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

МАТЕРІАЛИ

ІІІ-ої Міжнародної науково-технічної конференції

29-30 листопада 2018 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, присвяченої 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

Кузик А. Д. – проректор з науково-дослідної роботи ЛДУ БЖД, д.с.-г.н., професор полковник 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

Горбенко І. Д. – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, д.т.н., професор

Грицюк Ю. І. – професор кафедри програмного забезпечення, НУ «Львівська політехніка», д.т.н., професор

Дудикевич В. Б. – завідувач кафедри захисту інформації НУ «Львівська політехніка», д.т.н., професор

Корнієнко Б. Я. – завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, д.т.н., професор

Кузнецов О. О. – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Н. Каразіна, д.т.н., професор

Максимович В. М. – завідувач кафедри безпеки інформаційних технологій НУ "Львівська політехніка", д.т.н., професор

Мачуський Є. А. – завідувач кафедри фізико-технічних засобів захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", д.т.н., професор

Мельник А. О. – завідувач кафедри ЕОМ НУ "Львівська політехніка", д.т.н., професор

Меньшикова О. В. – заступник начальника навчально-наукового інституту цивільного захисту ЛДУ БЖД, к.т.н., доцент

Мороз Л. В. – професор. кафедри безпеки інформаційних технологій НУ "Львівська політехніка", д.т.н., доцент

Пархуць Л. Т. – професор кафедри захисту інформації НУ "Львівська політехніка", д.т.н., професор

Ренкас А. Г. – начальник навчально-наукового інституту цивільного захисту ЛДУ БЖД, к.т.н., доцент

Саченко А. О. – завідувач кафедри інформаційно-обчислювальних систем і управління Тернопільського Національного економічного університету, д.т.н., професор

Шевчук В.О. – завідувач кафедри міжнародних економічних відносин Львівської комерційної академії, д.е.н., професор

Яремчук Ю.Є. – директор Центру інформаційних технологій і захисту інформації Вінницького НТУ, д.т.н., професор

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

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

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

Rucinski A. *professor*, New-Hampsher University, Electronics and Commuter Engineering department (USA)

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

Вацлавик О. М. – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Максимів О. П. – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

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

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

Паркасевич М. І. – лаборант кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

ЗМІСТ

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ХМАРНИХ СЕРВІСІВ

Ірина Артищук, Оксана Гудзовата, Леся Хмілярчук

Львівський торговельно-економічний університет, м. Львів, Україна

The article outlines the prospects for the development of cloud services, highlights the main characteristics of clouds, describes the actions necessary for the effective management of information security of cloud services, analyzed the problems associated with cloud safety.

Keywords: information security, cloud computing, cloud safety, effective management of information security.

Хмарні сервіси, що дозволяють перенести обчислювальні ресурси й дані на віддалені інтернет-сервери, в останні роки стали одним з основних трендів розвитку IT-технологій.

Так, у 2017 році багатообіцяюча індустрія хмарних обчислень досягла 146 млрд доларів, а в 2018 році очікується близько 155 млрд. доларів — такий прогноз зробили аналітики компанії Forrester Research. Вони припустили, що левова частка всіх грошей на ринку дістанеться трьом гігантам - Amazon Web Services, Microsoft Azure та Google Cloud Platform. За оцінками Forrester Research, зараз щорічні темпи зростання ринку "хмарної" інфраструктури на макрорівні складають 22%. Але протягом наступних трьох років цей показник складе вже 35%. В дослідницькій компанії Synergy Research Group вважають, що рубіж у 200 млрд доларів буде пройдено у 2020 році. Разом з тим, дохід від продажу традиційного апаратного і програмного забезпечення буде знижуватись, оскільки робоче навантаження переходить у хмару.

Попит на користування хмарними обчисленнями збільшується з кожним роком завдяки їх основним характеристикам, що були найбільш комплексно і фундаментально охарактеризовані Національним інститутом стандартів і технологій (National Institute of Standards and Technology, NIST) [3]:

– самообслуговування на вимогу (On-demand self-service),
– широкий мережевий доступ (Broad network access),
– об’єднання ресурсів в пули (Resorce pooling),
– миттєва еластичність (Rapid elasticity),
– вимірюваний сервіс (Measured service).

Хмарні сервіси [2] відносно своєї архітектури розподіляються на 3 головні моделі:

- ✓ програмне забезпечення як послуга (SaaS),
- ✓ платформа як послуга (PaaS),
- ✓ інфраструктура як послуга (IaaS).

Хмарні обчислення та рішення для зберігання даних надають користувачам і підприємствам різноманітні можливості для зберігання і обробки їх даних у центрах обробки даних сторонніх виробників [1]. Організації використовують хмарні технології в різноманітних моделях обслуговування (SaaS, PaaS, та IaaS) так і розробницьких моделях (Private, Public, Hybrid, та Community).

Найбільш популярні хмарні сервіси, якими можна скористатися:

- Amazon S3
- DigitalOcean
- Dropbox
- Ex.ua-Fex.net
- Google Cloud Datastore
- Google Docs
- Google One
- Google Storage
- ICloud
- OneDrive
- OwnCloud
- Rackspace Cloud
- Salesforce marketing cloud
- Seafile
- Ubuntu One
- WeTransfer
- Wuala

Основним ризиком, який пов'язаний з використанням хмарного хостингу, вважається інформаційна безпека. Тому, управління інформаційною безпекою в хмарних сервісах є дуже важливим. Проблеми, пов'язані з безпекою хмарних обчислень можна поділити на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг (організації, які надають програмне забезпечення, платформи, чи інфраструктуру як послуги через використання хмарних технологій) і питання безпеки, з якими стикаються їх клієнти (компанії або організації, які розгортають додатки або зберігають дані на хмарі). Відповідальність йде в обох напрямках, тобто: постачальник повинен гарантувати, що їх інфраструктура знаходиться в безпеці і що дані та додатки клієнтів захищені, в той час як користувач повинен вживати заходи, щоб зміцнювати їх застосування, використовувати надійні паролі і перевірку автентичності.

Коли організація вибирає для зберігання даних або розгортання додатків публічну хмару, вона втрачає можливість мати фізичний доступ до серверів з інформацію. В результаті, конфіденційні дані не зазнають ризику інсайдерських атак. Згідно з недавнім звітом від Cloud Security Alliance, інсайдерські атаки треті за величиною загрози в області хмарних обчислень. Таким чином, постачальники хмарних послуг повинні забезпечити, ретельні перевірки для співробітників, що мають фізичний доступ до серверів в центрі даних. Крім того, центри обробки даних повинні постійно контролювати підозрілу активність.

Для того, щоб зберегти ресурси, скоротити витрати, та зберегти ефективність, провайдери хмарних послуг часто зберігають більше одного разу дані клієнта на тому ж сервері. В результаті, існує ймовірність того, що особисті дані одного користувача можуть бути доступні іншим користувачам (можливо, навіть конкурентам). Для вирішення таких складних ситуаціях, постачальники хмарних послуг повинні забезпечувати правильну ізоляцію даних і логічні сегрегації зберігання.

Архітектура безпеки хмари є ефективною, тільки якщо правильно реалізовано захист на місці. Ефективна архітектура безпеки хмари визначає проблеми, які виникатимуть з керуванням безпеки. Управління безпеки усуває проблеми пов'язані з контролем безпеки. Ці елементи управління вступають в дію для захисту будь-яких недоліків в системі і змен-шення впливів атак. Для того, щоб здійснювати ефективне управління інформаційною безпекою хмарних сервісів потрібно:

1.Визначити тип управління архітектурною безпекою хмари.
2. Визначити розміри безпеки у хмарі.
3.Здійснювати ефективне управління ідентифікацією.
4. Забезпечити фізичну безпеку.
5. Безпеку персоналу.
6. Доступність.
7. Безпеку додатків.
8. Приватність.

Отже, хмарний сервіс - це можливість завжди мати гарантований і безпечний доступ до особистої інформації, а також відійти від необхідності витрачати кошти на потрібні для цього інструментальні засоби. Безсумнівно, що на даний момент, хмарні технології є одним з найбільш затребуваних і необхідних напрямків в IT-сфері, тому управління їх інформаційною безпекою є найактуальніше питання як для провайдерів, так і для користувачів їхніми послугами. Частково це можна вирішити, а також шляхом запровадження системи управління інформаційною безпекою згідно існуючих стандартів безпеки.

Література

1. Захист даних в хмарних технологіях обчислень [Електронний ресурс]: Захист даних в хмарних технологіях обчислень // ВНТУ. – Режим доступу: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf. – Назва з екрану.
2. Облачная безопасность – взгляд из Европы. [Электронный ресурс]. – Режим доступа: http://cloudzone.ru/articles/analytics/51.html.
3. ISO/IEC 17788:2014 Information technology - Cloud computing – Overview and vocabulary [Text]. – impl. 15.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 16 p.

THE HOMOMORPHIC ENCRYPTION USING FOR CRYPTOGRAPHIC DATA PROTECTION ON SMART CARDS

Olexander Belej

Lviv Polytechnic National University, Lviv, Ukraine

In connection with the growth and development of information transmission media, telecommunications and computer networks, and especially the Internet, cryptography faces new challenges. One of these tasks is to provide computation on encrypted data. We considered the features of data encryption on smart cards using homomorphic encryption.

Keywords: cryptography, smart cards, homomorphic encryption, processor.

In the future, smart cards will no longer be designed for devices serving a single target application. Instead, there is a tendency to design universal cards with their own operating system, which can perform various functions [1]; thus, the only individual card will be able to interact with several service providers [2].

The difficulty of providing homomorphic cryptographic circuits with the necessary efficiency and crypto resistance leads to the question of why use homomorphic encryption instead of the usual one. The main interest in the study of homomorphic encryption is a wide range of applications, both theoretical and practical.

In order for the card to be able to cope with several applications, it was suggested that the card must contain the owner's data and that the card's operating system must import the code of the functions that will be performed on the data from the server [3]. Article [4] proposes an additional solution to ease the requirement that all sensitive data and processing will occur on the card. The idea is that some applications can work outside the card on homomorphy's encrypted data. For such applications, the card behaves not just as a passive device, since the card's operating system is responsible for encrypting and decrypting data, as well as controlling the access of external applications to data.

For comparison, here are two protocols for the operation of a universal smart card: one based on traditional calculations inside the card, and the other, on the use of delegation of calculations using homomorphic encryption.

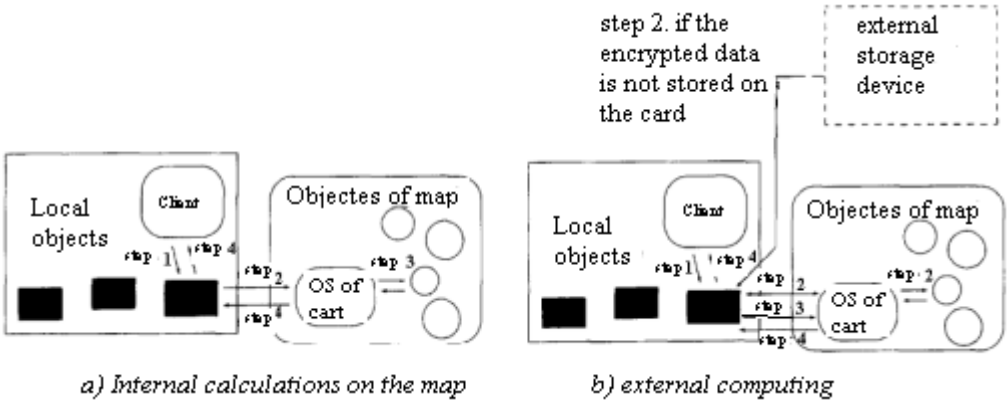
According to protocol 1 "Calculations inside the card", we implement the following algorithm: the client program points to a local object (also called a proxy or surrogate object); the client's proxy object methods perform procedural method calls in a map object. When making a procedural call using the card method, the proxy object provides the card with a certified code corresponding to the method being called; after verifying the integrity of the method certificate, the operating card of the system executes the method code on the data of the card objects; the card's operating system returns a response to the client program.

Formation of a multiprocessor environment formed from a processor of a card and one or more external processors. Thus, true parallelism is provided, although there is some asymmetry when the external processor tries to access data stored in the card: external processors must interact with the processor of the card in accordance with Protocol 2 below.

Especially resource-intensive applications can use external storage devices and external processors more powerful than on the card. Any application that operates on data stored in a map can benefit from the approach presented here. This includes service provider applications as well as initiator card applications, such as biometric verification (voice recognition, fingerprints, or handwriting), which typically require a large amount of storage and a large number of relatively simple operations.

The problem with the approach described in Protocol 1 (object-oriented or agent based) is that the smart card has to independently, in the final account, store and process all confidential data. Thus, limited storage space and card processing capacity can be a narrow place when a very resource-intensive client application is serviced or simply when several client applications

run in parallel. For such applications, we propose the following Protocol 2 (Figure 1), which assumes that the data of the map object can be processed outside the map in encrypted form.



a) Internal calculations on the map *b) external computing*

Figure 1. The external and internal calculations are on a smart card.

According to Protocol 2 "External Computing", we implement the following algorithm: the client program points to a local object; the methods of the local client object request an encrypted version of the map object data from the card. The card provides the necessary data after proper security checks; the methods of the local client object perform calculations on the encrypted data, find the desired (in encrypted form) result, and send it to the card operating system; the card's operating system runs a method in the card object, which interprets the result obtained from the client; the decrypted response is then returned to the client program.

Protocol 2 is an addition to Protocol 1. Thus, changes should only to a small extent affect the life cycle of the card as it is understood in Protocol 1. The map object used in both protocols has the following structure:

$$o = \left(\{d_t\}, \{I_t\}, \left\{E^t, D^t\right\}, \{A_t\}\right) \quad (1)$$

where $\{d_t\}$ is the encrypted data field, $\{I_t\}$ is a set of interface methods, is used in protocol 1, $\left\{E^t, D^t\right\}$ is a set of encryption/decryption algorithms available for this object, and $\{A_t\}$ is a set of - access control methods to be used in steps 2 and 4 of Protocol 2.

Encryption, decryption and access control methods are complete methods, that is, they contain their implementations. If used only with Protocol 1, obviously only $\{d_t\}$ $\{I_t\}$ and are required. Conversely, if it should be used only with protocol 2, then it is not required $\{I_t\}$.

And as we see, for this application it is quite sufficiently symmetric with fully homomorphic encryption.

The industry of homomorphic encryption is rich in both deep theoretical results and applications in practice. As we have seen, a compact, symmetric, fully homomorphic, crypto-resistant against attack by known open texts is suitable for most of them. In the near future, homomorphic cryptography tools will have an impact on the cloud services market, and to one degree or another on the appearance of modern information technologies.

References

1. S. Fau, R. Sirdey, C. Fontaine, C. Aguilar-Melchor, G. Gogniat. Towards practical program execution over fully homomorphic encryption schemes // P2p, parallel, grid, cloud and internet computing (3pgcic), 2013 eighth international conference on IEEE, 2013, p. 284–290.
2. C. Fontaine, F. Galand. A survey of homomorphic encryption for nonspecialists // EURASIP Journal on Information Security, 2007. Vol. 2007.
3. M. Van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan. Fully homo-morphic encryption over the integers // Advances in cryptology–eurocrypt 2010: Springer, 2010, p. 24–43.
4. P. V Parmar, S. B Padhar, S. N Patel, N. I Bhatt, R. H Jhaveri. Survey of various homomorphic encryption algorithms and schemes // International Journal of Computer Applications, 2014. Vol. 91, no. 8, p. 26–32.
5. D. Boneh, C. Gentry, S. Halevi, F. Wang, D. J Wu. Private database queries using somewhat homomorphic encryption // Applied cryptography and network security Springer, 2013, p. 102–118.

ОРГАНІЗАЦІЯ ВНУТРІШНЬОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Надія Божко

Коледж МНУ імені В.О. Сухомлинського, м. Миколаїв, Україна

The paper raises the importance of researching the safety of internal accounting and proposes recommendations for reducing the impact of information risks on enterprise.

Keywords: information risk, controlling, internal accounting.

Постановка проблеми. В умовах швидкого розвитку суспільства, істотно зріс вплив інформації та інформаційних ризиків на діяльність підприємства. Фактично інформація стала самостійним ресурсом бізнесу, без якого практично не можливо його ефективне управління.

Стан дослідження. Питанням вивчення впливу інформації на прийняття управлінських рішень присвячені наукові праці таких вчених, як В.М. Глушков, В.О. Новак, Ю.Г. Симоненко, В.П. Бондар. Практично в кожному дослідженні наголошується на необхідності вивчення економічної безпеки підприємства на основі зовнішньої, об'єктивної і сучасної інформації, яка збирається, обробляється і зберігається за допомогою наукових методів і технічних засобів, але аналізу якості внутрішньої інформації не приділяється належної уваги.

Мета статті – аналіз інформаційних ризиків підприємства, які впливають на його економічну безпеку.

Виклад основного матеріалу. Проведений аналіз свідчить про те, що інформаційні ризики розглядаються на ряді підприємств з точки зору зовнішнього оточення, та необхідність звернути більш пильну увагу на внутрішні інформаційні ризики, так як саме вони впливають на ефективність прийнятих рішень. Координація дій всіх структурних ланок підприємства передбачає передачу інформації конкретним користувачам таким чином, щоб вони правильно її сприймали і розуміли потенційну корисність. Недооцінка аналізу комунікаційного процесу всередині організації призводить до того, що отримана інформація не є якісною через відсутність системності та адресності її передачі і не дозволяє її ефективне використання управлінським персоналом.

У зв'язку з цим, особливого значення набуває проблема управління ризиками, пов'язаними з бухгалтерською інформацією. Така ситуація, з одного боку, пояснюється тим, що методологія ведення бухгалтерського обліку регламентована різними інструкціями, які передбачають однакові вимоги до обробки інформації і не враховують специфіку підрозділів, обсяги і цілі переданої інформації. З іншого боку, на комунікаційний процес підприємства значно впливає суб'єктивний фактор – компетентність персоналу. Основними вимогами до працівників обліку в комунікаційному процесі повинні бути такі, які знижують ступінь інформаційного ризику.

Виявлення ризиків, пов'язаних з порядком ведення бухгалтерського обліку та зниження їх негативного впливу на стан і результати діяльності підприємства, в даний час, є актуальною проблемою. З метою попередження та усунення такого роду ризиків необхідно мати ефективну систему контролю. Найпоширенішими, і визнаними інструментами контролю, за роботою бухгалтерських служб, з боку керівництва підприємства, є контролінг і внутрішній аудит. Саме вони допомагають організації досягати поставлених цілей, за допомогою систематизованого і чітко організованого підходу до оцінки та підвищення ефективності корпоративного управління ризиками, і підвищити інформаційну безпеку при веденні бізнесу в електронному середовищі [1, с. 214].

Висновки: Забезпечення інформаційної безпеки передбачає створення таких умов внутрішнього обліку, при яких інформаційні ризики не призведуть до виникнення загроз

банкрутства підприємства, це може бути реалізовано на основі функціонування єдиної бухгалтерської інформаційної системи підприємства.

Література

1. Інформаційні системи в сучасному бізнесі : навчальний посібник / В. С. Пономаренко, І. О. Золотарьова, Р. К. Бутова та ін. – Х. : Вид. ХНЕУ, 2011. – 484 с

ЗАБЕЗПЕЧЕННЯ ЯКОСТІ РЕГЛАМЕНТУЮЧИХ ДОКУМЕНТІВ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІЯЛЬНОСТІ

Сергій Шамов, Валерія Денисенко

Харківський навчально-науковий інститут ДВНЗ «Університет банківської справи», м. Харків, Україна

The importance of the quality of regulatory documents for ensuring information security of the activity is considered. Approaches to quality assurance of regulatory documents are analyzed. The practical aspects of application of the approach, which involves revealing in the unformalized texts the structures of descriptions of business processes and application to them of the rules of formal control are investigated. An estimation and comparison of the effectiveness of the methods of its implementation is carried out.

Keywords: information security, regulatory document, business process, analysis, correctness.

Необхідною умовою забезпечення ефективної інформаційної безпеки будь-якої діяльності є неухильне дотримання суб'єктами діяльності регламентів виконання заходів щодо захисту інформації, які містяться у відповідних документах організацій. За опублікованими даними [1], більшість інцидентів щодо її порушення пов'язана з некваліфікованими, помилковими чи навмисними діями людей, що свідчить, зокрема, про недостатність уваги як до якості виконання регламентів, так і до якості самих регламентуючих документів.

До забезпечення якості регламентуючих документів існують два основних підходи: ітераційне узгодження і корегування текстових описів, та автоматичний синтез текстового опису за формальним описом процесу у тій чи іншій графічній нотації, який попередньо ітераційно узгоджується та корегується, і перевіряється відповідними інструментальними програмними засобами. Обидва підходи стикаються з проблемами великої розмірності описів, складності мовних засобів для проведення їх контролю та корегування, і, як наслідок, неприйнятно великої трудомісткості і недостатньої ефективності їх застосування. Тому був запропонований підхід, що передбачає виявлення у неформалізованих текстах структур описів бізнес-процесів та застосування до них правил формального контролю [2]. Однак в опублікованій літературі відсутні відомості щодо практичних аспектів його застосування.

Метою дослідження є перевірка застосовності такого підходу до забезпечення якості реальних регламентуючих документів, оцінка та порівняння методів його реалізації.

В якості вихідних даних для дослідження були взяті текстові описи виробничого процесу типових виробничих ІТ компаній. Дослідження складалось з наступних етапів:

1) структурна розмітка та експертний аналіз тексту із фіксацією запитань і зауважень до нього, що виникли у експерта;

2) структуризація тексту, згідно із регламентом структурованого опису бізнес-процесів;

3) виявлення у структурованому тексті некоректностей – порушень формальної правильності описів процесів за критеріями методології SADT [3];

4) перетворення структурованого тексту у формальний опис бізнес-процесу мовою IDEF0, та його оцінка за критеріями цієї мови [4];

5) змістовна інтерпретація виявлених порушень коректності описів;

6) порівняльний аналіз отриманих результатів.

Аналіз отриманих результатів показав, що застосовані методи дозволили визначити і виявити в документах наступні типи порушень коректності описів процесів:

– структурна неповнота (СНП) – відсутність у складових процесу зовнішніх та/або внутрішніх зв'язків, необхідних для правильного здійснення процесу;

– функціональна неповнота (ФНП) – відсутність складових, необхідних для

правильного здійснення процесу;

– атрибутивна неповнота (АНП) – відсутність інформації про атрибут, обов'язковий для процесу або для його складової;

– відносна неповнота (ВНП) – відсутність складової опису, яка передбачена регламентом щодо змісту регламентуючого документу;

– порушення формулювання (ПФ) – назва складової процесу не відображає дію чи назва зв'язка не відображає сутність;

– порушення позначення (ПЗ) – фрагмент тексту є вказівкою на компонент процесу, яка порушує правила нотації формального опису процесу;

– протиріччя (ПР) – використання більше одної назви для одного компоненту процесу, невідповідність назви процесу і назв його складових або назви складової і назв її складових;

– неоднозначність (НО) – наявність однієї назви для декількох компонентів процесу.

Отриманий розподіл випадків порушення коректності описів процесів у регламентуючих документах за етапами дослідження та типами порушень наведений у таблиці 1 (застосовані позначення: «–» – порушення не виявлені; «×» – порушень не має).

Таблиця 1

Розподіл випадків порушення коректності описів процесів

Тип порушення	Етап 1	Етап 3	Етап 4
СНП	22	25	122
ФНП	10	–	1
АНП	–	8	11
ВНП	–	13	×
ПФ	12	×	×
ПЗ	7	×	×
ПР	2	×	×
НО	6	×	×
Всього	59	46	134

Проведене дослідження наочно показує, що регламентуючі документи мають велику кількість різноманітних помилок, які здатні значно ускладнити розуміння регламенту, що використання неякісно створених документів, які описують процеси діяльності установ може призвести до некоректного виконання процесів і істотно знизити рівень інформаційної безпеки. Отримані дані свідчать що методи аналізу описів процесів мають різну чутливість до порушень коректності описів, тому для проведення якісного аналізу потрібно їх сумісне використання. Також слід зазначити, що застосовані методи не забезпечують виявлення багатьох інших видів порушень коректності описів і тому потребують подальшого удосконалення і доповнення.

