогу реалізувати одні із найбільш важливих соціальних потреб цього віку – потреби в самостійності й автономії.

Онлайн-соціалізація проявляється через різні види Інтернет-активності.

Найбільшу перевагу діти надають такому виду Інтернет-діяльності як комунікативна. Багатьом тинейджерам психологічно і технологічно простіше спілкуватися у Мережі, ніж телефоном чи очно. Соціальні мережі дають змогу відчути їм приналежність до різних спільнот, створюють умови для самопрезентації, виконують функцію "сортування" кіл спілкування. Вони є своєрідним інструментом формування і накопичення соціального капіталу. У травні 2016 року Український центр вивчення громадської думки населення «Соцінформ» та MyMedia презентували результати досліджень, у рамках яких вивчалися тенденції використання українськими школярами медіа, соцмереж [1]. Як з'ясувалося, 85 % дітей з усієї України щодня(!) використовує соцмережу "Вконтакте". За "Вконтакте" слідує Instagram (25 %). А, ось, уже згадуваним Facebook (8 %), а також Twitter (8 %) українські діти не дуже захоплюються.

Мережею Інтернет, і зокрема соцмережами, школярі користуються з начальною метою під час підготовки домашніх завдань. Як до цього ставитися? З одного боку, діти використовують соцмережі для взаємодії з однокласниками і вчителями; з другого боку – відволікаються на них від уроків.

Результати опитування американського центру Common Sense Media (2015 р.) показали, що під час виконання домашніх завдань соціальні мережі використовує постійно відносно невелика кількість молодих людей: 1 % молодших підлітків і 6 % старших. У той же час, 12 % молодших і половина (50 %) старших підлітків стверджують, що вони час від часу, але все ж таки користуються послугами соціальних мереж під час підготовки домашнього завдання. Кожний п'ятий підліток (21 %) повідомив, що робить це

доволі часто. Більшість підлітків (55 %), які під час виконання домашніх завдань відвідують соціальні мережі, відзначили, що це не впливає на якість їх виконання [2].

Ще один різновид Інтернет-активності. Доволі багато дітей користуються сучасними мережевими технологіями з метою розваг: скачують музику і фільми, дивляться відео онлайн, користуються обмінниками файлів, грають в Інтернет-ігри самі з собою, з комп'ютером або з іншими людьми, викладають музику, відео або фотографії для спільного їх використання.

Можливість проявити самостійність і відчути себе дорослим, яку створюють соцмережі, для сучасного тинейджера є вкрай необхідною. У той же час, молоді люди, захоплені безмежними можливостями сучасних технологій, через відсутність достатнього життєвого досвіду часто самостійно не можуть розгледіти ризиків і загроз Мережі і в результаті потрапляють до когорти найбільш вразливих її користувачів.

Мережа Інтернет (у тому числі соціальні мережі), як нове середовище спілкування, породили невідомі до ери інформаційних технологій феномени. Вони представлені у широкому діапазоні і різноманітному калібрі. Розглянемо їх.

- Facebook-депресія – негативний результат впливу на психіку людини контактів у соціальних мережах. Люди, як правило, виставляють у соцмережах ті фотографії і новини про себе, які представляють їх у вигідному світлі. Через це у когось з їхніх друзів чи знайомих може скластися враження, яке і стане причиною депресії, що їхнє життя у порівнянні з чужим не настільки яскраве і насичене.
- Феномен Інтернет-залежності. Вчені розглядають такі основні види Інтернет-залежності, як нав'язливий веб-серфінг (безперервне безцільне блукання Всесвітньою павутиною, пошук інформації), жадоба віртуального спілкування і віртуальних знайомств (постійна участь у чатах, веб-форумах, надмірна кількість знайомих і друзів у Мережі, вражаючі обсяги листувань), like-залежність, залежність від online-ігор, нестримна марнотратність (непотрібні покупки в Інтернет-магазинах, гра по Мережі в азартні ігри), пристрасть до перегляду фільмів через Інтернет, кіберсексуальна залежність (нав'язлива тяга до відвідування порносайтів).
- Номофобія (від англ. nomobilephobia) – почуття страху опинитися без мобільного зв'язку, в тому числі без Інтернету.
- Ефект "google" – легше знайти, ніж запам'ятати. Молоді люди розглядають пошукові системи, як продовження свого інтелекту, а не як окремий інструмент отримання потрібної інформації.
- Селфоманія (від анл. self – сам, себе) – розлад психіки, який характеризується постійним (не менше 5 разів на день) бажанням фотографувати себе і викладати світлини в соціальній мережі, аби, на думку фахівців, компенсувати відсутність самоповаги.
- Інтернет-меми або медіавіруси – інформація, що немає ніякого корисного змісту, у той же час, викликає спонтанне зацікавлення у користувачів Мережі і набуває шаленої популярності.
- Спам (від. англ. spam) – це масове, неперсоніфіковане розсилання, з використанням спеціальних програм, комерційної, політичної та іншої реклами або іншого виду повідомлень людям, які не проявляли жодного бажання їх одержувати.
- Феномен "незнайомі друзі". До "незнайомих друзів" відносять користувачів соцмереж з, так званого, кола друзів, з якими діти ніколи не зустрічалися у реальному житті, у той же час, надали їм доступ до своєї персональної інформації, здійснюють спільну з ними діяльність в он-лайні, підтримують регулярну і близьку комунікацію і не відкидають можливість особистої зустрічі.
- Різні вияви онлайн-агресії:

- Флейм (від англ. flame – вогонь, полум'я) – вербальна агресивна реакція, що передбачає зумисне відходження від основної її теми і недотримання принципів конструктивної дискусії.
- Флуд (від англ. flood – повінь) – розміщення однотипної інформації на декількох гілках форуму чи різних форумах, одної повторюваної фрази, символів, однакових графічних файлів або просто коротких безглуздих повідомлень на веб-форумах, в чатах, блогах.
- Тролінг (від англ. trolling – ловля на блешню) – зумисна агресивна поведінка, яка виражається через розміщення в Інтернеті (на форумах, у дискусійних групах та ін.) підбурюючих, саркастичних, провокаційних або сатиричних повідомлень з метою викликати взаємні образи, конфлікти між іншими користувачами, втягнути їх в конфронтацію.
- Хейтерство (від англ. hate – ненависть) – демонстрація з використанням наклепу, провокацій і лицемірства у мережі Інтернет упередженого, вкрай негативного відношення (несприйняття і ненависті) до особи, як правило, більш успішної.
- Кріпіпаста (від англ. creepy – моторошний, copy-paste – копіювати і вставляти) – поширюваний мережею Інтернет контент жанру жахів у вигляді розповідей, легенд, зображень, анімацій, мета якого викликати відчуття страху у користувачів. Головні сюжети – вбивства, самовбивства, потойбічні явища.
- Кібербулінг (від англ. kiber – віртуальне, bullying – цькування, залякування, приниження) – агресивні зумисні, неодноразово повторювані, довготривалі дії, що здійснюються групою осіб чи однією особою з використанням електронних форм контакту, як правило, стосовно жертви, яка не вміє себе захистити, з метою викликати у неї страх і підкорити собі.

- Секстінг (від англ. "sex" – секс, "texting"– відправлення текстових повідомлень) – розсилання повідомлень непристойного змісту, як правило, надто відвертих світлин, засобами мобільного телефону або через Інтернет.
- Кібергрумінг (від анл. cybergroomind/childgrooming) – спроба налагодити в соціальних мережах контакт з дитиною з наміром схилити її до статевих стосунків, а також спонукання дітей за допомогою Інтернету до сексуальних дій.

Сьогодні ІТ-індустрія пропонує доволі велику кількість різноманітних способів, у тому числі з використанням технічних засобів, які дають змогу контролювати і регламентувати онлайн-життя дітей. Для того щоб діти жили у комфортному і безпечному середовищі, у тому числі віртуальному, ми, дорослі, маємо прискіпливо слідкувати за тим, як вони використовують соцмережі, як спілкуються, з ким взаємодіють, кому довіряють, а також вчасно попереджати про небезпеки, які чатують на них у інформаційному просторі Інтернет-мережі. Маємо переконання: лише скоординовані дії усіх членів суспільства, у тому числі дітей, зможуть подолати небажані наслідки невідворотної на сьогодні тенденції масової кіберсоціалізації.

## Література


1. Як школярі використовують медіа: соціологічне дослідження «Соцінформ» та MyMedia [Електронний ресурс]. – Режим доступу : http://osvita.mediasapiens.ua/mediaprosvita/kids/yak_shkolyari_vikoristovuyut_media_sotsiologichne_doslidzhennya_sotsinform_ta_mymedia
2. Соцсети выходят из моды [Электронный ресурс] // Дети в информационном обществе. – 2016. – № 2. – С. 34-39. – Режим доступа : http://detionline.com/assets/files/journal/24/24_web-(2).pdf

# ДОСЛІДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО ВИКОРИСТОВУЄ СТЕГАНОГРАФІЧНІ МЕТОДИ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В НЕРУХОМИХ ЗОБРАЖЕННЯХ

*Андрій Лагун, Володимир Пилипенко*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In this paper was analyzed the software, which uses steganographic techniques to hide information in an image and was realized example the attack of compression method to the filled container**

**Keywords: steganography, container, image, LSB, attack, PSNR**

Завдання захисту інформації від несанкціонованого доступу вирішувалося в усі часи історії людства. Для вирішення цього завдання існують два основних напрями: криптографія, яка приховує вміст повідомлення за рахунок шифрування, й стеганографія, в якій приховується сам факт існування таємного повідомлення.

На цей час, завдяки бурхливому розвитку інформаційних технологій особливу популярність одержала цифрова стеганографія для забезпечення захисту інформації, зокрема та частина стеганографії, яка використовує для приховування конфіденційної інформації графічні зображення, що передаються по обчислювальних мережах. Однак через невисоку оперативність та інформаційну ефективність, складність процесів обробки, синхронізації й вбудовування прихованої інформації в зображення-контейнери у вигляді цифрових зображень, дослідження відомих і розроблення нових стеганографічних алгоритмів є актуальною задачею.

Варто також зазначити, що зберігаючи таємницю листування, стеганографія створює умови для виникнення неконтрольованих інформаційних каналів, що дозволяє хакерам поширювати віруси через ці канали. Тому прогрес в області стеганографії може істотно змінити існуючі підходи до проблем інформаційної безпеки.

Відомо, що оцифровані кольорові зображення займають багато місця на диску, тому для зменшення їхнього розміру ці зображення зазвичай стискають. Існують алгоритми стиснення без втрат, за допомогою яких створюють файли цифрових зображень з розширеннями *bmp, png* і *gif*, і алгоритми стиснення з втратами, до яких належить стандарт *JPEG*. Стандарт *JPEG* за рахунок внесення в зображення непомітних для людського ока змін може стиснути зображення більше, ніж в 40 разів.

Особливість використання стеганографічних методів для зображень в *JPEG* форматі полягає в тому, що традиційні методи приховування інформації в зображеннях, наприклад метод заміни молодшого значущого біта (*LSB*), для формату стиснення з втратами не придатний, оскільки всі мінімальні зміни кольорів будуть вирізані фільтром шуму. Тому для стеганографічного використання *JPEG*- файлів можливі такі підходи:

– дописування прихованої інформації здійснюється в кінці файлу;

– приховування інформації відбувається в не основних даних файлу;

– приховування інформації використовує таблиці;

– приховування інформації здійснюється в частини між блоками даних файлу.

Більшість реалізованих програмних продуктів використовують метод заміни найменшого значущого біта. Цей метод дозволяє приховати інформацію шляхом заміни молодших бітів зображення на біти прихованої інформації. Відмінність між порожнім і заповненим контейнерами має бути не відчутна для органів людського зору.

Протягом досліджень було проведено дослідження програмних продуктів, що приховують інформацію різного вигляду в нерухомих зображеннях.

Найпростішими є програми, що працюють з командного рядка.

Програма *WNS* (білий шумовий шторм) передбачає попереднє шифрування прихованого повідомлення перед вбудовуванням у контейнер. Програма використовує

приховування інформації в частотній області зображення, а саме в спектральних коефіцієнтах. Основним недоліком *WNS* є завищені вимоги до розмірів контейнера.

Інша програма – *JSteg* призначена для приховування інформації у файлах формату *JPEG*. Ця програма використовує для приховування інформації спектральні коефіцієнти дискретного косинусного перетворення. Коефіцієнти, які дорівнюють нулю або одиниці, не змінюються, а інші можуть бути використані для вбудовування в них одного біта прихованої інформації з використанням алгоритму заміни найменшого значущого біта.

Розглянемо програми, що працюють під операційною системою *Windows.*

Однією з найпростіших програм є *Hide-in-Picture*, яка дозволяє закодувати та приховати файли у зображеннях. Ця програма створює додаткові записи колірної палітри, тому вихідне зображення початково має 32 кольори, а згенероване зображення з прихованою інформацією доповнює це число до 256 за рахунок створення нових кольорів.

Пакет прикладних програм *S-Tools* містить програми, що обробляють зображення у форматах *GIF, BMP, JPEG*, а також звукові *WAV*-файли. Крім того, пакет дозволяє шифрувати інформацію перед вбудовуванням. Під час приховування порожній контейнер (файл зображення) перетягують у вікно програми, потім у це ж вікно перетягують файл із даними будь-якого формату, вводять пароль, вибирають алгоритм шифрування і отримують заповнений зашифрований контейнер. Для кращого маскування прихованої інформації використовують строкаті зображення з великою кількістю півтонів і відтінків (наприклад букет польових квітів).

Для досліджень як контейнер було використано зображення на рис.1, а як приховану інформацію – зображення герба України (рис. 2). Спочатку здійснювалося вбудовування герба в контейнер, потім заповнений контейнер стискався за допомогою програми *WINRAR* (відбувалася атака на стегозображення методом стиснення). В результаті проведеної атаки отримано зображення, яке візуально не відрізняється від початкового.

Рис. 1. Початкове зображення

Рис. 2. Приховане зображення

Для оцінки якості приховування інформації в зображенні використовується коефіцієнт пікового відношення сигнал-шум (*PSNR*), що показує відмінність між порожнім і заповненим контейнером із зображенням і визначається таким чином:

$$PSNR = 10\lg\left(\frac{C_{\max}^2}{MSE}\right) \tag{1}$$

де $C_{\max}$ – максимальне значення піксела; *MSE* – середньоквадратична похибка:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \tag{2}$$

де *x* і *y* координати зображення, *M* і *N* – розміри зображення, $S_{xy}$ є сформоване зображення з прихованим вмістом; $C_{xy}$ – початкове зображення. Чим більше значення коефіцієнта пікового відношення сигнал-шум, тим вища якість приховування.

## Література


1. Хорошко В. О. Основи комп'ютерної стеганографії : навчальний посібник для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. – Вінниця : ВДТУ, 2003.
2. Конахович Г. Ф. Компьютерная стеганография / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

# СТЕГАНОГРАФІЧНИЙ ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ МЕТОДОМ КУТТЕРА-ДЖОРДОНА-БОСЕНА

*Наталія Кухарська, Дмитро Прокопечко*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The problem of information security through its steganographic hiding in a graphics container. Improving the method of Kutter-Jordan-Bossen that performs steganographic implementation of spatial data in raster image area. The improvement is the introduction of a method of additional rules that eliminate the problem of retrieval. The research results improved method in developed among its implementation.**

**Keywords: steganography, data hiding, data protection, introduction of data, spatial region.**

У зв'язку з бурхливим розвитком комп'ютерних технологій і активним проникненням їх у всі сфери людського буття однією з актуальних проблем на сьогодні є проблема захисту інформації.

Стеганографія як самостійна теоретично-прикладна наука дає змогу вирішувати такі важливі завдання інформаційної безпеки як захист авторських прав на мультимедійні дані від піратства за допомогою використання, так званих, цифрових водяних знаків, а також захисту конфіденційної інформації від ознайомлення сторонніх осіб під час обміну нею шляхом організації скритого каналу передачі даних.

На відміну від криптографії, що приховує вміст секретного повідомлення, стеганографія приховує сам факт його наявності. Таким чином, під поняттям приховання існування інформації з точки зору стеганографії розуміється не тільки неможливість виявлення в перехопленому повідомленні схованих даних, але й взагалі унеможливлення виникнення будь-яких підозр з цього приводу.

Шифрування конфіденційної інформації проблему неавторизованого доступу до неї повністю не вирішує, так як наявність зашифрованого повідомлення вже саме по собі привертає увагу “супротивника”. Перехопивши криптографічно захищений файл, він неодмінно зацікавиться ним й докладе максимум зусиль, щоб розшифрувати його. У зв’язку з цим, для передачі секретної інформації незахищеними каналами зв’язку сьогодні активно використовують також стеганографічні методи. Стеганографія не замінює, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі конфіденційного повідомлення, а якщо приховане повідомлення до того ж зашифроване, то воно матиме ще один, додатковий, рівень захисту.

Загальною рисою стеганографічних методів є те, що приховуване повідомлення вбудовується в інформаційно непримітний об'єкт (контейнер), який згодом відкрито пересилається адресатові.

Найбільш перспективним напрямком стеганографії на сьогоднішній день є цифрова стеганографія – напрямок комп'ютерної стеганографії, заснований на прихованні інформації в цифрових об'єктах, що початково мають аналогову природу (зображення, відео, звук). У зв'язку з розвитком апаратних засобів обчислювальної техніки й величезною кількістю каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації у файлах, обчислювальних мережах і т. п.

Метою роботи є розроблення комп’ютерних програм вбудовування/видобування секретної інформації для її зберіганні або передачі відкритими каналами зв'язку й дослідження стійкості побудованої стеганосистеми залежно від кількості прихованої інформації й особливостей самого процесу вбудовування.

Згідно алгоритму методу Куттера-Джордана-Боссена (КДБ) [5] конфіденційна інформація вбудовується в канал синього кольору зображення, що має RGB-кодування. Канал саме цього кольору обраний авторами не випадково, а виходячи з тих міркувань, що зорова система людини є найменш чутливою до змін внесених в синю складову.

Алгоритм методу КДБ ґрунтується на використанні методів екстраполяції (прогнозування) випадкових сигналів.

Екстраполяція – це метод, згідно якого результати отримані із спостережень над однією частиною деякого явища поширюються на його іншу частину. У більш вузькому сенсі – це визначення за рядом даних функції інших її значень поза цим рядом. У процесі видобування секретного біту, отримувачу необхідно передбачити початкове значення немодифікованого пікселя на основі значення декількох сусідніх пікселів, що розташовані у тому ж рядку і в тому ж стовпці заповненого стеганоконтейнера. Автори методу використовують "хрест" розміром 7x7 пікселів.

Перед вилученням повідомлення з стеганоконтейнера повинні бути відомі:

- заповнений контейнер;
- первинний ключ;
- кількість циклів обчислення координат;
- кількість дублюючих вбудовувань одного біта;
- розмір хреста – кількість пікселів зверху (знизу, зліва, справа) від оцінюваного пікселя.

У роботі використано удосконалення методу КДБ, запропоновані у [2]. Вони полягають у введенні в алгоритм методу додаткових правил, метою яких є усунення проблем видобування даних, що пов'язані з окремими випадками заповнення вихідного контейнера.

За рахунок модифікацій були усунені помилки видобування:

- секретних бітів з одиничним значенням з областей контейнера, в яких пікселі мають максимальне значення по синьому каналу;
- секретних бітів з нульовим значенням з областей контейнера, в яких пікселі мають мінімальне (нульове) значення по синьому каналу;
- секретних бітів з одиничним значенням з областей контейнера, в яких всі пікселі мають чорний колір;
- секретних бітів з областей контейнера, в яких містяться дрібні деталі, що сильно відрізняються за кольором від фону.

Досліджено, що метод стійкий до багатьох відомих видів атак: низькочастотної фільтрації зображення, його компресії, обрізання країв, розмивання.

Розроблені в середовищі Mathcad на основі використання методу КДБ програми можуть бути використані для вбудовування секретних даних у зображення з метою передавання їх загальнодоступними відкритими телекомунікаційними каналами.

## Література


1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М. : Солон- Пресс, 2009 – 272 с.
2. Защелкин К.В. Усовершенствование метода стеганографического скрытия данных Куттера-Джордана-Боссена / Защелкин К.В., Иващенко А.И., Иванова Е.Н. // Радіоелектронні і комп'ютерні системи. – 2013. – № 5. – С. 151-155.
3. Конахович Г.В. Компьютерная стеганография. Теория и практика / Конахович Г.В., Пузыренко А.Ю. – К. : "МК- Пресс"», 2006. – 288 с.
4. Кузнецов О.О. Методи обробки сигналів даних та зображень : навч. посібник / Кузнецов О.О., Кучук Г.А., Семенов С.Г. –.Харків : НТУ "ХПІ", 2011. – 310 с.
5. Kutter M. Digital Signature of Color Images using Amplitude Modulation / Kutter M., Jordan F., Bossen F. // Proc. SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.

# СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕКИ ПІДРОБЛЕННЯ ЕЛЕКТРОННИХ ЛИСТІВ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

*Олексій Максимів, Тарас Рак*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In this paper, we present the first user study on social engineering attacks in mail clients. That is, we discuss and show how attackers, in practice, can abuse some of the things for doing successful attack. Our results demonstrate that social engineering attacks are feasible and effective in practice.**

**Keywords: social engineering, information security, mail spoofing.**

Багато компаній, які думають, що проблему інформаційної безпеки можна вирішити лише за допомогою апаратних і програмних засобів, сильно помиляються. Технології безпеки, яким ми звикли довіряти, - мережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак і інші - малоефективні в протистоянні хакерам, які використовують методи соціальної інженерії (СІ).

Соціальна інженерія являє собою метод несанкціонованого доступу до інформації або системам зберігання інформації завдяки безпосередньої взаємодії з людиною. Так, на думку експертів компанії Gartner, соціальна інженерія представляє найбільшу загрозу для інформаційної безпеки [1]. Зокрема, як зазначає К. Мітнік у своїй книзі, саме «людський фактор по справжньому найслабша ланка в безпеці» [2]. Відповідно можемо стверджувати, що саме експлуатація людського фактору є свідомо більш виграшною стратегією для проникнення всередину організації.

Статистика застосування соціальної інженерії в сучасному світі [3]:

- Соціальна інженерія стала основним вектором нападу в 2015 році;
- Згідно з останнім річним звітом Human Factor, атакуючі в 2015 року залучали жертви шляхом використання електронної пошти, соціальних мереж і мобільних додатків для інфікування систем і викрадання даних;
- Дослідники виявили, що 99,7% шкідливих документів покладалися на соціальну інженерію, а не на автоматизований злом.

Для прикладу спробуємо розглянути один із методів СІ, який має назву e-mail spoofing, тобто метод атаки де підробляється інформація про відправника електронної пошти. Одержувач бачить повідомлення, яке нібито відправлене довіреним лицем, хоча насправді це лист від зловмисника.

Проводячи дослідження з цього приводу мною було виявлено, що найбільш вражені саме мобільні почтові клієнти. Для прикладу спробуємо використати певні методи підроблення адреси відправника. На рис. 1 наведено надзвичайно простий, проте доволі ефективний приклад підроблення електронної адреси, коли зловмисник в полі ім’я вказує «admin@ldubgd.edu», а в полі фамілія «.ua». Поштові клієнти в полі відправника відображають лише ім’я та фамілію відправника, що дуже похоже на оригінал відображений знизу.

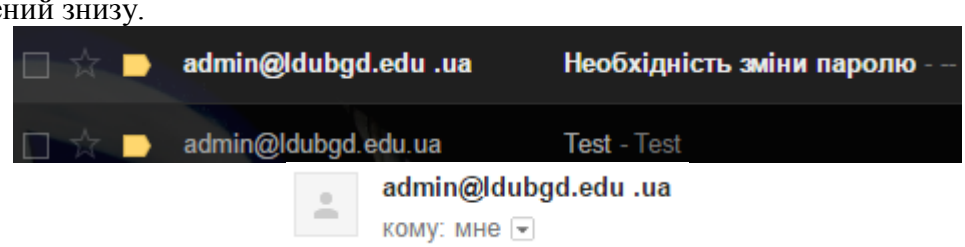



*Рис. 1 Приклад можливого листа від зловмисника та лист-оригінал для порівняння знизу*

Звичайно ж існують більш ефективніші засоби підроблення електронних адрес. Так, на рис. 2, 3 наведено приклад підроблення електронної адреси відправника за допомогою додатку SimpleEmailSpoofer. Можемо спостерігати, що поштовий сервіс gmail видав попередження про можливість загрози, проте мобільний додаток ніяких попереджень не містить. Враховуючи те, що нам за допомогою SMTP-команд вдалося змінити заголовок «Reply-To:» (автозаповнення адреси отримувача на необхідний нам), то ситуація стає критичною.