Література

1. Итоги 2017 года в сфере ИБ: угрозы, инциденты, тренды, события // Електронний ресурс – Режим доступу: https://ipiskunov.blogspot.com/2017/12/2017.html.
2. Шамов С. О. Застосування контролю якості описів процесів діяльності до вихідних документів реінжинірингового проекту / С.О. Шамов // Радіоелектронні і комп'ютерні системи. – 2012 – №6. – С. 158-163.
3. Денисенко В.О. Застосування регламентів формалізованого опису бізнес-процесів для оцінки якості текстового регламентуючого документу ІТ компанії / В.О. Денисенко, С. О. Шамов // Наукові дослідження молоді з проблем європейської інтеграції : матеріали VIII Міжнародної наук.-практ. конф. молодих учених та студентів. – Х. : ХНМІ ДВНЗ "УБС", 2018. URL: http://khibs.ubs.edu.ua/wp-content/uploads/2018/09/Disk_2018.rar
4. Денисенко В. О. Застосування нотації IDF0 для оцінки якості текстових регламентуючих документів / В. О. Денисенко, С. О. Шамов // II Всеукраїнській науково-практичній конференції «Сучасні інформаційні технології, засоби автоматизації та електропривод». – Харків, 19-21 квітня 2018. URI: http://dspace.dgma.donetsk.ua:8080/jspui/handle/DSEA/297

МЕТОД ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ IP-ТЕЛЕФОНІЇ

Віктор Гнатюк[1], Віталій Котелянець[2], Олег Ткаліч[1]

[1]Національний авіаційний університет, м. Київ, Україна
[2]Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Implementation of IP telephony in various spheres of human activity allows ordinary citizens to simplify their lives, to realize the main aspects of business: increasing sales, improving employee performance, improving customer service quality, automating work processes, providing the necessary information for management, and more. Using IP telephony is important to ensure that the necessary level of information security, because failure to implement this aspect can be a major financial and image loss. Therefore, the purpose of this work is to disable the implementation of intruders of cyber incidents in IP telephony. The research developed a method for increasing the cyber security of IP-telephony.

Keywords: IP-telephony, cyberincident, Asterisk, SIP, ATS.

Сьогодні людство отримало в своє розпорядження досить багато цікавих сучасних технологій, зокрема IP-телефонія, яка для пересічних громадян дозволяє спростити побут, для бізнесу реалізувати головні аспекти: збільшити продажі, підвищити ефективність роботи співробітників, підвищити якість обслуговування клієнтів, автоматизувати робочі процеси, надати необхідну інформацію для керівництва тощо. На ринку представлено велику кількість рішень для побудови IP-телефонії, проте беззаперечним лідером є вільне рішення комп'ютерної телефонії (в тому числі, VoIP) з відкритим вихідним кодом Asterisk від компанії Digium. Архітектура системи Asterisk (рис. 1) включає: мережу, обладнання, локальну операційну сисему та компоненти [1].

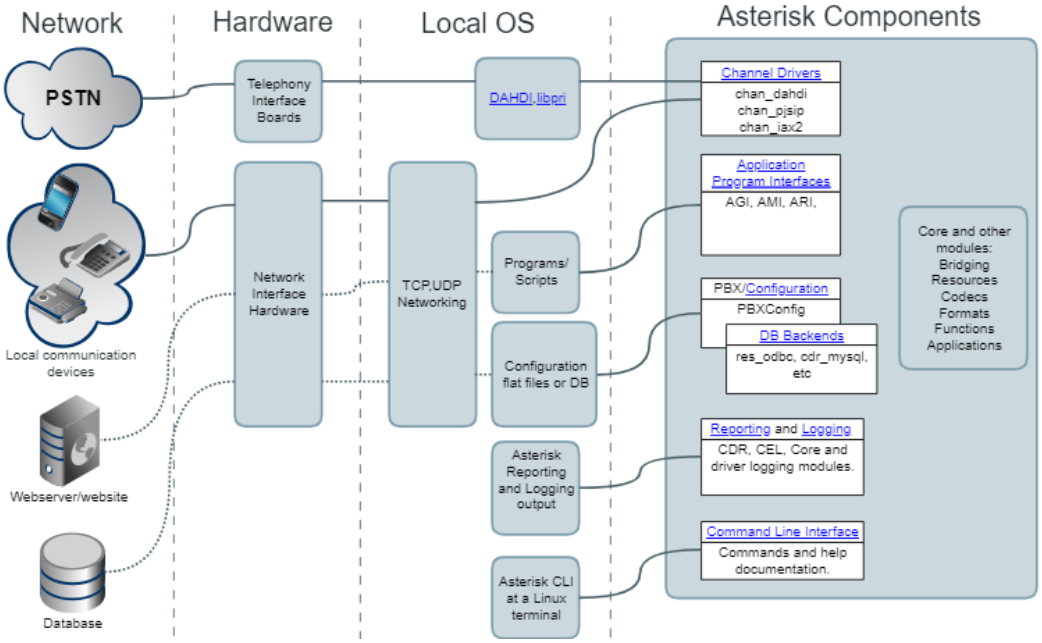


Рис. 1. Архітектура системи Asterisk

Використовуючи IP-АТС Asterisk важливо подбати про забезпечення необхідного рівня інформаційної безпеки, оскільки не виконання цього аспекту може нести з собою великі фінансові та іміджеві втрати. Як правило, «зламують», реалізують кіберінциденти [2], Asterisk з інших країн і починають здійснювати міжнародні дзвінки, після таких «зломів», організаціям приходять рахунки на десятки і навіть сотні тисяч у.о. Причому жертвою може стати як і велика організація (що не факт), так і маленька. В основному це дрібні організації, де безпеці Asterisk приділяється мінімальна увага. Сканування мережі Інтернет у пошуках чергової жертви триває постійно. Отримавши доступ до Asterisk, зловмисники можуть під'єднувати цілі організації на аккаунт жертви і здійснювати міжнародні дзвінки за їх рахунок. Тому, мета

даної роботи полягає у тому, щоб унеможливити реалізацію зловмисниками кіберінцидентів в IP-телефонії, для досягнення якої, розробимо метод підвищення кібербезпеки IP-телефоні. Розроблений метод складається з таких етапів.

Етап 1. Визначення видів вразливостей для IP-телефонії. Для реалізації цього етапу задамо множину видів вразливостей $\mathbf{V}$, які існують під час функціонування IP-телефонії [3-8]:

$$\mathbf{V} = \{\bigcup_{i=1}^{n} \mathbf{V_i}\} = \{\mathbf{V_1}, \mathbf{V_2}, ..., \mathbf{V_n}\}, \quad (i = \overline{1,n}), \tag{1}$$

де n – кількість можливих видів вразливостей.

Етап 2. Визначення послідовності кроків для реалізації кібератаки на IP-телефонію. Для реалізції цього етапу задамо множину кроків $\mathbf{S}$ для реалізації кібератаки на IP-телефонію:

$$\mathbf{S} = \{\bigcup_{i=1}^{n} \mathbf{S_i}\} = \{\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n}\}, \tag{2}$$

де $\mathbf{S_i} \subseteq \mathbf{S}$, $(i = \overline{1,n})$, n – кількість кроків зловмисника.

Етап 3. Підвищення рівня інформаційної безпеки IP-телефонії.

Для реалізції цього етапу задамо множину дій $\mathbf{A}$ для підвищення рівня інформаційної безпеки IP-телефонії:

$$\mathbf{A} = \{\bigcup_{i=1}^{n} \mathbf{A_i}\} = \{\mathbf{A_1}, \mathbf{A_2}, ..., \mathbf{A_n}\}, \tag{3}$$

де $\mathbf{A_i} \subseteq \mathbf{A}$, $(i = \overline{1,n})$, n – кількість дій для підвищення рівня інформаційної безпеки IP-телефонії.

Таким чином, у цій роботі розроблено метод підвищення кібербезпеки IP-телефоні, який за рахунок визначення видів вразливостей для IP-телефонії, визначення послідовності кроків, що чинить зловмисник для реалізації кібератаки на IP-телефонію та підвищення рівня інформаційної безпеки IP-телефонії, дозволяє ідентифікувати можливі види вразливостей для IP-телефонії, дослідити послідовність кроків для реалізації кібератаки на IP-телефонію та виконавши превентивні дії підвищити рівень інформаційної безпеки IP-телефонії.

Розроблений метод спрямований на те, щоб унеможливити реалізацію зловмисниками кіберінцидентів в IP-телефонії. Цей метод та сформовані на його основі засоби будуть корисними, насамперед, для системних адміністраторів, а також для фахівців з інформаційної безпеки у складі команд реагування на кіберінциденти типу CERT/CSIRT на які покладаються обов'язки щодо захисту ІТС в межах підприємств та організацій.

Література

1. Asterisk Architecture: [Електронний ресурс]. — Режим доступу: https://wiki.asterisk.org/wiki/display/AST/Asterisk+Architecture%2C+The+Big+Picture.
2. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі / В.О.Гнатюк // Безпека інформації. — №3 (19). — 2013. — С. 175-180.
3. Меггелен Дж., Мадсен Л., Сміт Дж. Asterisktм: майбутнє телефонії, 2-е видання. — Пер. з англ. — СПб: Символ-Плюс, 2009. — 656 с.
4. Платов М. Asterisk і Linux - місія IP-телефонія [Текст] / М. Платов // Системний Адміністратор. — 2005 р. — № 31. — С. 10-38.
5. База знань Asterisk: [Електронний ресурс]. — Режим доступу: asterisk.ru/knowledgebase.
6. Росляков А.В., Самсонов М.Ю., Шибаєва І.В. IP-телефонія. -М.: Еко-Трендз, 2003. —252 с.
7. Гольдштейн Б.С., Пінчук А.В., Суховицького А.Л. IP-телефонія. — М.: Радио и связь, 2001. — 336 с.
8. CITForum. Безпека IP-телефонії - польові замальовки. А.: [Електронний ресурс]. — Режим доступу: citforum.ru/security/articles/ipsec.

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ДОВІЛЬНОГО ІНТЕРВАЛУ

Наталія Кухарська

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The algorithms of steganographic methods of an arbitrary interval are considered in the work, the advantages and disadvantages of each of them are given, information on the bandwidth of the methods is given.

Keywords: information protection, steganography, text container, interval changing between sentences method, method of trailing spaces, modified method of trailing spaces, double spaces method between words, method for changing the code of spacing, method for changing the number of spaces at the end of text strings, the method for changing the number of spaces between words aligned to the width of the text.

Серед усього спектру методів забезпечення цілісності інформації в інформаційних системах та обмеження доступу до неї сторонніх користувачів особливе місце посідають стеганографічні методи. Їх відмінною рисою є те, що вони дають змогу приховати факт наявності секретної інформації. Досягається це шляхом вбудовування її у відкриті носії даних, які називають контейнерами. По суті, процес стеганографічного приховування зводиться до реалізації алгоритму синтезу двох цифрових носіїв – відкритої і з обмеженим доступом інформації.

Найбільш популярними стеганографічними контейнерами є графічні, текстові, аудіо- і відео- файли різних форматів. Стеганографічні методи використовують їх надлишковість, що дає можливість маскувати вбудоване повідомлення і, як наслідок, уникати прямих атак на секретну інформацію, оскільки невідомо, чи має вона місце в інформаційному потоці, і якщо так, то що є її носієм.

Розглянемо стеганографічні методи, які використовують як контейнери текстові файли. Виокремлюють три групи методів текстової стеганографії; методи довільного інтервалу, синтаксичні методи та семантичні [1]. Зупинимось на методах довільного інтервалу. Їх є доволі багато, інформацію вони приховують у вільних від місцях: у пропусках між словами, в кінці речень, в кінці рядків, використовують різні коди символу пропуск [2]. Їх застосування базується на міркуваннях, що зміни кількості пропусків чи їх кодів не призводять до кардинальних зовнішніх змін документу, не викликають смислових модифікацій речень, а отже пересічний користувач мав би їх не зауважувати.

В усіх методах довільного інтервалу на першому кроці алгоритмів приховуване повідомлення подається у вигляді послідовності біт. Методи довільного інтервалу відрізняються між собою способами приховування окремих біт повідомлення у тексті-контейнері, а отже і пропускною здатністю.

Пропускна здатність – це максимальний обсяг додаткової інформації, що може бути вбудований в один елемент контейнера. У випадку текстового контейнера таким елементом є символ.

Метод зміни інтервалу між реченнями кодує одиничний біт приховуваного повідомлення одним пропуском, нульовий – двома. Їх місце розташування – після символу завершення речення, наприклад, крапки. Недоліки методу: низька пропускна здатність (0,08 %), залежність від структури текстового контейнера, існування ймовірності руйнування прихованого повідомлення деякими текстовими редакторами, що мають властивість автоматично додавати один-два пропуски після символу кінця речення.

Метод хвостових пропусків відрізняється від попереднього методу лише розташуванням символів пропуску, що кодують повідомлення. Вони розміщуються у кінці рядків. Один пропуск у кінці рядка позначатиме нульовий біт, його відсутність – одиничний. Пропускна здатність порівняно з попереднім методом вдвічі більша (0,15 %), метод не залежить від структури документу, проте зберігається недолік спотворення повідомлення текстовими редакторами, які самі по собі додають пропуски в кінець рядків.

Крім того, не можливо прочитати повідомлення з роздрукованого на папері документу, оскільки периферійні символи пропуску у такому випадку є непомітними.

Модифікований метод хвостових пропусків. Єдиний метод довільного інтервалу, який за раз приховується не один біт повідомлення, а чотири. Кількість пропусків, які додають в кінець рядків дорівнює десятковому еквіваленту чотирьох бітів повідомлення, що вбудовується. Недоліки методу ті ж, що і для методу хвостових пропусків. Крім того, збільшення у порівнянні з попереднім методом пропускної здатності (0,63 %) призводить до зниження стеганостійкості методу. Пропуски в кінці рядка, а їх максимально, згідно алгоритму модифікованого методу, може бути аж п'ятнадцять, легше виявити, ніж один пропуск звичайного методу хвостових пропусків.

Алгоритм *методу подвійних пропусків між словами* дуже схожий до алгоритму методу зміни інтервалу між реченнями. Основана відмінність – пропуски, якими кодується повідомлення, розташовуються між словами, а не між реченнями. Пропускна здатність методу для текстового контейнера українською мовою – 1,75%.

Метод зміни кількості пропусків між словами вирівняного за шириною тексту. У процесі приховування повідомлення, згідно алгоритму методу, розглядають окремі слова тексту-контейнера, беруться до уваги лише ті, які оточені з обох боків пропусками. Якщо приховується біт "0", то додатковий символ пропуску додають після слова, якщо "1", то перед словом. Таким чином, кожний біт повідомлення потребує для свого приховання два символи пропуску тексту-контейнера. Крім того, виконуючи вимогу – вирівняти текст за шириною, деякі пари пропусків застосовують не для приховування інформації, а для форматування тексту. У зв'язку з цим, пропускна здатність методу невисока – 0,4 %.

Алгоритми двох наступних методів базуються на використанні символів пропуску, що мають різні коди: звичайного пропуску з кодом 32 та нерозривного пропуску з кодом 160.

Метод зміни коду пропуску. Цей метод для приховування секретної інформації використовує кожен символ пропуску тексту контейнера. Біт "1" кодується символом нерозривного пропуску, а біт "0" – символом звичайного пропуску. Пропускна здатність методу для українськомовного тексту-контейнера – 1,75 %.

Метод зміни кількості пропусків у кінці текстових рядків. Кількість пропусків, яку можна додати до рядка, обчислюють як різницю між кількістю символів у найдовшому рядку тексту і кількістю символів у розглядуваному рядку. Тип кожного доданого пропуску відповідає значенню біта, що приховується. Якщо приховується біт із значенням "0", то до рядка дописується звичайний пропуск (ASCII-код – 32), а якщо біт "1" – нерозривний пропуск (ASCII-код – 160).

Кожен розглянутий метод має свої недоліки та переваги. Не існує жодного методу цифрової стеганографії загалом, текстової зокрема, який би був найбільш прийнятним у порівняні з іншими у всіх випадках його застосування і гарантував стопроцентний рівень захисту. Надійність будь-якого методу може бути оцінена лише в контексті конкретної задачі та мети, яка має бути досягнута. Незважаючи на недоліки, методи довільного інтервалу мають підстави бути застосованими через розповсюдженість файлів текстового формату. Обмін текстовими файлами доступними засобами комп'ютерних мереж є звичною буденною справою, а, отже, не викликає жодних підозр у сторонніх осіб.

Література

1. Крижановська О. Л., Кухарська Н. П. Аналіз методів текстової стеганографії. *Проблеми та перспективи розвитку забезпечення безпеки життєдіяльності* : зб. наук. праць X Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів, м. Львів, 27 берез. 2015 р. Львів, 2015. С. 190-191.
2. Кухарська Н. П. Аналіз стеганографічних методів довільного інтервалу. *Вісник ЛДУ БЖД.* Львів, 2016. № 14. С. 7-16.

НЕЧІТКИЙ ЕКСТРАКТОР ДЛЯ ФОРМУВАННЯ БІОМЕТРИЧНИХ КЛЮЧІВ

Олександр Кузнецов[1], Роман Сергієнко[2], Анна Уварова[3], Валерій Смірнов[4]

[1] Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна
[2] Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів, Україна
[3] Конструкторське бюро «Південне» ім. М. К. Янгеля», м. Дніпро, Україна
[4] Університет митної справи та фінансів, м. Дніпро, Україна

In this paper methods of forming cryptographic keys from biometric images using fuzzy extractors are considered. A new scheme of a fuzzy extractor based on the McEliece cryptosystem is proposed.

Keywords: code based cryptosystem; fuzzy extractor; biometric cryptography.

Важливим напрямком сучасних досліджень в області кіберзахисту є біометричні методи автентифікації особистості [1-12]. Вони широко використовуються в різних додатках: криміналістиці, електронній комерції, захисту авторського права, електронному документообігу та ін.

В останні роки інтерес до біометричних методів значно розширився. Від традиційних біометричних систем, заснованих на порівнянні отриманих біометричних образів з збереженими еталонними копіями, сучасні технології перейшли до формування криптографічних ключів «на льоту». В цьому випадку біометричні дані вже не потребують зберігання або передачі, наявності складних і дорогих засобів захисту та інш., виключається можливість їх навмисної і / або випадкової компрометації. Всі процедури верифікації, ідентифікації і автентифікації виконуються за деперсоналізованими криптографічними ключами (паролями, кодами доступу, пін-кодами), а унікальні біометричні персональні дані особистості залишаються в безпеці. Формовані деперсоналізовані ключові послідовності будемо називати надалі біометричними ключами.

У даній роботі розглядаються методи формування криптографічних ключів з біометричних образів з використанням нечітких екстракторів [3, 4].

Традиційно нечіткі екстрактори [3, 4], як і попередні їм нечіткі контейнери [2], будуються з використанням методів завадостійкого кодування [13-15]. На початковому етапі біометричні дані в деякому сенсі «об'єднуються» з елементами завадостійких кодів (наприклад, з кодовими словами або синдромними послідовностями). Для нечітких екстракторів додатково формується відкритий допоміжний рядок (helper string), який «допомагає» в добуванні секретного параметра по нечітко заданій біометрії. На етапі безпосереднього використання застосовується завадостійке декодування, яке усуває можливу невизначеність (викликану спотвореннями, стирання та ін.) в наданих користувачем біометричних образах. Якщо відмінності в наборах характеристик не великі (не перевищують здатності кодів виправляти помилки), тоді нечіткі екстрактори (сховища) дозволяють однозначно відновити секретний параметр (біометричний ключ).

У даній роботі пропонується нова схема нечіткого екстрактора, в основі якої лежить кодова криптосистема Мак-Еліса [13, 16].

Схема Мак-Еліса запропонована в 1978 році [13] і за 40 років свого існування щодо неї не виявлено суттєвих вразливостей. У разі використання кодів Гоппи [17] з достатньою довжиною і кодовою відстанню ця криптосистема вважається надійним кандидатом на пост-квантове застосування, тобто передбачається її безпечне використання навіть в разі використання повномасштабних універсальних квантових комп'ютерів для вирішення завдань криптографічного аналізу [18, 19].

Наша пропозиція, з одного боку, використовує сильні сторони кодової криптосистеми: криптографічний стійкість, заснована на проблемі синдромного декодування; стійкість до квантових методів криптоаналізу; відносно висока швидкість

перетворення (в порівнянні з іншими криптосистемами з відкритим ключем). З іншого боку, наш екстрактор за допомогою підбору потрібних параметрів завадостійкого коду дозволяє забезпечити як завгодно малі ймовірності помилки першого та другого роду (False Rejection Rate – FRR, False Acceptance Rate – FAR). Використання підказки (helper string) значно знижує FRR, однак зі збільшенням виправної здатності коду це може збільшити FAR за рахунок неправильного «виправлення» біометричних ознак. Вибір компромісного рішення по параметрам коду з урахуванням характеристики виникаючих помилок, експериментальні дослідження FRR і FAR є перспективними напрямками подальшої роботи.

На закінчення відзначимо, що всі міркування, співвідношення і розрахункові значення було отримано для «ідеальних» умов, коли набори біометричних характеристик формуються у вигляді бінарних векторів з випадковими, рівноімовірними та незалежними помилками. В реальних умовах характер помилок може значно відрізнятися. Необхідно проводити подальші дослідження, в тому числі експериментального характеру для обґрунтування практичних рекомендацій щодо безпосереднього використання запропонованого нечіткого екстрактору.

Література

1. Hao F., Anderson R., Daugman J. “Combining cryptography with biometrics effectively: Technical Report UCAM-CL-TR-640”. Cambridge: University of Cambridge Computer Laboratory, 2005. 17 p.
2. A. Juels, M. Sudan, "A fuzzy vault scheme", Des. Codes Cryptography, vol. 38, no. 2, pp. 237-257, 2006.
3. Y. Dodis, R. Ostrovsky, L. Reyzin, A. D. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", SIAM J. Comput., vol. 38, no. 1, pp. 97-139, 2008.
4. Yevgeniy Dodis, Leonid Reyzin, Adam Smith. “Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006”. [On-line]. Internet: http://www.cs.bu.edu/~reyzin/papers/fuzzysurvey.pdf
5. H. Kang, Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura, "Cryptographie key generation from PUF data using efficient fuzzy extractors," 16th International Conference on Advanced Communication Technology, Pyeongchang, 2014, pp. 23-26.
6. N. Li, F. Guo, Y. Mu, W. Susilo and S. Nepal, "Fuzzy Extractors for Biometric Identification," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017, pp. 667-677.
7. Y. Wen and Y. Lao, "Efficient fuzzy extractor implementations for PUF based authentication," 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, 2017, pp. 119-125.
8. T. Kaur and M. Kaur, "Cryptographic key generation from multimodal template using fuzzy extractor," 2017 Tenth International Conference on Contemporary Computing (IC3), Noida, 2017, pp. 1-6.
9. N. K. Gupta and M. Kaur, "A robust and secure multitrait based fuzzy extractor," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017, pp. 1-6.
10. C. Huth, D. Becker, J. Guajardo, P. Duplys and T. Güneysu, "LWE-based lossless computational fuzzy extractor for the Internet of Things," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, 2017, pp. 154-154.
11. C. Huth, D. Becker, J. G. Merchan, P. Duplys and T. Güneysu, "Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things," in IEEE Access, vol. 5, pp. 11909-11926, 2017.
12. A. Schaller, T. Stanko, B. Škorić and S. Katzenbeisser, "Eliminating Leakage in Reverse Fuzzy Extractors," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 954-964, April 2018.
13. McEliece R. J. “A public-key cryptosystem based on algebraic coding theory”. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978, pp. 114-116.
14. Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. Springer, 1981, 432 p.
15. Blahut R. E. Theory and Practice of Error Control Codes. Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983, 500 p.
16. A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code-based electronic digital signature," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331-336.
17. V.D. Goppa, "A New Class of Linear Correcting Codes", Problems Inform. Transmission, 6: 3 (1970), 207-212.
18. D. Bernstein, J. Buchmann and E.Dahmen. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.

ЕВРИСТИЧНІ МЕТОДИ ГРАДІЄНТНОГО ПОШУКУ КРИПТОГРАФІЧНИХ БУЛЕВИХ ФУНКЦІЙ

Олександр Кузнецов[1], Іларіон Московченко[2], Микола Пастухов[2], Тетяна Кузнецова[1]

[1] Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна
[2] Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, Україна

In this article, heuristic methods of hill climbing for cryptographic Boolean functions satisfying the required properties of balance, nonlinearity, autocorrelation, and other stability indicators are considered. Comparative assessments of the effectiveness of the heuristic methods are considered.

Keywords: symmetric cryptography; nonlinear substitute blocks; boolean functions.

Важливим елементом більшості сучасних симетричних шифрів є нелінійні блоки замін, які описуються за допомогою булевих або, в загальному випадку, векторних криптографічних функцій [1-17]. Показники стійкості таких функцій (збалансованість, нелінійність, автокорреляция та ін.) безпосередньо впливають на ефективність симетричних шифрів, їх стійкість до більшості сучасних криптоаналітичних атак. Отже, дослідження методів побудови криптографічних булевих функцій є актуальною науковою задачею, що має важливе значення як для розвитку теорії побудови симетричних криптопримітивів, так і для прикладних аспектів їх використання в різних протоколах безпеки.

У даній роботі розглядаються евристичні методи побудови криптографічних булевих функцій, що задовольняють необхідним властивостям по збалансованості, нелінійності, автокореляції та іншими показниками стійкості. Зокрема, нами досліджуються метод градієнтного підйому В.Міллана, Е.Кларка, Е.Доусона, 1997 р [16] і розроблений на його основі метод градієнтного спуску [17].

Сутність методу градієнтного підйому полягає в підвищенні нелінійності булевої функції шляхом комплементації довільної позиції в таблиці істинності [16]. Кожна позиція відповідає унікальним вхідним даним. Метод дозволяє створити повний список / перелік таких вхідних даних функції, що комплементація будь-якої позиції буде збільшувати нелінійність криптографічної функції. Критерієм градієнтного пошуку є максимізація відстані по Хеммінгу між формованої послідовністю і послідовностями лінійних функцій. Проведені дослідження показали, що розглянутий метод обчислювально витратний і, при великому числі аргументів, вимагає виконання значного числа повторюваних ітерацій.

Метод градієнтного спуску заснований на комплементації позицій бент-послідовностей для градієнтного пошуку збалансованих булевих функцій за критерієм максимізації відстані Хеммінга між сформованими послідовностями і послідовностями всіх лінійних функцій [17]. Це дозволяє значно знизити обчислювальні витрати на пошук булевих функцій з необхідними криптографічними властивостями.

Слід зазначити, що імовірнісний пошук евристичними методами описується деяким випадковим процесом, конкретна реалізація якого суть випадкові величини - значення показників стійкості знайденої функції. Відповідні ймовірності настання шуканих випадкових подій вказують на середнє число спроб до успіху - побудови криптографічного булевої функції з необхідними властивостями. Таким чином, для оцінки обчислювальної ефективності евристичних методів, тобто оцінки відповідності отриманого результату необхідному, необхідно провести оцінку розподілу ймовірностей формування булевих функцій з різними криптографічними показниками.

В цій роботі пропонується методика оцінки обчислювальної ефективності методів градієнтного пошуку, заснована на побудові вибіркових (емпіричних) функцій розподілу, що характеризують ймовірність формування булевих функцій з показниками стійкості не

нижче необхідних. Як показник обчислювальної ефективності пропонується середнє число спроб, який буде потрібно виконати з використанням евристичного методу для формування криптографічної функції з необхідними властивостями.

Проведені дослідження показали, що метод градієнтного спуску, запропонований в [17], є ефективнішим Hill Climbing Method з [16]. Наприклад, формування криптографічної функції з автокореляцією AC = 24 і нелінійністю N = 116 для методу градієнтного підйому потребує в середньому близько 8000 спроб. Метод градієнтного спуску при тих же показниках потребує в середньому 4 спроби. При AC = 24 і N = 114 метод градієнтного підйому потребує в середньому близько 15 спроб, а метод градієнтного спуску - близько 3.

Запропонована методика оцінки обчислювальної ефективності евристичних методів може бути використана і для інших методів, в тому числі, що використовують розширений набір показників стійкості.

Література

1. Bharti and D. K. Sharma, "Searching boolean function using simulated annealing and hill climbing optimization techniques," 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, 2016, pp. 62-64.
2. D. Tang, C. Carlet and X. Tang, "Highly Nonlinear Boolean Functions With Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks," in IEEE Transactions on Information Theory, vol. 59, no. 1, pp. 653-664, Jan. 2013.
3. R. Asthana, N. Verma and R. Ratan, "Generation of Boolean functions using Genetic Algorithm for cryptographic applications," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, pp. 1361-1366.
4. M. A. Al Shehhi, Joonsang Baek and Chan Yeob Yeun, "The use of Boolean functions in stream ciphers," 2011 International Conference, Abu Dhabi, 2011, pp. 29-33.
5. Y. Wei, N. Ouyang and Y. Hu, "New construction of Boolean functions which satisfy multiple cryptographic criteria," 2009 Fourth International Conference, Xian, 2009, pp. 1-6.
6. C. Carlet, "On the Higher Order Nonlinearities of Boolean Functions and S-boxes," 2009 International Conference on Availability, Reliability and Security, Fukuoka, 2009, pp. 768-768.
7. E. Elsheh, A. BenHamza and A. Youssef, "On the nonlinearity profile of cryptographic Boolean functions," 2008 Canadian Conference, Niagara Falls, ON, 2008, pp. 001767-001770.
8. W. Millan, J. Fuller and E. Dawson, "New concepts in evolutionary search for Boolean functions in cryptology," Evolutionary Computation, 2003. CEC '03. The 2003 Congress on, 2003, pp. 2157-2164 Vol.3.
9. Z. Wang and G. Gong, "Discrete Fourier Transform of Boolean Functions over the Complex Field and Its Applications," in IEEE Transactions on Information Theory, vol. 64, no. 4, pp. 3000-3009, April 2018.
10. B. Mazumdar and D. Mukhopadhyay, "Construction of Rotation Symmetric S-Boxes with High Nonlinearity and Improved DPA Resistivity," in IEEE Transactions on Computers, vol. 66, no. 1, pp. 59-72, Jan. 1 2017.
11. S. Picek, C. Carlet, S. Guilley, J. F. Miller and D. Jakobovic, "Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography," in Evolutionary Computation, vol. 24, no. 4, pp. 667-694, Dec. 2016.
12. K. Verma and D. K. sharma, "Calculation of non-linearity and algebraic degree of constructed boolean function," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 501-505.
13. C. E, S. Liang and T. Zhang, "Construction Method of Boolean Functions Based on Genetic Algorithm," 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, Wuhan, 2011, pp. 1-4.
14. J. Fuller, E. Dawson and W. Millan, "Evolutionary generation of bent functions for cryptography," Evolutionary Computation, 2003. CEC '03. The 2003 Congress on, 2003, pp. 1655-1661 Vol.3.
15. C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan and T. Helleseth, "Generic Construction of Bent Functions and Bent Idempotents With Any Possible Algebraic Degrees," in IEEE Transactions on Information Theory, vol. 63, no. 10, pp. 6149-6157, Oct. 2017.
16. W. Millan, A. Clark, E. Dawson, "Smart Hill Climbing Finds Better Boolean Functions", Proceedings of the Workshop on Selected Areas on Cryptography SAC 97, Springer-Verlag, pp. 50-63, 1997.
17. Y. Izbenko, V. Kovtun and A. Kuznetsov, "The Design of Boolean Functions by Modified Hill Climbing Method," 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, 2009, pp. 356-361.

КОДОВІ КРИПТОСИСТЕМИ ДЛЯ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Олександр Кузнецов[1], Дмитро Прокопович-Ткаченко[2], Федір Курінний[2], Катерина Кузнецова[1]

[1] Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна
[2] Університет митної справи та фінансів, м. Дніпро, Україна

In this paper we consider a "provably" strong Code-based pseudorandom sequence generator whose cryptanalysis problem is reduced to solving a well-known and extremely complex mathematical problem of syndrome decoding (belonging to the NP-complex class). It was found that the generated sequences do not have the maximum period, the actual period is much lower than expected. In our work, we propose a new generator sheme that retains all the positive properties of the prototype, but the pseudorandom sequences which are formed have a maximum period.

Keywords: Code-based Pseudorandom Number Generator; "Provable" Security Model; Cryptographically Strong Pseudorandom Sequences; Periodic Properties.

Важливим напрямком у розвитку пост-квантових методів захисту інформації є криптографія, що засновано на завадостійких кодах [1,2]. У роботах [3-9] показано, що використання таких методів дозволяє забезпечити високу стійкість як до класичного, так і до квантовому криптоаналізу.

Перша кодова криптосистема була запропонована 40 років тому [3] і, при відповідних параметрах, залишається стійкою до цього дня [4-9]. Незважаючи на численні спроби криптоаналізу [5-9] схема Мак-Еліса на основі кодів Гоппи [10] вважається надійною альтернативою сучасним криптосистемам з відкритим ключем.

Подальший розвиток кодових криптосистем отримав в роботах [11-20]. Зокрема, в [11] запропонована еквівалентна по стійкості криптосистема Нідррайтера, яка покладена в основу схем електронного цифрового підпису [14, 15]. В [16] запропоновано новий варіант підпису, який використовує криптосистему McElice.

На сьогоднішній день Національний інститут стандартів і технологій (National Institute of Standards and Technology – NIST) США проводить відкритий конкурс пост-квантової криптографії (NIST PQC) [1, 2, 21-23], де аналізується 64 конкурсних пропозиції (з 82 попередньо поданих) за трьома основними напрямками: направлене шифрування, інкапсуляція ключів та електронний цифровий підпис [22]. Із загальної кількості конкурсних пропозицій третю частину займає криптографія на кодах [23]. Очікується [1, 23], що в найближчі десятиліття проект NIST PQC завершитися прийняттям серії стандартів пост-квантової криптографії з відкритим ключем.

Ще одним напрямком у розвитку криптографії на завадостійких кодах є побудова "доказовою" стійких генераторів псевдовипадкових послідовностей [25-27]. Суть "Provable" Security Model полягає у зведенні задачі криптоаналізу до вирішення добре відомої і надзвичайно складної математичної задачі (що відноситься до класу NP-складних), наприклад, факторизації, дискретного логарифмування, тощо [28]. Криптографічні примітиви, що відповідають такої моделі безпеки, прийнято називати «доказово» безпечними, тому що їх криптоаналіз можна порівняти з рішенням певної NP-складної математичної задачі. У контексті розвитку пост-квантової криптографії побудова і аналіз "доказовою" стійких генераторів безсумнівно є важливим і актуальним.

Метою даної роботи є аналіз "доказовою" стійкого генератора на кодах, запропонованого в [25], дослідження періодичних властивостей формованих псевдовипадкових послідовностей. В ході досліджень було виявлено, що формовані за допомогою генератору [25] послідовності не володіють максимальним періодом, фактичний період є значно нижчим за очікуваний. У нашій роботі пропонується нова схема генератора, яка зберігає всі позитивні властивості прототипу, проте псевдовипадкові послідовності мають максимальний період.

Література

1. D. Moody. “Post-Quntum Cryptography: NIST’s Plan for the Future.” The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. [On-line]. Internet: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].
2. Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone. “NISTIR 8105. Report on Post-Quantum Cryptography”, National Institute of Standards and Technology, Internal Report 8105, April 2016, 10 p. [On-line]. Internet: http://dx.doi.org/10.6028/NIST.IR.8105
3. R.J. McEliece “A public-key cryptosystem based on algebraic coding theory”. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978, pp. 114-116.
4. D. Bernstein, J. Buchmann and E.Dahmen. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.
5. V.M.Sidelnikov. “Cryptography and coding theory”. Proceedings of the conference "Moscow University and Development of Cryptography in Russia", Moscow State University, 2002, 22 p. (In Russian).
6. Anne Canteaut and Nicolas Sendrier. “Cryptanalysis of the original McEliece cryptosystem”. ASIACRYPT’98, volume 1514 of Lecture Notes in Computer Science, pp. 187-199.
7. Vladimir M. Sidelnikov and Sergey O. Shestakov. “On insecurity of cryptosystems based on generalized Reed-Solomon codes”, Discrete Mathematics and Applications, 1992, pp. 439-444.
8. L.Minder and A. Shokrollahi. “Cryptanalysis of the Sidelnikov Cryptosystem”, Advances in Cryptology - EUROCRYPT 2007, May 20-24, 2007, Proceedings, Springer Berlin Heidelberg, 2007, pp. 347-360.
9. D.J.Bernstein, T.Lange and C.Peters. “Attacking and Defending the McEliece Cryptosystem”. PQCrypto 2008. Lecture Notes in Computer Science, vol 5299. Springer, Berlin, Heidelberg, pp. 31-46.
10. V. D. Goppa. “New class of linear correcting codes”, Problems of information transmission, 1970, Vol. 6, issue.3. pp. 24-30. (In Russian) .
11. Niederreiter H. “Knapsack-type cryptosystems and algebraic coding theory”. Problem Control and Inform Theory, 1986, v. 15. pp. 19-34.
12. V.M. Sidelnikov, S.O. Shestakov. “On the system of encryption based on generalized Reed-Solomon codes”. Discrete mathematics, 1992, v. 4., №3. pp. 57-63. (In Russian)
13. T. R. N. Rao and K. H. Nam. “Private-key algebraic-coded cryptosystem”. Advances in Cryptology - CRYPTO 86, New York, NY: Springer, pp. 35-48.
14. Courtois, N., Finiasz, M., and N.Sendrier. “How to achieve a McEliece-based digital signature scheme”. In Advances in Cryptology - ASIACRYPT 2001, volume 2248, pp. 157–174.
15. M.Finiasz. “Parallel-CFS: Strengthening the CFS McEliece-based signature scheme”. In Biryukov, A., Gong, G., Stinson, D., eds.: Selected Areas in Cryptography. Volume 6544 of LNCS., Springer (2010), pp. 159 -170.
16. Alexandr Kuznetsov, Andriy Pushkar’ov, Nastya Kiyan and Tetiana Kuznetsova. “Code-Based Electronic Digital Signature”, The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018, 24-27 May, 2018, Kyiv, Ukraine, pp.
17. A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125-130.
18. Yu. V. Stasev, A. A. Kuznetsov. “Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes”. Cybernetics and Systems Analysis, Volume 41, Issue 3, pp. 354-363, May 2005.
19. A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko, "Construction of cascade codes in the frequency domain," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 131-136.
20. Yu.V. Stasev, A.A. Kuznetsov. “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes”. Kibernetika i Sistemnyi Analiz, No. 3, pp. 47-57, May-June 2005.
21. “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”, National Institute of Standards and Technology, 25 p.
22. Ray A. Perlner and David A. Cooper. “Quantum Resistant Public Key Cryptography: A Survey”, IDtrust ’09, April 14-16, 2009, Gaithersburg, MD, pp. 85-93.
23. Dustin Moody. “Let’s Get Ready to RumbleThe NIST PQC “Competition”, National Institute of Standards and Technology, April 18, 2018, 37 p.
24. “Computer Security Resource Center”. Round 1 Submissions. Created January 03, 2017, Updated June 25, 2018. [On-line] Internet: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
25. Jean-Dernard Fisher, Jacques Stern. “An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding”. EUROCRYPT’96 Proceeding, LNCS 1070, p. 245-255.
26. P. Gaborit, C. Lauradoux and N. Sendrier, "SYND: a Fast Code-Based Stream Cipher with a Security Reduction," 2007 IEEE International Symposium on Information Theory, Nice, 2007, pp. 186-190.
27. T. Wu and R. Wang, "Stream cipher by reed-solomon code," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 422-427.
28. “Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption”, April 19, 2004 - Version 0.15 (beta), Springer-Verlag, 829 p.

СТЕГАНОГРАФІЧНА СИСТЕМА З ПІДВИЩЕНИМ ВМІСТОМ ПРИХОВАНОЇ ІНФОРМАЦІЇ

Андрій Лагун

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

In the paper is considered algorithm of information hiding in the static images. Is shown that usage of the Huffman coding and pseudorandom number generator based on the irreducible polynomial increases the efficiency of hiding

Keywords: steganography, Huffman coding, binary tree, pseudorandom generator, container, least significant bit

На цей час значно зростають обсяги інформації, яка передається та зберігається людьми. В роботі будуть розглянуті способи побудови інформаційних систем, які дозволяють захистити передану інформацію і зменшити її розмір.

Для забезпечення захищеності інформації в інформаційних та комунікаційних системах використовуються різні методи захисту, які забезпечують виконання таких характеристик інформації як цілісність, конфіденційність та автентичність. Серед цих методів захисту можна виділити криптографічні та стеганографічні. Відомо, що криптографічні методи захисту інформації перетворюють інформацію до незрозумілого вигляду з використанням криптографічних алгоритмів, а стеганографічні приховують сам факт існування захищеної інформації.

Надалі будемо розглядати стеганографічні системи, які приховують інформацію в нерухомих зображеннях, використовуючи алгоритми стиснення інформації та псевдовипадкові генератори імпульсних послідовностей.

Взагалі кажучи, цифрове зображення є масивом значень пікселів у вигляді списку чисел. Під час приховування початковий масив перетворюється так, щоб зменшити обсяг пам’яті під початковим зображенням. Тоді прихована інформація вбудовується у ті області, якими можна знехтувати. На приймальній стороні відновлюється початкове зображення із закодованого і видобувається прихована інформація.

Найпростішим методом приховування інформації в нерухомих зображеннях є метод найменшого значущого біта [1]. В ньому замінюють останні значущі бітів прихованого зображення бітами прихованої інформації. В RGB зображенні кожному пікселу відповідає три байти (для інтенсивностей червоного, зеленого і синього кольорів). Приховану інформацію можна записувати в останній біт кожного байта, а саме один піксел зображення буде містити три біти прихованої інформації.

Розглянемо коротко різні алгоритми найменшого значущого біта.

Під час приховування в найпростіше записати приховувану інформацію, починаючи з верхнього лівого кута зображення-контейнера до правого нижнього попіксельно. Секретна інформація розподіляється в початковому зображенні нерівномірно.

Інший алгоритм псевдовипадково розподіляє приховане повідомлення у контейнері. Генератор псевдовипадкової послідовності використовує ключ, який використовується на передавальній і приймальній стороні.

Можливий також спосіб приховування, який використовує попередню фільтрацію, а саме пошук пікселів порожнього контейнера найменш помітних для людського ока, в які буде записуватися прихована інформація. У цьому випадку можна спробувати використати кілька найменших біт одного байта контейнера.

Найкращий алгоритмом приховування використовує попередню фільтрацію початкового зображення із псевдовипадковим генератором для визначення місць контейнера, в які буде записуватися прихована інформація.

Автором досліджено стеганографічний алгоритм найменшого значущого біта з використанням подвійного захисту прихованого повідомлення. Спочатку в алгоритмі відбувається кодування прихованого повідомлення адаптивним алгоритмом Хаффмена з

впорядкованим бінарним деревом [2], а потім закодовані значення розміщуються в порожньому контейнері – нерухомому зображенні з використанням псевдовипадкового генератора на основі незвідного поліному [3]. Структуру алгоритму наведено на рис. 1.

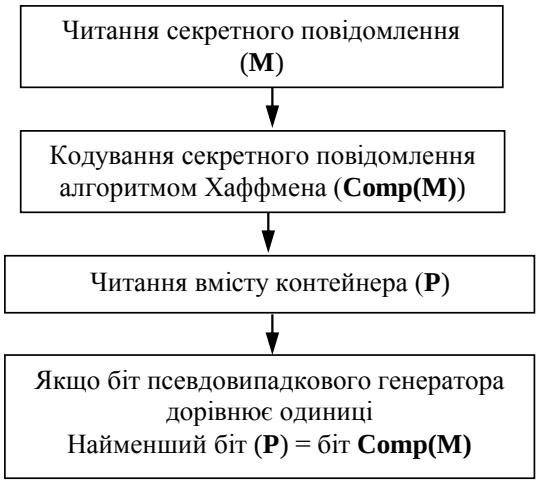


Рис. 1. Алгоритм приховування секретного повідомлення

Основною перевагою адаптивного алгоритму Хаффмена є відсутність потреби передавання на приймальну сторону таблиці кодування. При кожному кодуванні вхідних значень змінюється внутрішній хід виконання обчислень таким чином, що при наступному кодуванні такого ж символу формується інший код, тобто відбувається адаптація алгоритму до значень, що надходять для кодування. Зрозуміло, що цим алгоритмом можна кодувати будь-які цифрові дані, які одержані з текстової, графічної або звукової інформації. У всіх цих випадках кожне кодованим значенням буде або значення символу з таблиці кодування символів, або значення інтенсивності кольору з палітри кольорів, або значення амплітуди звукового сигналу.

Для приховування місця знаходження закодованого на попередньому етапі секретного повідомлення використовується псевдовипадковий генератор на основі 64-розрядного регістра зсуву з лінійним зворотним зв'язком, який для побудови послідовності біт використовує незвідний поліном $F(x)=x^{64}+x^4+x^3+x+1$. Цей поліном є примітивним за модулем 2 [3]. Для відтворення однакових послідовностей біт на приймальній та передавальній стороні використовується однаковий ключ. Фрагмент програми мовою *C++* для генератора має такий вигляд:

```
LFSR=(((((LFSR>>63)^(LFSR>>3)^(LFSR>>2)^LFSR)) & 0x0000000000000001)<<63)
        | (LFSR>>1)) & 0x0000000000000001;
```

Протягом процесу приховування вміст генератора перебирається із вмістом контейнера і для значень одиниць генерованої послідовності значення найменшого значущого біта пікселів контейнера записуються такими, як у прихованому повідомленні.

Стеганографічне зображення, отримане в результаті роботи алгоритму найменшого значущого біта, дуже чутливе до будь-яких модифікацій, а саме найменша обробка цього зображення може призвести до втрати прихованої інформації. Проте за рахунок попереднього кодування секретної інформації знайти її у заповненому контейнері є важким завданням.

Література

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю Пузыренко. – К. : МК-Пресс, 2006. – 249 с.
2. Лагун А.Е. Теорія інформації та кодування : навчальний посібник / А.Е. Лагун, Ю.І. Грицюк. – Львів : Вид-во СПОЛОМ, 2016. – 83 с.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. / B. Schneier. – New York : John Wiley and Sons, 1996.

ЗАХИСТ ВІД ПІДМІНИ КОРИСТУВАЧА У СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Тетяна Лаврик

Сумський державний університет, м. Суми, Україна

The article deals with information security problems and threats of distance learning systems. Impersonation fraud is one of the specific threats in distance learning systems. The article discusses the use of multifactor authentication to solve this problem.

Keywords: distance learning, security, threat, multifactor authentication, keystroke dynamics.

Дистанційне навчання є однією з найбільш перспективних форм підготовки сучасних фахівців і реалізується через систему дистанційного навчання (ДН), яка представляє собою складний комплекс програмних рішень.

Будь-яка система дистанційного навчання є частиною інтегрованої інформаційної системи навчального закладу, основними функціональними компонентами якої є веб-додаток, база даних і сервер [2, с. 10].

Типовий технологічний процес опрацювання інформації в системі дистанційного навчання може бути представлений таким чином:

1) підключення користувача до веб-сайту ДН;

2) авторизація користувача на сервері ДН;

3) запит на сервер ДН для надання доступу до ресурсів системи;

4) введення, модифікація або виведення інформації відкритого та/або обмеженого доступу;

5) отримання користувачем необхідного матеріалу та даних;

6) відключення користувача від ресурсів системи ДН [4].

Якщо розглядати саме такий технологічний процес з точки зору інформаційної безпеки, то можна виявити певні вразливості. Зокрема, найбільш уразливими будуть процеси:

- передачі ідентифікаційних та аутентифікаційних даних користувача;
- обміну даними між браузером віддаленого користувача та веб-сайтом ДН;
- авторизації користувача в системі ДН;
- обміну даними між сервером ДН і сервером інформаційної системи навчального закладу [4].

Такий висновок в першу чергу пов'язано з тим, що саме у процесі виконання даних дій найбільш вірогідною є спроба зловмисника реалізувати атаки на систему дистанційного навчання і отримати доступ до її ресурсів, сервісів і даних. Основними чинниками, що спричиняють подібні атаки, є уразливості веб-додатків і сервісів ДН, слабкі паролі і недоліки процесу аутентифікації користувачів на сервері ДН, помилки в конфігурації і адмініструванні системи ДН, шкідливе програмне забезпечення, слабкості системи захисту інформації. Виходячи з цього, у системах дистанційного навчання можна виділити такі загрози, як загрози реєстрації та аутентифікації, загрози достовірності результатів контролю знань та загрози впровадження шкідливих програм.