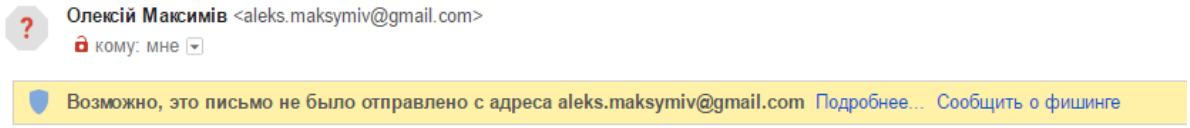



*Рис. 2 Приклад листа з підробленим електронним адресом відправника у поштовому клієнті Gmail.*

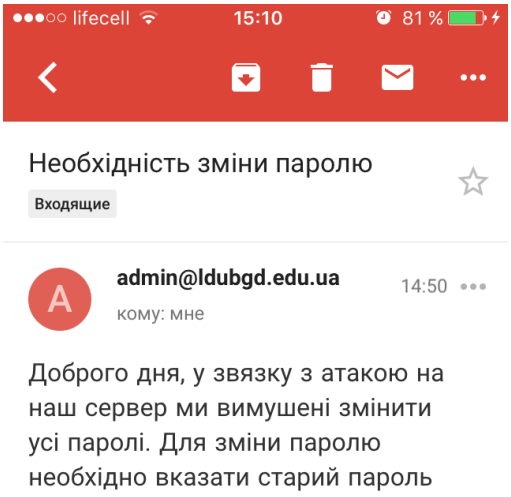



*Рис. 2 Приклад листа з підробленим електронним адресом відправника у мобільному поштовому клієнті Gmail.*

Так, нами було проведено експеримент який полягав у відправленні 5-ом різним людям електронного листа з підробленими адресами. В двох листах міститься прохання про надання паролю до електронної пошти, ще в трьох листах – документ з розширенням .doc, який містить в собі виконуваний файл. В результаті даних експериментів усі люди запустили виконуваний файл або надали паролі від електронної пошти (в залежності від змісту листа). По завершенню експерименту всі були попереджені про можливість такої загрози та змінені паролі.

Отже узагальнюючи вищесказане, можемо стверджувати, що загроза з боку соціальної інженерії була, є і залишатиметься в подальшому. Саме тому її необхідно мінімізувати використовуючи не лише програмно-апаратні засоби, а головним чином працюючи щільно з персоналом, проводячи навчання співробітників застосуванню політики безпеки і технікам протистояння соціальним інженерам.

## Література


1. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры. – СПб.: БХВ-Петербург, 2014. – 356 с.
2. Митник К., Саймон В. Л. Искусство обмана //М.: Компания АйТи. – 2004. – 360 с.
3. Безмалый В. Атаки социальной инженерии [Електронний ресурс] / В. Безмалый. – 2016. – Режим доступу до ресурсу: http://www.securitylab.ru/blog/personal/bezmaly/275366.php.

# ДОСЛІДЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ГЕНЕРАТОРА ДЖИФФІ

*Володимир Максимович[1], Микола Шевчук[1], Марія Мандрона[2]*

1. Національний університет «Львівська політехіка», м. Львів, Україна
2. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The article presents the results of Jiffy generator estimation with a different number of basic LFSR generators, and different degrees of their polynomials, carried out with the use of NIST statistical tests. The received results allow to optimize the generator parameters at the given parameters of the output pseudorandom sequence.**

**Keywords – pseudorandom generator, protection of information, pseudorandom numbers, statistic characteristics.**

Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових бітових послідовностей (ГПВБП) часто зустрічається в багатьох областях вимірювальної техніки, зокрема, при проектуванні і налагодженні потокових шифрів, та інформаційних технологій. При цьому вимоги до їх технічних характеристик відрізняються у залежності від мети їхнього застосування. Генерування псевдовипадкових послідовностей і перевірка на випадковість згенерованої послідовності є одними з найважливіших проблем сучасної криптології. У сучасних криптосистемах генератори псевдовипадкових послідовностей використовуються для створення ключової інформації і забезпечення параметрів цих систем.

Метою роботи є використання статистичних тестів Національного інституту стандартів і технологій (НІСТ) США для тестування генераторів псевдовипадкових бітових послідовностей на основі генератора Джиффі. Спрощена структурна схема генератора Джиффі наведена на рис. 1 [1]. До його складу входять три регістри LFSR1 – LFSR3 і мультиплексор MUX.

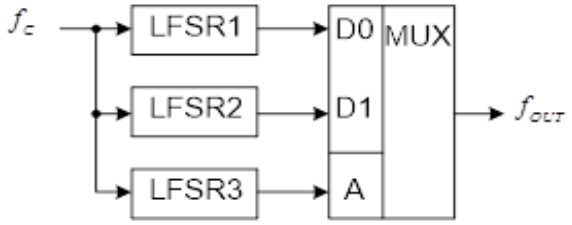



Рис. 1. Спрощена структурна схема генератора Джиффі

Генератор забезпечує перемішування двох імпульсних послідовносте з виходів LFSR1 і LFSR2 під керуванням послідовності з виходу LFSR3. У тому випадку коли значення періодів повторення вихідних послідовностей LFSR1, LFSR2, LFSR3 – $T_{1p}$, $T_{1p}$, $T_{1p}$ попарно взаємно прості числа, період результуючою послідовності дорівнює добутку $T_J = T_{1p} \cdot T_{2p} \cdot T_{3p}$ [1].

Нами були досліджені кілька варіантів побудови генератора Джиффі, при різних структурах LFSR. Для всіх LFSR був вибраний тип матриці $T_1$ і степінь матриці $r$=1. На рис. 2-3 наведені статистичні портрети вихідної послідовності досліджуваних генераторів Джиффі, отримані при випадково вибраних фіксованих початкових установках регістрів.

Таким чином, окремі тести NIST не пройдені. При цьому, в процесі імітаційного моделювання було зафіксовано, що період повторення вихідної послідовності $T_j > 10^9$.

Отже, навіть при малих степенях поліномів, вихідна псевдовипадкова послідовність не проходить один тести NIST.

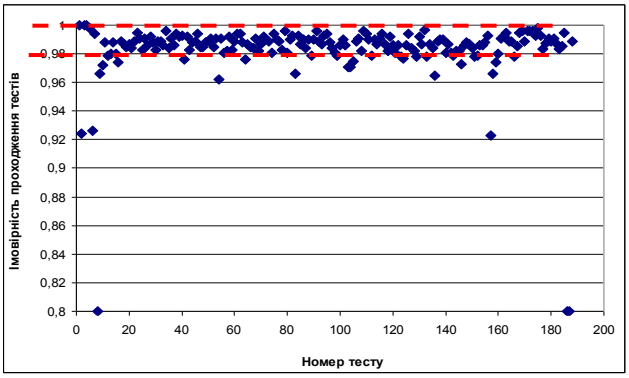



Рис. 2. Статистичний портрет генератора Джиффі (Варіант 1)

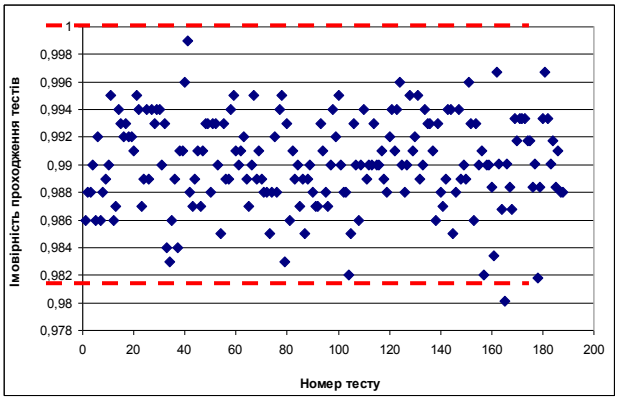



Рис. 3. Статистичний портрет генератора Джиффі (Варіант 2)

Як бачимо з рис. 3, досліджений генератор проходить усі тести NIST STS. Результати тестів знаходяться вище межі 0,98, що згідно вимог статистичного оцінювання за допомогою пакету NIST свідчить про достатню статистичну стійкість. В даному випадку усі тести NIST пройдені, і зафіксовано, що $T_j > 10^9$.

Кількість КЛБ, необхідних для побудови ГПВБП на основі генератора Джиффі, визначається сумарною кількістю розрядів усіх трьох LFSR – $n_1$, $n_2$, $n_3$, плюс один КЛБ для побудови мультиплексора:

$$A_{JIFFY} = n_1 + n_2 + n_3 + 1. \quad (1)$$

Криптографічним ключем ГПВБП на основі LFSR є початкові стани усіх трьох регістрів. Повна множина значень цих станів дорівнює $(2^{n_1} - 1) \cdot (2^{n_2} - 1) \cdot (2^{n_3} - 1)$, а довжина ключа визначається таким чином:

$$C_{JIFFY} = n_1 + n_2 + n_3. \quad (2)$$

Здійснене дослідження ГПВБП на основі генератора Джиффі показало, що навіть, не зважаючи на великий період повторення послідовності, при використанні малих значень степенів твірних поліномів генератори не є повністю статистично безпечними, але із збільшення степенів їх поліномів приводить до підвищення якості генератора. При зафіксованих значеннях цих поліномів ГПВБП на основі генератора Джиффі проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики і криптостійкість.

Отже, такі генератори можна використовувати у криптографії безпосередньо, проте їх можна використати, як елементи складнішої криптографічної системи.

## Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванова, И.В. Чугунков. – М. : НИЯУ МИФИ, 2012. – 400 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

# ДОСЛІДЖЕННЯ АДИТИВНИХ ГЕНЕРАТОРІВ ФІБОНАЧЧІ ДЛЯ ЗАСТОСУВАННЯ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

*Марія Мандрона, Білан Віра*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In the paper was researching modified version of the additive Fibonacci generator and was proposing a new algorithms of generators which have improved statistical characteristics.**

**Keywords: generator of pseudorandom bit sequence, a statistical security, protection of information.**

У сучасному інформатизованому світі псевдовипадкові числа широко використовуються в різних галузях науки і техніки, зокрема, у системах захисту інформації, у сучасних телекомунікаційних системах, у вимірювальній техніці. У сфері захисту інформації псевдовипадкові числа використовують для потокового шифрування каналів зв'язку, генерування ключів для криптосистем, хешування інформації, формування цифрового підпису, а також для створення різного роду зашумлень і т.д. Встановлено, що характеристики систем безпеки залежать від характеристик їх криптографічних підсистем, які визначаються не тільки використаними алгоритмами, але й якісними показниками використаних псевдовипадкових послідовностей. Оскільки безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема стає вразливою [1].

У багатьох працях проводилось дослідження роботи і статистичних характеристик адитивних генераторів Фібоначчі [1-3]. При цьому були виявленні варіанти їх побудови, що забезпечують високу якість, однак більшість з них орієнтовані на програмну реалізацію. В цій роботі акцентується увага на знаходженні нових алгоритмів роботи генераторів Фібоначчі із забезпеченням задовільних статистичних характеристик з можливістю апаратної реалізації, яка б забезпечувала високу швидкодію роботи.

***Метою роботи*** є дослідження модифікованої версії адитивного генератора Фібоначчі та знаходження нових алгоритмів роботи генераторів із забезпеченням задовільних статистичних характеристик з можливістю подальшої апаратної реалізації.

Адитивні генератори Фібоначчі є генераторами псевдовипадкових чисел, однак, вони одночасно можуть функціонувати і як генератори псевдовипадкових бітових послідовностей, що формуються на виходах окремих розрядів регістрів пам'яті [3].

Найбільш простий адитивний генератор Фібоначчі функціонує за алгоритмом:

$$X_{j+1} = (X_j + X_{j-1}) \bmod M, \quad (1)$$

де $X_j$, $X_{j-1}$ – значення чисел у регістрах, M – просте число

На генераторів формуються послідовності псевдовипадкових чисел у відповідності до виразів:

$$X_{j+1} = (X_j + X_{j-1} + a) \bmod m \quad (2)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + a) \bmod m \quad (3)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + X_{j-3} + a) \bmod m \quad (4)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + X_{j-3} + X_{j-4} + a) \bmod m \quad (5)$$

де $m=2^s$, $s$ – кількість двійкових розрядів структурних елементів. Значення змінної a визначається логічним рівнянням [2-3]:

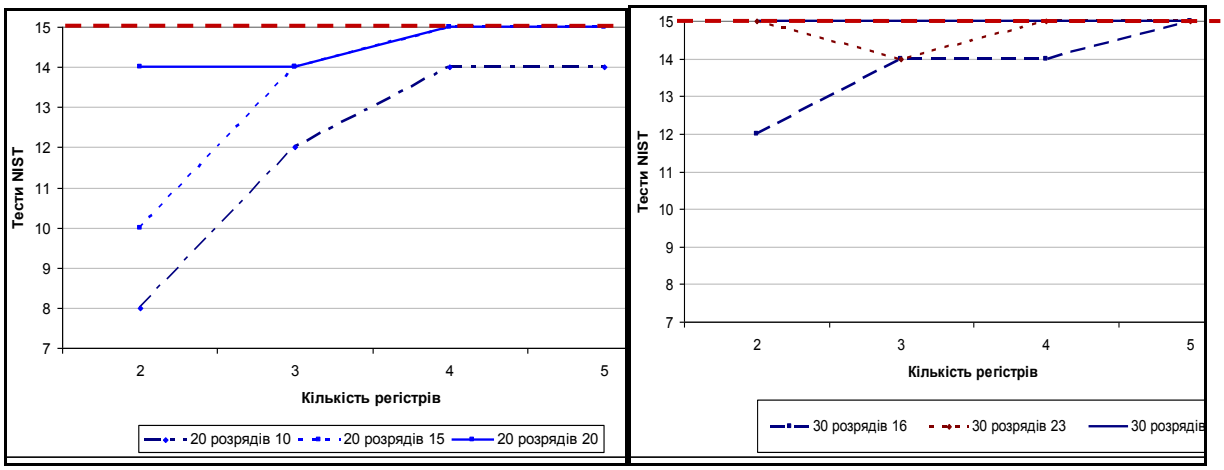
$$a = a_0 \ \text{xor} \ a_1 \ \text{xor} \ a_2 \ \text{xor} \ \cdots \ \text{xor} \ a_z, \quad (6)$$

де s – кількість двійкових розрядів, $a_i$ ($i$ = 0, 1,…, s). Кількість членів рівняння (6) може вибиратись з діапазону 0 … $s$.

Дослідження генераторів здійснювалось з використанням методики NIST. Вважається, що якщо досліджувана послідовність успішно пройшла усі 15 статистичних

тести, тоді робиться висновок, що така послідовність дійсно випадкова, отже її можна використовувати для побудови систем захисту інформації. Якщо ж хоча б один тест не пройдено, тоді вважається, що послідовність не відповідає вимогам випадковості.

На рис. 1*а* і *б* наведено залежності, які відображають вплив кількості структурних елементів на проходження тестів NIST. Кожна послідовність тестувалась 15 тестами [2] на графіках представлено результати тестування (для зручності межу проходження тестів позначено пунктирною лінією). На рис. 1*а* наведено результати дослідження генератора з такими параметрами: кількість двійкових розрядів – 20 біт із трьома варіантами значення змінної *a*, відповідно 10, 15 і 20 біт. На рис. 1*б* дослідження генератора з параметрами: кількість двійкових розрядів – 30 біт із трьома варіантами значення змінної *a*, відповідно 16, 23 і 30 біт.




*а* *б*

Рис. 1. Залежність проходження тестів NIST від кількості структурних елементів

Отже, за результатами проведених досліджень, як висновок можна підсумувати:

✓ збільшення кількості розрядів структурних елементів ГПВП позитивно впливає на статистичні характеристики;

✓ введення логічної схеми у структуру генератора призводить до збільшення періоду повторення генератора, а також до покращення статистичних характеристик згенерованих послідовностей;

✓ використання логічної схеми дає змогу, в якості модуля, використовувати степінь двійки, що дозволить значно спростити апаратну реалізацію генератора Фібоначчі;

✓ якщо кількість членів використаних у рівнянні (6), реалізованого в логічній схемі, є меншою, ніж половина кількості розрядів структурних елементів, то статистичні характеристики вихідних згенерованих послідовностей є незадовільними.

## Література


1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков : под ред. М.А. Иванова. – М. : НИЯУ МИФИ, 2012. – 400 с.
2. Mandrona M.M. Investigation of the Statistical Characteristics of the Modified Fibonacci Generators / M.M. Mandrona, V.M. Maksymovych // Journal of Automation and Information Sciences 10.1615/ JAutomatInfScien.v46.i12.60 pages 48-53.
3. Костів Ю.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / Костів Ю.М., Максимович В.М., Гарасимчук О.І., М.Мандрона М.М. // Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2013. – № 29. – С. 167-174.

# ВИЗНАЧЕННЯ ОСОБЛИВИХ ТОЧОК СКЕЛЕТОНУ ЗОБРАЖЕННЯ ВІДБИТКУ ПАЛЬЦЯ

*Роман Мельник , Тарас Красниця*

Національний університет «Львівська політехніка», м. Львів, Україна

**The known skeletonization algorithm was realized and the skeleton feature points were found. The algorithms were applied to detect the minutiae points in fingerprints such as the ends and branching**

Одним з способів опрацювання зображень є побудова скелетонів [1,2]. Скелетонізація є корисною не стільки для опису компонентів повномасштабного зображення, як для їх співставлення їх окремих частин та різних зображень в цілому. Яскравими прикладами застосування скелетонів є область розпізнавання рукописного та машинописного тексту, розпізнавання *X*, Y хромосом тощо.

Видалення максимального числа пікселів зображення без зміни форми його об'єкту називається скелетонізацією. Іншими словами, після побудови скелетону він повинен допомагати розпізнати саме зображення. Виділяють наступні властивості скелетону: лінії найтонші можливі; всі відрізки зв'язані між собою; каркас розташований в центрі об'єкту спостереження. Приклад зображення букви та його скелетона наведено на рис. 1.

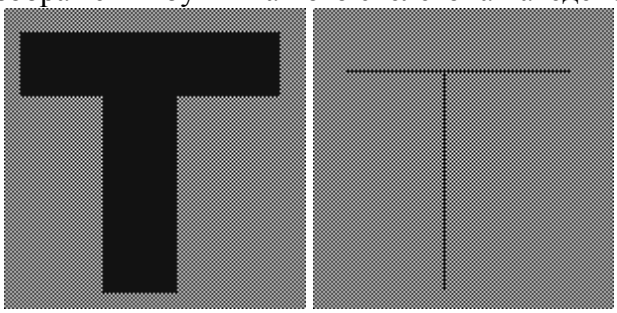


Рис. 1. Приклад скелетона

Розглянемо процес побудови скелетону з допомогою алгоритму Hilditch [http://cgm.cs.mcgill.ca/~godfried/teaching/projects97/azar/skeleton.html], достатньо простому і формалізованому. Алгоритм працює з бінарними зображеннями. Суть алгоритм полягає в ітераційному скануванні матриці пікселів зображення вікном позицій та поступовій заміні чорних пікселів на білі. Вікно алгоритму має розміри 3×3 або 4×4 позицій. Розглянемо версію алгоритму для вікна сканування розмірами 3×3. Тоді всі піксели у вікні пронумеровані від $p_1$ до $p_9$, як це показано на рис. 2.

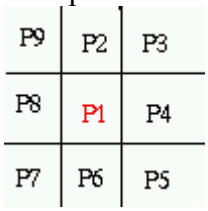



Рис. 2. Нумерація пікселів у вікні сканування.

При скануванні рішення про заміну кольору приймається щодо пікселя $p_1$ (в центрі вікна). Для отримання відповіді на питання чи піксель $p_1$ темного кольору залишати в скелетоні чи його колір поміняти на білий необхідно обчислити дві функції:

$B(p_1)$ = кількість ненульових сусідів для $p_1$

та $A(p_1)$ = кількість пар {0,1} в послідовності $p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_2$.

Найбільш яскравим прикладом застосування скелетонів є опрацювання відбитків пальців. Скелетоном усувають надлишкову інформацію та полегшують доступ до особливих точок, які є предметом дослідження та порівняння. На рис. 3. наведено приклад відбитка пальця та його скелетона.

Рис. 3.. Відбиток пальця та його скелетони

На скелетоні присутні особливі точки, а саме: розгалуження та початки (кінці) ліній. Розгалуження – це точки, в яких сходять три і більше ліній. Для букв "Y" та "X" особливі точки продемонстровано на рис. 4.

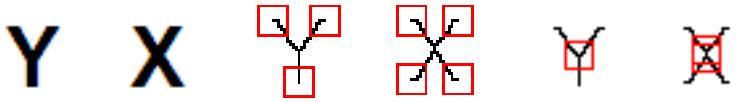



Рис. 4. Особливі точки: кінці ліній та розгалуження

Застосуємо до скелетона відбитку пальця алгоритм знаходження розгалужень та кінців ліній. Отримаємо зображення, на яких квадратами обведені позицій розгалужень (рис. 5,*а*) та кінців ліній (рис. 5.,*б*). На другому скелетоні алгоритмом фіксується також неінформативні початки (кінці) ліній. Вони, зазвичай, не використовуються для формування ознак на розпізнавання.

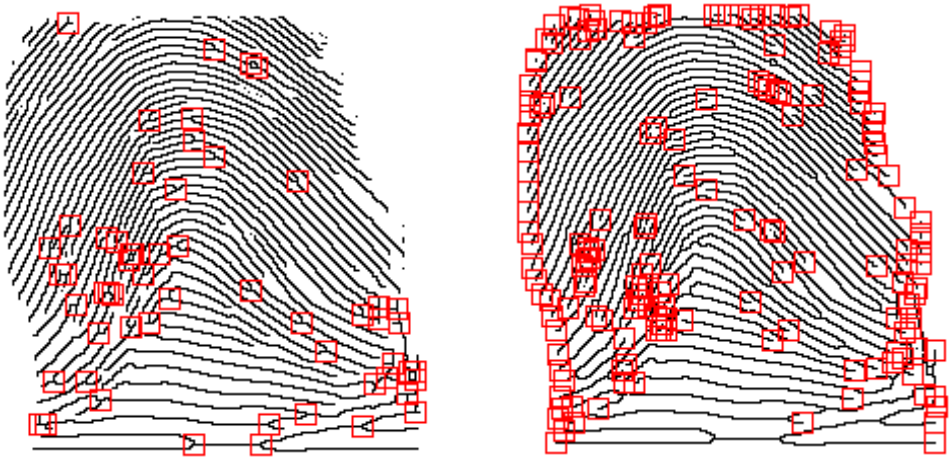


Рис. 5. Знаходження точок розгалужень та кінців ліній

## Література


1. Khalid Saeed, Marek Tabędzki, Mariusz Rybnik, Marcin Adamski, 2010. K3M: A universal algorithm for image skeletonization and a review of thinning techniques International. Journal of Applied Mathematics and Computer Science, vol.20.
2. Danielle Azar, Godfried Toussain, 1997. Hilditch's algorithm for skeletonization, thttp://cgm.cs.mcgill.ca/~godfried/teaching/projects97/azar/skeleton.html

# ІНФОРМАЦІЙНА МОДЕЛЬ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ КІБЕРФІЗИЧНОЇ СИСТЕМИ “IPHONE – WI-FI, BLUETOOTH – ДАВАЧІ”

*Валерій Дудикевич, Галина Микитин, Андрій Ребець*

Національний університет “Львівська політехніка”, м. Львів, Україна

**The complex security system (CSS) information model of the cyber-physical system (CPS) “iPhone – Wi-Fi, Bluetooth – sensors” was considered in the context of threats classes according to the STRIDE method and the structure of security “problem – service – technology”.**

З метою забезпечення інформаційної та функціональної безпеки КФС для виконання ними функціональних задач у різних предметних сферах актуальною проблемою є створення комплексної системи безпеки КФС, яка є методологічним підгрунтям забезпечення необхідного рівня захищеності компонент КФС – кібернетичного простору (КП), комунікаційного середовища (КС), фізичного простору (ФП). У цьому контексті розглянемо інформаційну модель КСБ одного з різновидів кіберфізичних систем “iPhone – Wi-Fi, Bluetooth – давачі” згідно парадигми та концепції побудови багаторівневої комплексної системи безпеки КФС [1] (рис. 1.).

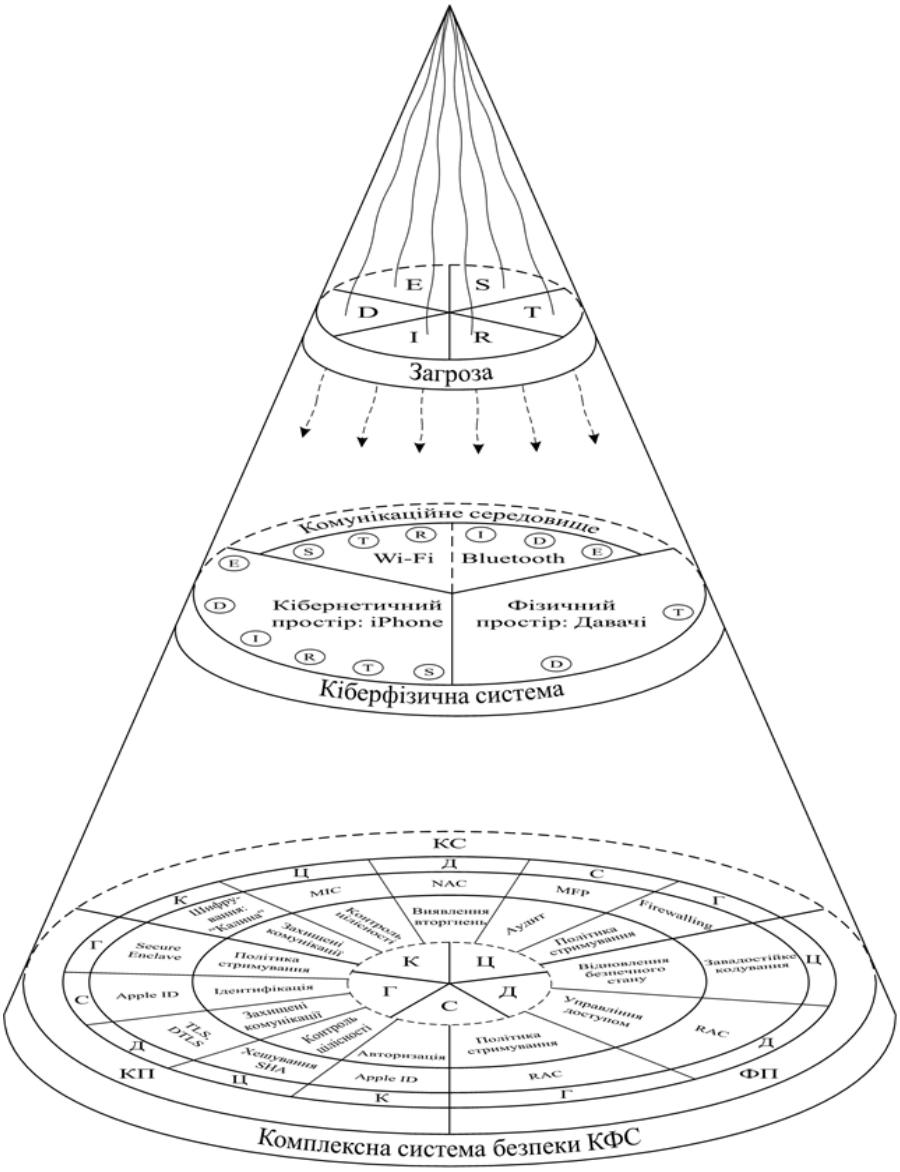



Рис. 1. Інформаційна модель комплексної системи безпеки КФС “iPhone – Wi-Fi, Bluetooth – давачі”

Центральним сегментом моделі є елементи структури КФС: КП – смартфон iPhone; КС – технології безпровідного зв'язку Wi-Fi, Bluetooth; ФП – МЕМС-давачі. Верхній сегмент представлений класами загроз за методикою STRIDE, які характерні для елементів КФС: КП, КС – S (підміна об'єктів), T (модифікація даних), R (відмова від авторства), I (розголошення інформації), D (відмова в обслуговуванні), E (підвищення привілеїв); ФП – T, D. Нижнім сегментом моделі є КСБ кіберфізичної системи, яка складається з підсистем – комплексних систем безпеки КП, КС та ФП, сформована для вирішення задач безпеки відповідних сегментів КФС: КП, КС – забезпечення конфіденційності (К), цілісності (Ц), доступності (Д), спостережності (С), гарантованості (Г); ФП – Ц, Д, Г. Вирішення задач безпеки забезпечують відповідні послуги безпеки на основі технологій захисту інформації у вигляді структури "задача безпеки – послуга безпеки – технологія захисту інформації" [2].

Структура КСБ кібернетичного простору КФС, представленого смартфоном iPhone: К – авторизація – Apple ID; Ц – контроль цілісності – хешування SHA; Д – захищені комунікації – TLS, DTLS; С – ідентифікація – Apple ID; Г – політика стримування – Secure Enclave. Структура КСБ комунікаційного середовища КФС – технологій безпровідного зв'язку: К – захищені комунікації – шифрування: "Калина"; Ц – контроль цілісності – MIC; Д – виявлення вторгнень – NAC; С – аудит – MFP; Г – політика стримування – Firewalling. Структура КСБ фізичного простору КФС, який включає МЕМС-давачі: Ц – відновлення безпечного стану – завадостійке кодування; Д – управління доступом – RAC; Г – політика стримування – RAC.

Послуги безпеки, які призначені для забезпечення задач безпеки, функціонують на основі технологій захисту. Зокрема, для iPhone, як КП, характерні такі загрози за STRIDE / технології захисту: S – соціальна інженерія / сертифікація програм; T – модифікація кодів доступу / низькорівневе шифрування AES-256; R – несанкціоновані покупки через програми / технологія фіксації дій користувача; I – несанкціонований віддалений доступ / SSL, VPN; D – експлойти / сертифікація Apple Root; E – заміна цифрових сертифікатів, підписів / шифрування файлів [3].

Загрози / технології захисту для КС – технологій безпровідного зв'язку Wi-Fi та Bluetooth: S – підміна пристроїв (атака man-in-the-middle) / ідентифікація обладнання; T – маніпуляція бітами / моніторинг підключень до мережі; R – несанкціоновані покупки через програми / технологія фіксації дій користувача; I – несанкціоноване використання ресурсів мережі / ідентифікація, аутентифікація користувачів; D – атаки DoS, DDoS / фільтрування пакетів; E – несанкціонований доступ до налаштувань обладнання / фіксація змін налаштувань.

Фізичний простір КФС, представлений МЕМС-давачами, передбачає такі загрози / технології захисту: T – модифікація показів / механізм здійснення контрольних вимірювань; D – перевищення порогових значень / самодіагностика.

Методологічними засадами побудови комплексної системи безпеки КФС є: системний підхід – принципи ієрархічності, структуризації, цілісності; синергетичний підхід – властивість емерджентності, що припускає наявність властивостей, які притаманні комплексній системі безпеки КФС в цілому, але не властиві її окремим елементам – комплексним системам безпеки КП, КС, ФП. Запропонована інформаційна модель КСБ кіберфізичної системи "iPhone – Wi-Fi, Bluetooth – давачі" відповідає базовій технічній моделі IT-безпеки згідно ISO/IEC 15408 і спрямована на забезпечення конфіденційності, цілісності, доступності, спостережуваності та гарантованості інформації в кіберфізичній системі "iPhone – Wi-Fi, Bluetooth – давачі".

## Література


1. Дудикевич В. Б. Парадигма та концепція побудови багаторівневої комплексної системи безпеки кіберфізичних систем / В. Б. Дудикевич, В. М. Максимович, Г. В. Микитин // Вісник Національного університету "Львівська політехніка" Автоматика, вимірювання та керування. – 2015. – № 821. – С. 3–8.
2. Information technology. Security techniques. Evaluation criteria for IT security. Part 1–3: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008. – [Active from 2009.01.01]. – Switzerland: ISO copyright office, 2009. – 56, 161, 150 p.
3. Apple iOS Security Guide. – [Electronic source]. – Regime of access: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ТУРИСТИЧНІЙ ГАЛУЗІ

*Богдан Мізюк[1], Орест Полотай[2]*

1. Львівський торговельно-економічний університет, м. Львів, Україна
2. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The basic methods of information security threats that accompany the activities of tourist companies.**

**Keywords: Information security, security of personal data, travel company**

Сучасний розвиток світової економіки характеризується все більшою залежністю ринку від значного обсягу інформаційних потоків. Незважаючи на дедалі більші зусилля по створенню технології захисту даних, їх вразливість не тільки не зменшується, а й постійно зростає. Тому актуальність проблем, пов'язаних із захистом потоків даних і забезпеченням інформаційної безпеки їх обробки і передачі, все більш посилюється. Проблема забезпечення внутрішньої інформаційної безпеки стає все більш актуальною для компаній туристичної галузі. Це пов'язано і з загостренням конкурентної боротьби на внутрішніх ринках, і з виходом компаній на міжнародний рівень. Багато з них вже не можуть забезпечити захист комерційної інформації власними силами і змушені користуватися послугами професіоналів.

Варто зазначити, що інформаційна безпека в туристичній галузі виступає одним з восьми складових безпеки туризму, під якою розуміють «особисту безпеку туристів, збереження їх майна та ненанесення шкоди навколишньому природному середовищу при здійсненні подорожей» [2].

Інформаційна безпека туристичної фірми, як правило, забезпечується тими ж процедурами і засобами, що і будь-якого іншого комерційного підприємства, але з урахуванням підвищеної кількості чутливих даних і транзакцій.

Інформаційну безпеку в туристичній галузі умовно можна поділити на два підвиди: безпека персональних даних та безпека інформаційного середовища [1].

Туристична галузь - одна з найбільш чутливих до загроз інформаційної безпеки. Це й не дивно - адже туристичні компанії обробляють різну конфіденційну інформацію про своїх клієнтів, а навіть звичайні відомості про туриста можуть сказати дуже багато про його смаки, звички, уподобання і стан здоров'я. Інформаційна безпека туристичної фірми може бути забезпечена тільки за умови суворого дотримання норм у сфері захисту персональних даних.

Крім цього, туризм - одна з галузей, у якій найбільш часто використовують платежі через мережу Інтернет. Бронювання номерів в готелях, резервування авіаквитків і іншої інфраструктури з оплатою через Всесвітню мережу - звичайнісіньке явище в сфері подорожей і туризму. Це все збільшує ризик втрати інформації про стан банківських рахунку, номери банківських карток та ін.. Тому однією з найважливіших завдань туристичних компаній є безпечна обробка банківських даних і реалізація всіх вимог PCI DSS (стандарту захисту даних в індустрії платіжних карт).

Для того, щоб захистити себе від витоку конфіденційної інформації, компанія, що працює в туристичній галузі, змушена запровадити внутрішню політику інформаційної безпеки, яка повинна забезпечувати дотримання певних вимог, серед яких основними є такі:

1) установка на всіх комп'ютерах антивірусного програмного забезпечення і регулярне його оновлення;

2) використання брандмауера - програмного або апаратного маршрутизатора, поєднаного з firewall (особливою системою, що здійснює фільтрацію пакетів даних), він не пропускає назовні внутрішні пакети локальної мережі підприємства і блокує доступ до неї чужих комп'ютерів ;.

3) захист електронної пошти (поставлений антивірус на корпоративний сервер електронної пошти);

4) використання Proxy-сервера. По-перше, це дозволить трохи скоротити інтернет-трафік. По-друге, це дозволить приховати від сторонніх очей внутрішні імена і адреси комп'ютерів. І, по-третє, це дозволить виявляти порушників, які підключилися до мережі підприємства з метою отримання доступу в Інтернет. [9]

5) постійний моніторинг стану комп'ютерів користувачів і локальної мережі;

6) документообіг підприємства в більшому ступені ведеться в електронному вигляді;

7) запроваджувати у функціонал компанії потужні технічні засоби захисту інформації, які повинні бути об'єднані в комплекс. Тільки одночасна злагоджена робота програмних і апаратних складових такого комплексу дає змогу оптимізувати службу інформаційної безпеки в повній мірі.

8) завдяки контролю над співробітниками туристичних агентств і моніторингу комп'ютерів в локальній мережі можна проводити ретельний аналіз усіх пересувань інформаційного потоку.

Наведені способи забезпечення інформаційної безпеки у компанії туристичної галузі є мало затратними і досить ефективними, з точки зору забезпечення безпеки компанії від безлічі загроз як зовнішніх, так і внутрішніх.

Варто відзначити й інший спосіб, такий як тотальне стеження за співробітниками, хоча відноситься цей спосіб до категорії складних і не потрапляє під категорію простих засобів. Крім того, не варто забувати, що забезпечення інформаційної безпеки не повинно завдавати шкоди діяльності компанії або створювати перешкоди для роботи співробітників, оскільки цей процес повинен доповнювати основну діяльність компанії.

## Література


1. Голод А.П. Безпека туризму як об’єкт регіональних економічних досліджень // А.П. Голод // Інноваційна економіка. – 2014. – № 4 (53). – С. 190-194
2. Маркіна І.А. Управління безпекою туристичного бізнесу / І.А. Маркіна // Экономика Крыма. – 2012. – № 1 (38). – С. 174-176.

# АВТЕНТИФІКАЦІЯ КОМП'ЮТЕРА В МЕРЕЖІ ЗА ШУМАМИ АУДІОПЛАТИ

*Олена Нємкова*

Університет банківської справи Львівський інститут, Львів, Україна

**The article is devoted to experimental studies of the noise audio card for network computer authentication. It was shown experimentally that autocorrelation functions of noise audio card are different for various computers. It was confirmed that set of parameters of the noise autocorrelation function uniquely identifies the audio card.**

**Keywords: noise audio boards, computer authentication, autocorrelation, distance Hemming**

Сучасні корпоративні комп'ютерні мережі зазнають десятки тисяч різноманітних атак, як зовні, так і зсередини. Значна частина нападів відбувається через порушення прав доступу. Це стає можливим завдяки слабкій автентифікації користувача. Для посилення автентифікації людей були розроблені біометричні методи. Для електронних пристроїв, одним з яких є комп'ютер, також необхідно розробити аналогічні методи, які дозволили б однозначно автентифікувати конкретний пристрій в критичних системи управління, Інтернеті речей, телемедицині тощо.

Шуми електронних пристроїв, особливо аудіоплат, привертають інтерес дослідників з кількох причин: як реалізація фізично не клонованої функції для автентифікації, а також для дослідження можливої компіляції файлу звукозапису. Аудіоплати однієї серії внаслідок мікроскопічних відхилень у складі комплектуючих мають неоднакові частотні передаточні характеристики, що призводить до відмінностей спектру шуму від модельного білого шуму.

В даній роботі експериментальне дослідження шуму звукової карти було проведено за допомогою програми Oscillometer. Частота дискретизації дорівнювала 44,1 кГц. На вхід аудіоплати нічого не подавалось. Амплітуда шуму виявилась малою – приблизно 0,2 мВ. Подальші обчислення було проведено у програмі MathCad. В експерименті було використано 12 комп'ютерів однієї серії. На кожному комп'ютері файл шуму записувався три рази. Запис тривав декілька секунд, що дало можливість використати один файл для організації багатьох послідовностей відліків шуму.

На рис.1 представлено функцію автокореляції шуму аудіоплати. Відстань між сусідніми точками по осі абсцис дорівнює часу дискретизації 1/44100 сек.

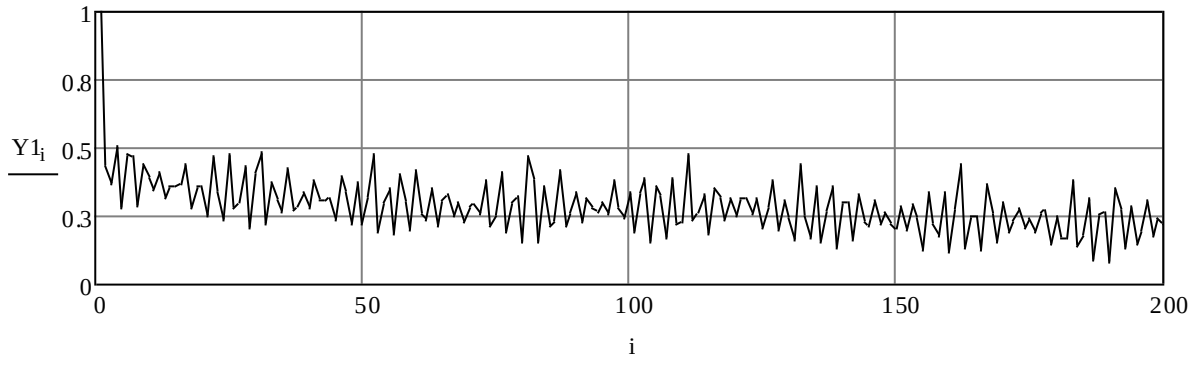



Рис.1. Функція автокореляції шуму аудіоплати

З'ясувалось, що вигляд функції автокореляції шуму є різним для кожного комп'ютера. Але якщо розраховано автокореляційні функції для файлів шуму, що записані з одного комп'ютера, то форма функцій практично однакова. На рис.2 показані функції автокореляції шуму для двох різних комп'ютерів. Наведено тільки частина

графіку автокореляційної функції, починаючі з сотого відліку. Довжина послідовності (32 відліки) обумовлена конкретним видом графіка з рис.1. Для того, щоб надійно розрізнити графіки однієї форми від іншої, запропоновано наступну процедуру. По-перше, розраховується лінійна інтерполяційна функція, що з'єднує точки функції автокореляції. По-друге, на кожній лінійній ділянці розраховується похідна та будується графік похідної, рис.3. На графіку похідних відмінності між різними комп'ютерами ще більш помітні.

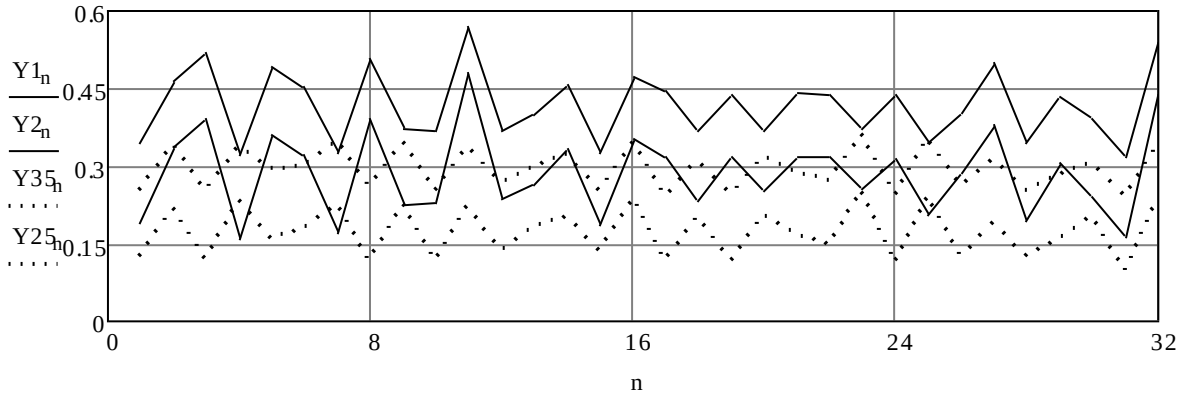



Рис.2. Функції автокореляції шумів від аудіоплат двох комп'ютерів, починаючи від 100 відліку

По-третє, записується бітова послідовність за правилом: якщо значення похідної додатне, то це відповідає одиниці, якщо від'ємне, то нулю. В результаті було отримано таки послідовності. Для першого комп'ютера (на графіку похідної суцільна лінія) це 11010010110110100101101011101001, а для другого 10101101010110101010010101011101.

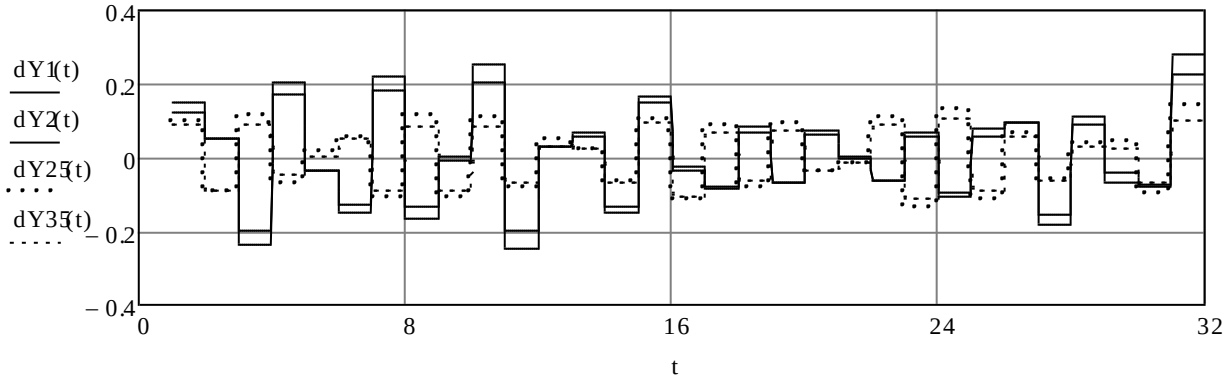



Рис.3. Похідні функцій автокореляції шумів аудіоплат двох комп'ютерів

Відстань за Хемінгом між послідовностями склала 18 при довжині послідовності 31 біт. Таким чином, послідовності на 58% не співпадають. Для практичної реалізації методики не потрібно будувати інтерполянту та розраховувати похідні. Бітові послідовності записуються за правилом: якщо наступне значення функції автокореляції більше попереднього, то записується одиниця, якщо менше попереднього, то нуль. Це значно пришвидшує процес автентифікації. Слід зауважити, що використання шуму в якості автентифікатора потребує розробки протоколу обміну між двома сторонами для запобігання атаки типу маскарад.

## Література

1. Chaplyha, V., Nyemkova, E., and Shandra, Z. 'Technique of Measuring of Identification Parameters of Audio Recording Device', Proceedings of 18 International Conference Information Technology for Practice 2015, Ostrava, pp. 209-218.

# RESEARCH OF IDENTIFICATION OF INFLUENTIAL GROUPS OF AGENTS IN SOCIAL NETWORK FOR INFORMATION SECURITY

*Mariia Chernetska, Liliya Nikiforova*

Vinnytsia National Technical University, Vinnytsia, Ukraine

**The report describes existing methods of identifying of agents of privacy threats using social networks. Earlier achievements and prospects of the development direction are specified.**

**Keywords: threat, agent, information privacy, social network.**

The economic stability of the enterprise is based on a number of parameters, which include confidentiality, integrity and availability of information related to its activity. Technical and software tools are not able to protect information against leakage completely, it is impossible to completely eliminate the human factor.

Social networks are an integral part of modern life. Members of social networks publish their personal information without any reservations. There is also the posibility intentional or accidental disclosure of confidential information of the company, where these participants work. With the increasing spread of information through social networks interest about it is also growing.

Research of communication indicators in social networks and identifying agents of influence is an important area of research and developments, which is important for business information activities in ensuring their safety.

There is a small amount of quantitative indicators of identifying agents of influence. Most of indicators are based on psychological characteristics that may be well hidden by potential agent during tests.

In [1] a research using sociogram of 11 people was conducted, in which each of the surveyed were asked to introduce themselves in this group, determine his position and predict actions of other people.

In [2] a method of identifying agents of threats based on modification of sociometric indices that do not require direct survey of potential agents was described and investigated. This method is a promising tool for identifying agents of privacy threats among agents who are a part of a social network. Grouping of numerical coefficients allows to perform quantitative analysis of information processes in the social network. Developed program is a powerful tool that allows to detect informal agents of influence in the network, agents who are ignored by the network and agents who ignore the network. Specified work describes a research of identifying agents of threats of confidentiality of one group in social network.

Further development of this direction is the expansion of research on a specific set of social networking groups to identify cross-results for agents and bringing them into a network of agents of influence.

## References

1. Smith R.A. Understanding the Influential People and Social Structures Shaping Compliance [Електронний ресурс] / R.A. Smith, E.L. Fink // Journal of Social Structure. — 2015. — Vol. 16. — 15 ı. — Режим доступу: https://www.cmu.edu/joss/content/articles/volume16/SmithFink.pdf
2. Нікіфорова Л. О., Горох Н. В., Лєбєдєва Г. О., Салієва О. В. Дослідження показників неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності // Реєстрація, зберігання і обробка даних. – 2016. – Т. 18, № 1. – С.52-62

# ПРОБЛЕМАТИКА МЕТОДІВ ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ТА ШЛЯХИ ЇХ УДОСКОНАЛЕННЯ

*Іван Опірський*

Національний університет «Львівська політехніка», м. Львів, Україна

**The analysis of unauthorized access methods ("Delphi method", "objectives tree" method, morphological analysis, forecasting informal) in information networks of state and given their characteristics.**

**Keywords: unauthorized access, forecasting, state information network, prediction object, prediction method, forecast, Delphi method, the method of "tree-goals", informal prediction, brainstorming**

Прогнозування або пророкування ситуацій чи подій діляться на повторювані, тимчасово повторювані та унікальні. Для повторюваних ситуацій пророкування (прогнози) формулюються у виді наукових законів чи закономірностей. Науковий закон – це типовий прогноз, вірний в різний час і в різних місцях, якщо складаються деякі умови.