З аналізу безпеки сучасних систем дистанційного навчання можна виділити такі загрози достовірності результатів контролю знань, від яких не захищається жодна система, зокрема загрози підміни користувача та загрози використання програмних ботів і скриптів. Інші загрози є типовими для всіх інформаційних систем і для захисту від них у системах ДН або вже реалізовані необхідні механізми, або від них неможливо захиститися.

Для вирішення проблеми підміни користувача у системі ДН можливе використання механізму багатофакторної аутентифікації.

Багатофакторна аутентифікація здійснюється за допомогою захищених механізмів двох або більше типів. Прикладом є застосування для аутентифікації пароля разом із апаратним засобом захисту інформації (токеном) або біометричної аутентифікації разом із паролем.

Використання методів аутентифікації за допомогою апаратних засобів у системах ДН не є рентабельним у зв'язку з постійним зростанням і зміною користувачів, а також високим ступенем їх територіальної розосередженості. Подібна ситуація і з методами біометричної аутентифікації за райдужною оболонкою, сітківкою ока, геометрією рук тощо. Вони також вимагають наявності у кожного віддаленого користувача спеціального дороговартісного обладнання [1].

Проаналізувавши методи за біометричними параметрами людини, для захисту від загрози підміни користувача обрано двофакторну аутентифікацію на основі парольного захисту та біометричного методу на основі клавіатурного почерку. Важливим для умов дистанційного навчання є те, що обрані фактори не потребують додаткових витрат.

Сучасні дослідження показують, що клавіатурний почерк користувача володіє деякою стабільністю, що дозволяє досить однозначно ідентифікувати користувача. Застосовуються статистичні методи обробки вихідних даних і формування вихідного вектору, що є ідентифікатором даного користувача. В якості вихідних даних використовують тимчасові інтервали між натисканням клавіш на клавіатурі та час їх утримання. При цьому, тимчасові інтервали між натисканням клавіш характеризують темп роботи користувача, а час утримання клавіш характеризує стиль роботи з клавіатурою –різкий удар або плавне натискання. У роботі [3] наведено результати порівняльного аналізу відомих математичних моделей, методів та засобів біометричної аутентифікації за клавіатурним почерком. Також встановлено важливий висновок, що саме прихований моніторинг клавіатурного почерку під час набору вільного тексту є перспективним напрямом подальших досліджень у галузі інформаційної безпеки, оскільки уможливлює підвищення достовірності аутентифікації особи [3].

Зважаючи на викладене вище, актуальним є ґрунтовне дослідження питання захисту від загрози підміни користувача у системах дистанційного навчання і розроблення програмного рішення для захисту на основі двофакторної аутентифікації.

Література

1. Головань В.Г. Інформаційна безпека систем дистанційного навчання / В.Г. Головань, В.В. Сергєєв, В.Н. Герасимов // Наукові записки Міжнародного гуманітарного університету. – 2013. – № 18. – С. 240 – 242.
2. ІТ-забезпечення діяльності інноваційного університету: досвід українського вишу: монографія / А. В. Васильєв, В. О. Любчак, Ю. О. Зубань [et al.] ; За заг. ред. А.В. Васильєва. – Суми : СумДУ, 2016. – 173 с.
3. Лупенко С. А. Компаративний аналіз моделей, методів та засобів аутентифікації особи в інформаційних системах за її клавіатурним почерком / С. А. Лупенко, Н. Р. Шаблій, А. М. Лупенко [Електронний ресурс] // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. - 2014. – № 806. - С. 141-147. – Режим доступу: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_23
4. Оладько В. С. Модель оценки защищенности систем дистанционного образования вузов / В. С. Оладько // Образовательные технологии и общество. – 2016. – Т. 19, № 1. – С. 360-376.

СТАНДАРТ ISO 27001: ОГЛЯД

Надія Майданюк[1], Олена Чугаєва[2]

[1] Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України

[2] ДВНЗ "Київський національний економічний університет імені Вадима Гетьмана", м. Київ, Україна

The issue of the information security management system according to the international standard ISO 27001 is considered. The standard contains requirements in the field of information security for the creation, development and maintenance of the information security management system.

Keywords: ISO 27001, information technologies, information security, standard, information security management.

Сучасний розвиток інформаційних технологій (ІТ) істотно розширює можливості ефективного ведення бізнесу, створює інноваційні конкурентні переваги, відкриває перед компаніями нові ринки. Водночас розвиток ІТ супроводжують і певні вади, що полягають у загостренні проблем інформаційної безпеки суб'єктів господарювання, зростанні кіберзлочинності. Вплив інформаційних ризиків реалізується через уразливість інформаційних систем, що підтримують різні види господарської діяльності промислових підприємств, та виникнення збитків компаній є наслідком витоків конфіденційної інформації, збоїв у роботі інформаційних мереж і систем. У зв'язку з цим, виникає необхідність забезпечення інформаційної безпеки суб'єктів господарювання як соціально-економічних систем у цілому.

Міжнародні стандарти серії ISO (ISO/IEC 17799, ISO 27001) є основоположними в сфері управління інформаційною безпекою. Вони представляють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику. Аналогом міжнародному стандарту ISO 27001 є ДСТУ ISO/IEC 27001:2015.

Стандарт ISO 27001 визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації». ISO 27001:2015 являє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації, а стандарт ISO 27002:2015 виступає в якості керівництва по впровадженню, яке може використовуватися при проектуванні механізмів контролю, вибраних організацією для зменшення ризиків інформаційної безпеки. Стандарт ISO 27001 визначає процеси, що представляють можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки; встановлює вимоги до розробки, впровадження, функціонуванню, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації.

Згідно з міжнародним стандартом ISO 27001, система управління інформаційною безпекою – це «частина загальної системи управління організації, яка заснована на оцінці ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки».

У відповідності з вимогами ISO/IEC 27001 система управління інформаційної безпеки повинна містити такі етапи [1,2,3]:

1 етап – планування - фаза створення, створення переліку інформації, оцінки ризиків і вибору заходів та механізмів захисту;

2 етап - дія - етап реалізації та впровадження відповідних заходів;

3 етап – перевірка - фаза оцінки ефективності та надійності функціонування створеної системи. Проведення внутрішнього аудиту системи, виявлення недоліків.

4 етап – удосконалення - виконання коригувальних дій по покращенню функціонуванню системи;

При створенні системи управління інформаційної безпеки потрібно керуватися відповідними заходами. Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків і можливих втрат, якщо відбудеться порушення безпеки інформаційно-комунікаційними системами мереж.

Отже, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Література

1. ISO/IEC 27001:2013, Information Security Management - Specification With Guidance for Use
2. ISO/IEC 27001:2018, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
3. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. Поправка (ISO/IEC 27001:2013; Cor 1:2014, IDT): [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=69727

АНАЛІЗ СТАНУ ЗАБЕЗПЕЧЕННЯ КОНФІДЕЦІЙНОСТІ ІНФОРМАЦІЇ ПРО КОРИСТУВАЧА В ІНТЕРНЕТІ

Олексій Максимів

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The problem of receiving and transmitting information about the user, for today is especially acute. There are a number of mechanisms that can avoid this, but the question arises as to how well they do it. In this work we analyze the state of ensuring user confidentiality with the Do Not Track function.

Keywords: information security, Do Not Track, user confidentiality.

Збір інформації про користувачів інтернету розпочалось ще наприкінці 90-их років, однак лише протягом останніх років це набуло такого масового поширення. Основним фактором що сприяв і надалі сприяє розвитку темпів та кількості інформації про користувачів, це, безсумнівно, можливості її використання в контексті реклами, що дозволяє збільшити доходи компаній шляхом визначення цільової аудиторії. Все це призвело до створення цілого ряду агенств, які здійснюють моніторинг за поведінкою користувача та збирають інформацію про історію його пошуків, обрані ним товари, сайти які він відвідує тощо.

Про існування проблеми отримання інформації такого типу, без згоди самих користувачів, яскраво свідчить скандал з Facebook в 2018 р. Як свідчать останні аналітичні дослідження, Facebook може збирати дані навіть про тих людей, у яких немає акаунтів в цій соціальній мережі [1]. Відповідно, відсутність елементів прозорості та регуляторних рамок посилило інтерес населення щодо їх конфідеційності, що і зумовило більше детальніше дослідження процесу отримання інформації про дії користувача в Інтернеті та методи протидії передачі цієї інформації третій особі.

В основі механізму відслідковування дій користувача лежить процес збору та подальший аналіз файлів cookie. Зазначені файли дозволяють зберігати інформацію, отриману від веб-сайтів, тим самим ідентифікуючи користувача при наступному відвідувані, що дозволяє відповідному веб-сервісу визначити чи заходив користувач раніше і проаналізувати дії, які він виконував (для прикладу заходив в особистий кабінет). Такий підхід дозволяє в значній мірі упростити процес роботи з різноманітними веб-ресурсами, особливо на етапі визначення користувача.

Разом з цим, сервер і браузер постійно обмінюються cookie файлами, які зазвичай містять в собі конфідеційну інформацію, таку як імя користувача, найчастіше відвідувані сторінки, адреса звідки здійснюється підлкючення тощо. Відповідно, аналізуючи файли cookie можливо побудувати портрет кожного унікального користувача. Вказана технологія дозволяє веб-сайтам зберігати унікальний ідентифікатор у вашому веб-переглядачі, що надає змогу компаніям відслідковувати весь процес переміщення користувача, навіть на інших сайтах, що для багатьох людей сприймається як вторгнення в їхню конфідеційність.

Переважна більшість спроб забезпечення конфідеційності особистої інформації були занадто складними для звичайних користувачів, або вимагали доволі довгого та точного виконання вказаних інструкцій, що користувачами абсолютно не сприймалося. Допомогти в цьому повинен був механізм Do Not Track (DNT), запропонований ще в 2009 р. DNT — це HTTP-заголовок, який може бути включений до повідомлення HTTP і може приймати одне з бітових значень (0 або 1). Вказані значення дозовляють вказати серверу, який отримує запит, чи дозволяється відстежувати інформацію про користувача. Відповідно, якщо встановлено значення “1”, то це означає, що користувач відмовляється від стеження за ним, а “0” означає що користувач згоден щодо збору інформації про нього [2].

На даний момент механізм DNT інтегрований в усіх пяти найбільш використовуваних браузерах. Поряд з цим, зазначену технологію активно рекламують та підтримують такі компанії як Google, Apple, Microsoft і Mozilla, що надає користувачеві

відчуття впевненості, що його інформація є захищеною та ніким не відслідковується. Однак, як свідчать дослідження Gizmodo, дана функція не працює взагалі [2].

Основна проблема полягає в тому, що у разі активації функції DNT, браузер лише сповіщає відповідний веб-сервіс про те, що користувач не хоче аби його інформація збиралася чи передавалася іншими сторонами, а відповідні дії про те, відслідковувати чи не відслідковувати користувача уже приймає сам веб-сервіс. І якщо певні веб-сайти дійсно дотримуються відповідних запитів користувача про надання конфідеційності, то ряд ресурсів, серед яких Google, Facebook і Twitter, цей запит ігнорують.

Отже, у чому полягає основна причина того, що інструмент який повинен забезпечувати конфідеційність інформації насправді не робить нічого? Перш за все, без юридичної підтримки та відповідних повноважень, реальне використання цього механізму ніколи не зможе бути інтегроване на належному рівні. Прибутки, які отримуванні інтернет компаніями на основі аналізу отриманих даних з метою виявлення потенційного клієнту завжди будуть на першому місці аніж особисте життя самого користувача. Відповідно, якщо веб-сервіс продовжує відслідковувати інформацію про користувача, хоча сам користувач такої згоди не давав, то власники цього сервісу повинні нести покарання.

Аналізуючи вищесказане, можемо зробити висновки щодо існуючого стану забезпечення конфідеційності інформації користувачів. Техологія DNT не просто не виконує свій основний функціонал, що ще гірше — вона вводить в оману користувачів, надаючи їм хибну надію про те, що їхні дані є захищеними та не попадуть в руки інших людей. По аналогії з практикою масового прийняття блокувальників реклами через велику кількість дратуючих вспливаючих вікон, звуків та інших схожих причин, веб індустрія повинна зреагувати на існуючу проблему конфідеційності користувачів і відстежувати їх переміщенння в Інтернеті лише за їх особистою згодою. За інакших умов, нас чекає схожа ситуація щодо самостійного забезпечення користувачами власної безпеки і блокування великої кількості вихідної інформації, що спричинить ще більшу втрату коштів для власників інтернет-компаній зі сторони маркетингових компаній.

Література

1. The weird and surprising things I found in the file Facebook has on me. [Электронный ресурс]. – Режим доступа: https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12003431.
2. Goodrich B. An Analysis of the ‘Do Not Track’ Header / B. Goodrich. // COMP 116: Introduction to Computer Security. – 2018.
3. 'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything [Електронний ресурс]. – Режим доступу: https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324

ВИНАГОРОДА ЗА ПОМИЛКУ – ГЕНІАЛЬНО ТА ПРОСТО

Ганна Мамонова, Владислав Полторак

ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», м. Київ, Україна

Even the most thought-out systems are subjected to attacks by hackers and other external vulnerabilities. Therefore, the issue of information security and round the clock protection deserves special attention if the company wants to be successful in the market. Fortunately, an effective and optimal solution to this issue for software owners already exists. It's called Bug Bounty.

Keywords: information security, bug bounty, software, bug hunters.

Всі ми з шкільних років пам'ятаємо не приємне завдання – знайти власну помилку чи то в диктанті, чи в розрахунках. Коли справа стосувалась математики багато хто починав роботи цей приклад як то кажуть «з нуля». Важко побачити помилку, особливо якщо вона саме ви її і зробили. А якщо це результат серйозної інтелектуальної праці багатьох людей. Як швидко знайти помилку?

Bug Bounty програми (з англ. "винагорода за помилку") – програми, які використовуються розробниками програмного забезпечення, за допомогою яких спеціалісти з кібербезпеки можуть отримати винагороду за знаходження помилок, пов'язаних з інформаційною безпекою програми. Дані програми дозволять розробникам швидко знайти причину помилки та усунути її, перш ніж широка публіка дізнається про неї. Bug bounty програми реалізовані у таких компаніях, як Mozilla, Facebook, Yahoo!, Google, Reddit, Square і Microsoft.

Перша Bug Bounty програма була запущена 10 жовтня 1995 року компанією Netscape. Вона пропонувала винагороду тим, хто знайде слабкості в їх основному продукті Netscape Navigator 2.0 Beta. Улітку 2004 року, через 9 років після Netscape, свою програму також запустила компанія Mozilla для свого веб-браузера Firefox. А в 2011 році компанія Facebook запустила програму "Whitehat", яка триває й нині. За час свого існування дана програма виплатила близько 2 млн. дол. винагород (в т. ч. 1,5 млн. лише за 2013 рік).

Чим же Bug Bounty програми такі привабливі для великих компаній? Велику роль тут відіграє економічний фактор. Сукупна вартість програми для організацій є значно дешевшою, ніж найм спеціальних фахівців для проведення повного аудиту інформаційної безпеки і тестів на проникнення. Крім того, така кампанія найчастіше виявляється більш ефективною. Численні Bug Hunters (так називають людей, що займаються пошуком вразливостей) за короткий термін перевірять сервіс практично на всі можливі вразливості.

Крім того, Bug Bounty програми можуть принести користь не лише приватним компаніям. Міністерство оборони США за допомогою програми пошуку вразливостей виявило понад сто потенційних небезпек в своїх електронних ресурсах. Це перша подібна ініціатива, проведена на рівні федеральних служб. У проекті Пентагону взяло участь понад 150 фахівців, а представники відомства, в тому числі міністр оборони США Ештон Картер, назвав програму відмінним способом підвищити рівень безпеки систем відомства при невисоких витратах.

Але разом з користю такі програми несуть і складності: звіти, які постійно надходять, потрібно оперативно розглядати і виправляти помилки, описані в них, а в разі більш-менш популярного ресурсу кількість репортів може досягати сотень в день, серед яких ще потрібно знайти ті, які описують реально існуючу проблему. Можна виділити наступні переваги та недоліки програми. Плюси програми: безперервність процесу тестування; вартість (виплати винагород будуть менше вартості найманих фахівців); широке покриття. Мінуси програми: велика кількість повторних репортів (повідомлень про одну й ту ж помилку); вузька спрямованість;складність ручної обробки репортів.

Для покращення роботи програм необхідно створити систему автоматичної обробки звітів, узаконити (легітимізувати) роботу Bug Hunters, уніфікувати шаблон для звітів. У майбутньому програми Bug Bounty будуть продовжувати розвиватися та поширюватися. Бюджети програм будуть лише зростати, адже найголовнішим показником якості сучасного програмного забезпечення є його інформаційна безпека.

Література

1. https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3
2. https://cybersecurityventures.com/bug-bounty-report-2017/
3. https://uk.wikipedia.org/wiki/Bug_Bounty
4. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/february/21feb18_fs

ЖИТТЄВА КОМПЕТЕНТНІСТЬ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Людмила Марцева

Житомирський державний технологічний університет, м. Житомир, Україна

Nowadays when the Ukrainian society is transforming and its values are changing the role of pedagogical science as a life creator is increasing in training of the information security specialists. Besides a professional training the attention should be paid to their moral psychological education and upbringing of the devotion to national values. The awareness of learning as a creative process helps to form the professional world outlook and motivation. The educational process has to be guided to the obtaining of life strategies and competency. This demands the using of competency building and practical based approaches.

Keywords: information security, pedagogical science as a life creator, professional training, competency building approach, practical based approach.

Проблеми підготовки фахівців для вирішення завдань інформаційної безпеки актуальні нині для всіх країн світу. Першочерговий інтерес викликає досвід підготовки фахівців у країнах ЄС, США, Китаї, Японії. Формування політики в галузі ризиків передбачає увагу до підготовки фахівців з інформаційної безпеки та їх діяльності для вирішення завдань особливо в кризових та конфліктних ситуаціях. Зазначені фахівці мають орієнтуватися в безпеці бізнес-діяльності, питанні забезпечення безперервності бізнесу, безпеці інформаційних технологій, фізичній безпеці, безпеці навколишнього середовища та інших аспектах безпеки.

Становлення незалежної України припало на новий етап розвитку людської цивілізації – формування інформаційного суспільства як нової суспільно-економічної формації. Фахівці з інформаційної безпеки нині надзвичайно затребувані на ринку праці. У сучасному інформаційному суспільстві доступ до інформації та вміння нею керувати є провідною рисою, а вміння науково обробити інформацію та захистити інформаційно-комунікаційний простір країни сприяє інформаційній та економічній інтеграції країни. Інтелектуальний ресурс нашої країни – це молоді люди, які є основним важелем прогресивних змін у країні, підвищенням авторитету та конкурентоспроможності держави на міжнародній арені. Їх освітня підготовка потребує пріоритетного розвитку ще й тому, що забезпечує незалежність та національну оборону країни.

Україна, як і провідні країни світу, здійснює базову підготовку фахівців з інформаційної безпеки з вищою освітою за трьома групами галузей знань: у галузі безпеки, у галузі інженерії, у галузі соціальних наук, бізнесу і права.

На наш погляд, окрім фахової підготовки студентів у вищому навчальному закладі заслуговує на увагу їх морально-психологічна підготовка, виховання відданості національним цінностям. В умовах трансформації українського суспільства, коли відбувається зміна цінностей, зростає роль педагогіки життєтворчості. Життєтворчість – це особлива форма виявлення творчої природи майбутніх фахівців у галузі безпеки. Усвідомлення навчання як творчого процесу допомагає у формуванні морально-світоглядного, цілісно-спрямованого та мотиваційного компонентів майбутнього фахівця. Навчально-виховний процес повинен бути спрямований на оволодіння життєвими стратегіями та компетентностями (побудовою індивідуального способу життя, уміння обирати оптимальний режим інтелектуальних, емоційних, та фізичних навантажень, посилення гнучкості та конкурентоспроможності). Це вимагає використання компетентнісного та практикоорієнтовоного підходу в підготовці студентів, покликаного подолати прірву між освітою та вимогами життя. Важливо нині, на наш погляд, дослідникам зазначеної проблеми зосередити увагу на:

- виявленні умов ефективного формування життєвої компетентності фахівців з інформаційної безпеки;

- розробці моделі розвитку життєвих компетентностей майбутнього фахівця з інформаційної безпеки;
- перебудові освітнього простору у вищому навчальному закладі на діагностичній основі та апробації інструментарію для оцінки рівня досягнень студента у формуванні життєвої компетентності (вміння визначати життєву стратегію, уміння володіти собою, уміння розвивати потребу в самовдосконаленні, формування соціально активного ставлення до життя, освоєння на сучасному рівні політичних, економічних та правових знань, здатність передбачати наслідки своїх вчинків і дій тощо).

Зрозуміло, що дослідження та реалізація зазначених питань залежить від інноваційної культури науково-педагогічних кадрів вищого навчального закладу, рівня їх компетентності, уміння реалізовувати перспективні ідеї в практичне життя. Побудова моделі педагогіки життєтворчості вимагає переосмислення принципів, які визначають змістовий вектор професійної підготовки студентів, технологію навчання та управлінські рішення в підготовці фахівців у галузі безпеки. Зазначенні принципи відображені в категоріях знання про сутність, зміст і закономірності фахової підготовки, спрямованої на розвиток і саморозвиток фахівця як суб'єкта творчої діяльності. Особистісно зорієнтована педагогіка, спрямована на формування життєвої компетентності майбутніх фахівців з інформаційної безпеки, передбачає індивідуально зорієнтовану допомогу, створення умов для реалізації інтелектуальних, емоційних здібностей і можливостей. Підготовка фахівця, який не лише засвоює інформацію, а й може особистісно зростати, освоювати прогресивні форми життєтворчості, формує конкурентоздатну особистість у суспільстві з ринковою економікою, яка вміє планувати стратегію власного життя, орієнтуватись у системі цінностей, визначати свій життєвий шлях.

Література

1. Азаров С.С. Особливості підготовки фахівців із інформаційної безпеки / С.С. Азаров, В.Г. Кривуца, О.В. Тітов, В.О. Хорошко / / Захист інформації. - 2006. - № 1. - С. 4-18.
2. Марцева Л.А. Оптимізація професійної підготовки майбутніх фахівців / Л.А. Марцева // Матеріали міжнародної науково-практичної конференції, 16-17 травня 2017 р. / За заг. ред. Романовського О.Г., - Х.: НТУ «ХПІ», 2017. С. 137-140.

ЕЛЕМЕНТ БЕЗПЕКИ NEAR FIELD COMMUNICATION

Олег Вацлавик, Богдан Маркевич

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The security element on the SIM card can be directly connected to the NFC interface, even when the voltage is fed by the phone rather than the NFC interface instead. This allows the security element to work together with the NFC interface in card emulation mode, even when the battery of the phone is practically discharged.

Keywords: security element, Near Field Communication, hardware module, operating system.

Деякі функції, які залежать NFC, наприклад, додатки для проведення платежу, або покупки електронних квитків вимагають, щоб дані які зберігаються в пам'яті були захищені, так як зловмисник потенційно може маніпулювати даними або читати їх з пам'яті. Дані, доступ до яких може отримати зловмисник, можуть бути дуже критичні - наприклад, відомості про банківську карту, отримавшидоступ до яких, зловмисник може створювати клони карт.

Тому ці критичні додатки повинні працювати в захищеному середовищі, бажано на окремому чіпі, а не в основному процесорі телефону. Елемент безпеки (ЕБ) являє собою комбінацію апаратних і програмних засобів, які забезпечують механізми захисту для підтримки безпечного середовища для зберігання і виконання.

ЕБ повинен мати операційну систему, в якій додатки встановлюються і використовуються (як правило, додатки встановлюються у вигляді JAVA-аплетів). Приклад таких ОС: MULTOS (Multi Application Card Operating System) або Java Card OS .

Існує кілька варіантів апаратних модулів, які можуть слугувати як елемент безпеки в смартфонах (Рис. 1).