По відношенню до тимчасово повторювальних ситуацій чи подій виявляються тимчасові закономірності (тимчасові типові прогнози). Складність тимчасових закономірностей є в тому, щоб вчасно визначити момент після якого вони перестають в достатній мірі проявлятись.

Більшість соціальних феноменів неможливо з достатньою повнотою описати науковими законами, що мають прості формулювання. Гуманітарні науки є в своїй більшій частині корисними для фіксації або відображають специфічні реалії конкретних подій чи ситуацій, особливо це стосується НСД.

Можливі, бажані і доступні варіанти прогнозуємих подій мають таке співвідношення рис. 1.

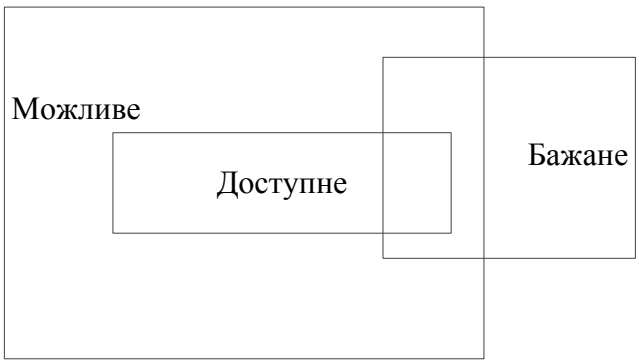



Рис. 1. Варіанти прогнозованих подій

При цьому розрізняються можливості суб’єктів:

1) При відсутності протидії зі сторони інших суб’єктів; при наявності такої протидії;

2) Принципіальні: так, що не суперечать відомим спільним представленням;

3) Реальні: не потребують для свого здійснення якої-небудь рідкої події, рідкого збіг обставин, находження особливо ефективних рішень

Існує багато методів прогнозування і їх варіантів,орієнтованих на різні предметні області, різні горизонти прогнозування, різні технічні можливості прогнозування тощо. При використанні для завдань деяких типів вони перевірені і надали позитивні результати. При використанні з деякими завданнями вони сумнівні, проте зазвичай дозволяють визначити хоча б коло можливостей.

При прогнозуванні НСД необхідно враховувати відмінності між ймовірністю і можливостями. Ймовірність – характеристика, багатократних подій, що повторюються, а можливість – характеристика подій унікальних і різних.

При визначення якості прогнозів треба мати на увазі наступне. Оцінка ймовірностей подій, що даються після того, як події сталися, помітно відрізняються від оцінок, що даються до вчинення події, оскільки моди схильні завишати ймовірність того, що вже було.

Тому причини того, що прогнози не здійснюються можна сформулювати таким чином:

- не вірний вибір методу прогнозування;
- помилки в використанні методу прогнозування;
- недостатність чи помилковість вихідних даних;
- недостатні затрати інтелектуальних сил на складання прогнозів.

Компонентами системи прогнозування є наступне:

- теоретичні основи;
- технології прогнозування;
- вихідні данні;
- колекція чужих прогнозів;
- експерти в предметних сферах;

Якщо об'єкт прогнозування добре відомий, а це ІМД, то основна важкість прогнозування є в переробці великої кількості наявних відомостей; а якщо про них мало, що відомо, то основна проблема – в нестачі засобів.

Якщо НСД не ізольований, а має великий вплив ззовні, НСД виникає необхідність прогнозувати не тільки процеси в самій системі, але і надає а неї великий вплив.

Прогнозування буває: формальне, неформальне, змішане (має властивості формального і неформального).

Прогнозування феноменів, які не залежать (або мало залежать) від дій яких-небудь злочинців, може здійснюватися формально. Прогнозування феноменів, які істотно залежать від дій деяких зловмисників, зазвичай потребують припущень про результати інтелектуальної діяльності цих зловмисників, а саме мають здійснюватись неформально.

Методи неформального прогнозування поділяються на індивідуальні і колективні.

В змішаних методах прогнозування застосовується формальна обробка неформально отриманих результатів або неформальна обробка формально отриманих результатів.

Система прогнозування не може працювати весь час з одним і тим же горизонтом, з одним і тим же ступенем достовірності: бувають нестійкі ситуації, в яких навіть невелика перевага деяких дій може повернути течію подій в довільну сторону. В таких ситуаціях сильно наближується горизонт прогнозування і знижується його точність.

## Література


1. Малюк А.А. Информационная безопастность: Концептуальные и методические основы защиты информации/ Малюк А.А. – М: Высшая школа, 2004. –280с.
2. Тимченко А.А. Основы информатики системного проектирования объектов новой техник / А.А. Тимченко, А.А. Радионов. – Наукова думка. – Киев.: 2000.− 152 с.
3. Михайлов С.Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции / С.Ф. Михайлов, В.А. Петров, Ю.А. Тимофеев. – М.: Связь, 1995. – 56 с.
4. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа / Щеглов А.Ю. – С.Пб.: 2004. – 384 с.

# АВТОМАТИЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

*Дмитро Пантелюк, Володимир Ромака*

Національний університет "Львівська політехніка", м. Львів, Україна

**This paper examines the issue of automation of processes of information security management. Information security management functions examined. Automated ISMS model proposed.**

**Keywords: information security management system, automation, information security functions**

**Вступ**

Щоб забезпечити послідовність та злагодженість виконання заходів забезпечення інформаційної безпеки (ІБ) ними необхідно управляти, що полягає в плануванні, моніторингу, оцінці ефективності та модифікаціях, якщо така потреба виникає. У цій діяльності важливим моментом є збирання, обробка, аналіз та обмін інформації. Це займає найбільшу частину діяльності з управління процесами ІБ. Навіть при незначній області впровадження системи безпеки це чималий обсяг робіт: зустрічі, інтерв'ю, запис отриманої інформації, аналіз даних, вироблення стратегій та коригувальних заходів, розробка планів і т.д. Великий обсяг робіт означає і великий обсяг інформації. Виникає питання: як забезпечити ефективну роботу з таким об'ємом інформації?

З метою автоматизації процесів збору даних, їх аналізу та взаємодії, створення загального інформаційного поля для всіх учасників процесів ІБ розроблена інформаційно-логічна модель автоматизованої системи управління безпекою підприємства.

**Аналіз процесів управління інформаційною безпекою підприємства**

Виділяють наступні основні процеси управління [1]:

- збір та аналіз даних про стан ІБ в організації;
- оцінку та управління ризиками;
- розробку і впровадження захисних заходів;
- управління інцидентами ІБ;
- реалізацію і впровадження відповідних механізмів контролю;
- моніторинг функціонування механізмів контролю, оцінка їх ефективності та впровадження відповідних коригувальних впливів.

Ці процеси можна охарактеризувати понятійним апаратом у вигляді чотирьох об'єктів: «загроза», «ризик», «захід», «засіб захисту», достатній для побудови системи менеджменту інформаційної безпеки (СМІБ). Загроза вказує на можливість заподіяння шкоди підприємству, ризик кількісно (або якісно) описує загрозу і служить для оцінки безпеки підприємства. Змінювати стан безпеки можна шляхом запровадження заходів, а відслідковувати зміни - шляхом аналізу значень ризиків. Результат запровадження заходів описується встановленими засобами захисту для протидії можливим загрозам.

**Побудова моделі автоматизованої системи управління безпекою**

Автоматизація процесу менеджменту ІБ полягає у веденні бази даних заходів захисту і накопиченні статистики їх використання через журнал подій. Ця база даних по суті є основним інструментом фахівця з безпеки, який використовується для обліку виконуваних робіт. Організаційно необхідно забезпечити роботу служби безпеки таким чином, щоб інформація про всі проведені заходи і використані засоби захисту зберігалися в базі даних.

На основі проаналізованих вище процесів управління можна представити схему взаємозв'язку об'єктів, необхідних для побудови СМІБ за допомогою діаграми UML[2] (рис. 1). Для кожного заходу зазначаються опрацьовані ризики і об'єкти, які з ними пов'язані. Один захід може діяти відразу на кілька ризиків, зменшуючи ймовірності і збитки на різні величини. Для кожного ризику показуються його початкові ймовірність і

збитки, а також кінцеві – з урахуванням ужитих заходів. Основне призначення системи – надати співробітникам підрозділу, відповідальним за ІБ інструмент організації заходів, пов'язаних із забезпеченням безпеки окремих інформаційних об'єктів, а керівнику підрозділу безпеки - інструмент моніторингу і аналізу ризиків та оцінки ефективності заходів.

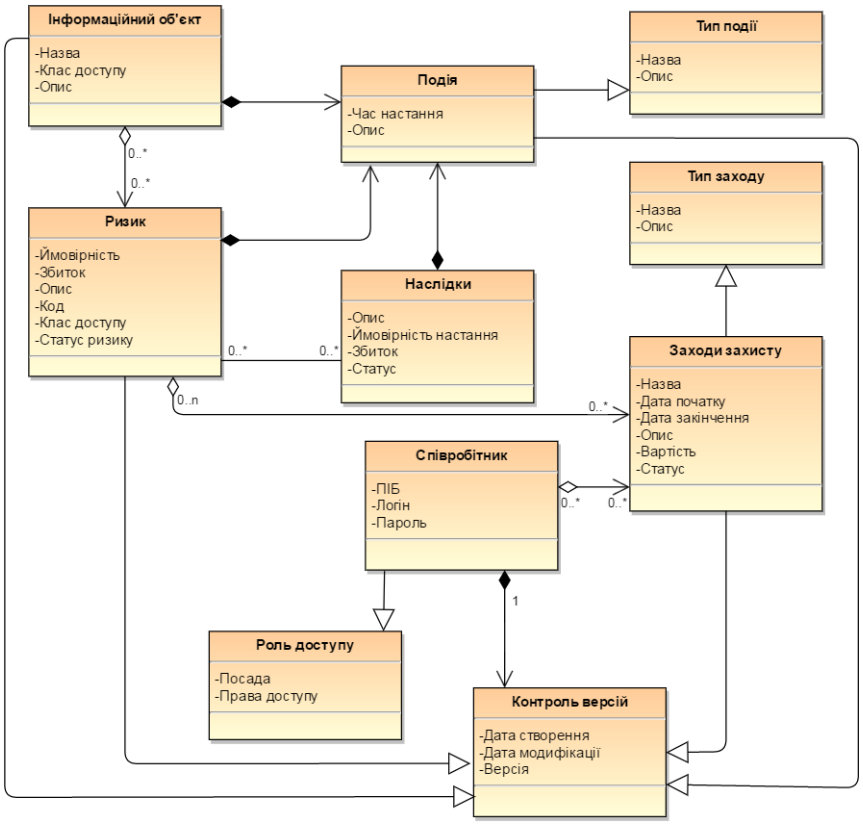



Рис. 1. Діаграма класів системи УІБ

**Висновок:**

При організації системи управління безпекою сучасного підприємства необхідно забезпечити тісний контакт співробітників підрозділів інформаційних технологій і забезпечення безпеки. Єдиний інформаційний простір підприємства формується з урахуванням необхідності використання його елементів для керування безпекою. Інформаційна підтримка прийняття рішень по забезпеченню комплексної безпеки підприємства здійснюється на основі використання актуальних знань, що накопичуються в єдиному інформаційному просторі. Система управління ІБ включає можливість ведення бази даних заходів і надання інструментарій оперативної роботи співробітникам підрозділів, що забезпечують безпеку підприємства. Запропонована модель може бути використана компаніями при побудові власних рішень для забезпечення ІБ.

## Література


1. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems — Requirements
2. Буч Г, Рамбо Дж., Джекобсон А. UML. Проектирование программных комплексов, информационных систем. – М.: ДМК Пресс, СПб.: Питер, 2003, – 432 с.

# ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ЯК МЕХАНІЗМ АНАЛІЗУ ЕФЕКТИВНОСТІ СИСТЕМИ ПРИМАНКИ ДЛЯ МЕРЕЖІ WI-FI

*Роман Банах[1], Андріян Піскозуб[1], Ярослав Стефінко[2]*

1. Національний університет «Львівська політехніка», кафедра захисту інформації, м. Львів, Україна
2. Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій, м. Львів, Україна

**Each honeypot neither should not be too easy victim, which may be suspicious, nor too difficult for attacker, since it may prevent attacker from accessing device. Methods of penetration testing for Wi-Fi networks are analyzed in this paper, what can be useful during Wi-Fi honeypot development.**

**Keywords: honeypot, Wi-Fi, penetration testing**

Задача будь-якої системи-приманки — піддатись атаці або несанкціонованому дослідженню зі сторони зловмисників, що згодом дозволить вивчити їх стратегію та визначити перелік засобів, за допомогою яких можуть бути нанесені удари по стратегічних об'єктах мережі. Реалізація системи-приманки може являти собою як мережу вразливих пристроїв, так і спеціально виділений сервер із віртуальними ресурсами, або ж один мережевий сервіс, завдання якого — привернути увагу зловмисників [1].

Система-приманка являє собою ресурс, який не несе собою ніякої користі окрім як відвернення уваги від справжніх інформаційних об’єктів, а при взаємодії з нею інформація збирається. Після аналізу взаємодії будується статистика методів, якими користуються зловмисники, а також визначається наявність нових рішень, які згодом будуть застосовуватися в боротьбі з ними.

Система приманка не повинна бути занадто легкою здобиччю для зловмисника, оскільки може викликати підозру у досвідченого зловмисника. У гіршому ж випадку така система приманка стане легкою здобиччю зловмисника-початківця, що не дасть бажаної інформативності, а лише завдасть збитків її власнику. Використання системи приманки із високим рівнем захисту також не має сенсу оскільки така модель стане не приступною фортецею для зловмисника [2].

Сучасні small or home office (SOHO) Wi-Fi точки доступу дають їх власникам можливість захистити свою мережу за допомогою стандартних механізмів автентифікації, таких як Wired Equivalent Privacy (WEP) та Wi-Fi Protected Access (WPA) v1 або v2. Сьогодні використання WEP для захисту Wi-Fi мереж не можна вважати надійним методом, оскільки його компрометація займає від 10 до 20 хвилин в залежності від вибору довжини ключа. Проблема полягає у реалізації вибору вектора ініціалізації, що використовується як псевдовипадкова послідовність для шифрування даних. Використання механізмів WPA/WPA2 дозволяє більш надійно захистити доступ до мережі. Та все ж вони не можуть гарантувати цілковитої захищеності, оскільки на отриманий після перехоплення спеціальний пакет «рукостискання», може бути застосована атака грубої сили, в результаті успішного завершення останньої пароль буде добуто. Ефективність механізмів WPA/WPA2 забезпечується довжиною ключа, Мінімальна довжина ключа механізмів WPA/WPA2 складає 8 символів, і максимальна 63 символів таблиці кодування ASCII. У відповідності до збільшення кількості символів у ключі – збільшується і криптостійкість даного механізму. У разі, якщо кількість символів дорівнює восьми, і усі символи є лише цифровими значеннями, то сучасний середньостатистичний комп’ютер справиться з такою задачею приблизно за 20 хвилин, в залежності від словника який використовується у атаці [3-5].

Ще одним механізмом автентифікації користувачів став протокол Wi-Fi Protected Setup (WPS), який дозволяє користувачеві майже автоматично отримати доступ до мережі.

Згодом після введення його в експлуатацію, було виявлено, що даний протокол є вразливим до атаки грубої сили. В разі експлуатації даної вразливості зловмисник отримає доступ до такої мережі за декілька годин. WPS є додатковою функцією, яка може привернути увагу зловмисника.

Окрім вище згаданих механізмів автентифікації існують і додаткові, на приклад приховування імені ідентифікатора точки доступу (SSID), або фільтрація мобільних клієнтів за унікальною MAC-адресою мережевого пристрою. Такі методи не можуть гарантувати захисту мережі від підготованих зловмисників, але можуть виступити у якості захисту від «випадкового» зловмисника. Такий підхід дозволить впевнити зловмисника, що ціль може не є системою-приманкою, а всього лиш не правильно налаштованою.

Результатом успіху є взаємодія зловмисника із системою-приманкою. Відповідно до цього вона повинна бути правильно зконфігурована. Для того щоб зробити оцінку поточного стану захищеності, та виявити вразливості, ми можемо використати методику тестування на проникнення. А саме тестування за методом чорної коробки (black box penetration testing). Автоматизація такого тестування дасть змогу оцінити складність злому системи приманки.

**Висновки:** системи-приманки збирають інформацію про характер поведінки зловмисників і про їх способи впливу на визначену ціль. З такою інформацією фахівці з інформаційної безпеки розробляють стратегії відображення атак зловмисників. Та не правильне використання систем-приманок може принести більше шкоди, а ніж користі.

Різні варіанти розміщення приманок можуть дати повну картину щодо тактики нападника.

Наступними кроками досліджень буде створення математичної моделі, яка допоможе визначити ефективність системи-приманки у взаємодії із зловмисником.

## Література


1. Сучасні системи віртуальних приманок на основі технології honeypot / Гнатюк С.О., Волянська В.В., Карпенко С.В. // Науково-практичний журнал «захист інформації» № 3. – 2012. – 107-115 с.
2. Методи та засоби аналізу систем приманок в процесі зламу / Дудикевич В.Б., Піскозуб А.З., Тимошик Н.П., Тимошик Р.П., Дуткевич Т.В. // Науково-технічний журнал «захист інформації» № 1, 2009 – 27-31 с.
3. Оцінка ефективності систем захисту інформації / Гарасимчук О.І., Костів Ю.М. // Інформатика, математичне моделювання та інформаційні технології. Вісник КНУ імені Михайла Остроградського. Випуск 1/2011 (66). Частина 1. – 2011. – 16-20 с.
4. Інформаційна модель безпеки технологій зв’язку. / Дудикевич В. Б., Хорошко В. О., Микитин Г.В., Банах Р.І., Ребець А.І. // Информатика та математичні методи в моделюванні 2014 Том 4. – №2. – 137-148 с.
5. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв’язку / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець, Р.І. Банах // Інформаційна безпека Східноукраїнський Національний університет імені Володимира Даля № 4(12) – 2013. – 16-22 с.

# АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ УРЯДУВАННІ

*Марія Мандрона, Олександр Поліщук*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**In the paper considers features of e-government system. There are analyzes the essence and content of information security at various levels of government. It was found the main remedies that do are used to create mechanism of ensuring safety in the system of e-governance.**

**Keywords: e-government, information, information security system.**

Використання технологій електронного урядування (ЕУ) є важливим фактором, що дає змогу забезпечити вирішенню проблем української держави, таких як: непрозорість, закритість, високий рівень корумпованості органів влади; формування механізмів децентралізації, демократичного контролю та участі громадян у розробці та реалізації державної політики; повернення довіри громадян до інститутів та посадовців органів державної влади та місцевого самоврядування.

Основними цілями ЕУ є [1-3]:

• підвищення якості та доступності державних послуг для громадян та бізнесу, спрощення процедур і скорочення адміністративних витрат;

• підвищення якості управлінських процесів, контроль за результативністю та ефективністю діяльності органів державної влади та органів місцевого самоврядування;

• забезпечення відкритості інформації про діяльність органів державної влади й місцевого самоврядування, розширення доступу до неї та надання можливості безпосередньої участі людини та інститутів громадянського суспільства в процесах підготовки й експертизи проектів політико-адміністративних рішень.

Впровадження ЕУ робить систему державного управління більш уразливою з боку різного роду загроз: кіберзлочинності, кібертероризму, кібервійн, проведення спеціальних інформаційних операцій, розповсюдження недостовірної інформації, маніпулювання свідомістю громадян тощо. Тому обов'язковою підсистемою сучасних інформаційно-телекомунікаційних систем є підсистеми захисту інформації, що застосовуються в електронному урядуванні.

***Мета роботи*** полягає в аналізі систем захисту електронного урядування.

Аналізуючи напрями та сутність забезпечення інформаційної безпеки у внутрішньо системному функціонуванні органів виконавчої влади можна сказати, що їх характеризує сама компетенція, котра пов'язана із виконанням покладених на них державою, функцій і завдань. До характеристик, що дають змогу описати дану систему належать такі [4]:

- ✓ доступність – можливість за прийнятний час отримати необхідну інформаційну послугу будь-яким суб'єктом виконавчої влади;
- ✓ цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни;
- ✓ конфіденційність – захист від несанкціонованого ознайомлення.

Коли ж розглядати сутність та зміст інформаційної безпеки, то вони проявляються по-особливому на кожному з рівнів системи органів влади, зокрема на [2]:

– стратегічному (загальнодержавному);

– тактичному (органів влади, установ тощо);

– оперативному (структурних підрозділів органів державної влади, місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації).

Таким чином, можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення. У зв'язку з цим слід виділити такі її рівні:

- *законодавчий та нормативно-правовий* – закони, нормативно-правові акти, тощо;

- *адміністративний* – дії загального характеру, що вживаються органами виконавчої влади;
- *процедурний* – конкретні процедури забезпечення інформаційної безпеки;
- *програмно-технічний* – конкретні технічні заходи забезпечення інформаційної безпеки.

Нижче зазначені основні засоби захисту [4, 5], які використовуються для створення механізму забезпечення безпеки.

**Технічні засоби** реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Уся сукупність технічних засобів поділяється на апаратні й фізичні.

**Програмні засоби** являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

**Організаційні засоби** – це організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення та експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їх життєвого циклу.

**Морально-етичні засоби** реалізуються у вигляді різних норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи.

**Законодавчі засоби** захисту визначаються нормативно-правовими актами, якими регламентуються норми та правила користування, обробки й передачі інформації обмеженого доступу. За порушення цих правил встановлюються відповідальність.

Технології захисту інформації передбачають впровадження технічних рішень та технічних засобів захисту складових інформаційної інфраструктури. До них належить:
антивірусне програмне забезпечення; системи управління доступом; міжмережеві екрани; системи аутентифікації (смарт-карти, біометрічні системи тощо); системи виявлення вторгнення; управління політиками; сканування на наявність уразливих місць; системи криптографічного захисту; механізми фізичного захисту.

Що стосується боротьби з кіберзлочинами, то сюди відносяться системи ідентифікації та аутентифікації користувачів, криптографічного перетворення інформації, антивірусного захисту, аудиту та моніторингу подій в мережі.

У сукупності отримані результати аналізу дали змогу з'ясувати механізми забезпечення захисту інформації в електронному урядуванні, а також визначити напрями удосконалення систем електронного урядування в цілому.

## Література


1. Державна програма інформатизації та комп'ютеризації вищих навчальних закладів I – II рівня акредитації на 2005 – 2008 роки [Текст] : Постанова Кабінету Міністрів України від 8 вересня 2004 р. N 1182 // Офіційний вісник України. – 2004. – № 36. – С. 40.
2. Державна програма інформатизації та комп'ютеризації вищих навчальних закладів I – II рівня акредитації на 2005 – 2008 роки [Текст] : Постанова Кабінету Міністрів України від 8 вересня 2004 р. N 1182 // Офіційний вісник України. – 2004. – № 36. – С. 40.
3. Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності [Текст]: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. №1452 // Офіційний вісник України.– 2004. – № 44. – С. 123
4. Кукарін О.Б. Електронний документообіг та захист інформації: навч.посібн. / О.Б. Кукарін. – К: НАДУ, 2015. – 84 С.
5. Опорний конспект лекцій. [Дзюба С.В., Жиляєв І.Б., Полумієнко С.К, Рубан І.А., Семенченко А.І.] /За ред. А.І. Семенченка. – Київ, 2012. – 264 с.

# ВИКОРИСТАННЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ ДЛЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

*Орест Полотай, Ростислав Гриник*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The main methods of social engineering, attackers are using in the course of unautorized access to information. We describe the essence of socio-technical systems. The features of social engineering as a socio-technical actors attacks.**

**Keywords: social engineering, information, fishing, pretexting**

Останнім часом, все більшої популярності набуває поняття «соціотехнічна система». Не важко зрозуміти, що соціотехнічна система є однією з підвидів систем, під якими розуміють сукупність елементів та взаємних зв'язків між ними, яким володіють конкретними властивостями, метою, цілями та функціями. Соціотехнічні системи, це сукупність соціальних та технічних систем складовою яких є людина-керуючий ЕОМ, разом з сукупністю його знань, та навичок. Дана людина (оператор) взаємодіє з технічним пристроєм, що призводить до підвищення ефективності поставлених перед нею цілей. [1].

Забезпечення безпеки на сьогоднішній момент є об'єктивною необхідністю ефективного управління в соціотехнічних системах, оскільки такі системи виступають якнайкращим плацдармом для реалізації соціоінженером/соціотехніком (зловмисником) інформаційних операцій та атак, тобто так-званих соціотехнічних атак.

Як відомо, соціоінжера за рівнем своєї підготовки до здійснення соціотехнічної атаки поділяють на новачка, аматора та професіонала і за ймовірністю отримання несанкціонованого доступу різних рівнів до інформації їм наділяють ступінь в межах від 1 до 3 (1 – найменший ступінь, 3 – найбільший).

В залежності від того, під яку категорію підпадає соціальний інженер, він використовує для здійснення несанкціонованого доступу різні методи соціального інжинірингу (соціальної інженерії). Під даними методами розуміються такі методи, які мають на меті використовувати людський чинник як джерело отримання соціоінженером необхідної йому інформації. При використання методів соціального інжинірингу, соціоінженери експлуатують в своїх цілях довірливість, лінь, люб'язність і навіть ентузіазм своїх жертв. Для цього соціоінженер намагається переконати суб'єкти атаки надати йому інформацію, що забезпечує доступ до корпоративних систем або їх ресурсів [2].

Якщо порівнювати атаку, в основі якої лежать методи соціальної інженерії, та кібернетичні атаки, то перший вид атак має на меті нанести шкоду не комп'ютерній системі, а її користувачам, використовуючи при цьому, в якості допоміжних, різноманітні технічні засоби.[3].

Основна тактика соціальної інженерії - за допомогою психологічних методів (наприклад, спілкуючись начебто від імені сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо).

Для успішної реалізації методів соціального інжинірингу, соціоінженери можуть використовувати певні джерела даних про свої потенційні жертви, або так звані ігрові площадки, в межах яких здійснювати певні етапи атаки. Сюди можна віднести різноманітні соціальні мережі, соціальні закладки, соціальні каталоги чи соціальні бібліотеки.

Бурхливий розвиток ІТ-технологій, дає змогу соціоінженеру повний набір засобів для здійснення несанкціонованого доступу до інформації, за допомогою методів соціальної інженерії. Нескладно прогнозувати, що завдяки процесу глобальної комп'ютеризації соціоінженери на довірі не відчуватимуть дефіциту жертв.

В природі виділяють багато методів соціальної інженерії, існує їх класифікація за певними ознаками, характеристиками на особливостями проведення. Серед усіх методів соціального інжинірингу, найбільш розповсюдженими є наступні: претекстинг, фішинг, аналіз сміття, індивідуальні підходи та інші. Розглянемо коротко кожні з них.

Претекстинг – застосування заздалегідь розробленого сценарію, щоб змусити вибрану жертву до розголошення інформації чи виконання дій, які необхідні зловмиснику та які зазвичай вона б не здійснила [3].

Фішинг – метод, який полягає в тому, щоб заволодіти інформацією приватного характеру нечесним шляхом. Сюди можуть відноситись оманливі листи від банків, організацій з шкідливими веб-посиланнями. Сюди також можуть відноситись телефонні дзвінки, під час яких соціоінженер може видавати себе за будь-яку особу.

Метод аналізу сміття полягає у використанні зловмисником не знищеної інформації з корзини (у випадку електронного сміття) або паперових документів.

До індивідуальних підходів відносяться такі методи як залякування (шантаж), переконання, виклик довіри.

Також, якщо відштовхуватись від класифікації методів соціального інжинірингу, то тут можуть поділятись методи за дистанційністю здійснення, за типом атакованого джерела, за порушенням характеристик безпеки інформації.

Методам соціального інжинірингу слід приділяти серйозну увагу, оскільки, як свідчить статистика вони стають дедалі популярними, особливо на території України.

## Література


1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
2. Озерський К.Г. Соціотехнічні методи несанкціонованого доступу до інформації. Веб-сайт молодіжної електронної наукової школи-конференції «Актуальні проблеми захисту інформації та інформаційної безпеки». [Електронний ресурс]. – Режим доступу з http://stavkombez.ru/conf/category/section2/
3. Соціальна інженерія. Веб-сайт Вікіпедія. [Електронний ресурс]. – Режим доступу з https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека)

# ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ КЛЮЧІВ

*Роман Рикмас*

ТОВ «Юнісервіс», м. Львів, Україна

**In the article is given description of using electronic keys for software protection. Also are considered different types of keys and the software that comes with them, advantages and disadvantages of using this type of protection**

**Keywords: software protection, electronic keys.**

Перед компаніями, які займаються розробкою та продажом своїх програмного забезпечення (ПЗ) постає питання захисту своєї інтелектуальної власності від несанкціонованого використання. Для вирішення цієї проблеми на сьогоднішній час існує декілька шляхів. Більшість виробників ПЗ використовують різні програмні модулі, які контролюють доступ користувачів з допомогою ключів активації, серійних номерів, тощо. Такий захист дешевший і не може претендувати на надійність. З допомогою мережі Інтернет можна знайти безліч програм, які дозволяють нелегально згенерувати ключ активації (генератори ключів), або заблокувати сам запит на активацію. Крім цього не слід недооцінювати легальних користувачів, які можуть розповсюдити свій серійний номер.

Ці очевидні недоліки програмного захисту привели до створення апаратних способів захисту ПЗ. Основна ідея такого захисту полягає в тому, для захисту програми існує певний апаратний пристрій. Його відтворення чи втручання в його роботу задача набагато складніша ніж робота з програмними модулями захисту.

Одним з видів апаратного захисту є використання електронних ключів. Електронний ключ – це апаратний засіб, призначений для захисту ПЗ і даних від копіювання, нелегального використання та несанкціонованого розповсюдження. Основою цієї технології є спеціалізована мікросхема, або захищений мікроконтролер, що мають унікальні для кожного ключа алгоритми роботи. Такі ключі також мають захищену незалежну пам'ять невеликого обсягу, більш складні пристрої можуть мати вбудований криптопроцесор (для апаратної реалізації шифруючих алгоритмів), годинник реального часу. Апаратні ключі можуть мати різні форм-фактори, але найчастіше вони підключаються до комп'ютера через USB. Також зустрічаються з LPT- або PCMCIA-інтерфейсами.

Існує велика кількість електронних ключів (HASP, Hardlock, Guardant, Sentinel, Eutron SmartKey, КАТРАН) від різних виробників, але принцип їх роботи схожий.

Технологія захисту від несанкціонованого використання ПЗ побудована на реалізації запитів з виконавчого файлу до ключа з наступним аналізом відповіді.

Слід зазначити такі види запитів до ключа як:

- Перевірка наявності ключа та ліцензії на використання захищеного ПЗ.
- Зчитування з ключа необхідних для запуску програми даних з ключа.
- Запит на розшифрування даних та виконавчого коду програми.
- Запит на розшифрування даних зашифрованих раніше самою ж програмою
- Перевірка цілісності програмного коду шляхом порівняння контрольної суми.
- Запит до вбудованих в ключ алгоритмів, даних чи годинника.

Для прикладу більш детально розглянемо ключі HASP від SafeNet. Крім самих електронних ключів в комплект захисту входить ПЗ, яке дозволяє автоматизувати захист програми. Цікавою є технологія AppOnChip з допомогою якої можна певний алгоритм виконувати на мікропроцесорі ключа.

Електронні ключі HASP за призначенням поділяються на три типи: Master Key, Developer Key та робочі ключі.

Master Key – службовий ключ, який використовується для захисту ПЗ. Дозволяє створювати прошивки інших ключів (керувати ліцензіями) та захищати програмний продукт. Для кожного нового розробника випускається свій Master Key.

Developer Key. Також службовий ключ, який на відміну від Master Key дозволяє захищати ПЗ, але не дозволяє управляти ліцензіями.

Робочі ключі. Електронні ключі призначені для використання користувачем ПЗ і містять відомості про ліцензію. Існує 7 видів робочих ключів HASP. Ці ключі відрізняються між собою апаратними можливостями. В таблиці 1 приведено основні характеристики таких ключів.

Таблиця 1

Характеристики робочих ключів HASP

| Назва ключа | Ліцензії | Обсяг пам'яті | Особливі можливості |
|---|---|---|---|
| Basic | 1 | - | - |
| Pro | 39 | 112 байт захищеної пам'яті доступної для читання/запису<br>112 байт ROM | |
| Max | 231 | 4 кБ захищеної пам'яті доступної для читання/запису<br>2 кБ ROM | Підтримує технологію AppOnChip. |
| Time | 233 | 4 кБ захищеної пам'яті доступної для читання/запису<br>2 кБ ROM | Містить годинник реального часу, який використовується для ліцензування. Підтримує технологію AppOnChip. |
| Drive | 233 | 2 Гб/ 4 Гб флеш-пам'яті<br>4 кБ захищеної пам'яті доступної для читання/запису<br>2 кБ ROM | Аналог ключа Max з додатковим об'ємом флеш пам'яті. |
| Net | 233 | 4 кБ захищеної пам'яті доступної для читання/запису<br>2 кБ ROM | Дозволяє управляти кількістю користувачів, які одночасно використовують ключ (10/50/250). Підтримує технологію AppOnChip. |
| NetTime | 2000 | 4 кБ захищеної пам'яті доступної для читання/запису<br>2 кБ ROM | Суміщає функції ключів Max та Net. |

В комплект розробника для ключів HASP входить утиліта Envelop. Вона дозволяє автоматизувати процес захисту ПЗ та підтримує багато програмних платформ (Win32, x64, Mac, Andoid). Утиліта Envelop дозволяє захистити як саму програму, так і її окремі компоненти і навіть функції в коді програми. З її допомогою можна загрузити виконавчий код в пам'ять ключа, щоб скористатись технологією AppOnChip.

Згідно вказівок SafeNet для досягнення максимального захисту потрібно комбінувати можливості утиліти Envelop та створювати власний захист і звернення до ключа використовуючи API для роботи з драйвером ключа та службою захисту.

Використання електронних ключів захисту HASP має як переваги так і недоліки. До переваг такого захисту належить те що апаратний захист не відкидає всіх можливостей програмного захисту. Оскільки кожен ключ обладнаний шифрувальним процесором, то ПЗ, яке використовує ключ може з його допомогою шифрувати свої файли даних.

Наявність ключа дозволяє не прив'язувати ліцензію до конкретного комп'ютера, що дає можливість користувачеві встановити програму на декілька комп'ютерів, але програма зможе працювати тільки тоді коли їй буде доступний ключ.

Додаткової надійності захисту надає технологія AppOnChip. Вона дозволяє захистити як сам алгоритм, так і програму, тому що для емуляції ключа зловмиснику доведеться відтворити роботу самого алгоритму.

Наявність ключів з вбудованим годинником дозволяє випускати обмежені часом ліцензії, здавати програмне забезпечення в оренду. Час ліцензії при тому повністю не залежний від часу, який встановлений на комп'ютері користувача.

Одним з основних недоліків використання ключів HASP є їх висока вартість, яка впливає на кінцеву вартість програмного продукту. Такі апаратні ключі не можуть використовуватись з безкоштовними чи пробними програмними продуктами. Також з економічної доцільності вартість програмного продукту має бути вищою за вартість ключа.

Ключ неможливо передати користувачеві миттєво, як це може бути з використанням серійних номерів чи ключів активації. Якщо програмний продукт захищений ключем HASP придбано, то потрібен час аби відправити ключ поштою чи кур'єрською службою до користувача. Це в свою чергу викликає певні незручності в порівнянні з програмним захистом.

Ключ вимагає вільних USB-портів на комп'ютері де буде встановлений. У великих організаціях, де використовується багато програмних продуктів виділяють окремі сервери під задачі роздавання ліцензій. На таких серверах може міститись значна кількість ключів від різних виробників програмних продуктів.

Використання електронних ключів HASP та програмного забезпечення Envelop дозволяє швидко захистити програмний продукт. Envelop пропонує широкі можливості як для налаштування захисту для різних програмних платформ з врахуванням їх особливості. Для виробника програмного забезпечення використання електронних ключів дає можливість заощадити ресурси на розробці власних рішень для захисту та швидко отримати надійно захищений продукт. Для користувачів надається зручний спосіб управління ліцензіями на програмні продукти без прив'язки до комп'ютерів, на які вони встановлені.

## Література


1. Скляров Д. В. Искуство защиты и взлома информации – СПб: БХВ-Петербург, 2004. – 288 с.
2. Сайт компанії SafeNet [Електронний ресурс]. – Режим доступу: http://www.safenet.com
3. Аппаратная защита программного обеспечения [Електронний ресурс]. – Режим доступу: http://z-group.org.ua/art_apparatnaja_zashchita.html
4. Оценка эффективности систем защиты программного обеспечения [Електронний ресурс]. – Режим доступу: http://www.infocity.kiev.ua/hack/content/hack139.phtml

# ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ЛАЗЕРНИМ КАНАЛОМ

*Вадим Сінюгін*

Вінницький національний технічний університет, м. Вінниця, Україна

**In paper is investigated the problem of protecting acoustic speech information from leaks on laser channel and is substantiated features of this problem and possible ways to solve it**

**Keywords: protection of information, technical channels, a laser channel**

Не дивлячись на розвиток і широке використання засобів обчислювальної техніки і представлення інформації в цифровому вигляді, існує проблема витоку інформації технічними каналами, а саме технічними каналами витоку інформації яка оброблюється у технічних засобах передавання інформації, технічними каналами витоку інформації при передаванні її по каналам зв'язку, технічними каналами витоку зорової інформації та технічними каналами витоку мовної інформації [1].

В залежності від середовища розповсюдження мовних сигналів і способів їхнього перехоплення технічні канали витоку інформації розділяють на акустичні, віброакустичні, електроакустичні та лазерні.

Різке зростання об'ємів інформації, що передається обумовило необхідність освоєння оптичного діапазону і систем обробки інформації на його основі [2].

Одним з актуальних каналів витоку мовної інформації на сьогоднішній день є лазерний канал. Лазерний канал витоку інформації відноситься до технічного каналу витоку мовної інформації. Говорячи про мовну інформацію, перш за все, мається на увазі проведення переговорів, нарад тощо. Витік інформації лазерним каналом здійснюється шляхом опромінення вібруючих поверхонь лазерним променем в акустичному полі тонких відбиваючих поверхонь (скла вікон, картин, дзеркал і тому подібне). Відбите лазерне випромінення (дифузне чи дзеркальне) модулюється по амплітуді і фазі (по закону вібрації поверхні) і приймається приймачем лазерного випромінення, при демодуляції якого виділяється мовна інформація [3].

Лазерне прослуховування є порівняно новою технологією. Проблема протидії знімання інформації з використанням лазерного мікрофона залишається досить актуальною і водночас однією з найменш вивчених у порівнянні з іншими засобами промислового шпигунства. Особлива привабливість таких систем обумовлена тим, що вони дозволяють вирішувати задачі знімання мовної інформації максимально безпечно, на відстані, опосередковано, уникаючи необхідності знаходження в приміщення з ціллю розміщення там закладних пристроїв, що завжди було пов'язано з ризиком, а також завдяки доступності, в наш час, достатньої кількості засобів, які дозволяють створювати такі системи самостійно і з мінімальним затратами [4]. Крім того, виявлення лазерного мікрофона досить складно, а в ряді випадків технічно нездійсненне. Для кожного виду апаратури технічної розвідки існує відпрацьована технологія її пошуку. Так для пошуку і локалізації радіомоніторингу успішно використовуються програмно-апаратні комплекси радіомоніторингу та індикатори поля, для пошуку пристроїв, які мають напівпровідникові елементи – нелінійні локатори. Існують комплекси, які дозволяють оцінювати рівень побічних електромагнітних випромінювань, є пристрої виявлення диктофонів та інше. А ось проблема оцінювання ступеня вразливості конкретного приміщення для знімання інформації з використанням лазерних мікрофонів залишається відкритою. Очевидно, що необхідним є збалансований підхід, оснований на реальній, комплексній і методично досконалій оцінці вразливості та захисту кожного конкретного об'єкта чи приміщення. Однак, при найближчому розгляді виявляється, що в цій області практично немає

серйозних напрацювань і, що саме головне, немає інструментів, які б дозволили проводити об'єктивні дослідження такого роду, а тому існує необхідність створення нових методів, засобів, покращення існуючих методів, які б забезпечували достатній рівень захисту інформації від витоку лазерним каналом.

З усього вище викладеного можна зробити висновок, що лазерні системи розвідки є досить ефективним засобом отримання інформації на відстані від об'єкту спостереження. Тому, для виключення загрози лазерного прослуховування потрібні нові або вдосконалені методи захисту інформації від витоку лазерним каналом, та засобів, які б не тільки обмежувались генераторами шуму.

## Література


1. Чекатков А.А., Хорошко В.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.
2. Железняк В.К., Чернова И.С., Оценка модели оптико-электронного канала утечки речевой информации / В.К. Железняк, И. С. Чернова // Фундаментальные науки. Информационные технологии. 2015. – № 12. – С. 33-39.
3. Зайцев А.П., Шелупанов А.А, Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защити информации.- Москва: «Машиностроение». -2009 г. – 508 с.
4. Laser Spy Device [Електронний ресурс]. Режим доступу: http://www.lucidscience.com/pro-laser%20spy%20device-1.aspx

# БЕЗПЕКА ІНФОРМАЦІЇ У ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

*Володимир Самотий[1], Уляна Дзелендзяк[2]*

1. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
2. Національний університет "Львівська політехніка", м. Львів, Україна

**Threats to information security in mobile applications using the technology of augmented reality is discussed. Key factors in the strategy to reduce the risks of augmented reality are presented.**

**Keywords: augmented reality, data security, keylogger, Trojans, visibility, phishing, cybercriminals.**

## Вступ

Доповнена реальність (Augmented Reality, AR), яка йде своїм технологічним корінням у 60-і роки XX століття, є близькою до того, щоб здійснити перехід в статус технології масового поширення. Але, як і будь-яка інша технологія, доповнена реальність поряд з новими можливостями несе в собі і нові ризики з точки зору безпеки. Тому, необхідно мати чітке уявлення про інтеграцію існуючих засобів безпеки в нові рішення на основі технологій доповненої реальності. Оскільки доповнена реальність поряд з новими можливостями загрожує ризиками з точки зору безпеки та конфіденційності, при її використанні необхідно задуматися про застосування засобів інформаційного захисту [2].

## Захист інформації у мобільних додатках з використанням технології доповненої реальності

На відміну від віртуальної реальності, яка переносить користувачів у змодельований візуальний світ, доповнена реальність у реальному часі накладає згенеровані комп'ютером візуальні, аудіо- та тактильні сигнали на природне поле зору людини, а також слуховий і дотиковий фон. Таким накладенням можуть виступати навігаційні дані для водія автомобіля, схеми для ремонту електронних приладів і навіть дистанційне проектування рук хірурга під час складної операції. Якщо говорити про майбутнє доповненої реальності, то думки експертів розходяться. Співзасновниця Geoloqi Ембер Кейс стверджує, що доповнена реальність перейде на новий рівень тільки тоді, коли користувачі зможуть самі створювати різні об'єкти, анімацію та програми [3]. Технологія доповненої реальності найближчим часом повинна стати доступною не тільки для розробників, але і для звичайних користувачів. Це означає, що даний контент буде дуже швидко поширюватися по мережі.

Якщо оцінювати ризики доповненої реальності, то найбільш очевидними є відволікаючі фактори. Наприклад, занадто велика кількість інформації, що знаходиться в полі зору водія, загрожує фатальними наслідками. Менш очевидною є загроза проникнення в системи доповненої реальності хакерів з подальшим вторгненням в приватне життя, викраденням цифрових даних і ризиками фізичної безпеки.

У статті, опублікованій у 2014 році в журналі Communications of the ACM, містилися попередження про потенційні загрози. Хакер може підмінити вихідну інформацію системи доповненої реальності, змушуючи користувача повірити, що згенеровані комп'ютером об'єкти (наприклад, підроблені знаки обмеження швидкості) - реальні. Можливий й інший сценарій: оскільки додаткам доповненої реальності потрібен доступ до даних, зібраних за допомогою різноманітних датчиків, шкідливий додаток може викрадати інформацію про поле зору або місцезнаходження користувача.

Для організацій, які не приготувалися до впливу доповненої реальності на мережу і безпеку, ризик є набагато серйознішим, оскільки з'являється все більше і більше додатків, які використовують доповнену реальність.

Уявіть собі двох співробітників компанії: один працівник підключає свій мобільний пристрій до принтера в офісі, щоб отримати керівництво або онлайн інструкції про заміну тонера або витягнення зімятого паперу. Другий– інженер, який використовує планшет для отримання інформації про ремонт критично важливого обладнання на електричній підстанції. Вони обидва є реальними користувачами доповненої реальності і в цьому легко побачити комерційний потенціал та переваги. Однак, крім цього, нескладно побачити і присутні ризики. Трафік, який дозволяє робити всі ці «чари», проходить через вашу мережу, розкриваючи деталі IP-адреси, місця розташування, типу пристрою, права доступу користувача і багато іншого [4]. Якщо хакер перехоплює такий трафік, то він може дізнатися про місце знаходження та інші персональні дані користувача.

У додатках AR можливості для шкідливих програм є практично безмежними. Це і кейлогери для захоплення облікових даних користувача, і мобільні троянські програми віддаленого доступу (mobile remote access Virus — mRAT), які можуть заразити пристрій та таємно перехоплювати дані та комунікації, або агент, який через мобільний пристрій завантажує шкідливе програмне забезпечення в мережу. Тому, дуже важливим питанням для організацій є забезпечення контролю додатків доповненої реальності в їхній мережі, щоб спрацювати на випередження і організувати необхідні захисні заходи. Крім того, велике значення має навчання і підвищення обізнаності персоналу, оскільки людські помилки та неуважність часто є ключовою вразливістю, якою користуються кібер-злочинці.

Наступним чинником у стратегії зниження ризиків AR має бути видимість (visibility) трафіку додатків в мережі. Щоб забезпечити захист від впливу на свої конфіденційні дані або від впровадження шкідливих даних, підприємства повинні гарантувати повну видимість в режимі реального часу і розуміння свого мережевого трафіку на протязі всього часу.

Стрімке зростання ринку віртуальної реальності робить обговорення ризиків ще більш актуальним. У звіті 2016 Emerging Technology Domains Risk Survey доповнена реальність названа однією з десяти технологічних областей, які в разі злому можуть привести до серйозних збоїв (у сфері безпеки, конфіденційності, фінансової або операційної) [2].

## Висновок

При розробленні та використанні мобільних додатків з доповненою реальністю необхідно враховувати можливі ризики з точки зору безпеки та конфіденційності. Найбільш поширеними з них є фішинг (сукупність прийомів, призначених для отримання доступу до такої секретної інформації, як логіни і паролі), а також використання різноманітних шкідливих додатків [1]. Існуючі методи та засоби підвищення безпеки (наприклад, шифрування даних, що передаються по бездротових каналах) дозволяють захистити вхідну і вихідну інформацію. Але для цього необхідно мати чітке уявлення про інтеграцію засобів безпеки в сферу доповненої реальності.

## Література


1. Горячев А. Защита мобильных приложений от кибератак / Горячев А. // Журнал “Information Security/ Информационная безопасность” №4, 2014.
2. Дуайт Дэвис. Реальные риски дополненной реальности / Дуайт Дэвис [Електронний ресурс]. – Режим доступу до ресурсу: http://www.osp.ru/cw/2016/12/13050187/
3. Неймовірно, але факт: 5 технологій, за якими майбутнє [Електронний ресурс]. – Режим доступу до ресурсу: http://news.finance.ua/ua/news/-/303645/nejmovirno-ale-fakt-5-tehnologij-za-yakymy-majbutnye
4. Чому доповнена реальність додає ризику в мережі [Електронний ресурс]. – Режим доступу до ресурсу: http://it-ua.info/news/2016/09/21/chomu-dopovnena-realnst-doda-riziku-merezh.html
5. Sandor C. Immersive mixed-reality configuration of hybrid user interfaces. / C. Sandor, A. Olwal, B. Bell and S. Feiner. // In ISMAR ‘05, pp. 110–113, 2005.

## ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ В СИСТЕМІ LINUX ВІД DOS АТАК

*Володимир Самотий, Шевченко Олександр*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The paper studied the methods of DoS-attacks were examples of their use are also provided recommendations to address them.**

**Keywords: DoS-attack, linux, smurf, fraggle, buffer overflow, overflow server log-files.**

Сучасний світ інформаційних технологій – дуже динамічний та відносно злагоджений механізм. Нові розробки з'являються щодня та потребують постійної готовності вчитись у спеціалістів, що їх обслуговують. Кожна організація намагається йти в ногу з прогресом та використовувати нові рішення для автоматизації процесів і підвищення ефективності праці персоналу, але існує і темна сторона медалі. Кількість загроз цілісності, доступності та конфіденційності інформації зростає в аналогічній прогресії. Щодня зростає необхідність в покращенні існуючих та розробці нових методів та засобів захисту. Багато підприємств у наш час використовують операційні системи сімейства UNIX для побудови корпоративних систем, однією з таких ОС є Linux.