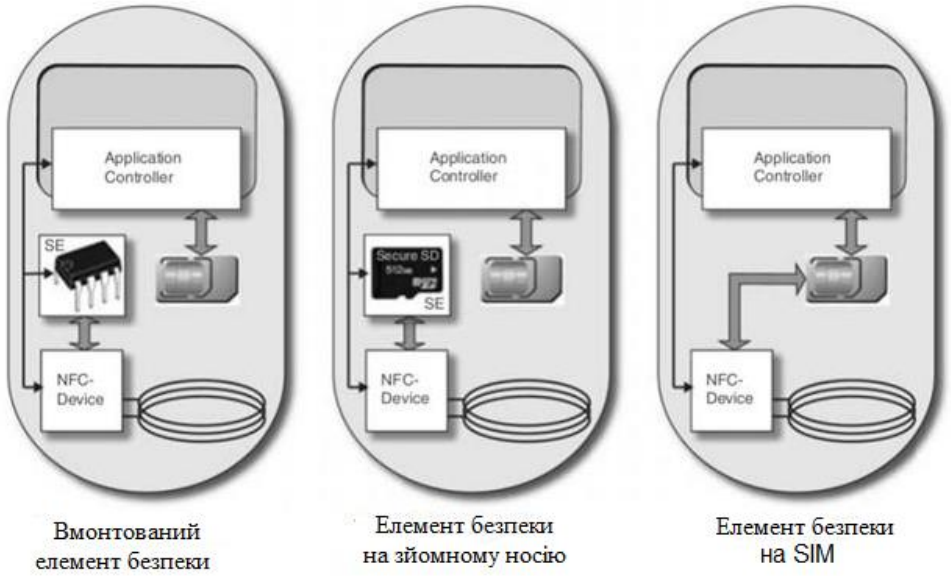


Рис. 1. Варіанти апаратних модулів, що використовуються в якості ЕБ

Вбудований апаратний ЕБ може бути безпосередньо вбудований в телефон. Тому він не може бути видалений або переведений в інший девайс. Це рішення має деякі недоліки: права доступу до вбудованого ЕБ повністю контролюються виробником телефону і якщо вони строгі, то ЕБ не може навіть дозволити встановити користувальницькі додатки.

UICC (Universal Integrated circuit card) ЕБ міститься на SIM / USIM-карті мобільного телефону і може обслуговувати кілька додатків, випущених різними постачальниками додатків.

Знімний носій (наприклад, SD-карта) складається з пам'яті, вбудованої смарт-елемента карти і смарт-карти контролера. Він забезпечує такий же високий рівень безпеки, як смарт-карта і сумісний з більшістю основних стандартів для смарт-карт. Його переваги в тому, що він легко змінюється в діапазоні від телефону до телефону - на відміну від UICC, який пов'язаний з певним номером мобільного телефону.

Елемент безпеки містить операційну систему, яка дозволяє запускати кілька додатків у віртуальній машині поверх рідної ОС смартфона. Типова ОС використовується в ЕБ – JavaCard OS. Вона має фреймворк під назвою Java Card Runtime Environment (JCRE), який підтримує програми, реалізовані в обмеженої версії мови Java (підмножина конструкцій оригінального мови Java і бібліотечних функцій). Використання віртуальної машини дозволяє відокремити критично важливі дані, від всіх інших. Однак і тут є свої підводні камені.

Операційна система елемента безпеки може запускати обмежена кількість додатків і тримати в пам'яті обмежена кількість даних. Залишається питання, що буде з важливими даними, що містяться в пам'яті елемента безпеки, якщо необхідно буде зберегти нові дані, але місця в пам'яті для збереження не буде. Крім того, не виключена помилка розробника, який може не вказати, що його програма має запускатися з використанням елементу безпеки. Сам же елемент безпеки, не може розпізнавати додатки, які передають дані що підлягають захисту.

Література

1. Minihold R. Near Field Communication (NFC) Technology and Measurements. White Paper. – http:// eetimes.com/electrical-engineers/education-training/ tech-papers/secure/rohde-and-schwarz/4213132?isSurveySuccess=True
2. Fisher J. NFC in cell phones: the new paradigm for an interactive world. – IEEE Communications Magazine, 2009, v.46, №6, p.22.
3. Smart Posters: how to use NFC tags and readers to create interactive experiences that benefit both consumers and businesses. – April 2011, www.nfcforum.org/resources/white_papers/NFC_Smart_ Posters_White_Paper.pdf
4. Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications. – http:// www.nfc-forum.org/resources/white_papers/nfc_ forum_marketing_white_paper.pdf

АВТОМАТИЗОВАНА СИСТЕМА ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ “БІОМЕТРИЧНІ ТЕХНОЛОГІЇ”

Валерій Дудикевич, Галина Микитин, Мар’ян Мельник

Національний університет Львівська політехніка, м. Львів, Україна

The stages of creation of the automated system of information processing with restricted access for the subject area – biometric technologies as a web-resource are considered.

Keywords: biometric systems, automated information processing system, restricted access, database, algorithmic software.

На сьогодні розвиток розумних об’єктів вимагає впровадження біометричних технологій безпеки, зокрема ідентифікації відбитків пальців, т. і. [1, 2]. У цьому сегменті актуальним є створення автоматизованої системи обробки інформації з обмеженим доступом (АСОІ з ОД), як web-ресурсу, та вибір користувачем відповідної статичної/ динамічної біометричної системи для впровадження у проектування розумних об’єктів. Розглянемо етапи створення АСОІ з ОД. *Якісний аналіз даних у предметній сфері – біометричні системи.* В результаті групування біометричних систем, як статичних та динамічних, в табл. 1 представлений сегмент характеристик однієї з динамічних систем – рукописного підпису.

Таблиця 1

Характеристики біометричної технології – рукописний підпис

2	A	B	C	D	E	F	G	H	I	J
динаміці	Метод отримання біометричних параметрів	Ймовірність відмов у доступі, %	Ймовірність помилкової ідентифікації (без муляжа), %	Ймовірність помилкової ідентифікації (з муляжем), %	Збереження таємниці образу у процесі ідентифікації, %	Реєструючий пристрій	Зразок	Досліджувані параметри	Фізичне явище в основі: алгоритму	Пристрій, фото, вартість, (у.о.)
21	Рукописний підпис	0,5-5	0,5-5	0,5-5	8-40	планшет для підпису, перо для введення даних	зображення підпису і значення відповідних динамічних вимірів	швидкість, порядок ліній, тиск і зовнішній вигляд підпису	Сканування процесу підпису за допомогою скла спеціального планшета	WACOM STU-520 SIGN&SAVE  50-100

Концептуальна модель предметної сфери – біометричні системи. На основі основних принципів системного аналізу створена комплексна модель, в якій об’єднуються зв’язками окремі частини предметної сфери, забезпечуючи цілісність системи: статичні і динамічні біометричні технології. В моделі точно виділені існуючі властивості і взаємозв’язки частин складного об’єкта, відображається його докладний опис, що забезпечує ієрархічність системи: різновиди статичних і динамічних систем за ознаками біометричної ідентифікації. В моделі забезпечується багатоаспектність завдяки розгляду об’єкта (статичних/ динамічних систем) з різних точок зору: характеристик, наприклад A – J (табл.1).

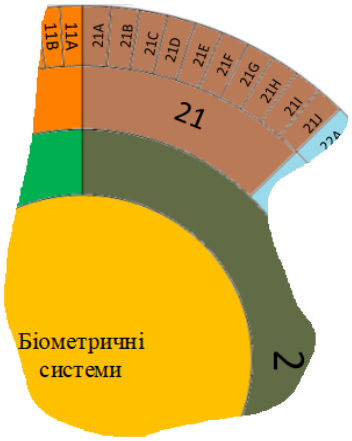


Рис. 1 Сегмент концептуальної моделі

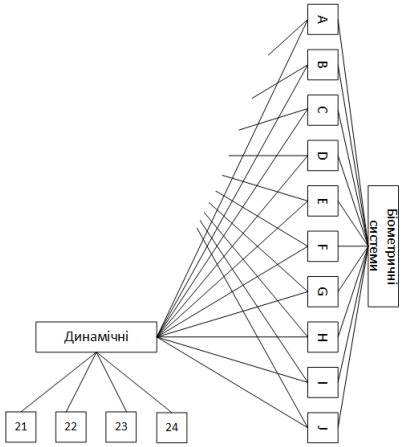


Рис. 2 Сегмент інформаційної моделі

Інформаційна модель предметної сфери – біометричні технології, зокрема у сегменті динамічних систем відображає наявні зв'язки між компонентами (рис.2): 21 – рукописний підпис; 22 – клавіатурний почерк; 23 - ЕКГ; 24 – характеристики і особливості голосу.

Обґрунтування вибору: реляційної бази даних (РБД), PHP. Критерії вибору РБД: представлення двовимірними таблицями найбільш наглядно розкриває обрану предметну сферу; PHP – мова програмування, яка в організаційно-технічному просторі сумісна з РБД та з системою управління базою даних MySQL . На рис. 3, 4 відповідно представлено структуру бази даних та алгоритм роботи АСОІ з ОД.

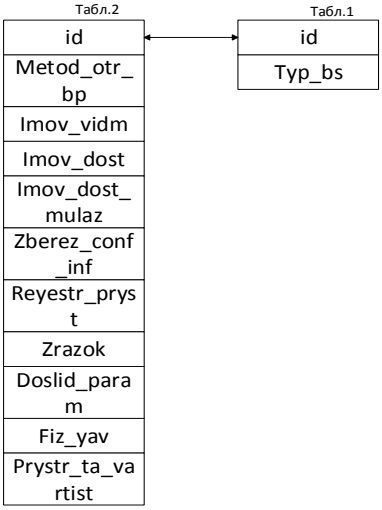


Рис. 3 Структура бази даних

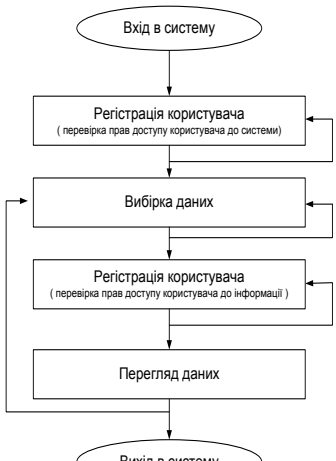


Рис. 4 Алгоритм роботи АСОІ з ОД

Програмне забезпечення АСОІ з ОД. Інтерфейс АСОІ з ОД реалізований мовою програмування PHP у вигляді web-сторінки. Загальне функціонування системи здійснюється на основі технології Apache-MySQL-PHP. В результаті розроблення АСОІ з ОД отримано web-ресурс у предметній сфері – біометричні системи для користувачів та проектантів безпечних розумних об'єктів: вікно входу в систему, вікно головної сторінки, вікно каталогу статичних/динамічних біометричних систем.

Література

1. Розумне місто – основа для зручного та безпечного життя. [Електронний ресурс]. – Режим доступу: https://biz.nv.ua/ukr/bisin3g/rozumnij-misto-osnova-dlja-zruchnogo-i-bezpechnogo-sposobu-zhittja-410924.html
2. Монастирський Л., Лозинський В., Бойко Я., Соколовський Б. Розпізнавання відбитків пальців у недорогій біометричній системі// Електроніка та інформаційні технології. – 2018. – Випуск 9. – С. 120–124

СИСТЕМИ ПРОТИПОЖЕЖНОГО ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ – НЕВІД'ЄМНА ЧАСТИНА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Євген Морщ[1], Сергій Ємельяненко[2]

[1] ДСНС, м. Київ, Україна
[2] Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Fire protection systems as a component of a comprehensive information security system, it should be noted that the choice of the necessary fire protection system depends not only on the quality of fire protection of the object of information activity and its cost, but also the quality of protection of information circulating there.

Keywords: fire protection, complex system, information protection, fire, information

Відповідно до [1] комплексна система захисту інформації (далі – КСЗІ) – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

У [2] пропонується враховувати вплив можливої пожежі, як один з видів змін умов фізичного середовища, під час створення моделі загроз і формування вимог до КСЗІ.

Дійсно, пожежа може бути загрозою цілісності інформації та мати різну суб'єктивну природу, як випадкову (ненавмисну) та і навмисну. Буде дуже прикро та економічно не обґрунтовано забезпечити надійний захист інформації на об'єкті інформаційної діяльності (далі – ОІД) за допомогою технічних засобів, при цьому не забезпечити пожежну безпеку об'єкту. Порушник не отримавши доступу до інформації буде мати змогу знищити її разом із засобами технічного захисту спричинивши пожежу. Саме тому організаційно-технічні заходи спрямовані на захист ОІД від пожежі повинні бути враховані під час їх проектування, будівництва, реконструкції, технічного переоснащення, капітального ремонту, експлуатації та бути невід'ємною частиною КСЗІ.

Комплекс технічних засобів, що змонтований на об'єкті, призначений для виявлення, локалізування та ліквідування пожеж без втручання людини, захисту людей, матеріальних цінностей та довкілля від впливу небезпечних чинників пожежі відповідно до [3] є системою протипожежного захисту (далі – СПЗ).

Враховуючи особливості ОІД, їх категоріювання в залежності від виду інформації, що на них циркулює, проектування СПЗ на цих об'єктах може здійснюватися за спеціальними нормами (галузевими нормами, або індивідуальними технічними умовами), але у загальному випадку проектування, монтування, перевірка відповідності і підтримання експлуатаційної придатності СПЗ здійснюється відповідно до будівельних норм ДБН В.2.5-56:2014 Системи протипожежного захисту (Fire protection systems).

Склад систем протипожежного захисту відповідно до [3] наведено на рис. 1.

Як бачимо, існує багато типів СПЗ, тому якщо розглядати їх як складову КСЗІ, слід зазначити, що від вибору необхідної СПЗ залежить не тільки якість протипожежного захисту ОІД та його собівартість, а й якість захисту інформації, що на ньому циркулює.

Як висновок, слід наголосити на необхідності вивчення вимог пожежної безпеки майбутніми фахівцями у сфері технічного захисту інформації з метою якісного застосування набутих знань у практичній діяльності.

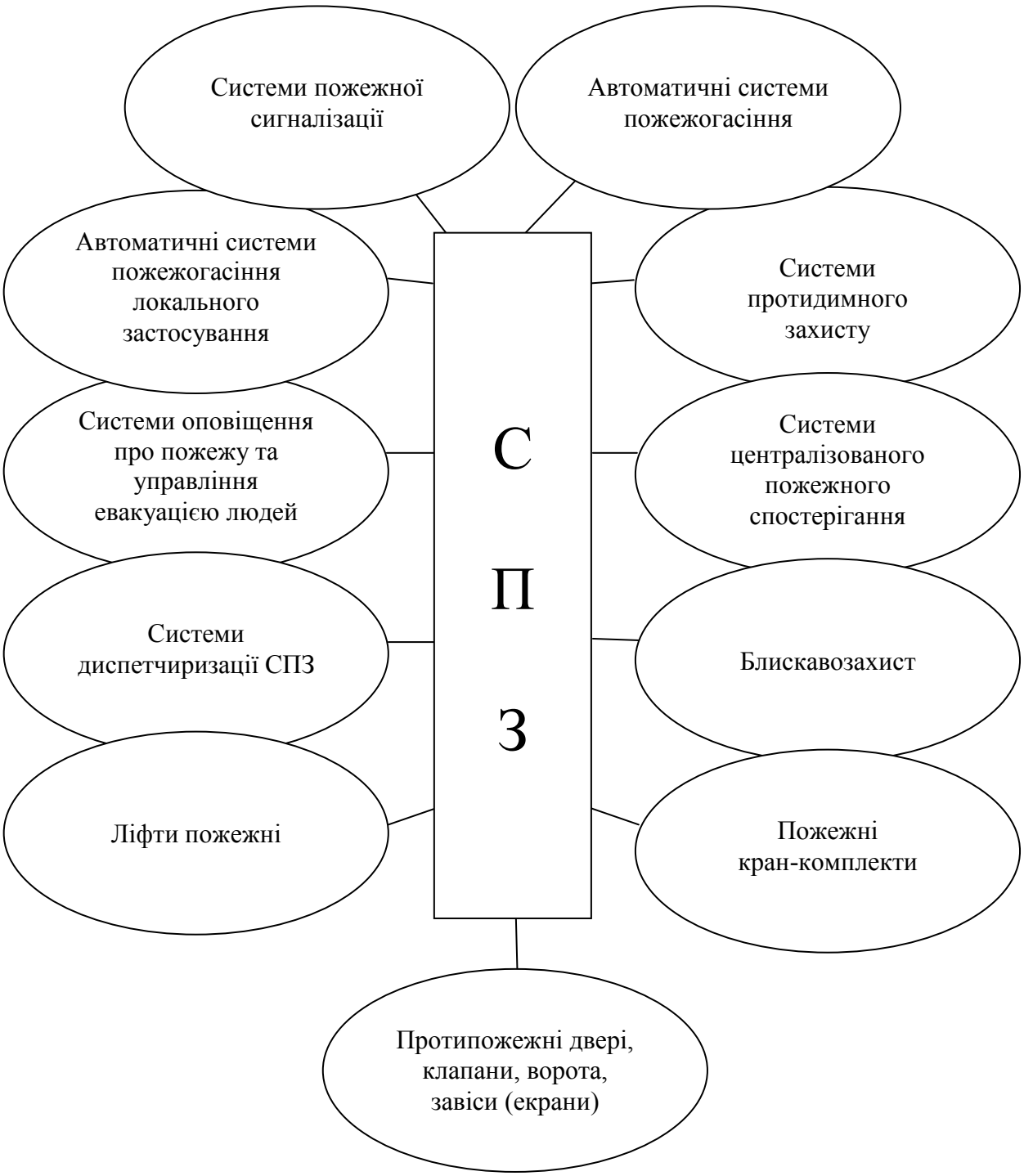


Рис. 1. Склад систем протипожежного захисту

Література

1. Закон України «Про захист інформації в інформаційно-телекомуніаційних системах».
2. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 № 53, із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.
3. ДБН В.2.5-56:2014 Системи протипожежного захисту, затверджені наказом Мінрегіону України від 13.11.2014 № 312.

СТАН УКРАЇНСЬКОГО ЗАКОНОДАВСТВА В ЧАСТИНІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анастасія Петренко, Анна Кириленко

Державний вищий навчальний заклад "Київський національний економічний університет імені Вадима Гетьмана", м. Київ, Україна

Information security is an integral part of each of the national security spheres, therefore, effective legislation is a top priority for the country to protect all existing structures. Gaps in legislation can create significant threats and therefore exists a requirement for continuous review and improvement.

Keywords: information security, cybersecurity strategy, personal data, legislation.

Сьогодні спостерігається різке зростання інцидентів в області інформаційної безпеки, які мають широке поширення і набувають загрозливого характеру. Багато з подібних атак зачіпають коло приватних, корпоративних, а також державних інтересів. Водночас дії спеціалістів з питань забезпечення кібербезпеки мають відповідати чинному законодавству. Інформаційні технології настільки швидко розвиваються, що найчастіше законодавча база висвітлює застарілі аспекти або взагалі не створена.

Українське законодавство вже має низку нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави та шлях подолання цих проблем. [1, 2]

Одним із найважливіших кроків на шляху розбудови системи кібербезпеки України є "Стратегія Кібербезпеки України" (далі Стратегія), затверджена 15 березня 2016 року указом Президента України. Новий закон в першу чергу спрямований на формування загальної державної політики у галузі кібербезпеки, а також розподіл ролей між різними державними інституціями. Зокрема, він регулює повноваження спецслужб для здійснення кіберзахисту країни. [1]

На даний момент триває активна реалізація низки спільних проектів між Україною та іншими державами щодо кібербезпеки. Серед них – допомога американського уряду з підготовки українських фахівців з кіберзахисту, консультації з іноземними радниками, постачання технічного обладнання для Центру оперативного реагування на кіберзагрози тощо. [3]

Верховною Радою України ухвалено "Закон про захист персональних даних", введений в дію з 1 січня 2014 року. Цей закон накладає на Україну ряд зобов'язань. А саме: забезпечити дотримання прав і свобод людини, зокрема права на недоторканність приватного життя. Відповідно до закону будь-які відомості, які дають змогу ідентифікувати конкретну фізичну особу, можна віднести до персональних даних. Така інформація є конфіденційною і може оброблятися тільки за згодою цієї фізичної особи. [2] Серед головних нововведень — повноваження з контролю за додержанням цього закону покладено на омбудсмена країни.

Так, наприклад, Telegram оновив свої правила конфіденційності. Щоб відповідати закону про захист персональних даних та запитам державних органів, месенджер видаватиме IP-адреси і номери телефонів людей, яких підозрюють в терористичній діяльності лише за рішенням суду. [4]

Кіберпростір є важливим аспектом в житті будь-якої людини та суспільства. Але гострим постає питання забезпечення інформаційної безпеки на всіх рівнях від звичайного користувача до держави. За останній час Україна зробила прогресивні кроки у створенні ефективної національної системи кібербезпеки. Проте законодавча база поки що лише частково охоплює елементи, які потрібні для ефективної та швидкої протидії кіберзагрозам. Вже ні в кого не викликає сумнів, що законодавство країни у галузі інформаційної безпеки має відповідати міжнародним стандартам і цей процес має

відбуватися динамічно. Варто додати, що чітке виконання прийнятих законів додасть Україні міжнародного іміджу.

Література

1. Указ Президента України «Стратегія кібербезпеки України» від 15 березня 2016 року № 96/2016 – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016
2. Закон України «Про захист персональних даних» від 1 червня 2010 року №2297-VI – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2297-17
3. Кібербезпека: виклики та завдання. Тетяна Попова – [Електронний ресурс]. – Режим доступу: https://blogs.pravda.com.ua/authors/popova/5aa639aaa527c/
4. Захист персональних даних. Тарас Шарий – [Електронний ресурс]. – Режим доступу: http://www.visnuk.com.ua/uk/publication/100005066-zakhist-personalnikh-danikh-2

АНАЛІЗ КЛЮЧОВИХ ПРИНЦИПІВ ПОЛОЖЕННЯ ПРО ЗАХИСТ ФІЗИЧНИХ ОСІБ У ЗВ'ЯЗКУ З ОПРАЦЮВАННЯМ ПЕРСОНАЛЬНИХ ДАНИХ І ПРО ВІЛЬНИЙ РУХ ТАКИХ ДАНИХ

Сергій Гнатюк, Вікторія Сидоренко, Юлія Поліщук

Національний авіаційний університет, м. Київ, Україна

The rapid development of methods and tools for conducting a cyberattacks, caused the great amount of incidents which are aimed at stealing, modification and compromise personal data. According to that problem, the Regulation was developed, which set out requirements for processing that data. In the paper General Data Protection Regulation (GDPR) was researched and analyzed it applicability to the Ukrainian business.

Keywords: cybersecurity, personal data, information security, GDPR.

У сучасному інформатизованому світі інформація про особу та її персональні дані є критично важливим об'єктом, який, безумовно, потребує захисту. Розуміючи важливість цього питання, Європейський Парламент і Рада розробили Положення про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (далі – Положення), що застосовується для компаній, які територіально знаходяться в Європейському Союзі (далі – ЄС), проте, не обмежується лише ними: сфера дії закону поширюється, частково, і на українські компанії. З огляду на це, метою дослідження є аналіз Положення та дослідження його застосовності для українського ринку.

Положення вступило в дію 25 травня 2018 року. і застосовується як до країн-членів ЄС, так і до компаній, які знаходяться поза межами ЄС у випадку обробки інформації, яка належить або ідентифікує громадянин ЄС. У Положенні немає загальних вимог, що є вагомим недоліком, оскільки компаніям доводиться самостійно визначати актуальний рівень відповідності Положенню та робити висновки про найкращий спосіб досягнення відповідності. Положення, в першу чергу, зосереджується на даних фізичних осіб, які визначаються у двох категоріях «персональні дані» та «спеціальні персональні дані»: «**персональні дані**» – будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома чиниками, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи (Стаття 4 (1) [1]); «**спеціальні персональні дані**» – особисті дані, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання; членство в профспілці; генетичні дані, біометричні дані, оброблені виключно для ідентифікації людини; дані про здоров'я; дані про статеве життя людини або сексуальну орієнтацію (Стаття 4 (13), (14) та (15), Стаття 9 та твердження (51)-(56) Положення [1]).

Є деякі дані, які, відповідно до Положення, не вважаються персональними даними [2]: реєстраційний номер компанії; електронна адреса; анонімізовані дані.