*Метою роботи* є дослідження методів здійснення атак типу «відмова в обслуговуванні», а також методи захисту від них.

Linux – загальна назва UNIX-подібних операційних систем, які розроблені в рамках проекту GNU (проект по розробці ВПЗ). Linux працює на величезному різноманітті архітектур процесора, починаючи від ARM закінчуючи Intel x86. [1] Найбільш відомими і поширеними збірками є ArchLinux, CentOS, Debian. Linux був розроблений в спробі створити безкоштовну альтернативу комерційним UNIX-середовищам.

Хакерам набагато легше здійснити DoS-атаку на систему, ніж отримати повний доступ до неї. Існують різні причини, через які може виникнути DoS-умова, тобто така ситуація, при якій користувачі не можуть отримати доступ до ресурсів, які надає сервер, або доступ до них ускладнений:

Насичення смуги пропускання – зазвичай зловмисники користуються "флудом" - атака, пов'язана з великою кількістю зазвичай безглуздих або сформованих в неправильному форматі запитів до комп'ютерної системи або мережевого обладнання, що має своєю метою або призвела до відмови в роботі системи з-за вичерпання системних ресурсів - процесора, пам'яті або каналів зв'язку.[2] Є кілька різновидів флуду:

*HTTP-флуд* – атакуючий надсилає маленький за обсягом HTTP-пакет, але такий, щоб сервер відповів на нього пакетом, розмір якого в сотні разів більше. Навіть якщо канал сервера в десять разів ширше каналу атакуючого, то все одно є великий шанс наситити смугу пропускання жертви.

Атака Smurf або ICMP-флуд - один з найнебезпечніших видів DoS-атак, так як у комп'ютера-жертви після такої атаки відбудеться відмова в обслуговуванні практично з 100% гарантією. Зловмисник використовує трансляцію розсилку для перевірки працюючих вузлів в системі, відправляючи ping-запит. У ній по широкомовною адресою зловмисник відправляє підроблений ICMP пакет. Потім адресу атакуючого змінюється на адресу жертви. Всі вузли надсилають їй відповідь на ping-запит.

Атака Fraggle є повним аналогом Smurf-атаки, де замість ICMP пакетів використовуються пакети UDP, тому її ще називають UDP-флуд. Принцип дії цієї атаки простий: на сьомий порт жертви відправляються echo-команди по широкомовному запиту. Потім підміняється ip-адреса зловмисника на ip-адресу жертви, яка незабаром отримує

безліч відповідати на них. Їх кількість залежить від числа вузлів в мережі. Ця атака призводить до насичення смуги пропускання і повної відмови в обслуговуванні жертви.

Переповнення сервера log-файлами – некваліфікований адміністратор може неправильно налаштувати систему на своєму сервері, шляхом відмови від встановлення певний ліміт. Хакер скористається цією помилкою і буде відправляти великі за обсягом пакети, які незабаром займуть все вільне місце на жорсткому диску сервера.

Переповнення буфера - виникає в тому випадку, якщо програма через помилки програміста записує дані за межами буфера. Припустимо, програміст написав додаток для обміну даними по мережі, який працює з будь-яким протоколом. У цьому протоколі суворо вказано, що певне поле пакету максимум може містити 65536 байт даних. Але після тестування програми виявилося, що в її клієнтської частини в це поле не потрібно поміщати дані, розмір яких більше 255 байт. Тому і серверна частина прийме не більше 255 байт. Далі зловмисник змінює код додатка так, що тепер клієнтська частина відправляє всі допустимі по протоколу 65536 байт, але сервер до їх прийому не готовий. Через це виникає переповнення буфера, і користувачі не можуть отримати доступ до додатка.

Недостатня перевірка даних користувача – призводить до нескінченного або тривалого циклу або підвищеному тривалого споживання процесорних ресурсів (аж до вичерпання процесорних ресурсів) або виділення великого обсягу оперативної пам'яті (аж до вичерпання доступної пам'яті).[2]

Недоліки в програмному коді – зловмисники шукають помилки в програмному коді будь-якої програми або операційної системи, змушують її обробляти такі виняткові ситуації, які вона обробляти не вміє. За рахунок цього виникають помилки

DoS-атаки на уразливості в програмному забезпеченні на DNS-серверах. Їх ще називають атаками на кеш. У процесі цієї атаки зловмисник підміняє IP-адресу DNS-сервера домену жертви. Після чого атакується при запиті HTML-сторінки, потрапляє або в «чорну діру» (якщо IP-адреса був замінений на неіснуючу), або на сервер зловмисника. Другий випадок більш фатальний, так як зловмисник легко може отримати доступ до особистих даних нічого не підозрюючи жертви. Розглянемо на прикладі, як це відбувається. Припустимо, що клієнт хоче потрапити на Web-вузол компанії microsoft.com. Але використавши уразливість в DNS-сервері компанії, зловмисник підмінив IP-адреса вузла microsoft.com на свій. Тепер жертва автоматично перенаправляється на вузол до атакуючого.

Більшість наведених методів атаки легко уникнути коректним налаштуванням серверу. Також одним з ефективних способів захист серверу на ОС Linux, є створення скрипту, який здійснює перевірку log-файлів та активних з’єднань серверу на наявність великої кількості звернень з однієї IP-адреси.

## Література


1. Войтов Н. М. Основи роботи з Linux / Н. М. Войтов. – Москва: ДМК Пресс, 2011. – 216 с.
2. Флєнов М. Linux очима хакера / Михайло Флєнов. – Санкт-Петербург: БХВ-Петербург, 2012. – 467 с.

# ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНО-КЕРУЮЧОЇ СИСТЕМИ УПРАВЛІННЯ ОХОРОНОЮ ПРАЦІ ПІДПРИЄМСТВ НА ОСНОВІ ВИКОРИСТАННЯ МУЛЬТИАГЕНТНИХ ТЕХНОЛОГІЙ

*Аліна Сірик*

Національний університет харчових технологій, м. Київ, Україна

**In the report the mathematical model of intelligent agents in the structure information management system, which differs from the existing informational model of the production environment, which describes the parameters of harmful and dangerous factors. This model allows to take into account the dynamics of the state vector the safety and the change of the vector regulatory framework for labor safety in the power sector of the food industry.**

**Keywords: labor protection, regulatory and legal framework, information management system, energy company, information object, intelligent agent, food company.**

На сучасних підприємствах харчової промисловості, а зокрема і в енергетичному господарстві таких підприємств, широко використовуються інформаційно-керуючі системи. За допомогою таких систем керівник енергетичного господарства спілкується з диспетчерами, черговими енергетиками, дільничними підрозділами та іншими. Крім того, дані системи можуть бути використані для пошуку рішення щодо вибору сукупності заходів для підвищення рівня безпеки праці в енергетичному господарстві підприємств харчової промисловості. В доповіді під поняттям «агент» розуміється програма, яка допомагає посадовій особі вирішувати службові питання. Ця програма автоматизую роботу посадової особи, але ні в якому разі не заміняє посадову особу. Програма надає посадовій особі альтернативні рішення із прорахованими показниками ефективності та збитків по кожному рішенню, а посадова особа вже сама приймає рішення на виконання тих чи інших заходів, виходячи із своєї суб'єктивної думки, досвіду, почуттів, тощо. Разом з тим, агенти є у кожної посадової особи. Всі агенти виконують ряд функцій. Історично склалось так, що агенти мали б замінити секретаря у кожної посадової особи. В примітивному розумінні агент має виконувати всі функції секретаря-референта (звісно, які можна автоматизувати): складати графік роботи своєму керівнику, узгоджувати з іншими агентами час наради по визначеним питанням, надавати керівнику інформацію про поточний стан справ на підприємстві, коригувати порядок денний керівника у відповідності до розпоряджень верхніх керівників, надавати інформацію по запиту із нормативної бази, надавати пропозиції щодо сукупності заходів по забезпеченню безпеки праці на виробництві та багато інших функцій. В доповіді запропоновано математичну модель інформаційного агента [1] посадової особи енергетичного господарства підприємств харчової промисловості. Дані агенти діють в рамках функціонування інформаційно-керуючої системи управління охороною праці в енергетичному господарстві підприємств харчової промисловості. Основними функціями агентів є (на відміну від традиційних) врахування зміни вхідних даних законодавчо-номативної бази з охорони праці та відслідковування динаміки зміни вектору стану охорони праці, який описується параметрами небезпечних та шкідливих факторів виробничого середовища. При цьому всі агенти узгоджують між собою і визначають оптимальну сукупність заходів забезпечення безпеки праці. Після цього посадові особи приймають рішення на виконання цих заходів. Змінений вектор стану, мультиагентної системи працює на новому циклі, знову пропонує наступну сукупність, знову якісь заходи виконуються, щось покращується і так далі.

В доповіді інтелектуальний агент, пропонується визначати як структуру вигляду: $IA = <N_{IA}, SA, VIA, M_{VB}, VO>$, де $N_{IA}$ – ім'я інтелектуального агента; $SA$ – структура атрибутів, яка визначається аналогічно структурі атрибутів для інформаційних об'єктів;

*VIA* = {IA} – множина вкладених інтелектуального агента; $M_{VB}$ – механізм вибору моделі функціонування, *VO* = {O} – множина інформаційних об'єктів, що реалізовують сценарії роботи інтелектуального агента.

Інтелектуальний агент на підставі критеріїв вибору моделі функціонування, закладених в $M_{VB}$, приймає рішення про реалізацію в даний момент часу деякого сценарію роботи і ініціалізує відповідний інформаційний об'єкт. Інформаційний простір інтелектуального агента визначається як сукупність інформаційних об'єктів та інтелектуальних агентів, що оточують $I_{Ai}$ і взаємодіють з ним: $V_{IA_i} = (AR^i_{IA}, AR^i_{IO})$, де

$$AR^i_{IA} = (N_{IA\,j}, A^{\xi}_{IA_j}, ..., A^{\psi}_{IA_j}, N_{IA\,I}, A^{\xi}_{IA_I}, ..., A^{\psi}_{IA_I}),$$

$$AR^i_{IO} = (N_{IO\,j}, A^{\xi}_{IO_j}, ..., A^{\psi}_{IO_j}, N_{IO\,I}, A^{\xi}_{IO_I}, ..., A^{\psi}_{IO_I}).$$

Модель вибору поведінки *IA* може бути подано: *MVB* = (*MIS, MG, MSR, MA*), де *MIS* – модель інформаційного середовища, *MG* – модель цілевизначення, *MSR* – модель пошуку рішення, *MA* – модель активних дій.

Модель цілевизначення будується таким чином

$$MG_{IA_i} = (SS_{IA_i}, FSS_{IA_i}, GS_{IA_i}, G^{top}_{IA_i}, G^{down}_{IA_i}, FG^{D}_{IA_i}, FG^{S}_{IA_i}, FAG_{IA_i}, SMA_{IA_i}(t)).$$

Тут *SS* – множина стратегій, що розуміються як методи вибору цілей $SS = (S_i | i = 1,...,n)$, *FSS* – функція вибору стратегії; *GS* – множина статичних цілей, $G^{top}$ – множина цілей, що отримуються даним *IA* від агентів більш високого рівня ієрархії, $G^{down}$ – множина цілей, які можуть бути передані *IA* нижніх рівнів; $FG^D$ – функція формування динамічних цілей, $FG^S$ – функція вибору статичних цілей; *FAG* – функція вибору активних цілей, тобто цілей, прийнятих до реалізації; *SMA* – стан навколишнього мультиагентного оточення. Під пошуком рішення слід розуміти знаходження шляху досягнення мети або цілей даним *IA* в поточному стані мультиагентного оточення. Оскільки різні структурні підрозділи енергетичного господарства підприємств харчової промисловості володіють своєю специфікою в тому числі і при прийнятті рішень, то навряд чи є можливим застосування деякого універсального методу пошуку рішення для всіх підсистем інформаційно-керуючої системи.

В запропонованій моделі *IA* пропонується наступний варіант пошуку рішення. Вважаємо, що *IA* має визначену множину статичних цілей $GS = \{gs^i | i = 1,...,n\}$. Апріорі відомі шляхи досягнення цілей, тобто побудовані інформаційні об'єкти $(IO^i | i = 1,...,n)$, функціонування яких повинне вести до $gs^i$. Тут кожен інформаційний об'єкт покриває деякий план. Усередині ж цього плану, тобто в моделі поведінки інформаційного об'єкта, можуть бути сформовані довільні повідомлення і довільні послідовності дій. Тоді модель пошуку рішення задається функцією пошуку рішення $SR: GS \to VO$ де *VO* – множина вкладених інформаційних об'єктів і-го інформаційного агента. Це відображення однозначне, але не взаємно, оскільки можливо, що декілька цілей досягаються одним і тим же інформаційним об'єктом. Модель активних дій визначається відображенням $AD: GA \to VO$, яке вибирає необхідні для запуску у нинішній момент інформаційного об'єкта. Побудована модель пошуку рішення в узагальненій моделі інтелектуального агента дозволяє описати такі відомі класи моделей реалізації поведінки як моделі із зумовленою кінцевою множиною елементарних дій; моделі з множиною планів; моделі з довільними повідомленнями і діями. На базі даної моделі можуть створюватися нові моделі реалізації поведінки інтелектуального агента, що поєднують механізми різних класів.

## Література

1. Глибовець А.М. Програмні агенти / Глибовець А.М., Глибовець М.М., Гороховський С.С., Сидоренко М.О. // М. — К.: НаУКМА, 2013, – 204 с.

# APPLICATION THE ARTIFICIAL NEURAL NETWORK IN THE INTRUSION DETECTION SYSTEM

*Anna Slyvka, Rostyslav Grynyk*

Lviv State University of Life Safety, Lviv, Ukraine

**Defined a term "intrusion detection system" and described the main classification. Shown the general structure of the neural network. Descripted the options of neural networks usage in systems, which detect network attacks and described the main positive and negative aspects of such systems. Analyzed the advantages of using fuzzy neural networks in IDS.**

**Keywords: artificial neural network, fuzzy set, intrusion detection system (IDS).**

Having become a sensation in the 1950s-1960s, neural networks as the embodiment of physiological and biological aspects remained in the shadow of traditional computing and were forgotten for long, but interest in neural networks (hereafter referred to as ANN) is growing rapidly these days due to the ability to use ANN in a wide variety of human activities.

Many life-sustaining activities that were within human intellect's control only as it was mistakenly considered, appeared to be susceptible to theoretical and applied computing capabilities pertaining to "artificial intelligence." ANNs are inspired by biology, since they consist of elements, which features are similar to most elementary functions of biological neurons [1]. ANNs are constructed by artificial interacting neurons that act as simple handlers of information; a figure of simple neural network is suggested by Fig. 1. Thus, creating a multiple network of artificial neurons and ensuring control of their interaction, we can perform quite complex tasks.

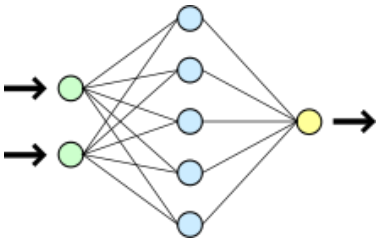


*Fig. 1. The scheme of the simple neural network. Green represents the input neurons, blue - hidden neurons, yellow - output neuron*

Such basic properties as educability, generalization and abstraction justify the use of neural networks in intrusion detection systems. Intrusion detection system (Intrusion) is a hardware or software tool designed to detect unauthorized attempts to access a computer system or network or unauthorized management via the Internet [2]. The number of IDS technologies have emerged. Each type has its own pros and cons in features of detection, configuration, and overall cost.

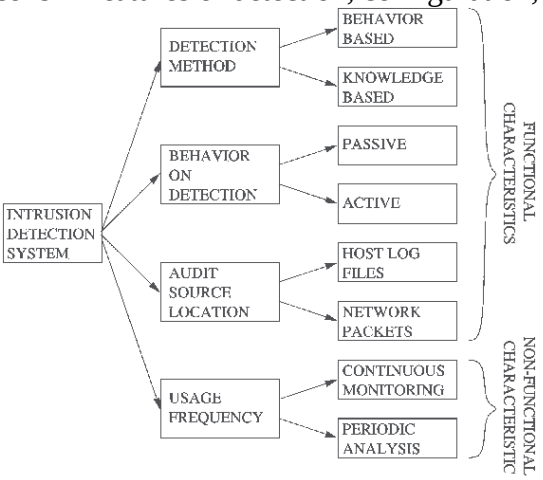



*Fig. 2. Characteristics of intrusion detection system [3].*

There are two types of intrusion detection systems: network IDS and host IDS. Intrusion detection process is a complex operation that consists of three main components:

• detection of patterns that indicate any violations required by security policy;
• identification of the sources that may contain the patterns of violations of security policy;
• usage the various methods of information analysis [4].

Intrusion detection systems provide an additional level of protection of information systems when combined with intrusion prevention system (IPS). Often both types operate as one, thus forming a comprehensive system of IDPS (IDS i IPS).

In modern systems of detecting network intrusion attacks (IDS) one can observe different modes of using neural networks. For example, the neural network can be used as a complement to existing expert systems aimed at filtering the inbox in order to reduce the number of false operations, which are common in most expert systems. Thus, sensitivity of the system increases as the expert system receives data only on events that are considered suspicious. If the neural network began identify new attacks as a result of training, the expert system must be updated, otherwise these attacks will be simply ignored.

If the neural network is a complete intrusion detection system, the analysis of information with regard to system-related misuse is conducted during traffic processing. Any cases that are identified as possible attacks, are processed by the automatic attack response system or redirected to the security administrator. In comparison with the previous approach, this principle possesses only one level of analysis, which greatly accelerates the speed of its work. In addition, such an intrusion detection system is highly adaptive.

One of the main drawbacks of the neural network is preconception, or "opacity" of formation of results after the analysis. However, hybrid neuro-expert or neuro-fuzzy systems allow to see the system of fuzzy rules in the structure that are automatically adjusted in neural network teaching. The adaptive property y of fuzzy neural networks enables:

• to solve separate tasks of identifying threats;
• to juxtapose the users' behavior with existing templates in the system;
• to generate new rules automatically when the new types of threats appear.

One way to optimize the intrusion detection system is to combine it with genetic algorithms. For example, to protect networks from application-governmental attacks designed to breach the availability of resources, the neural network is used to detect tokens of attacks in network traffic, identification of data formats, which are transmitted, and genetic algorithms - to get close to the best decision in managing traffic routes and parameters in the presence of non-identification attacks accuracy in terms of lack of information or information "noise". In addition, fuzzy sets can be applied to the implementation of active security audit of the system. Fuzzy neural network has the following advantages:

• distributed computing parallelism;
• adaptive neuro-fuzzy information security systems (fuzzy rules);
• the possibility of classifying threats;
• objectivity, or "transparency" of structure analysis;
• functional stability and security of the components.

Development of intellectual instruments of detection of attacks and unauthorized information processes in a network, which is built on the benefits of adaptability property, has always been a promising trend in the use of neural networks in intrusion detection systems.

## Literature


1. Why artificial neural networks?. [Electronic resource] - Access: http://www.victoria.lviv.ua/html/wosserman/vstup.htm#v2
2. The system of detection of attacks. [Electronic resource] - Access https://uk.wikipedia.org/wiki/IDS
3. A Study on Recent Trends and Developments in Intrusion Detection System.- IOSR Journal of Computer Engineering (IOSR-JCE) [Electronic resource] - http://www.iosrjournals.org/
4. Intrusion detection systems and their application tools. [Electronic resource] - Access: http://5fan.ru/wievjob.php?id=3960

# БІТ-РЕВЕРСНИЙ АЛГОРИТМ ПЕРЕСТАВЛЕННЯ ІНФОМАЦІЙНИХ ДАНИХ

*Богдан Смерека, Ігор Процько*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The bit-reversal algorithms for mupping from one sequence to another are considered. The algorithm of the bit-reversed number sequence with powers of two is analized. The main operations of the additions/substructions of *rev*(4*i*-1) to *rev*(1) or *rev*(2) are presented this algorithm.**

**Keywords: bit-reversal algorithm, permutation, numerical computation.**

Перестановки інформаційних даних широко застосовуються в технологіях захисту як мовних [1,2] так й інших даних найрізноманітнішої природи. Для перепорядкування послідовності даних широко застосовують їх перерозміщення на основі операції реверсу послідовності даних. В двовимірному переставленні інформаційних даних матимемо вид за рис. 1.

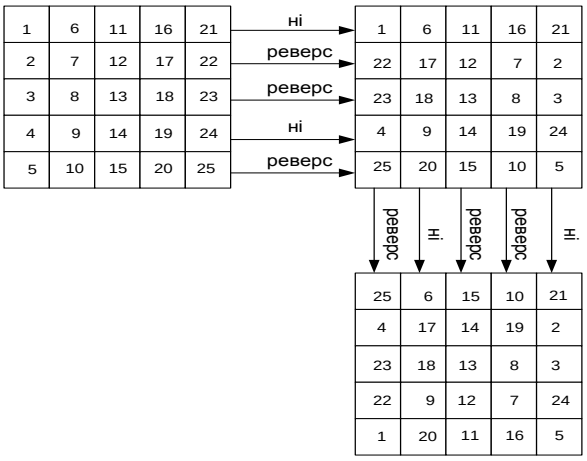



Рис. 1. Двовимірне переставленні послідовності інформаційних даних на основі операції реверсу

Також дана операція стосується процесу ефективної обчислення ДПФ обсягів $N=2^n$. Алгоритми швидкого перетворення Фур'є (ШПФ) зводяться до виконання ряду більш коротких ДПФ [3]. В цьому випадку розділяють вхідну послідовність перетворення $x[n]$ на дві частини обсягом $N/2$, в одну з яких входять $x[n]$ з парними номерами, а в другу – з непарними (рис. 2). Алгоритми ШПФ, які основані на разбитті послідовності $x[n]$ на частини, називаються алгоритмами з проріджанням в часі або по частоті. В потоковому графі (рис.2) ребра позначені коефіцієнтами $W^r_N = e^{-j(2\pi/N)r}$, включають $N$ комплексних множень і $N$ комплексних додавань на кожному кроці. В загальному кількість кроків обчислення рівне $log_2N$, і відповідно, складність алгоритму оцінюється як $O(N\ log_2N)$. Алгоритм суттєво економить час виконання в порівнянні з прямим методом обчислення, так наприклад для $N = 2^{10} = 1024$ з прямим обчисленням $N^2 = 2^{20} = 1\ 048\ 576$, а $N \log_2 N = 10\ 240$, тобто ефективність алгоритму збільшується на два порядки.

З натуральної послідовності індексів $i$= 0, 1, 2, 3, 4, 5, 6, 7 у вхідних даних $x[i]$ отримуємо послідовності індексів $i$=0, 4, 2, 6, 1, 5, 3, 7 змінену за операцією реверсу бітів для вихідних даних $X[i]$. Тобто, в потоковому графі ШПФ обсягів $N=2^n$ отримуємо послідовність вихідних даних $X[i]$ в біт реверсивному порядку.

Під операцією *реверсу бітів* або зворотнім переставленням бітів (bit-reversal permutation) розуміють розміщення бітів в бінарному даному в зворотньому порядку. Тобто, *rev*(i) - це *n*-бітове ціле число, утворене шляхом розміщення в зворотньому порядку

старших бітів на місці молодших бітів початкового бінарного представлення ("задом наперед").

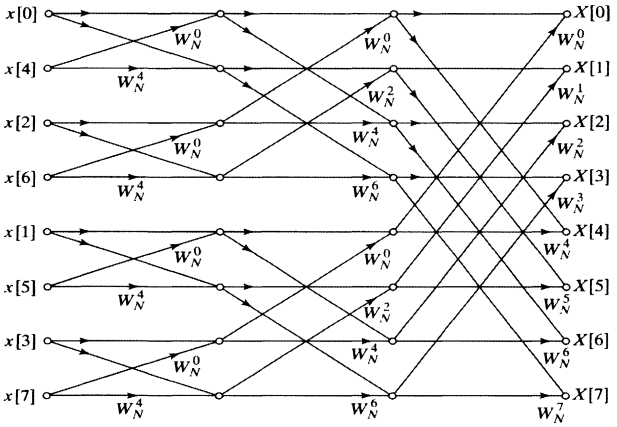



Рис. 2. Потоковий граф ШПФ обчислення 8-точкового ДПФ
з натуральною вхідною послідовністю $x[i]$ і біт реверсивною на виході $X[i]$

Існують різноманітні алгоритми виконання реверсу бітів [3]. Один з методів виконання реверсу бітів проводиться за допомогою бітових операцій [4]. Наприклад, виконання реверсу бітів для 32-розрядного даного $x$ необхідно двічі виконати зсув бітів на шістнадцять розрядів, що відповідають виразу: $(x \,\&\, 0000FFFF_{16}) << 16 \mid (x \,\&\, FFFF0000_{16}) >> 16$.

Виконання зсувів та двох логічних операцій можна замінити виконанням арифметичних операцій додавання або віднімання. Варто зауважити, що $rev(i) = \sim rev(N\text{-}1\text{-}i)$, де ~ операція $n$-розрядної інверсії бітових значень, $i=0(1)N/2\text{-}1$. Тобто, достатньо обчислити біт-реверсну послідовність індексів на інтервалі для половини значень. Для цього алгоритм визначення біт-реверсної послідовності індексів вихідних даних використовує початкові значення $rev(1)$, $rev(2)$, $rev(N/2\text{-}1)$, де $N=2^n$, тобто виконання операцій додавання/віднімання проводиться над $n$ - розрядним двійковим числом.

Наприклад, для $N=16$, визначення $N/2=8$ значень 4-розрядної послідовності біт-реверстних індексів проводиться за початковими значеннями $rev(1)=1000$, $rev(2)=0100$, $rev(7)=1110$, які легко сформувати в $n$-бітових числах. Обчислення біт-реверсної послідовності решти індексів виконується за допомогою операцій:

$rev(3)=rev(1)+rev(2)$; $rev(6)=rev(7)-rev(1)$; $rev(5)=rev(7)-rev(2)$; $rev(4)=rev(5)-rev(1)$.

В загальному для $N=2^n$ алгоритм зводиться до виділення $k=2^{n-3}$ секцій по чотири $n$-розрядних біт-реверстних послідовностей. Використовуючи початкові значення $rev(1)=100\ldots0$ і $rev(2)=010\ldots0$ та крайні значення кожної секції $rev(4i\text{-}1)$, де $i=2,3,\ldots,k$ , виконується обчислення біт-реверсної послідовності решти індексів кожної секції за допомогою операцій додавання або віднімання.

На програмному рівні алгоритм реалізується з використанням логічних та арифметичних (додавання, віднімання) операцій для переставлення послідовності даних на основі біт-реверсу їх індексів, який може застосовуватись в багатьох прикладних задачах захисту інформації.

## Література


1. Патент 25783А Україна, G06F7/04. Пристрій для формування і відбору переставлень. /Процько І.О., Рашкевич Ю.М.,(Україна) /Заявл. 24.12.96; Опубл. 30.10.98, Бюл. №5.
2. D. Slimani, F. Merazka, Encryption of speech signal with multiple secret keys. 3rd World Conference on Information Technology (WCIT-2012), Vol 03 (2013) p. 808-814 .
3. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. - М.: Мир, 1978. -848с.
4. Anne Cathrine Elster, Fast bit-reversal algorithms. International Conference on Acoustics, Speech, and Signal Processing, ICASSP-88, 1989, vol.2, p.1099 - 1102.
5. Г. Уоррен. Алгоритмические трюки для программистов. — М: Издательский дом "Вильямс", 2003.-288с.

# ПОЄДНАННЯ ТА МОДИФІКАЦІЯ МЕТОДОЛОГІЙ ДЛЯ РОЗРОБЛЕННЯ ГНУЧКОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

*Тарас Стецяк, Володимир Ромака*

Національний університет "Львівська політехніка", м. Львів, Україна

**Combination of main principles of Adaptive Project Framework, Agile Methodology and Information Technology Infrastructure Library in order to develop advice and recommendations to obtain flexible and dynamic cyber-security strategies.**

Аналіз документів Європейського агентства з мережевої та інформаційної безпеки [1-3], які окреслюють підходи до впровадження стратегії кібербезпеки, показав, що дані напрацювання, даючи основні поняття щодо змісту стратегій, носять здебільшого суб'єктивний характер, оскільки базуються лише на досвіді розробників.

Ми вважаємо, що даним напрацюванням *бракує підходу з точки зору менеджменту*. Іншими словами, при розробленні кожного розділу спочатку самої стратегії, від визначення мети стратегії до залучення всіх зацікавлених сторін, міжнародного співробітництва та забезпечення балансу між правом особи на конфіденційність, правом громадськості на інформацію та необхідністю держави забезпечити безпеку своїх громадян, інфраструктури та власних інтересів, і аж до розроблення конкретних політик, рекомендацій, правил, інструкцій, *повинна застосовуватися конкретна методологія управління проектом*.

З іншого боку, методології, що нині застосовуються в кібербезпеці, постійно зазнають змін та корекцій, оскільки виникають все нові вразливості і загрози, а відтак вимоги до систем захисту. Більше того, виникають фактори, що суттєво змінюють середовище функціонування як конкретної політики безпеки для певного підприємства чи галузі, так і стратегій кібербезпеки цілої країни. У той же час, автори [1-3] зазначають, що стратегія повинна мати цілісний, зв'язаний, всеохоплюючий та обґрунтований характер, бути гнучкою та пружною.

*Метою* представленого дослідження є розроблення підходу впровадження стратегії кібербезпеки, який усуне описані вище недоліки, суть якого в розробленні гібридної методології шляхом об'єднанні кількох найбільш прийнятних методологій управління проектами (розроблення стратегії розглядається як проект).

Основною методологією, яку обрали автори, і на котрій буде базуватися стратегія, є адаптивне управління проектами. У цій методології обсяг проекту є змінною, а час і вартість є константами для проекту. Таким чином, в ході реалізації проекту, обсяг проекту коригується для того, щоб отримати максимальну ефективність та найвищий коефіцієнт повернення інвестицій.

Оригінальна авторська методика ставить в центр клієнта при виборі напрямів та шляхів досягнення максимальної ефективності [4]. У випадку ж забезпечення кібербезпеки та розроблення стратегії кібербезпеки, доцільно за основу взяти безперервність виконання основної діяльності підприємства, галузі тощо, а також рівень безпеки найслабшої ланки при здійсненні цієї діяльності. Основні принципи: орієнтації на кінцеву мету, ґрунтування на окремих компонентах, систематично повторюваних циклів, керованості ризиком, здатності витримувати зміни. Кроки, або фази методології: моніторинг, дослідження та оцінювання, планування, реалізація (шляхом циклічного планування, імплементації, щоденних зустрічей, перегляду результатів та постійного вдосконалення), контрольна точка (вивантаження та імплементація всього досягнутого в попередніх фазах), перегляд результатів.

Гнучка методологія застосовується, у першу чергу, щоб забезпечити дотримання п'ятого принципу адаптивного управління проектами – здатності витримувати зміни. У процесі управління проектом важливо вміння швидко адаптуватися до змін, відстежувати

останні тенденції розвитку і вміти одержувати з них вигоду. Також необхідно вміння створювати динамічну команду проекту на основі співпраці і гнучкості, можливості знаходження компромісу. Важливу роль відіграють зацікавлені сторони. Вони контролюють і перевіряють проект на кожній стадії, а члени команди, у свою чергу, правильно і своєчасно коригують проект, забезпечуючи найвищий з можливих коефіцієнт повернення інвестицій та безперервність виконання основної діяльності.

Методологія інфраструктури інформаційних технологій - бібліотека найбільш ефективних методів організації та управління для підприємств та галузей, що ведуть свою діяльність в області інформаційних технологій, а також для будь-яких суб'єктів, які бажають побудувати ефективний процес управління і взаємодії як всередині організації, будь то підприємство, організація чи ціла країна, так і з зовнішніми зацікавленими сторонами. Ця методологія потрібна з двох причин: необхідність залучення всіх зацікавлених сторін, в тому числі на міжнародному рівні; кібербезпека нерозривно зв'язана з IT-сферою - програмним забезпеченням, протоколами передачі даних, алгоритмами шифрування, принципами побудови баз даних, тощо, і тому при розробленні стратегії на питаннях розроблення та імплементації як прикладних програм так і програм захисту має бути зроблений особливий акцент. Базові процеси методології: управління інцидентами, управління проблемами, управління конфігураціями, управління змінами, управління релізами, управління рівнем послуг, управління потужностями, управління доступністю, управління безперервністю, управління фінансами.

То ж, гнучка методологія і методологія інфраструктури інформаційних технологій є допоміжними до методології адаптивного управління проектами, проте необхідними для досягнення цілісності стратегії. Допоміжні методології застосовуються лише там де це доцільно, детальніше і на прикладі застосування комбінації трьох методологій буде подане в наступних роботах авторів цієї статті.

Чим же ця методологія, заснована на комбінації трьох методологій проект-менеджменту, відрізняється від звичних методологій і в чому її перевага ?

По-перше, ця методологія буде комплексною і всеохоплюючою не лише з точки зору не то керівництва, IT-менеджерів, менеджерів з захисту інформації чи користувача, а з точки зору будь-якої зацікавленої сторони, оскільки, за необхідності, враховує їх думку щодо особливостей, нюансів та важливості кожного бізнес-процесу, їх вхідної та вихідної інформації. По-друге, комбінації принципів методологій, що були розглянуті в статті, дають змогу включити в кожен розділ стратегії кібербезпеки та похідних від неї документів такі важливі і нерозривно зв'язані в наш час з кібербезпекою питання: плану дій у випадку непередбачуваних обставин, атак, збоїв, відмов, кризис-менеджменту, плану відновлення, ліквідації або зведення до мінімуму наслідків непередбачуваних обставин, атак, збоїв, відмов, швидкої та адекватної реакції на зміни в кібер-середовищі, не виділяючи для цього окремих, "відірваних" та узагальнених розділів.

## Література


1. ENISA National Cyber Security Strategies [Electronic resource] / ENISA project team // Setting the course for national efforts to strengthen security in cyberspace. – 2012. – 15 p. – Access mode: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
2. ENISA National Cyber Security Strategies [Electronic resource] / ENISA project team // Practical Guide on Development and Execution. – 2012. – 45 p. – Access mode: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
3. ENISA An evaluation Framework for National Cyber Security Strategies' [Electronic resource] / ENISA project team // ISBN: 978-92-9204-109-0. – 2014. – 42 p. – Access mode: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
4. Robert K. Wysocki Adaptive Project Framework: Managing Complexity in the Face of Uncertainty / Robert K. Wysocki // Published by Addison-Wesley Professional. – 2010. – 384 p.

# ШИФРУВАННЯ КЛЮЧІВ БАЗИ ДАНИХ В СЕРЕДОВИЩІ MS SQL SERVER

*Григорій Тріль*

Львівський Торговельно-Економічний Університет, м. Львів, Україна

**In Microsoft SQL Server 2008 for the first time implemented a transparent database encryption. Transparent Encryption encodes the entire database. When a data page is written from memory to disk, it is encrypted. When the page is loaded back to RAM. The database on the disk is completely encrypted.**

**Keywords: database, management system, transparent encryption, administrator accounts, privileged access, user, coded keys, asymmetric method.**

Одним з основних видів шифрування баз даних є прозоре шифрування (TDE), в якому шифрування і дешифрування виконуються абсолютно прозоро для користувачів. Використовувати переваги шифрування може будь-який користувач, який для зберігання своїх даних використовує систему керування базами даних Microsoft SQL Server. При цьому не потрібно модифікувати або доопрацьовувати програми.

Зокрема, у Microsoft SQL Server 2012 функції шифрування значно покращено і розширено. Для збільшення надійності криптографічного захисту й зменшення навантаження на систему застосовується спеціальна ієрархія ключів:

1. Кожна база даних шифрується за допомогою спеціального ключа - Database Encryption Key.
2. Database Encryption Key шифрується сертифікатом, який створений в базі даних Master.
3. Сертифікат бази даних Master шифрується її головним ключем.
4. Головний ключ БД Master шифрується головним ключем служби Service Master Key.
5. Головний ключ служби SMK шифрується службою захисту даних операційної системи.

Наочно схема роботи із зашифрованою базою даних виглядає наступним чином:

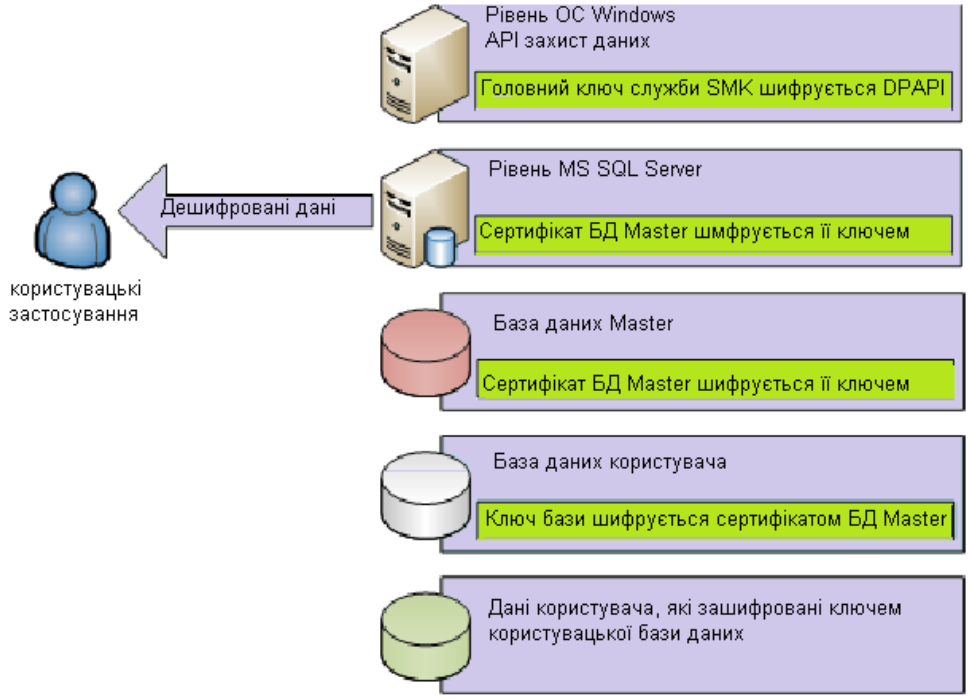



Рис. 1. Схема роботи бази даних із зашифрованим ключем

У наведеній схемі використовується, як симетричне, так і асиметричне шифрування. Симетричне шифрування є менш вимогливо до ресурсів системи, але вкрай вразливе в управлінні криптоключа. Асиметричний метод, навпаки, захищений на етапі менеджменту ключів, але, відповідно, вимагає значно більше обчислювальних ресурсів. Використання комбінації обох методів дозволяє нейтралізувати недоліки кожного з них, але підвищити безпеку і продуктивність в цілому.

Так, база даних захищається більш швидким симетричним шифруванням, що, при обліку великих обсягів інформації, є кращим. У свою чергу, ассиметричному шифрування піддаються ключі шифрування бази, розмір яких незрівнянно малий, але критичність їх захисту вище. Використання такого підходу на серверах з низьким рівнем вводу/виводу, низьким споживанням процесорного часу і оперативною пам'яттю, що є достатньою для зберігання великих масивів інформації, впливає на 3-5% продуктивності при підключенні TDE. Сервери з меншим об'ємом ОЗП, програмне забезпечення яких навантажують ЦП і систему вводу/виводу, будуть страждати на 28%, що досягається асинхронним виконанням процедур SQL (розпаралелення процесів).

При включенні функції Transparent Data Encryption для будь-якої користувацької бази відбувається наступне:

• шифрується база, для якої включено шифрування;

• шифрується журнал транзакцій для користувача бази даних;

• шифрується загальна тимчасова база даних tempdb.

Також слід зазначити, що Transparent Data Encryption (TDE) не замінює криптографічні можливості SQL Server 2005. Шифрування в MS SQL Server 2005 року працює на рівні значень і стовпців, а Transparent Data Encryption (TDE) – на рівні бази даних (на більш високому рівні). Такий підхід не захистить від системного адміністратора або адміністратора SQL Server, але ідеально протистоїть крадіжці або вилучення самої бази даних.

Microsoft SQL Server створює власний сертифікат, який приймається клієнтом, але шифрує лише інформацію про з'єднання. В Microsoft SQL Server завжди шифруються мережеві пакети, що пов'язані з входом в систему. Якщо сертифікат не був наданий на сервері під час запуску, SQL Server створює сертифікат, який використовується для розшифровки пакетів входу. Таке шифрування забезпечує:

- надійність з'єднання між сервером СУБД і клієнтом;

- пакети передачі повідомлень та входу в систему та СКБД підтримуються протоколом TLS.

Для шифрувати інформації по каналу «клієнт-сервер-клієнт» потрібно видаляти сертифікат кореневого сервера, імпортувати його на клієнтські станції та налаштувати схему взаємодії криптоалгоритмів. Найбільш результативною схемою буде шифрування трафіку симетричним методом тоді, коли ключі захищаються відкритими сертифікатами.

Новітні програмні застосування Microsoft SQL Server 2012 дозволяють системним адміністраторам та програмістам суттєво покращити та інтегрувати програмне забезпечення безпеки системи керування базами даних. Це забезпечується завдяки розширеним можливостям комбінування блокових і потокових технологій шифрування з симетричними і асиметричними методами, реалізації прозорого шифрування баз даних, захисту мережевих з'єднань і окремих програмних застосувань.

## Література


1. М. Каба. MySQL и Perl – СПб.: Питер, 2001.
2. Бен Форта SQL за 10 минут – М: Вильямс, 2015.

# ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ТУРИСТИЧНОМУ БІЗНЕСІ

*Ірина Тучковська*

Львівський торговельно-економічний університет, м. Львів, Україна

**The article deals with theoretical and methodological framework and practical tools of information technology for information security in the tourism business. The role and place of information technology in management of tourism enterprises. The basic steps for creating operating systems use different types of information technologies in tourism.**

**Keywords: information technology, information security, tourism, strategic management, management, e-business, virtual organization.**

Оскільки туристичний ринок є одним із найбільш динамічних та, на відміну від інших риків, характеризується великою кількістю учасників, значною їх географічною роз'єднаністю, швидким оновленням інформації, то основною метою є розроблення теоретичних і методологічних засад та практичних рекомендацій щодо застосування сучасних інформаційних технологій (ІТ) в управлінні підприємствами туристичного бізнесу. Відповідно до поставленої мети передбачено вирішення таких завдань: поглибити теоретико-методологічні засади застосування ІТ для забезпечення інформаційної безпеки в управлінні суб'єктами туристичної діяльності; систематизувати інноваційні підходи до маркетингової діяльності туристичних підприємств із застосуванням різноманітних ІТ.

Проблема інформаційної безпеки має давнє походження і стала особливо важливою у наш час, коли використання інформаційних технологій відбувається вже практично у всіх сферах нашого життя. Як показала практика, туристична сфера є інформаційно-насиченою, оскільки характеризується різноманітністю ділових зв'язків із партнерами, динамічністю бізнес-процесів, індивідуалізацією туристичних послуг, технологічним удосконаленням та високою конкуренцією. У зв'язку з цим, розвиток туристичного бізнесу стає неможливим без впровадження сучасних ІТ, які забезпечують: інтеграцію і зв'язок; покращання якості послуг; передачу великого обсягу інформації; збільшення швидкості обслуговування та ефективність діяльності; можливість враховувати потреби кожного індивідуального клієнта; ефективний зворотній зв'язок. У практичній діяльності туристичних підприємств застосовуються різноманітні види ІТ, а саме: глобальні розподільчі системи; системи бронювання та резервування; електронні інформаційні системи; інформаційні системи менеджменту; мобільні системи зв'язку; послуги глобальної комп'ютерної мережі Інтернет.

Застосування сучасних ІТ підвищує інформаційну безпеку та якість туристичних послуг. Нині в туризмі використовують глобальні розподільчі системи (Global Distribution System), які забезпечують швидке і зручне бронювання квитків на транспорт, резервування місць у готелі, прокат автомобілів, обмін валют, замовлення квитків на спортивні та культурні заходи і т.д. Найбільшими глобальними розподільчими системами на міжнародному ринку туристичних послуг є AMADEUS, Worldspan, Galileo, Sabre. Такі системи дозволяють резервувати всі основні складові туристичної інфраструктури, тобто вони фактично утворюють загальну інформаційну систему, яка пропонує розподільчі мережі для всієї туристичної галузі за забезпечує її інформаційну безпеку.

Останнім часом із динамічним розвитком комп'ютерної техніки, можливістю вільного доступу до мереж, появою і використанням різноманітних новітніх ІТ у різних галузях економіки набули поширення комп'ютерні системи бронювання. Зростання обсягів туризму впливає на транспортну і комунікаційну сфери, які внаслідок зростаючого

попиту на подорожування стали одними з головних споживачів інновацій і продуктів інформаційних технологій, а саме систем комп'ютерного бронювання, електронних систем інформації і комунікацій. Зі збільшенням кількості авіакомпаній, транспортних засобів, а також зростання обсягів авіаперевезень постала необхідність створення і впровадження комп'ютерних систем бронювання, останні ж стали основним інструментом для резервування авіаквитків.

Комп'ютерні системи бронювання дозволяють суттєво покращити якість обслуговування споживачів за рахунок скорочення часу на оформлення квитків, підвищення якості та ефективності роботи персоналу авіакомпаній. Впровадження систем бронювання дозволило суттєво скоротити час на обслуговування споживачів, забезпечити резервування в режимі он-лайн, знизити собівартість послуг, оптимізувати формування маршруту туристів за ціною, часом польоту й іншими завданнями.

Туристична сфера є інформаційно-насиченою, тому для забезпечення якісного рівня її управління необхідно використовувати сучасні ІТ, що забезпечать її інформаційну безпеку. Таким чином, інформаційний і туристичний ринки повинні задовольняти потреби всіх категорій споживачів, які бажають отримати туристичну послугу, а держава – підтримувати і сприяти розвитку як традиційних туристичних підприємств, що орієнтуються на клієнтів, які надають переваги особистому спілкуванню під час придбання послуги, так і віртуальних фірм, які можуть задовольнити потреби клієнтів, що надають переваги Інтернет-технологіям.

## Література


1. Рудой А. Рекреативные потенции / А. Рудой // Комп&ньон. — 2006. — № 26. — С. 30–34.
2. Туристичні потоки. Пасажирські перевезення. Кількість проведених виставкових заходів [Електронний ресурс] / Офіційний сайт Держ. ком. статистики України. — Режим доступу : http://www.ukrstat.gov.ua.

# ДОСЛІДЖЕННЯ ФОРМУВАННЯ ЕФЕКТИВНОЇ МНОЖИНИ РОБОЧИХ МІСЦЬ НА ПІДПРИЄМСТВІ З УРАХУВАННЯМ КЛАСІВ ДІЯЛЬНОСТІ ІСНУЮЧОГО ПЕРСОНАЛУ ТА ЇХ РІВНЯ ДОПУСКУ

*Олександр Цимбал, Анатолій Шиян*

Вінницький національний технічний університет, м. Вінниця, Україна

**The paper examined the methods and approaches to determine the most effective distribution of functional responsibilities in the company. Also considered methods of distribution by sphere of activity workers in the enterprise, and consideration of access levels, which set by the company that is the object of forming effective set of workplaces.**

**Keywords: functional responsibilities, activity sphere, the division of powers, access levels.**

Організаційні методи захисту інформації є одними з основних заходів для організації роботи підприємства в якому циркулює інформація доступ до якої обмежений. Така інформація може становити комерційну таємницю що може бути цінною для конкурентів і становити безпосередню загрозу даному підприємству.

Існуючі сьогодні методи захисту інформації є в першу чергу адміністративними заходами спрямованими на підвищення ефективності захисту інформації за рахунок різноманітних адміністративних заходів. Одними з основних заходів можна вважати здійснення аудиту доступу до даних що містять конфіденційну інформацію на підприємстві, та організацію системи навчання та підвищення кваліфікації персоналу що має безпосередній доступ до конфіденційної інформації. Отже можна зробити висновок що розподіл функціональних обов'язків на підприємстві є дуже важливим та відповідальним моментом для виконання вимог організаційного захисту інформації.

Методи що ефективно розподіляють функціональні обов'язки між працівниками є не так поширені, тому дана область є досить актуальна для розвитку. Дослідження в цій сфері підвищують ефективність роботи на підприємстві завдяки вибору найоптимальніших множин робочих місць. Дані методи використовують різноманітні моделі поведінки людей які є ключовими при розробці механізмів управління персоналом [1], так як дозволяють передбачити ймовірну поведінку працівника на підприємстві.