Основною частиною Положення є опис процедури опрацювання даних. Відповідно до Статті 4 (2), «опрацювання» означає будь-яку операцію або низку операцій з персональними даними або наборами персональних даних з використанням автоматизованих засобів або без них, такі як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення. Приклади опрацювання даних: управління персоналом та адміністрування заробітної плати; доступ до / консультування бази даних контактів; що містять особисті дані; надсилання рекламних листів; знищення документів, що містять особисті дані; розміщення /поширення фотографій людини на веб-сайті; зберігання IP-адрес або MAC-адрес; відео-зйомка (CCTV).

Проте, Положення не застосовується в повній мірі а) «... якщо обробка персональних даних не є основною частиною бізнесу і діяльність не створює ризиків для фізичних осіб (наприклад, призначення посадових осіб із захисту даних не є обов'язковим (далі - DPO)); б) «... якщо компанія, що є постачальником послуг, розташована за межами ЄС. За умови, що компанія спеціально не орієнтує свої послуги на фізичних осіб в ЄС, вона частково не підпадає під вимоги Положення». В іншому випадку, діяльність, яка створює високі ризики для прав і свобод фізичних осіб, незалежно від розміру компанії веде до повного виконання вимог Положення.

Компанії, які зосереджують свою діяльність на: розробці програм; хмарних рішень, які працюють з європейськими персональними даними; аутсорсингові IT-компанії; інтернет-магазини; соціальні мережі; банки; медичні компанії; організатори громадських заходів, але знаходяться за межами ЕС мають в обов'язковому порядку відповідати вимогам Положення. На рис. 1. представлена схема для діагностики необхідності компанії відповідати вимогам Положення.

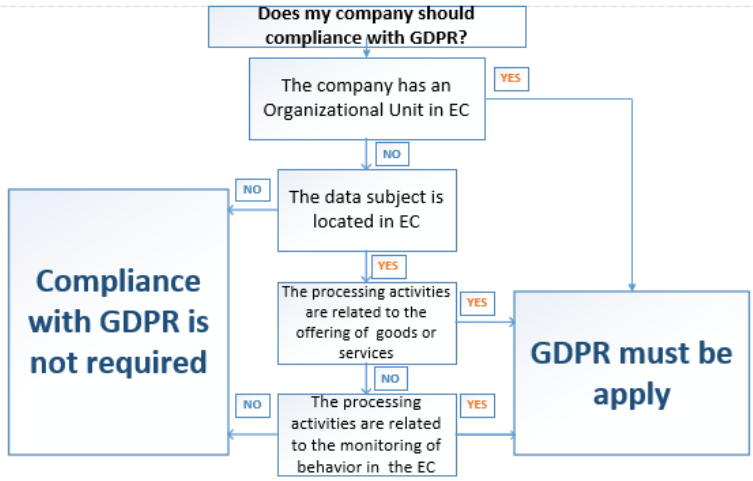


Рис. 1. Процедура діагностики необхідності компанії відповідати вимогам Положення

У випадку, якщо компанія повинна відповідати вимогам Положення, але не виконує ці вимоги, для цієї компанії застосовуються такі санкції: перший етап – формальне письмове попередження: може бути видане для компанії навіть у випадку неминучих порушень; незнання закону не є дійсним виправданням для його порушення; другий етап – вимагання від компанії, які порушують Положення, регулярно проводити періодичні перевірки цілісності даних, щоб забезпечити відповідність, що також означає передачу аудиторії доступу до потенційно чутливої та конфіденційної інформації; третій етап – для компаній, які порушили будь-яку частину законодавчого пакету після початкових санкцій, можуть бути оштрафовані на суму до 20 мільйонів євро або 4 % прибутку компанії за рік, залежно від того, що більше. З точки зору захисту персональних даних та вимог, які регламентуються Положенням, цей документ є досить вагомим, оскільки змушує компанії, які знаходяться в ЄС (і не тільки) покращувати свої системи обробки інформації та забезпечувати більш високий рівень інформаційної безпеки. Проте, на сьогодні Положення потребує доопрацювання, оскільки в документі описані лише загальні вимоги, які, наприклад, не дають змоги штрафувати компанії або зрозуміти, хто саме поза межами ЄС має проводити перевірки на відповідність Положенню.

У роботі проаналізовано Положення, досліджено, які основні моменти можуть бути застосовані для українського бізнесового сегменту, які санкції слідують за не виконання вимог Положення.

Література

1. EU General Data Protection Regulation (EU-GDPR), 2018. URL: http://www.privacy-regulation.eu/en/index.htm.
2. Rules for business and organisations, 2018. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БЕЗПРОВІДНИХ МЕРЕЖ СТАНДАРТУ 802.11

Орест Полотай

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Protective protocols of WEP and WAP wireless networks are considered and the peculiarities of their operation and data encryption are described.

Keywords: information security, protection protocols, encryption.

Всі сучасні бездротові пристрої (точки доступу, бездротові адаптери і маршрутизатори) підтримують протокол безпеки WEP (Wired Equivalent Privacy), який був спочатку закладений в специфікацію бездротових мереж IEEE 802.11. Даний протокол є свого роду аналогом провідної безпеки, проте реально ніякого, еквівалентного провідним мережам рівня безпеки, він, звичайно ж, не забезпечує.

Протокол WEP дозволяє шифрувати потік переданих даних на основі алгоритму RC4 з ключем розміром 64 або 128 біт – ці ключі мають так звану статичну складову довжиною від 40 до 104 біт і додаткову динамічну складову розміром 24 біта, звану вектором ініціалізації (Initialization Vector, IV).

Процедура WEP-шифрування виглядає наступним чином. Спочатку передані в пакеті дані перевіряються на цілісність (алгоритм CRC-32), після чого контрольна сума (integrity check value, ICV) додається в службове поле заголовка пакету. Далі генерується 24-бітний вектор ініціалізації (IV), а до нього додається статичний (40 або 104-бітний) секретний ключ. Отриманий таким чином 64 або 128-бітний ключ і є вихідним ключем для генерації псевдовипадкового числа, яке використовується для шифрування даних. Далі дані змішуються (шифруються) за допомогою логічної операції XOR з псевдовипадковою ключовою послідовністю, а вектор ініціалізації додається в службове поле кадру.

Протокол WEP є далеко не найкращим способом захисту бездротової мережі. Після публічної демонстрації численних вразливостей WEP, IEEE приступив до розробки стандарту 802.11i, покликаного усунути ці недоліки.

Однак процес його створення затягнувся, в зв'язку з чим один з наброс-ков (Draft 3) став використовуватися в якості проміжного рішення. Цей стандарт отримав назву Wi-Fi Protected Access (WPA). В WPA для аутен-тіфікаціі станції і мережі може використовуватися інфраструктура 802.1 X або загальний ключ [2].

На відміну від WEP ключі шифрування генеруються при встановленні з'єднання, а не розподіляються статично. Після успішної аутентифікації сервер RADIUS передає станції значення, яке використовується для ідентифікації даної сесії - кельмою (МК). Станція і сервер RADUIS на основі МК виводять Pairwise Master Key (PMK), який передається точки доступу сервером RADIUS. Для генерації PMK використовується псевдовипадкова функція (PRF), заснована на хеш-функції HMAC-SHA-1. Отримане значення ключа прив'язується до поточної сесії між точкою доступу і станцією.

Ключ PMK потім використовується точкою доступу і клієнтом для генерації ключа Pairwise Transient Key (PTK). Ключ PTK, довжина якого складає 512 біт, в подальшому розділяється на 4 ключа: Key Confirmation Key (KCK), Key Encryption Key (KEK) і два ключа шифрування Temporal Key 1 і 2 (TK1 / TK2).

Ключ KCK застосовується в процесі виведення ключів шифрування для аутентифікації клієнта. Значення KEK, використовується для захисту ключів шифрування широкомовного і групового трафіку Group Transient Key (GTK). Ключ GTK повинен бути однаковий для всіх станцій однієї мережі (BSS), тому він генерується точкою доступу і передається всім станціям. Ключі TK1 / TK2 застосовуються для захисту трафіку. Конкретні деталі їх застосування залежать від використовуваного криптоалгоритму [3].

Процес генерації ключа PMK заснований на обміні чотирма керуючими повідомленнями (4-way handshake, см IEEE802.11i):

- точка доступу відсилає станції випадкове число ANonce;
- станція генерує випадкове число SNonce і використовує функцію PRF-512 для виведення PTK на підставі PMK, ANonce, SNonce і MAC-адрес пристроїв. Значення SNonce відсилається на точку доступу, причому це повідомлення захищається за допомогою функції контролю цілісності, що розраховується на основі ключа KCK;
- точка доступу отримує SNonce, виводить значення PTK і перевіряється цілісність повідомлення за допомогою отриманого значення KCK. Якщо дані коректні, станції відсилається інформація про підтримувані режимі безпеки і ключ GTK;
- станція перевіряє параметри безпеки на збіг із значеннями, отриманими під час сканування (в Beacon або Probe Response), і цілісність отриманого повідомлення. Якщо відхилень не виявлено – точці доступу відсилається підтверджуючий пакет.

В якості алгоритму шифрування в WPA використовується Temporary Key Integrity Protocol (TKIP), заснований на RC4, що дозволяє реалізувати сумісність з устаткуванням, що підтримує WEP. При використанні TKIP довжина вектора (TKIP Sequence Counter, TSK) ініціалізації збільшена до 48 байт, що знижує ймовірність його повторення.

Ключ шифрування перемішується з MAC-адресою і TSK, і отримане значення використовується в якості ключа RC4. Таким чином, при застосуванні TKIP для кожного пакета використовується свій унікальний ключ WEP.

Таким чином, WPA вирішує такі проблеми WEP [1]:

- статичний ключ шифрування;
- відсутність контролю цілісності повідомлень;
- недостатня довжина вектора ініціалізації.

Використання RC4 в якості основного алгоритму шифрування вже не задовольняє сучасним вимогам безпеки. У зв'язку з цим в стандарті 802.11i описується обов'язкове використання протоколу Counter Mode with CBC-MAC Protocol (Ccmp) для шифрування трафіку. У цьому протоколі, описаному в RFC 2610, використовується в якості криптографічного примітиву алгоритм AES-128, який є в даний час державним стандартом Сполучених Штатів Америки.

У таблиці 1 наведено відповідність між різними назвами протоколів захисту бездротових мереж і криптоалгоритмами, які ними використовуються.

Таблиця 1

Стандарти захисту безпровідних мереж

Назва	Стандарт	Функції безпеки	Інші назви
WPA	802.11i Draft 3	TKIP, RC4	Transition Security Network (TSN)
WPA2	802.11i	TKIP, RC4 CCMPЯК1P, AES/RC4	Robust Secure Network (RSN)

Як видно з таблиці, підтримка WPA2 або 802.11i означає, що для шифрування може використовуватися TKIP. В налаштуваннях підключення до бездротової мережі можна вибрати як WPA-TKIP, так і WPA2-TKIP.

Однак пристрої, які не підтримують WPA2 (наприклад, КПК на базі Windows Mobile), не можуть працювати з мережею, налаштовану на використання WPA2-TKIP, в зв'язку з деякими відмінностями в процесі встановлення з'єднання.

Література

1. Гейер Дж. Беспроводные сети. Первый шаг: Пер. с англ. – М.: [Электронный ресурс] Издательский дом "Вильямс", 2005. – 192 с.: ил.
2. Мерритт М. Безопасность беспроводных сетей [Текст] / М. Мерритт. –М.: Книга по Требованию, 2015. – 282 с.
3. Радке Хорст-Дитер Все о беспроводных сетях / Хорст-Дитер Рад-ке , Йеремиас Радке. – М.[Электронный ресурс]: НТ Пресс, 2011. – 320 с.

МЕТОД ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ НА ОСНОВІ НЕЙРОМЕРЕЖ

Андрій Приймак, Юрій Яремчук

Вінницький національний технічний університет, м. Вінниця, Україна

An experimental study was made of the possibility of using a two-level neural network with a built-in sigmoid activation function to improve the accuracy of user identification by keyboard handwriting and proposed a method based on this mathematical apparatus. A comparison of the proposed identification method with existing ones showed an increase in the accuracy of user identification by 1-15%.

Keywords: information security, user authentication, neural network, keyboard handwriting, time functions.

З розвитком новітніх технологій проблема інформаційної безпеки набуває все більшої актуальності. Зважаючи на розвиток шпигунських технологій і цифрової техніки, котрі дозволяють все більш ефективно проводити атаки на комп'ютерні системи, зокрема корпоративні мережі, досягти конфіденційності можна тільки шляхом створення комплексного захисту інформації. І одним із основних елементів такої системи захисту є підсистема, що забезпечує ідентифікацію користувача комп'ютера.

Традиційні методи ідентифікації та автентифікації, що базуються на використанні карток, електронних ключів чи інших переносних ідентифікаторів, а також паролів і кодів доступу, мають суттєві недоліки. Головним недоліком таких методів є неоднозначність ідентифікованої особистості [1]. Для ідентифікації використовують атрибутивні розпізнавальні характеристики. Цей недолік можна усунути, використовуючи біометричні методи ідентифікації, наприклад, динаміку натискання клавіш користувачем. Біометричні характеристики є невід'ємною частиною людини і тому їх не можна забути, загубити чи передати іншому. Ще одним не менш важливим недоліком традиційних методів ідентифікації є складність виявлення підміни ідентифікованого користувача [2].

На сьогодні існує багато методів ідентифікації користувача за клавіатурним почерком, проаналізувавши найвідоміші з них, видно, що точність ідентифікації знаходиться в межах від 78% до 93,59% [3].

Порівняльна характеристика існуючих методів

Назва методу	Точність, %
Метод Леггета, Умпресса і Вільямса	89,5
Метод Джойса й Гопала	78
Метод Расторгуєва	90
Метод Сакета Махешварі та Вікрама Пуді	85,22–93,59
Метод Нура Ханура	90–92

Запропонований метод включає у себе дев'ять основних етапів збору інформації за допомогою часових функцій та подальшої її обробки на основі навченої нейромережі для ідентифікації користувача за клавіатурним почерком. Основні етапи такі [4]:

— збір усіх необхідних даних;
— підготовка та нормалізація даних;
— робота функцій синхронізації;
— основний аналіз компонентів;
— автоматичний підбір параметрів навчання;
— навчання мережі;
— перевірка правильності навчання;
— коригування параметрів;
—готовність до подальшого використання.

Для збору інформації для порівняння та ідентифікації користувача нейромережею пропонується використовувати п’ять часових функцій (час затримки, затримка «вгору-вниз», затримка «вниз-вниз», затримка «вгору-вгору», загальний час). В свою чергу нейронна мережа являє собою двошарову систему прямого доступу до мережі з 70-ма сигмовидними прихованими нейронами та 10-ма сигмовидними вихідними нейронами.

Запропонований метод складається з таких двох основних етапів:

1. Для проходження реєстрації користувач вводить ключові фрази 2 рази. Під час введення ключових фраз функції синхронізації аналізують текст, який вводить користувач. Отримані дані додаються до векторних функцій, а потім одразу зберігаються у вигляді шаблонів до бази даних, для того щоб перевіряти їх під час входу до системи. Функції синхронізації будуть перевіряти правильність вводу та порівнювати їх з шаблонами зареєстрованих користувачів. Після цього доступ користувачу дозволяється або забороняється.

2. Після того як зареєстрований користувач захоче отримати доступ до системи, йому необхідно буде ввести 2 рази ключовий текст. Під час введення тексту, функції синхронізації будуть перевіряти правильність введення та порівнювати їх із шаблонами зареєстрованих користувачів. Після цього доступ користувачу дозволяється або забороняється.

Основний аналіз головних компонентів виконується за функціями синхронізації для того, щоб зменшити їх, перш ніж вони будуть служити вхідними даними для нейронної мережі. Після того, як користувач створений, він повинен провести навчання нейронної мережі, яка також зберігається у базі даних. Після цих кроків навчена нейронна мережа та шаблони функцій готові до ідентифікації користувача.

Провівши експериментальні тести за участю восьми програмістів було отримано результат точності, що в середньому становить 93 %. Час навчання нейронної мережі склав 6 хвилин, що є швидшим за існуючі методи ідентифікації користувача за клавіатурним почерком з використанням багаторівневих нейромереж.

Порівнюючи існуючі та запропонований метод ідентифікації користувача за клавіатурним почерком на основі дворівневої нейронної мережі із вбудованою сигмоїдною активаційною функцією, було зроблено висновок, що точність ідентифікації зросла на 1–15 %, відносно показників існуючих методів. Метод Сакета Махешварі та Вікрама Пуді [5] має схожі показники точності, але між запропонованим та існуючим методом є декілька суттєвих відмінностей: у своїй роботі Сакет Махешварі та Вікрам Пуді використовували п’ятирівневу нейронну мережу; на навчання їх нейромережі було необхідно 9 хвилин. У запропонованого методу час навчання нейронної мережі складає 6 хвилин, що є швидшим на 3 хвилини і, як результат, є значно ефективнішим при використанні, оскільки час ідентифікації користувача зменшується, а висока точність ідентифікації зберігається.

Література

1. Gavan Leonard Tredoux, Steven J. Harrington. Method and system for providing authentication through aggregate analysis of behavioral and time patterns. Xerox Corporation, Norwalk, CT, 2016.
2. Harun N., Woo W.L. and Dlay S.S. Performance of Keystroke Biometrics Authentication System Using Artificial Neural Network (ANN) and Distance Classifier Method. International Conference on Computer and Communication Engineering (ICCCE 2010). 11–13 May 2010, Kuala Lumpur, Malaysia, 2010.
3. Armin Ebrahimi, Jeff Weitzman. User Identification Management System and Method. ShoCard, Inc., Palo Alto, CA — 15/878,353. 2018.
4. Данилюк І.І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж / І.І. Данилюк, В.В. Карпінець, А.В. Приймак, Ю.Є. Яремчук, О.І. Костюченко // Реєстрація, зберігання і обробка даних. – Т. 20, №2, 2018. – С. 68–76
5. Saket Maheshwary, Soumyajit Ganguly, Vikram Pudi. Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics. Conference: 2017 International Joint Conference on Artificial Intelligence (IJCAI), At Melbourne, Australia, 2017.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Дар'я Рожко, Орест Полотай

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The essence of technical protection of information with the use of organizational and technical methods of protection is described. The main methods and measures for ensuring technical protection of information are given. Described organizational level tasks, which are solved to provide information security in an automated system.

Keywords: information security, unauthorized access, organizational protection, technical protection.

Те, що інформація має цінність, люди усвідомили дуже давно. Її створюють, зберігають, транспортують, продають і купують, а значить – крадуть і підробляють - і, отже, її необхідно захищати. Одним словом, виникнення індустрії обробки інформації призвело до виникнення розробки засобів захисту інформації.

Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованих систем та осіб, які користуються інформацією.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених в автоматизованих системах правил розмежування доступу.

Залежно від можливих загроз несанкціонованого доступу до інформації методи захисту можна розділити на такі групи: технічні (апаратні), організаційні, програмні.

Технічний захист інформації – це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист інформації в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації.

У звичному розумінні ця діяльність спрямована на запобігання витоку інформації технічними каналами, її блокуванню та порушенню цілісності.

Основні методи і заходи забезпечення технічного захисту інформації:

- використання захищеного обладнання;
- регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації;
- інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;
- пошук, виявлення і блокування закладних пристроїв.

У технічному захисті інформації важливою є атестація об'єкта захисту – офіційне підтвердження органом сертифікації або іншим спеціально уповноваженим органом наявності на об'єкті захисту необхідних й достатніх умов, які забезпечують виконання встановлених вимог та норм ефективності захисту інформації.

Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж таки відбулося, доступу до інформації, у тому числі за допомогою її маскування. Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація, другу - генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, що «перекривають» потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Прикладом є екрановані приміщення. Екранування направлене на зниження потужності небажаних випромінювань, які можуть утворити електромагнітний канал витоку інформації. У

цілому, екранування приміщень потрібне з метою: віддзеркалення, локалізації, поглинання та зміни структури електромагнітного поля.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в автоматизованій системі:

- організація робіт з розробки системи захисту інформації;
- виховання й навчання обслуговуючого персоналу й користувачів;
- обмеження доступу на об'єкт і до ресурсів системи;
- планування заходів;
- сертифікація засобів захисту інформації;
- атестація об'єктів захисту;
- контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему. Вони повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися система; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Отже, потрібно чітко розуміти, що будь-які засоби захисту інформації не гарантують абсолютну безпеку і надійність даних, проте вони суттєво мінімізують ризик втрат. При проведенні аналізу та об’єктивної оцінки фахівець з інформаційної безпеки повинен підібрати найефективніші методи та засоби захисту інформації від несанкціонованого доступу, тобто визначити межі розумної безпеки і витрат з одного боку і підтримки системи в працездатному стані з іншого.

Література

1. Закон України «Про захист інформації в автоматизованих системах» від 05.07.94.
2. Положення про технічний захист інформації в Україні від 11.04.2008.
3. НД ТЗІ 2.5–004–99 критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

COMMON VULNERABILITIES IN MODERN HOSTING

Oleksii Maksymiv, Yuriy Rudyk, Andrii Rudyk

Lviv State University of Life Safety, Lviv, Ukraine

The levels of cloud computing and cyber security are considered. Approaches to information security of cloud hosting are given. 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. Therefore, the issue of improving the safety of cloud services and hosting requires a variety of attention.

Keywords: hosting, cyber security, vulnerability, cloud computing, safety, quality.

Every day the influence of the internet spreads to more and more aspects of our everyday lives. This encourages modern business entrepreneurs try to establish a web presence in order to reap the benefits of the exposure it offers. Since hosting a website or an online application on a local device takes a lot of effort, knowledge and resource dedication, people will look for specialized service providers that help ease the process [1].

Thus, there is a need for reliable and high-quality data exchange and application of methods and tools of software. This will increase the effectiveness of the fire and rescue units, the quality of interaction, the exchange of data and the evaluation of results. The economic effect is justified by reducing the response time and eliminating the consequences of emergencies, reducing the dependence on the hardware aging of the equipment, the flexibility of the application of web-based software and platform independence [2].

Research methods. In the work the complex method of research is used, which includes: analysis and generalization of scientific achievements in the field of information technologies, application of statistics of hosting.

Aside from attracting the website's target audience, a publicly available resource will also attract potential threats. With the intent of stealing or corrupting your data, hackers will attempt using the vulnerabilities of your hosting environment to gain access to the data they seek. Today's hosting providers are well aware of the danger their servers are in, and so they take precautionary measures to keep the data they host safe using several security services as well as software. Unfortunately, security breaches still take place on a daily basis due to exploits of both software vulnerability as well as the ever-present human factor.

SQL injections are a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to manipulate the data stored in the back-end database any way they please. SQL injection is one of the most prevalent types of web application security vulnerabilities [3].

A security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the server configuration. A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. Security misconfigurations gives hackers access to private data or features and can result in a complete system compromise. With resources being stretched thin on a hosting server, some Hosting providers will often cut corners in their configurations, so that fewer resources are consumed when security services are performing their scheduled checks/tasks. This definitely puts website owners in a tough spot, often choosing between the price of a well-protected server or a cheaper, less secure alternative.

With security software hounding potential malicious code, they will often interfere with the work done by the actual owner. These are so called "false-positive" triggers that will stop updates from going live due to them containing keywords that can be potentially used in a harmful way. In these cases users will choose usability over security by whitelisting those keywords, opening a window of opportunity for those with ill intent.

Safety as a component is an important element of the overall PQoS - perceived quality of service - is an assessment of the quality of information service in terms of perception of the user as a customer of this service.

Lastly, there is always the human factor to each digital security measure, as social engineers will try tricking hosting owners or hosting providers into sharing login credentials to resources otherwise inaccessible for them. This method of hacking doesn't require in-depth technical knowledge nor complex scripts, thus no firewall can shield it off. People working within IT should stay vigilant in regards to what details they share and to whom.

References

1. Maksymiv O, Rak T, Menshikova O, Deep convolutional network for detecting probable emergency situations, Data Stream Mining & Processing (DSMP), IEEE First International Conference, 2016.
2. Рак Т., Рудик Ю., Рудик А. Засоби оперативного управління діяльністю підрозділів ДСНС з використанням ІТ-технологій на базі геоінформаційного комплексу, Львів, АСВ, 2015– С. 267-270.
3. Most common web security vulnerabilities [online source] https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

АНАЛІЗ ДОРОЖНЬО-ТРАНСПОРТНИХ ПРИГОД ІЗ ПОСТРАЖДАЛИМИ НА ТЕРИТОРІЇ МІСТА ЛЬВОВА

Володимир Самотий[1], Уляна Дзелендзяк[2], Олег Пелех[2]

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

Historical data of traffic accidents in Lviv has been analysed. Daily and weekly frequency of road accidents has been analysed. Also, dependence of the number of traffic accidents on weather conditions has been shown.