Дана робота описує процес розподілу функціональних обов'язків з урахуванням полюсів дихотомій для класів діяльності на підприємстві та формування множини функціональних обов'язків для кожного із суб'єктів інформаційної безпеки з урахуванням як класу їх діяльності та їх рівня допуску до інформації з обмеженим доступом.

Подальшим розвитком даної теми і напрямку в цілому є розширення поля досліджень та застосування методів для пошуку ідеальних кандидатів для певних функціональних обов'язків.

## Література

1. Shiyan, Anatoliy A., Technologies for HR-Managers: Typology for Person's Economic Behavior, Applications and Mechanism Design (May 1, 2011). – 373 p. – Режим доступу до ресурсу: http://ssrn.com/abstract=1827706 or http://dx.doi.org/10.2139/ssrn.1827706.

# METHOD OF IDENTIFYING CONFIDENTIALITY THREATS AGENTS ON THE COMPANY

*Yanna Chaikovska, Liliya Nikiforova*

Vinnytsia National Technical University, Vinnytsia, Ukraine

**In the report the method, which grounded in this model, is proposed for protection of the company from leaks of confidential information.**

**Keywords: confidence, threat agent, motivation, protection, company,**

Today every enterprise has to organize a security process. A confidential information can be the most valuable asset of a business, the providing of information security system of the enterprise can contribute to successful progress of a business.

Confidential Information means all trade secrets, proprietary information, know-how, and confidential information of Company including but not limited to: any and all technical, business or financial information or property, owned by or licensed to Company, or otherwise relating to Company and/or any of its subsidiaries, affiliates and related entities which is heretofore or hereinafter disclosed to Supplier, including but not limited to information regarding Company's goods or services, processes, personnel, finances, business plans, studies, analyses, projections, research, market data, operations, apparatus, computer software, know-how, trade secrets, inventions, equipment, tools, molds, dies, fixtures, parts, prototypes, samples, drawings, test results, material and manufacturing specifications, suppliers, customers, employees, processes, licensing and any other ideas or information relating to Company's business or Company Products, the Supplies or any business or activity in which Company is engaged, regardless of the form of disclosure, whether or not disclosed in a writing marked "Confidential" or in some similar manner or identified as confidential; improvements derived by Supplier from the information identified in Subsection or from access to Company's facilities; any and all software, reports, memoranda, documents, developments, or other results produced by Supplier in the performance of providing Supplies that are directly related to Company's business and not primarily to general technology used by Supplier in the conduct of its core business.

The most vulnerable element of information security system of any objects, especially are people. People or organizations that constitute a threat to the information security of the enterprise calls agents. The main characteristics of agents are: access, knowledge, motivation.

Often people are the confidential information leakage on the enterprise because of lack of their motivation to work on the enterprise. Material and moral dissatisfaction of agent is the reason of destructive motivation, that causes threats to confidentiality.

In [1,2] the model for motivation of confidentiality agents was obtained. In the report the method, which grounded in this model, is proposed for protection of the company from leaks of confidential information.

## References

1. Нікіфорова Л. О. Метод розрахунку рівня вмотивованості співробітників щодо збереження конфіденційності інформації в задачах інформаційної безпеки / Л. О. Нікіфорова // Інформаційна безпека. – 2014. - №4(16). – С.175-182.
2. Нікіфорова Л. О. Узагальнена модель оцінки рівня вмотивованості агентів загроз в задачах забезпечення безпеки об'єктів на мікро та макрорівнях/ Л. О. Нікіфорова // Сучасний захист інформації. – 2015. – №4. – С.71–76.

# ДО ПИТАННЯ УДОСКОНАЛЕННЯ МЕХАНИЗМІВ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ЕЛЕМЕНТІВ ФУНКЦІОНАЛЬНОГО ПОЛЯ МОНІТОРИНГУ У ПЕРЕДУМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

*Роман Шевченко*

Національний університет цивільного захисту України, м. Харків, Україна

**In this paper, under a single concept development of information and communication logistics of hybrid type, the basic approaches to the formation of the security information and communication fields of functional elements monitored premises emergencies. The proposed some theoretical solutions for its further implementation.**

**Keywords: information security, information and communication logistics, monitoring premises in emergencies.**

Як вже зазначалось раніше [1] однією з областей внутрішнього управління в системі інформаційно-комунікаційної логістики є забезпечення інформаційної безпеки елементів функціонального поля моніторингу у передумовах НС. З погляду загальних критеріїв інформаційної безпеки засобів комп'ютерних систем [2] та класифікації загроз, які прогнозуємо матимуть місце [3, 4] у функціональному полі моніторингу у передумовах надзвичайних ситуацій, необхідно узагальнити концептуальні положення інформаційної безпеки (рис. 1).

Передусім зазначимо, що в рамках розбудови інформаційно-комунікативного апарату аналізу функціонування та створення поля моніторингу у передумовах надзвичайних ситуацій, реалізація загроз інформаційної безпеки утворює додаткове (штучне) поле інформаційно-комунікативної критичності, яке нерівномірно посилює відповідне природно поле інформаційно-комунікативної критичності викликане особливостями та завданнями функціонального поля моніторингу у передумовах надзвичайних ситуацій (рис. 1). Суперпозиція інформаційно-комунікативних критичностей штучного і природного полів не змінює принципових підходів до створення схем та відповідних процесів її компенсації.

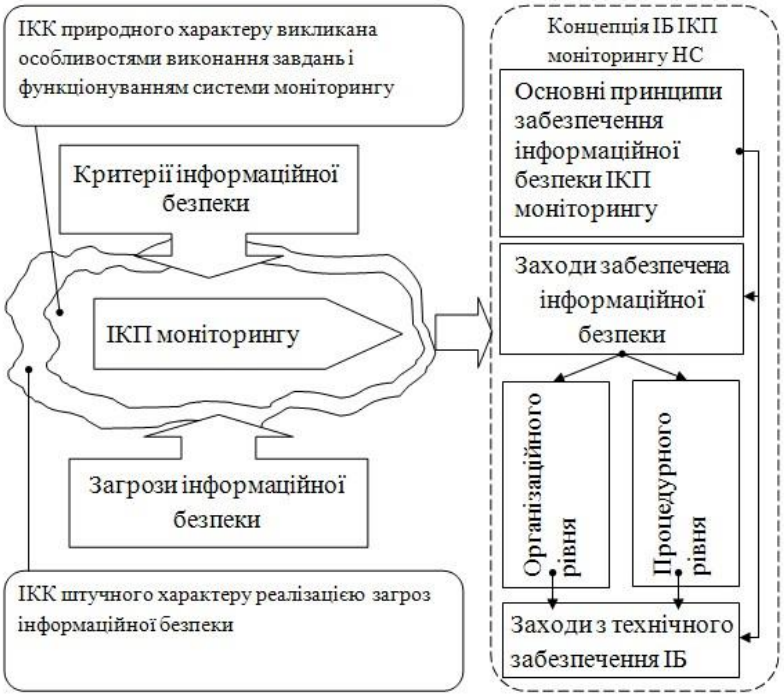



Рис. 1. Схема розробки концепції інформаційної безпеки (ІБ) інформаційно-комунікативного елементів функціонального поля моніторингу у передумовах надзвичайних ситуацій

Від так забезпечення інформаційної безпеки ІКП моніторингу у передумовах НС можна розглядати, як двохскладовий процес подолання загроз інформаційної безпеки, а саме (рис. 2):

А) подолання інформаційних загроз як окремого штучного джерела інформаційно-комунікативної критичності широкого спектру. Відповідно їх подолання базуються на загальних підходах інформаційно-комунікативної компенсації викладених у [5] з додатковими (організаційними та технічними) заходами фізичного усунення штучного джерела [3, 4];

Б) подолання інформаційних загроз, які не впливають на рівень інформаційно-комунікативної критичності. Відповідно їх подолання базується на загальновідомих методологічних підходах, організаційних та технічних реалізаціях [3, 4].

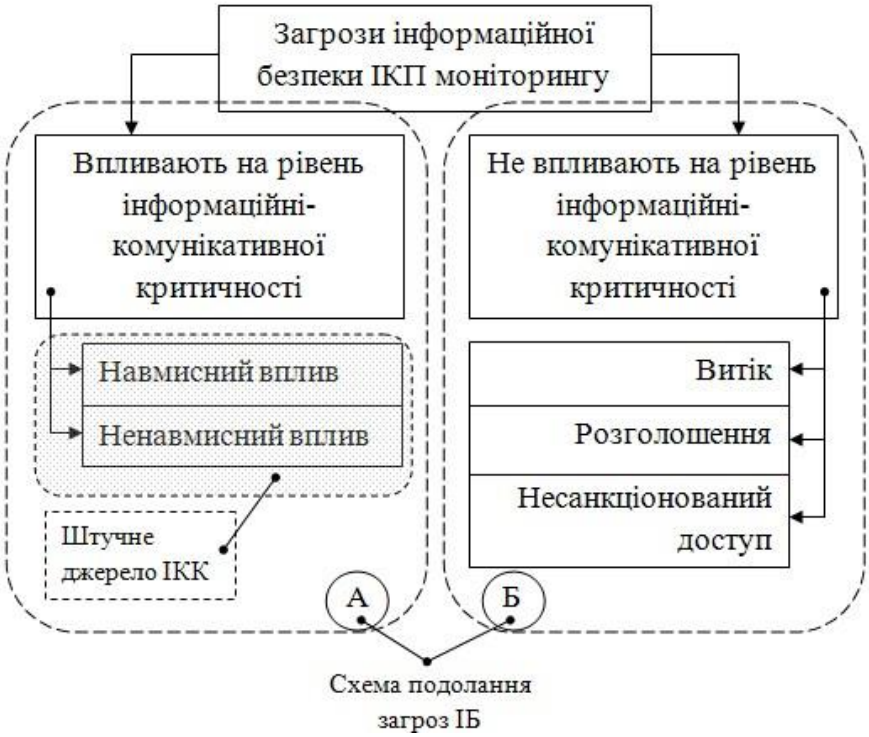



Рис. 2. Класифікація загроз інформаційної безпеки за якістю впливу на функціональне поле моніторингу у передумовах надзвичайних ситуацій.

Як бачимо найбільш складним з погляду інформаційно-комунікативних процесів є схема подолання загроз ІБ (А).

## Література


1. Шевченко Р.І. Дослідження умов внутрішнього управління інформаційно-комунікативним потоком в рамках розбудови інформаційної логістики системи моніторингу надзвичайних ситуацій [Текст] / Р.І. Шевченко // Системи обробки інформації. – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 7 (144). – С. 189 – 195.
2. Международные стандарты по оценке безопасности информационных технологий «Оранжевая книга» (TCSEC) [Електрон.ресурс]. – Режим доступу: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/oranzhevaja_kniga_tcsec/
3. Партыка Т.Л. Информационная безопасность: Учебное пособие [Текст] / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. [Текст] / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
5. Шевченко Р.І. Формування теоретичних основ інформаційно-комунікативного компенсування функціональної критичності гібридних систем від дії зовнішнього впливу різної природи, в рамках концепції створення матеріально-інформаційно-розумної системи моніторингу надзвичайних ситуацій [Текст] /Р.І. Шевченко// Збірник наукових праць Харківського університету Повітряних Сил – Харків: ХУПС ім. Івана Кожедуба, 2016. – № 1 (46). – С. 136 – 141.

# АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ВУЛИЦІ ЛЬВОВА

*Богдан Шпортко, Ігор Процько*

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

**The global trends in the field of the video surveillance, functions and capabilities of modern video surveillance systems are specified and the basic parameters of the provision avideo surveillance are described.**

**Keywords: video surveillance, cloud, digital technology**

У наш час жоден, навіть невеликий та незначний об’єкт не мусить залишатися без цілодобового контролю системи відеоспостереження. Правильне розташування камер дозволить отримувати повну відеоінформацію про все, що відбувається на відповідних вулицях, в будинках, підприємствах.

Системи відеоспостереження - це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. устаткування), призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах. Відеоспостереження є сьогодні невід'ємним елементом будь-якої сучасної системи безпеки.

Протягом декількох останніх років, відбувається перехід у напрямку цифрових систем відеоспостереження з аналогових (коаксіальний кабель). Наявні гібридні системи є, в основному там, де аналогові камери вже присутні, і потрібні великі зусилля на заміну кабельної розводки. Винятково цифрові версії використовують лише IP-камери, відеозображення з яких, передаються приватною або публічною мережею IP до центральної станції відеоспостереження за для перегляду і/або запису. Передавання відео здійснюється винятково комерційними IT-системами (маршрутизатори, комутатори та інше). Головним завданням у цьому разі, є надійне та безпечне передавання інформації. Цифрові технології, включають у себе як переваги (якість зображення), так і новий набір проблем (пам'ять і вимоги до пропускної здатності, а також різноманітність форматів та методів стиснення.

В роботі проаналізована оснащеність системами відеоспостереження двох центральних вулиць міста Львова (рис. 1.). За даними розміщення відеокамер в результаті аналізу створеної зони відеонагляду вироблені рекомендації, які необхідно враховувати для підвищення ефективності роботи системи відеоспостереження даної вулиці в проведенні оперативної профілактики та забезпечення безпеки жителів і гостей міста, будинків і магазинів, дорожнього руху.


Рис. 1. Розташування та напрямлення відеокамер вулицях центральних вулиць міста Львова

На рис. 1 подано розташування відеокамер в місті Львові по вулиці Князя Романа та по проспекту Шевченка . Треба відзначити те, що відеокамери (рис. 1) не є однією системою і не мають великого потенціалу для попередження певних порушень та

знаходження певних людей на цих вулицях. Тому для покращення ефективності відеонагляду необхідно впроваджувати сучасні системи, що включають інтегроване програмне забезпечення відеоданих системи хмарного відеоспостереження (рис. 2). Система відеонагляду сконфігурована згідно до моделі клієнт-серверної архітектури забезпечує клієнтське обладнання повним спектром роботи з необхідними функціями. Створюється окремий департамент централізованого контролю за функціями системи, сервер якої запущений на високопродуктивному програмному забезпеченню SQL Server.

Шляхом інтеграції програмного забезпечення відеоданих системи хмарного відеоспостереження з додатком аналізу відеопотоку система стає універсальною для всіх галузей застосування. Додаток аналізу відеопотоку зможе визначати, використовуючи гнучку базу даних, наприклад, чи дозволено проїхати даній машині з даними номерними знаками на територію, чи знаходити порушників (визначення за рисами обличчя). Додаток аналізу відеопотоку зможе без зайвих складнощів визначати кількість людей, які пройшли в певному напрямку, що може стати цікавими статистичними даними для будь-яких сфер застосування.

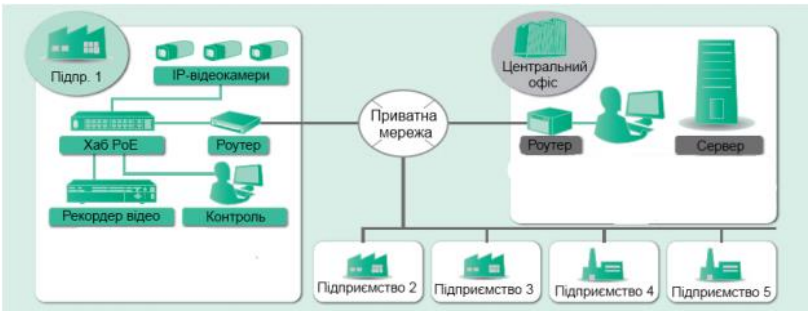



Рис. 2. Модель інтегрованого програмного забезпечення централізованого відеонагляду

Концептуальна модель системи хмарного відеоспостереження, що використовує сервіс аналізу відеоданих зображена на рис. 3.

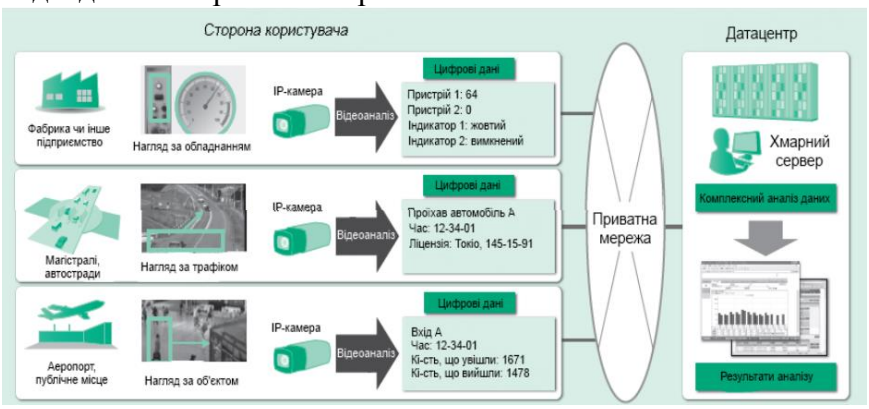



Рис. 3 Модель системи хмарного відеоспостереження, що використовує сервіс аналізу відеоданих

З допомогою сучасних хмарних технологій витрачається менше часу на пошук порушень та знаходження певних осіб, також вирішується проблема захисту ресурсів пам'яті для самих відеоспостережень адже дані будуть зберігатися відалено, такі системи набагато ефективніші і відповідають європейським стандартам.

## Література


1. Фауре Э.В. Система охранного видеонаблюдения со скрытым каналом / Э.В. Фауре // Вісник ХНУ. – 2008. – №4. – С. 231-235.
2. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
3. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
4. http://videokamera.in.ua

# ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ТЕКСТІВ МАНІПУЛЯТИВНОГО ХАРАКТЕРУ

*Наталія Яворська, Руслан Козак*

Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

**Theses report describes basic concepts such as information, misinformation and the ability to detect manipulative character text using machine learning techniques. Also features of manipulation text are described in detail, which can identify them.**

**Keywords: manipulative influence, misinformation, methods of machine learning, information security.**

Упродовж останніх декількох років он-лайн соціальні мережі (ОСМ) стали не лише зручним засобом комунікації, а й важливим та одним з потенційно достовірних джерел інформації для значної кількості людей. Водночас спостерігається сильна позитивна кореляція між використанням соціальних мереж та кількістю зловживань ЗМІ щодо поширення дезінформації [1]. Залежно від конкретних умов та мети поширення інформації або дезінформації в ОСМ, зловживання можна виявити у таких галузях як охорона здоров'я, політика, фінанси і тенденції розвитку технологій. Вони є головними джерелами дезінформації в різних контекстах, яка може спричиняти значний вплив на бізнес, політику і повсякденне життя [2], а отже й на інформаційну безпеку суспільства.

Виявлення дезінформації в великих обсягах даних є складним завданням. Для автоматизації цього процесу створено методи з використанням машинного навчання і методи обробки природної мови. Проте через семантичний характер контенту точність автоматизованих методів обмежена і досить часто вимагає «ручного втручання». Обсяг даних, що генеруються в ОСМ, настільки великий, що робить завдання опрацювання тексту в реальному часі надзвичайно затратним в обчислювальному відношенні. У цій доповіді запропоновано методику для визначення змісту дезінформації з використанням понять, заснованих на когнітивній психології.

Вкрай важливо зрозуміти такі пов’язані поняття як інформація та дезінформація [3]. Визначення інформації зрозуміле за самою своєю природою, але потрібно визначити різні форми інформації, які вона може приймати. Користувачі зацікавлені у використанні соціальних мереж для поширення певного виду інформації, щоб змінити поведінку або ставлення людей. У кіберпросторі маніпулювання інформацією з метою впливу на семантичну природу інформації та спосіб, в якому вона інтерпретується користувачами, часто називають семантичними атаками. Семантичні атаки в соціальних мережах можуть бути результатом поширення інформації в різних формах.

У роботі [4] наведено декілька формулювань поняття «маніпуляція»:

- вид психологічного впливу, майстерне виконання якого призводить до прихованого збудження у іншої людини намірів, які не збігаються з її актуально існуючими бажаннями;
- вид психологічного впливу, при якому майстерність маніпулятора використовується для прихованого впровадження в психіку адресату цілей, бажань та намірів або установок, які не збігаються з тими, які є у адресата у даний момент;
- вид психологічного впливу, що використовується для досягнення одностороннього виграшу шляхом прихованого залучення людини до виконання певних дій.

Отже, повідомлення, яке має маніпулятивний характер, можна назвати дезінформацією.

Визначивши для кожного повідомлення інформаційного потоку, що аналізується, такі характеристики як час та дату опублікування, автора, джерело публікації, країну

джерела публікації, мову, кількісні показники «маніпулятивності» тощо, видається можливим та доцільним ідентифікувати текст маніпулятивного характеру [5] за допомогою методів машинного навчання (рис. 1).

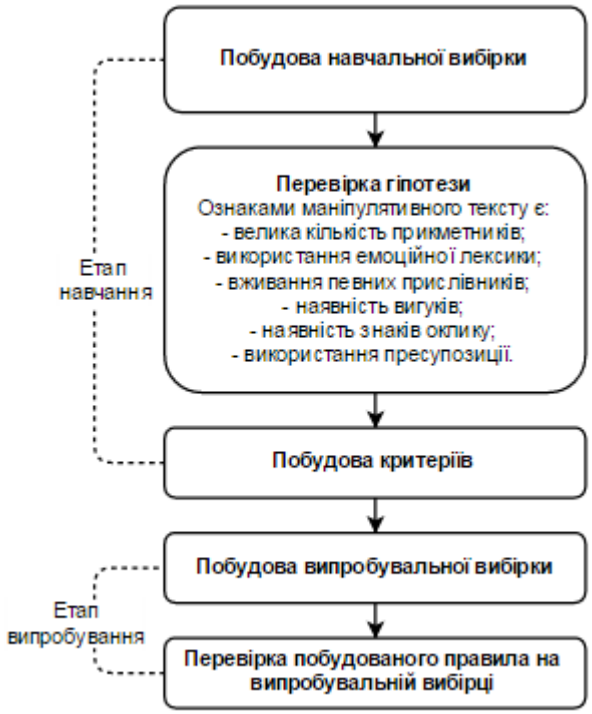



Рис. 1. Етапи ідентифікації тексту

Присутність дезінформації як явища в суспільстві та її наявність в ОСМ вивчалися досить широко з психологічної точки зору. Огляд механізмів, за допомогою яких дезінформація поширюється, те, наскільки ефективними є заходи щодо виправлення становища, а також підходи, які можуть бути впроваджені на основі когнітивної психології, можна знайти в [6]. На думку авторів поширення дезінформації є результатом пізнавального процесу за допомогою «приймачів», що ґрунтується на основі їхнього оцінювання істинності інформації. Прийняття інформації є скоріше нормою, ніж її відхилення, для більшості людей.

Одним із перспективних напрямів подальших досліджень є розробка формальних моделей маніпулятивного впливу та вивчення особливостей автоматизації процесу виявлення дезінформації.

## Література


1. Karlova NA, Fisher KE: “Plz RT”: A social diffusion model of misinformation and disinformation for understanding human information behaviour. Inform Res 2013, 18(1):1–17.
2. Mintz AP: Web of deception: Misinformation on the Internet. Information Today, Inc., New Jersey, USA; 2002.
3. Stahl BC: On the difference or equality of information, misinformation, and disinformation: A critical research perspective. Inform Sci: Int J Emerg Transdiscipline 2006, 9: 83–96.
4. Лігачова Н. Маніпуляції на ТБ. Маніпулятивні технології в інформаційно-аналітичних телепрограмах українського телебачення: моніторинг, рекомендації щодо захисту від впливу та запобігання застосуванню. Принципи відкритої редакційної політики телеканалів / Н. Лігачова, С. Черненко, В. Іванов. Київ : Телекритика, Інтерньюз-Україна – 2003.
5. Fallis D: A conceptual analysis of disinformation. iConference, Chapel Hill, NC, California, USA; 2009.
6. Lewandowsky S, Ecker UK, Seifert CM, Schwarz N, Cook J: Misinformation and its correction continued influence and successful debiasing. Psychol Sci Public Interest 2012, 13(3):106–131. 10.1177/1529100612451018.

# ПОКАЖЧИК АВТОРІВ

**ТЕЗИ ДОПОВІДЕЙ**

**ІІ Міжнародної науково-технічної конференції**

# ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СУСПІЛЬСТВІ

**24-25 листопада 2016 р.**

Відповідальний за випуск – професор **Самотий В.В.**

Комп'ютерне макетування та верстка – **доцент Лагун А.Е.**

**Друк ЛДУ БЖД**
**79007, Україна, м. Львів, вул. Клепарівська, 35,**
**тел./факс: (032)233-32-40, 233-24-79**
**e-mail: ldubzh.lviv@mns.gov.ua**

Підписано до друку 18.11.2016 р.
Формат 60x84/16. Гарнітура Times New Roman.
Друк на різографі.
Ум. друк. арк.. 11,5. Наклад 60 прим.