Keywords: accident analysis, accident data, road accidents, road safety, open data, data analysis.

Згідно з офіційною статистикою [1], щороку у дорожньо-транспортних пригодах (ДТП) в Україні травмуються більше 30 тис. осіб та понад 3 тис. осіб гине. Згідно з даними Опендатабот [2], за січень-квітень 2018 року, Львівська область посідає друге місце в Україні за кількістю ДТП і перше місце за кількістю смертельних ДТП. На даний момент система безпеки транспортного руху в Україні опирається на засоби профілактики і попередження ДТП, хоча, сучасний розвиток інформаційних технологій та наукових методів дозволяє діяти на випередження – прогнозувати, а відповідно, і запобігати виникненню аварійних ситуацій на транспортних шляхах, цілеспрямовано здійснюючи вплив там, де аварія ще не відбулася, але є висока її ймовірність. Хоча, конкретну аварію практично неможливо передбачити, через випадкову природу ДТП, дослідники визначили, що агрегація великої кількості аварій на достатню площу території та інтервал часу, дає можливість встановити певний рівень передбачуваності, який можна описати математичними та статистичними зв'язками, беручи до уваги різноманітні фактори впливу (інтенсивність трафіку, погодні умови) [3]. На жаль, в Україні немає централізованих детальних даних про ДТП, які давали б достатньо інформації для аналізу причинно-наслідкових подій аварійності на автошляхах країни.

Проаналізуємо інформацію про зареєстровані у 2015 році ДТП у місті Львові, опубліковану на Порталі відкритих даних Львова [4] у CSV-файлі, який містить дані про тип, дату, час скоєння та адресу ДТП. Як інструмент для аналізу та візуалізації великих наборів даних обрано Python, який зарекомендував себе як універсальний інструмент для різноманітних наукових задач. Для обробки та підготування даних, використано Python-інструмент pandas, із допомогою якого дані зчитано із CSV-файлу, відформатовано, конвертовано у необхідні типи та проаналізовано частково відсутні дані. Наступний крок – конвертування адрес ДТП у формат просторових даних та прив'язування географічних координат до кожної адреси. Для цього завдання використано Python-бібліотеку GeoPy, що дозволяє проводити процес геокодування за допомогою систем геокодерів. Як систему геокодування вибрано картографічний сервіс HERE. Для геокодування у бібліотеці GeoPy є функція geocode, що приймає як параметр адресу, яку потрібно конвертувати у просторові дані.

Для ефективного аналізу погодних факторів впливу, потрібно дізнатися метеорологічні умови для кожного окремого випадку ДТП. Такі дані отримано з допомогою сервісу Dark Sky, який надає доступ до історичних погодних даних будь-якої точки світу. Щоб взаємодіяти із Dark Sky, потрібно зареєструватися та отримати унікальний API ключ. Для зручності отримання даних, Dark Sky пропонує бібліотеки-обгортки. Для роботи обрано бібліотеку-обгортку Dark Sky API для Python 3 – Forecastiopy. Дана бібліотека містить 9 класів, основний з яких – ForecastIO здійснює підключення, формує URL-адресу запиту та отримує дані з Dark Sky API. Для того, щоб дізнатися у світлу чи темну пору доби трапилася ДТП, використано Python-бібліотеку ephem, яка надає інструменти для виконання астрономічних обчислень.

Найбільша концентрація аварій із постраждалими спостерігається на вулицях у центрі міста: проспекті Свободи та вул. П. Дорошенка (рис. 1), 63% аварій, у яких є постраждалі, трапилися в світлу пору доби. Це пов’язано із тим, що трафік у денний час більш насичений. Як свідчать дані досліджень [5], [6] та статистики [7], максимальна кількість ДТП, у яких постраждали чи загинули люди, спостерігається у суботу та неділю, а мінімальна – у вівторок. Аналіз даних аварійності міста Львова має дві відмінності: пік аварій із постраждалими зміщується із суботи-неділі, у згаданих вище роботах, на п’ятницю-суботу; мінімальна кількість аварій із постраждалими у Львові спостерігається у неділю, тоді як у згаданих роботах – у вівторок (у Львові на вівторок припадає мінімум протягом робочого тижня). На рис. 2 наведено десять вулиць міста з найбільшою кількістю ДТП, у яких є постраждалі за даними 2018 року.

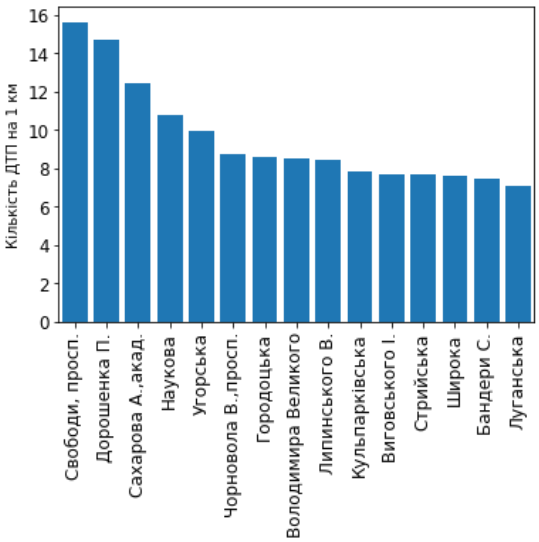


Рис. 1. Кількість ДТП із постраждалими на 1 км

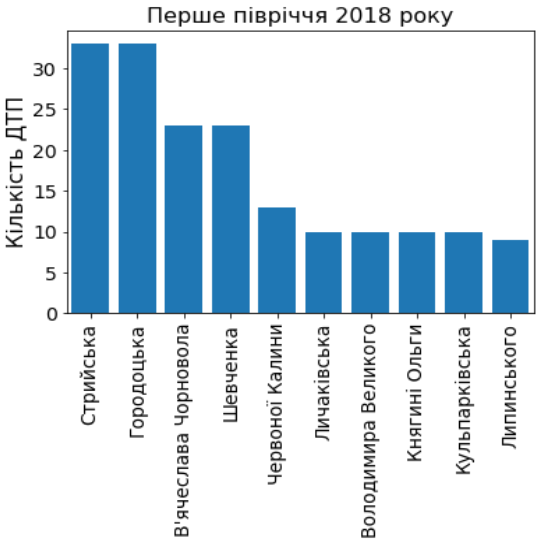


Рис. 2. Топ-10 вулиць міста за кількістю ДТП, у яких є постраждалі

На території міста Львова протягом останніх років спостерігається значне зростання кількості учасників дорожнього руху, тому аналіз розподілу дорожньо-транспортних пригод, а також, візуальне відображення та прогнозування дорожньо-транспортних пригод з метою попередження та мінімізації трагічних випадків та завдання шкоди здоров'ю і майну учасників дорожнього руху набуває все більшого значення.

Література

1. Death on the roads [Електронний ресурс] // http://roads.live.kiln.digital/. – 2015. – Режим доступу до ресурсу: World Health Organization.
2. Названі області, в яких частіше гинуть люди під час ДТП [Електронний ресурс] // Опендатабот. – 2018. – Режим доступу до ресурсу: https://opendatabot.ua/blog/193-dtp-regions.
3. Measuring the contribution of randomness, exposure, weather, and daylight to the variation in road accident counts / E. Hermans, T. Brijs, T. Stiers, C. Offermans. // Accident Analysis & Prevention. – 1995. – №27. – С. 1–20.
4. Інформація про ДТП 2015 [Електронний ресурс] // Портал відкритих даних Львова. – 2016. – Режим доступу до ресурсу: https://opendata.city-adm.lviv.ua/dataset/dtp2015.
5. Rural road safety – overview of crash statistics / M. Symmons, N. Haworth та I. Johnston // Monash University Accident Research Centre – 2014.
6. Analysis of Weekday, Weekend, and Holiday Accident Frequencies/J. Pigman, R. Rizenbergs and D. Herd// University of Kentucky – 1980.
7. Statistics of fatal and injury road accidents in lithuania, 2013–2016 / Lithuanian Road Administration – 2017.

СТРУКТУРА СЕМАНТИЧНОГО ТЕЗАУРУСУ ДЛЯ ЛЕКСИКОГРАФІЧНИХ КРИПТОСИСТЕМ

Євген Самойлик, Роман Одарченко, Тетяна Жмурко, Вікторія Лукашенко

Національний авіаційний університет, м. Київ, Україна

At present, various virtually stable cryptographic systems have been developed that have been used to solve a wide range of applications, where it is necessary to provide reliable protection against violations of the confidentiality of information transmitted by open communication channels. However, these cryptosystems do not guarantee a formal, theoretically proved impossibility of their hacking. Therefore, in this paper a fundamentally new approach was proposed for the protection of confidential information - lexicographic cryptosystems. For their effective work the structure of the semantic thesaurus was proposed.

Keywords: cybersecurity, thesaurus, cryptography, information security, lexicographic systems.

Неодмінним елементом будь-якої досконало стійкої криптосистеми, що заснована на застосуванні певним чином побудованої лексикографічної системи, є тезаурус бази захисту інформації у прикладній системі, де ця криптосистема використовується. У даному випадку тезаурус – це семантичний словник, структура якого відображає структуру семантичних зв'язків між смисловими конструкціями мови відображення прикладної області його застосування. У досконало стійких криптосистемах структура семантичних зв'язків між елементами тезауруса має бути відображена на формальному рівні. Визначення цієї структури є основним завданням даного розділу.

Будемо вважати, що тезаурус будь-якої мови взагалі TZ_M або будь-якого суб'єкту окремо TZ_S має ієрархічну прошаркову структуру і за ступенем абстрагування відображення смислових образів розподіляються на i рівнів, де $i = 1, 2, \ldots, i$ – кількість рівнів абстрагування відображення смислових образів, якими оперує колективний інтелект носіїв цієї мови взагалі або індивідуальний інтелект суб'єкту розумової діяльності окремо, а I_{max} – максимальна кількість рівнів абстрагування відображення SO, що є доступною інтелекту. Так що, простір смислових образів, доступний суб'єкту (або групі суб'єктів), тобто його тезаурус TZ_S, є дискретним, кінцево-мірним, який щодо рівнів абстрагування представлення образів має прошаркову коренево-подібну структуру (рис. 1).

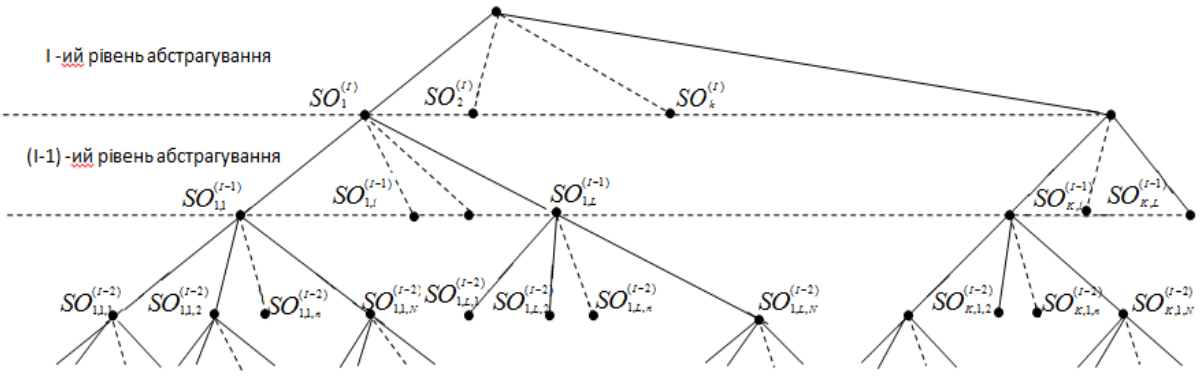


Рис. 1. Прошаркова коренево-подібна структура тезаурусу

За таким визначенням будь-який тезаурус TZ (зокрема, TZ_M або TZ_S) складається із сукупності підтезаурусів семантичних одиниць усіх доступних для розуміння рівнів абстрагування $TZ^{(i)}$, де $i=1,2, \ldots, I$. При цьому підтезауруси у складі TZ розташовані прошарками у вигляді гілко-подібної кореневої системи, що розростаються зверху униз. В основі кореня лежить семантичний образ $SO^{(I+1)}$ з максимальним $(I+1)$-им рівнем абстрагування відображення SO, що є доступним інтелекту у конкретній області розумової діяльності. Перший знизу від основи кореню прошарок підтезаурусів, що складають множину

$\{TZ^{(I)}{}_k\}$, визначають простір $\{SO^{(I)}{}_k\}$, що конкретизують $SO^{(I+1)}$ із *I*-им рівнем абстрагування відображення смислових образів. Другий знизу від основи кореню прошарок підтезаурусів, що складають множину $\{TZ^{(I-1)}{}_{k,l}\}$, визначають простір $\{SO^{(I-1)}{}_{k,l}\}$, що конкретизують $SO^{(I)}$ із більш детальним (*I*-1)-им рівнем абстрагування відображення смислових образів. І т.д. – від більш узагальненого до більш конкретного відображення смислових образів.

Так що, структуру тезаурусу *TZ* у загальному випадку можливо представити у вигляді рекурентної коренево-подібної схеми як:

$$TZ \in \{TZ^{(I)}{}_k\},\ \text{де}\ TZ^{(I)}{}_k \in \{TZ^{(I-1)}{}_{k,l}\},\ \text{де}\ TZ^{(I-1)}{}_{k,l} \in \{TZ^{(I-2)}{}_{k,l,n}\},\ \ldots \quad (1)$$
$$K \qquad\qquad L \qquad\qquad N$$

$$\text{де}\ TZ^{(2)}{}_{k,l,n,\ldots,p} \in \{SO^{(1)}{}_{k,l,n,\ldots,j}\}.$$
$$J$$

У виразі (1) прийнято наступні позначення: TZ(I)k - тезаурус І-го рівню абстрагування представлення SO; I∈ {1, 2,… i,…,… , Imax} – кількість рівнів абстрагування відображення SO, що доступна інтелектові; Imax – теоретично будь-яке велике, але скінчене ціле; k∈ {1, 2,… , K} – порядковий номер елемента TZ(I)k у множині тезаурусів, що у сукупності визначають простір смислових образів І-го рівню абстрагування, тобто {SO(I)}; K – кількість тезаурусів І-го рівню абстрагування відображення SO , що входять до складу TZ.

$TZ^{(I-1)}{}_{k,l}$ - тезаурус (*I-1*)-го рівню абстрагування представлення *SO*, що конкретизує смислові образи $TZ^{(I)}{}_k$, де $l \in \{1,2, \ldots, L\}$ – порядковий номер тезаурусу (*I-1*)-го рівню абстрагування у множині тезаурусів, які у сукупності визначають простір смислових образів (*I-1*)-го рівню абстрагування у рамках тезаурусу $TZ^{(I)}{}_k$; *L* – кількість тезаурусів (*I-1*)-го рівню абстрагування відображення *SO*, що входять до складу $TZ^{(I)}{}_k$;

$TZ^{(I-2)}{}_{k,l,n}$ - тезаурус (*I*-2)-го рівню абстрагування представлення *SO*, що конкретизує смислові образи $TZ^{(I-1)}{}_{k,l}$, де $n \in \{1,2, \ldots, N\}$ – порядковий номер тезаурусу (*I-2*)-го рівню абстрагування у тезаурусі $TZ^{(I-1)}{}_{k,,l}$; *N* – кількість тезаурусів (*I-2*)-го рівню абстрагування відображення *SO*, що входять до складу $TZ^{(I-1)}{}_{k,l}$;

$TZ^{(2)}{}_{k,l,n,\ldots,p}$ - тезаурус другого рівню абстрагування представлення *SO*, що конкретизує смислові образи $TZ^{(3)}{}_{k,l,n,\ldots,s}$, де $p \in \{1,2, \ldots, P\}$– порядковий номер тезаурусу другого рівню абстрагування у складі тезаурусу третього рівню$TZ^{(3)}{}_k$, .д. уздовж ланцюгу тезаурусів із зростанням значення індексу *i*;

$SO^{(1)}{}_{k,l,n,\ldots,j}$ - семантичний словник, що відображає тезаурус $TZ^{(2)}{}_{k,l,n,\ldots,p}$; *J* - кількість слів у тезаурусі $TZ^{(2)}{}_{k,l,n,\ldots,j}$.

Отже, структура тезаурусу *TZ* представляється у вигляді розгалуженого кореня підтезаурусів $TZ^{(i)}$, де $i \in \{1, 2,\ldots,\ldots, I_{max}\}$.

Висновки. В даній роботі запропоновано формальну структуру тезаурусу смислових образів для будь-якої мови взагалі або для будь-якого суб'єкту окремо. Показано, що такий тезаурус має ієрархічну прошаркову структуру і за ступенем абстрагування відображення смислових образів розподіляється на *i* рівнів, де $i = 1, 2, \ldots, I$ – кількість рівнів абстрагування відображення смислових образів, якими оперує колективний інтелект носіїв мови взагалі або індивідуальний інтелект суб'єкту розумової діяльності окремо, а *I* – максимальна кількість рівнів абстрагування відображення *SO*, що є доступною інтелекту. Так що, простір смислових образів, доступний суб'єкту (або групі суб'єктів), є дискретним, кінцево-мірним, який щодо рівнів абстрагування представлення образів має прошаркову коренево-подібну структуру.

Література

1. Смарт Н. Криптография / С.А. Кулешова (пер.с англ.). — М. : Техносфера, 2006. — 519 с.
2. Математичні основи крипто аналізу: навч. посібник / Сушко С.О.,Кузнецов Г.В., Фомичова Л.Я., Корабльов А.В. – Д.: Національний гірничий університет, 2010. -465 с.
3. Коблик Н. Курс теории чисел и криптографии – М.: Научное изд-во ТВП, 20001. – 254 с.
4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: «Гелиос АРВ», 2001. – 479 с.

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОЇ ДІЯЛЬНОСТІ БАНКІВ НА ФІНАНСОВИХ РИНКАХ

Сергій Шамов, Альона Сарбаш

Харківський навчально-науковий інститут ДВНЗ «Університет банківської справи», м. Харків, Україна

The threats to the information security of commercial activity of banks in financial markets are considered, the system of counteraction to these threats is proposed, and a means to support decision-making on the implementation by the dealer of the bank of trading operations on the basis of intellectual prediction of changes in the value of financial instruments.

Keywords: information security, dealer of the bank, forecast, intellectual means, neural network.

Інформаційна безпека, як показник якості, характеризує захищеність інформації, а також інформаційних систем (ІС) від випадкових або навмисних дій, які можуть завдати шкоди власникам цієї інформації та цих систем. Питання, пов’язані з її забезпеченням останнім часом набувають особливої актуальності в зв'язку з появою нових вразливостей банківських ІС, а також великою кількістю атак кіберзлочинців у фінансовому секторі світової економіки.

Проведене дослідження [1] показало, що для роботи торговельних ІС банків існує низка взаємно пов’язаних загроз: кібератак, вразливості технологій, використання блокчейн, нестачі кваліфікованих кадрів, панічних настроїв та інші. Більшість з них є предметом постійної уваги фахівців з інформаційної безпеки і блокуються або послаблюються чисельними технічними засобами. Однак загрозі неефективності управління власною діяльністю дилера, реалізація якої здатна призвести до кризових і навіть катастрофічних наслідків, досі не приділялося достатньої уваги. Тому запропоновано для протидії цій загрозі доповнити засоби торговельних ІС інтелектуальними засобами автоматичного моніторингу новин, їх зіставлення з інформацією про поточні курси фінансових інструментів, урахування отриманого результату в алгоритмах обчислення технічних індикаторів, та їх використання в засобах прийняття рішень щодо управління діяльністю дилера банку (рисунок 1) [2].

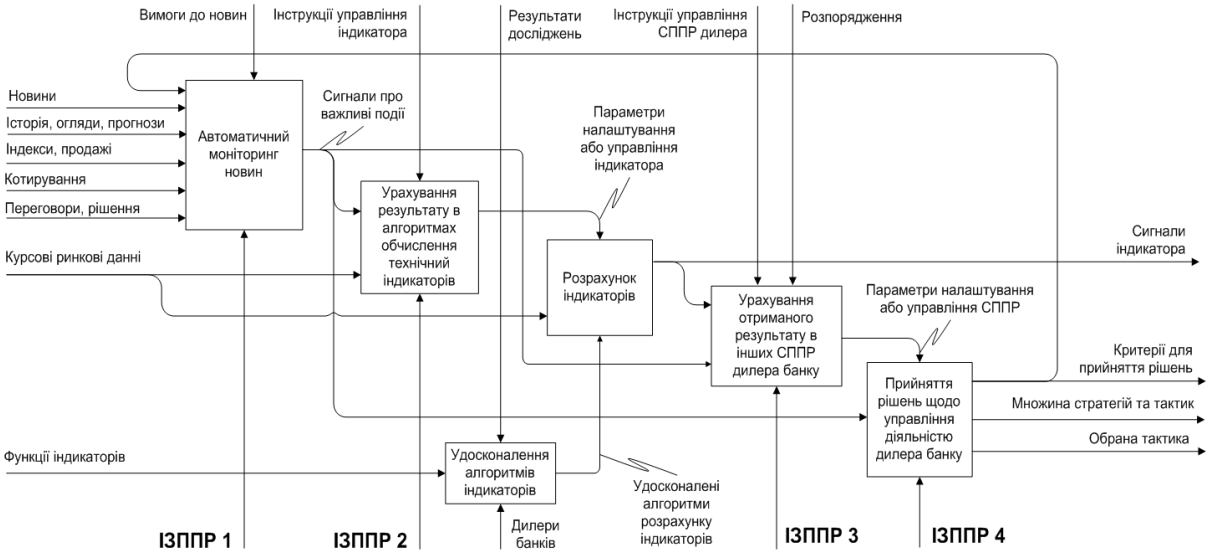


Рис. 1. Застосування інтелектуальних засобів захисту діяльності дилера (розробка авторів)

Основні інтелектуальні технології, що використовуються при створенні систем підтримки прийняття рішень, це: генетичні алгоритми, формально-логічних підхід, штучні нейронні мережі. Проведений їх аналіз показав, що застосування нейромережного підходу

є найбільш ефективним для вирішення поставлених завдань за умов швидкоплинних змін у закономірностях ринкових процесів, особливо для прогнозування курсів фінансових інструментів. Придатність нейронної мережі до прогнозування безпосередньо випливає з її здатності до узагальнення і виділення прихованих залежностей між вхідними та вихідними даними. Після навчання мережа здатна передбачити майбутнє значення послідовності на основі декількох попередніх значень і відомих чинників, дозволяє наближувати прогноз до точних значень неперервної функції. Практичну застосовність такого підходу досліджено за допомогою ST Neural Networks.

В результаті навчання п'ятьох нейронних мереж були знайдені кращі з них для прогнозування курсу відкриття та закриття позицій за валютною парою UAH/USD та отримано їх прогнози. Середня абсолютна процентна похибка, яка використовується для порівняння точності прогнозів різнорідних об'єктів прогнозування, курсу відкриття позиції склала 0,1113%, а курсу закриття позиції – 0,108%. Вважається, що прогноз має високу точність, якщо цей показник <10%. Тож отримані прогнози мають достатньо високу точність, тоді як класичні методи, розраховані на застосування до рядів з більш помітними та очевидними структурними закономірностями, за умов складності та нелінійності структур ряду вхідних даних виявляються непридатними для використання.

Застосування нейромережного прогнозування дозволило удосконалити алгоритми розрахунку технічних індикаторів, усунути проблему систематичного запізнення у виявленні значущих ситуацій і побудувати програмний засіб формування випереджаючих рішень щодо здійснення торговельних операцій. Для технічного аналізу обрані індикатори серії Moving Average: SMA, DEMA, SMMA. Для формування рішень обчислюються відхилення між індикаторами. На основі розпізнавання значущих ситуацій та найменших відхилень індикаторів один від одного пропонуються сигнали (рекомендацій чи попереджень) щодо здійснення торговельних операцій. Схема прийняття рішень на основі нейромережних прогнозів зображена на рисунку 2.

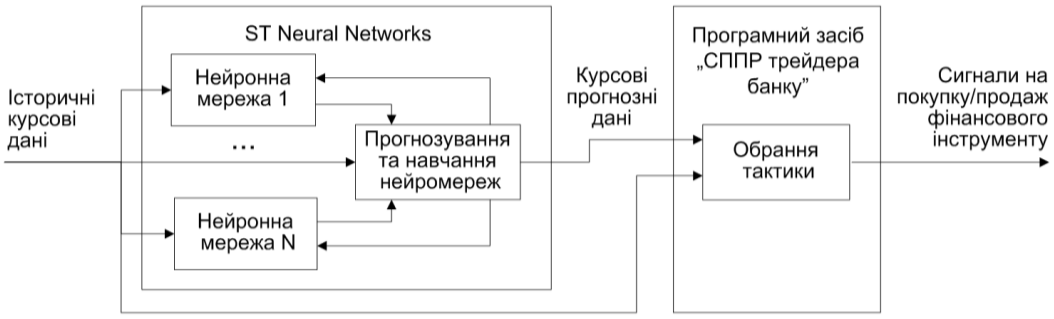


Рис. 2. СППР на основі нейромережних прогнозів (розробка авторів)

Таким чином, запропонований нейромережний підхід дозволяє розв'язати проблему запізнення сигналів технічних індикаторів та отримувати їх прогнозні значення. Побудований інтелектуальний засіб підтримки прийняття рішень, на основі застосування нейромежевого підходу дозволяє удосконалити інформаційну безпеку торговельної діяльності банків на фінансових ринках.

Література

1. Шамов С. О. Загрози діяльності брокерських компаній / С. О. Шамов, А. О. Сарбаш / Вісник Черкаського університету. Серія Економічні науки. – 2017. – №1. – С. 112 – 117.
2. Shamov S. Means of countering threats in communication systems of broker companies / Shamov S., Sarbash A., Florov S. [Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International], (October 10-13, 2017, Kharkiv, Ukraine). – PP. 187–192. DOI: 10.1109/INFOCOMMST.2017.8246377.

МЕТОДИКА ОЦІНЮВАННЯ РИЗИКІВ У ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Владислава Савчук, Олена Наумчак

Житомирський військовий інститут ім. С. П. Корольова, м. Житомир, Україна

Today, threats to information security, the main component of which is the, are becoming widespread. The extent of such threats can be determined through risk assessment. Risk assessment with the participation of a social component is possible due to consideration of all factors of their occurrence. For this purpose, a method of quantitative evaluation, information security risk based on factor analysis has been developed. For effective risk management, it is necessary to determine which of them are critical, which is possible due to their quantitative assessment.

Keywords: information security, factor analysis, security risk, social component.

Загроза є ймовірною перешкодою цілям та завданням суб'єкту господарювання, а ризик вимірює, оцінює цю загрозу, дає уявлення щодо математичного виразу ймовірності настання таких перешкод, тобто оцінка ризику є ступенем загрози. Розроблено безліч нормативно-правових документів, що визначають методології їх визначення для організацій, основними з яких є "Керівництво з управління ризиками в інформаційних технологіях" NIST 800-30 [1]; стандарти ISO/IEC 27002 та ISO/IEC 31000 [2] COBIT (контрольні цілі для інформації і суміжних технологій) [3]. Проте основною особливістю теперішнього часу є поєднання технологічної та соціальної компоненти, що призводить до винекнення гібридних загроз. Для цього розроблялись нові методики оцінювання ризиків [4-6].

Проблема наведених методологій полягає в тому, що вони призначені для профільних задачах, та не описують деталей для реалізації кількісної оцінки ризиків і залишають не врахованим спектр факторів що впливають на інформаційну безпеку з боку соціально-технічної компоненти. Найбільш повно врахувати фактори дозволяє методика FAIR, основою якої є факторний аналіз [6]. Він заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тих або інших негативних наслідків. Зміна фактора є ознакою загрози в кібернетичному просторі. Оскільки на сучасні інформаційні системи впливають безліч факторів, зазвичай використовується багатофакторний аналіз.

Виділяють дві групи внутрішніх факторів, що впливають на появу загрози: наявність активів чи процесів які цікавлять зловмисника та можуть стати об'єктом загроз; уразливості інформаційної системи для яких характерна соціо-технічна складова. Окрім цього важливо враховувати і зовнішні фактори, що в більшості впливають на соціальну компоненту ризику загрози.

Узагальнюючи вище наведені методи оцінювання ризиків метод кількісного оцінювання ризиків полягатиме в наступних кроках:

1. Інтегроване представлення набору активів, схильних до ризиків. Таке представлення засноване на використанні фундаментальної моделі архітектури організації. Вона може бути представлена онтологією підприємства, зокрема моделлю Захмана (ZF) [7], яка може бути подана у вигляді матриці:

$$ZF = A \times P \qquad (1)$$

де А – це категорія активів; Р – це точка зору на перспективу опису різних аспектів діяльності організації та її існування (актив, процес, бізнес-процес).

2. Визначення уразливостей інформаційних систем з урахуванням особливостей діяльності організації. Відповідно до ISO/IEC 27005 [2] уразливості пов'язані з властивостями активу і можуть бути класифіковані відповідно до типу активів.

3. Оцінювання активу, послуги чи бізнес-процесу та уразливостей – відокремлення критичних і некритичних ресурсів, розглядають функціональні залежності між рівнями, щоб з'ясувати, який ресурс відіграє критичну роль в організації. Кількісна оцінка ризику за категоріями активів R_A може визначатись за виразом:

$$R_A = K_A * V_A \quad (2)$$

K_A- кількість активів в категорії A, V_A- вартість активів категорії A.

Кількісний показник ризику за уразливостями $R_{ур}$ визначається за виразом:

$$R_{ур} = K_{ур} * K_A + V + T \quad (3)$$

де $K_{ур.}$– кількість уразливостей за типом активів, V – вартість обладнання чи програмного забезпечення, що може бути виведена зі строю; T – час простою інформаційної системи.

3. Виділення меж поширення ризику, тобто визначення чи поширеться загроза на інші ресурси та оцінювання їх за кроком 2.

4. Визначення зовнішніх факторів відповідно до особливостей діяльності та структури організації та інформаційних систем, що в них циркулюють. Фактори, що представляють собою соціальну компоненту можуть бути представлені як:

1) висока інтенсивність інформаційних впливів в зовнішньому середовищі [8], визначається за виразом:

$$F_{інф.впл.} = \prod_{i=1}\left(\lambda_i \left(\prod_{j=1}^{n} A_{ij}\eta_{ij}\mu_{ij} \right) \right) \quad (4)$$

де $F_{інф.впливів}$ – фактор інтенсивності інформаційних впливів в зовнішньому середовищі; A_{ij} – протестні акції i-ої форми (на 100 тис. населення); n – кількість протестних акцій i-ої форми; μ – ваговий коефіцієнт масовості j-ої протестної акції i-ої форми; ji , η – ваговий коефіцієнт тривалості j-ої протестної акції і-ої форми; λ_i – ваговий коефіцієнт небезпеки протестних акцій i-ої форми.

2) соціально-економічний – кількість громадян з доходом нижче прожиткового мінімуму , який обчислюється як відсоток кількості громадян, сумарний рівень доходів яких нижче прожиткового мінімуму [9], представлено виразом:

$$F_{соц.ек.} = (N_{меж.бідності}) / N \times 100 \quad (5)$$

де $F_{соц.ек.}$ – відсоток населення за межею бідності; $N_{меж.бідності}$ – кількість громадян з доходом нижче прожиткового мінімуму; N – загальна кількість населення країни чи регіону де діє організація.

Таким чином, послідовне виконання приведених кроків дає можливість врахувати в повному об’ємі фактори ризиків, та на їх основі знайти кількісну оцінку ризику.

Література

1. NIST, ”NIST SP-800-30rev1,” 2012. [Online]. Available: http://www.nist.gov/customcf/get pdf.cfm?pub id=91091. [Accessed August 2018].
2. International Organization for Standardization, ISO/IEC 27005:2011. Information security risk management.
3. COBIT 5: A Business Framework for the Governance and Management of Enterprise ISACA, 2012.
4. Сучасні підходи до оцінки ризиків інформаційних технологій. [Електронний ресурс]. – Режим доступу: http://www.auditagency.com.ua
5. CRAMM user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001
6. Методика факторного аналізу інформаційних ризиків An Introduction to Factor Analysis of Information Risk (FAIR) [Online]. – Available: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.
7. The Concise Definition of The Zachman Framework by: John A. Zachman. URL: https://www.zachman.com/about-the-zachman-framework. 8
8. Соціальна безпека: сутність та вимір. наук. доп. / О.П. Коваль. – К.: НІСД, 2016. - 34 с
9. Харазішвілі Ю. Проблеми інтегрального оцінювання рівня економічної безпеки держави / Ю. Харазішвілі, Є. Дронь // Банківська справа. –2015. –№ 1. – С. 3–21 30

ПОКРАЩЕНИЙ ГЕНЕРАТОР ФІБОНАЧЧІ ДЛЯ ВИКОРИСТАННЯ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Марія Шабатура, Валерія Войтович

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The statistical characteristics of the classical Fibonacci generator is researched. The generator is proposed to be improved by changing the structural scheme. Was shown the statistical porter of the Fibonacci Generator, which had improved results than classical generator.

Keywords: pseudorandom number generator, information security systems, statistical characteristics, test NIST.

Для забезпечення безпеки комп'ютерних систем критично важливо мати алгоритми, що задовольняють такому критерію як непередбачуваність. Іншими словами, навіть знаючи алгоритм генератора й всі попередні елементи послідовності, повинне бути максимально трудомістким обчислення наступних елементів. Потреби в потужних наукових обчислювачах набагато обганяють можливості вдосконалювання складних архітектур багатопроцесорних систем, і, що головне, ці потреби дуже погано узгоджуються з реальними бюджетами наукових організацій. Як не дивно, але в обох ситуаціях роль генератора псевдовипадкових чисел украй важлива. Характеристики систем безпеки здебільшого залежать від характеристик їхніх криптографічних підсистем, які визначаються не тільки алгоритмікою, але і якісними показниками саме використовуваних ГПВЧ або апаратних генераторів випадкових чисел.

Під час дослідження класичного генератора Фібоначчі підтвердився відомий факт про незадовільні статистичні характеристики, що свідчить про не випадковість послідовностей, які генеруються такими генераторами.

Рівняння роботи класичного генератора Фібоначчі

$$x_i = (x_i + x_{i-1}) \bmod m \tag{1}$$

На рис. 1 наведено статистичний портрет класичного генератора Фібоначчі.

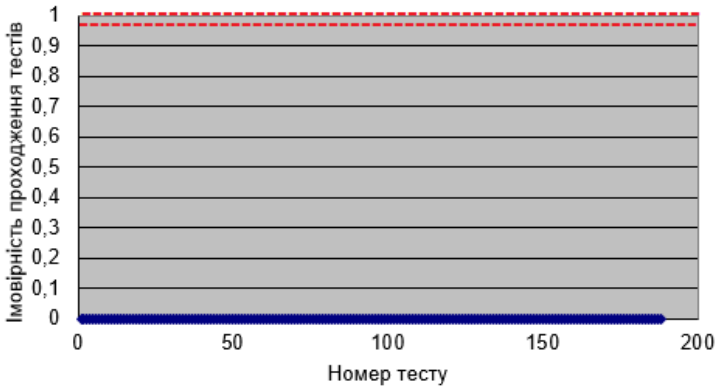


Рис. 1. Статистичний портрет класичного генератора Фібоначчі

Для покращення статистичних характеристик, було побудовано модифікований генератор Фібоначчі шляхом доповнення рівняння (1), додаванням половини першого регістру. Покращений генератор буде містити, регістри x, x1, x2, два комбінаційні суматори КС (рис. 2). На виході МГФ формується послідовність ПВЧ відповідно до виразу:

$$x_i = (x_i + x_{i-1} + x_i / 2) \bmod m \tag{2}$$

де x – значення у регістрах.

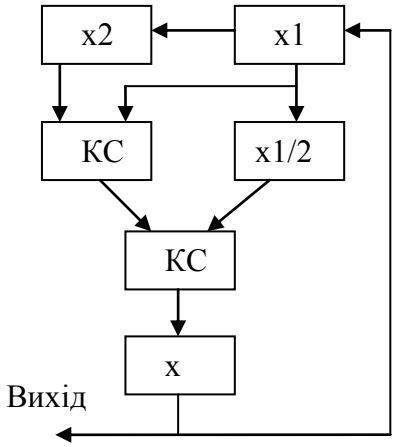


Рис. 2. Структурна схема модифікованого генератора Фібоначчі

На рис. 3 наведено отримані статистичні характеристики бітової послідовності з виходу покращеного генератора. Усі дослідження здійснювалися з допомогою американського набору статистичних тестів NIST [3].

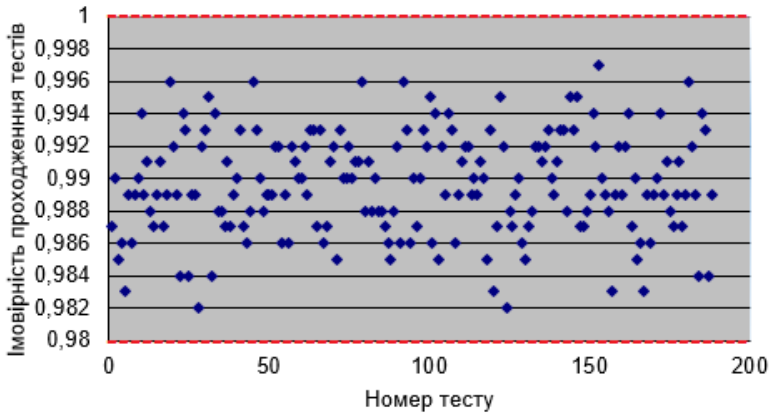


Рис. 3. Статистичний портрет класичного генератора Фібоначчі

Із рис. 3 видно, що всі тести успішно пройдено, всі значення тестів потрапили в межі довірчого інтервалу, який позначено двома пунктирними лініями. Це означає, що запропонований варіант удосконалено генератора Фібоначчі генерує послідовність, яка відповідає вимогам випадковості.

За результатами проведених досліджень можна зробити висновок, що основним чинником, який дозволив істотно покращити статистичні характеристики ГПВЧ, побудованого на основі класичного генератора Фібоначчі, є додавання до їх структури половини попереднього значення.

Література

1. Иванов, М.А. Криптографические методы защиты информации / М.А. Иванов.- М.: КУДИЦ-ОБРАЗ, 2012.-368с.
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. NIST SP80022. A statistical Test Suite of Random and Pseudorandom Number Generators for Cryptographic Applications: [Електронний ресурс]. April 2000. Доступний з: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf.
4. Implementation of modified additive lagged Fibonacci generator / Mandrona M.M., Maksymovych V.M., Harasymchuk O.I., Kostiv Yu.M. // Challenges of Modern Technology, Vol. 7, No 1, 2016, Pp. 3-6
5. Generator of pseudorandom bit sequence with increased cryptographic security / [M.M. Mandrona, V.M. Maksymovych, Yu.M. Kostiv, O.I. Harasymchuk] // Metallurgical and Mining Industry: scientific and technical journal – 2014. – No. 5. – Pp. 25-29

АВТОМАТИЧНА ПОБУДОВА МОНІТОРИНГУ БЕЗПЕКИ ВИДІЛЕНОГО СЕРВЕРА ЗА ДОПОМОГОЮ NETDATA ТА ANSIBLE

Богдан Сухомлінов

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Collaboration of Ansible and Netdata to build monitoring and alerting system on dedicated information system. Main purpose -- automation building system to get real time security alerts.

Keywords: information security, devops, automation, deployment, ansible, security monitoring, netdata.

Головною тенденцією розвитку інформаційного середовища сучасного світу є суттєве збільшення об'ємів даних, швидкості їх обробки та доставки кінцевому споживачу. Безкомпромісність у наданні доступу до ресурсу, стабільність роботи, масштабованість системи (за умови високого навантаження), забезпечення HA (high availability) -- де-факто стали стандартом на просторах Інтернету для будь-якого інформаційного ресурсу. Всі ці фактори можливі лише за умови коректної роботи системи на всіх її рівнях, налаштування яких робота цілої команди спеціалістів.

Проте, з ростом системи, недоцільно пропорційно збільшувати штат працівників, що її обслуговують. Це не тільки не рентабельно, але й збільшує ризик впливу "людського фактору". Натомість вартісним рішенням є введення автоматизації, зокрема для побудови самої системи та її моніторингу, доставка (deployment) продуктивного коду та введення його в дію. Оскільки це непрямий обов'язок ані системних адміністраторів (автоматизації побудови), ані програмістів (автоматизація доставки коду), поступово виникла нова професія: devops -- development and operations [1].

Головною метою devops є не тільки автоматична побудова середовища, але введення в дію інструментів, для автоматизації "автоматичної побудови середовища". Головним тут є принцип "IaaC" (Infrastructure as a Code) -- написання конфігурацій для розгортання. Це має ряд переваг: можливість швидкого повторного створення середовища; постійне покращення існуючих конфігурації для ще швидкого введення системи в дію; контроль системи, її компонентів, доступів до системи, тощо; колаборація та розподіл обов'язків між командою devops, і як наслідок розподіл повноважень між командою (наприклад, не кожен з команди має доступ до production-оточення); тощо.

Окремим обов'язком є введення в дію системи моніторингу та оповіщення (alerts). Під моніторингом розуміється оперативне отримання інформації щодо роботи всіх компонентів системи. Це можуть бути як типові показники: навантаження на процесор, кількість вільної оперативної пам'яті, чи дискового простору, навантаження на мережу. Це можуть бути більш спеціалізовані дані: для прикладу, для веб-порталу кількість одночасних користувачів, навантаження на базу даних, кількість працюючих нод. І нарешті, це можуть бути вузько-спеціалізовані дані: кількість отримання виділених помилок "на відмову" в аплікації, дельта змін між реплікаціїями між нодами центральної бази даних. Кожну з цих метрик можна зобразити різними шляхами для представлення відповідальним за роботу системи особам, на кожну з цих метрик можна ввести тригер на оповіщення цих осіб.

Система оповіщення має не тільки створювати оповіщення про виникнення критичної ситуації, але й попередити їх. Наприклад сповіщати про швидке закінчення дискового простору, значне зростання кількості одночасних підключень на веб-порталі (можливий ddos) чи високу дельту при реплікації (можлива подальша розсинхронізація нод бази даних). Також оповіщення можуть бути на прямими, тобто для виникнення оповіщення потрібних ряд факторів (тригерів).

Окремою темою є моніторинг та оповіщення безпеки інформаційної системи. Найпростішим практичним застосуванням, можна вважати сповіщення при невдалих спробах отримати несанкціонований доступ до системи (fail2ban) чи кількість поточних залогінених користувачів (наприклад, можна створити тригер "оповіщення якщо бодай один користувач успішно увійшов в систему"). В сукупності це дасть можливість базово моніторити периметр безпеки.

В роботі розглянуто розгортання системи моніторингу та оповіщення засобами Ansible [2]. Ansilbe - це Open Source [3] інструмент автоматизації, "швейцарський ніж" для devops. Написаний на Python (можливість суттєво розширювати функціонал за рахунок написання модулів та плагінів) та використовуючи OpenSSH (не потрібно вводити новий стосів доступу до середовища), він може конфігурувати системи, розгортати ПЗ на великій кількості серверів, і все це використовуючи простий формат YAML, що дозволяє швидко створювати нові конфігурації побудови.

В якості системи моніторингу виступає Netdata [4]. Netdata це Open Source [5] інструмент моніторингу продуктивності та здоров'я системи в реальному часі. Основними перевагами є висока швидкодія на ряду з дуже мінімальним використанням системних ресурсів, а також велика кількість метрик та плагінів "з коробки": після встановлення доступно біля двох тисяч метрик. Має вбудовану систему оповіщення, що дозволяє будувати алерти по кожній з метрик, і отримувати сповіщення по email, telegram, slack, pager duty, тощо. Також в комплекті з Netdata встановлюється даемон StatsD, що дозволяє знімати телеметрію з додатків, що можуть взаємодіяти зі StatsD.

Для моніторингу та оповіщення більш вузько-спеціалізованих додатків, функціонал Netdata можна розширювати за допомогою плагінів, які можна писати на Python, NodeJS, bash. Також варто згадати можливість інтеграції Netdata з іншими інструментами моніторингу: Prometheus, Graphite, OpenTSDB, Kafka, Grafana тощо.

Комбінація з Ansible та Netdata дозволяє швидко та ефективно розгорнути середовище моніторингу та оповіщення на будь-якій системі під управлінням Linux, доступом по OpenSSH та встановленим Python на кінцевих машинах. Результатом роботи є набір YAML-конфігурацій для Ansible у відкритому доступі [6] і не потребує ніяких додаткових залежностей, окрім наведених вище.

Робота, має практичне застосування на інформаційних системах та буде актуальною для системних адміністраторів, а також спеціалістів з інформаційної безпеки. Також наявний чималий потенціал до впровадження покращень, удосконалень до YAML-конфігурацій та також плагінів для Netdata.

Література

1. DevOps [Електронний ресурс] // wikipedia free encyclopedia – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/DevOps.
2. Ansible Documentation [Електронний ресурс] // Read the Docs – Режим доступу до ресурсу: https://docs.ansible.com/ansible/latest/index.html.
3. Netdata Wiki [Електронний ресурс] // GitHub – Режим доступу до ресурсу: https://github.com/netdata/netdata/wiki.
4. Netdata [Електронний ресурс] // GitHub – Режим доступу до ресурсу: https://github.com/netdata/netdata/
5. Dnull Sec Ops[Електронний ресурс] // GitHub – Режим доступу до ресурсу: https://github.com/dnullsecops

СТВОРЕННЯ РАДІОЖУЧКА ЯК ТЕХНІЧНОГО ЗАСОБУ ДЛЯ ПІДСЛУХОВУВАННЯ

Ігор Суль, Орест Полотай

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The principles of work and features of radio beetles are described. The diagram of the radio walker is shown. The finished radiogue is shown and its features are described.

Keywords: technical means of listening, radio tunes.

Радіожучок – спеціальний пристрій для прослуховування. Принцип дії радіожучка полягає в перехопленні акустичного сигналу, активізується при вільній лінії телефонного зв'язку. Згідно класифікації, радіо жучки можна віднести до технічних засобів розвідки, які використовують технічні канали витоку мовної та акустичної інформації [2].

Радіожучки можуть бути тимчасовими і стаціонарними. Стаціонарні моделі «жучків» потребують електроживлення, тому встановлюються в телевізорах, торшерах, люстрах, розетках та інших побутових предметах. Тимчасові прилади встановлюються в місцях, де їх знайти практично неможливо: в книгах, оббивці меблів, біжутерії і т.п.

Дуже часто радіожучки маскують під сірникові коробки, кулькові ручки, гудзики та інші малопомітні речі. За допомогою таких «жучків» можна перехопити розмову на відстані 20-30 метрів, а радіус передачі інформації обмежується трьома сотнями метрів. Правда, за допомогою проміжних ретрансляторів радіус передачі сигналу можна збільшити в кілька разів, особливо якщо «жучки» встановлюються на металевих поверхнях, які служать додатковим антеною. Головний недолік цих пристроїв в тому, що вони критично обмежені за часом записи, найчастіше тривалість їх роботи обмежена декількома десятками годин.

Подібні радіозакладки можуть працювати в досить широкому діапазоні частот, починаючи від 10 МГц і закінчуючи 1000 МГц і більше. Але найпопулярнішими діапазонами вважаються 20 - 25 МГц, 130 -174 МГц і 400 - 512 МГц. Підвищення частоти дозволяє збільшити дальність дії сигналу в бетонних будівлях, але цей процес вимагає наявність спеціальних радіоприймачів або перетворюють приставок до побутових УКХ-приймачів.

Для того, щоб надійніше сховати сигнал передачі, професіонали застосовують такі прийоми: спеціально розтягують спектр сигналу, застосовують здвоєну модуляцію частоти, зменшують подібну потужність із застосуванням проміжних ретрансляторів і т.п. Після таких дій виявити «жучки» досить важко, і без допомоги фахівця перевірити приміщення на наявність «жучків» неможливо.

Для створення власного радіожучка була використана схема, яка зображена на рис. 1 [1].

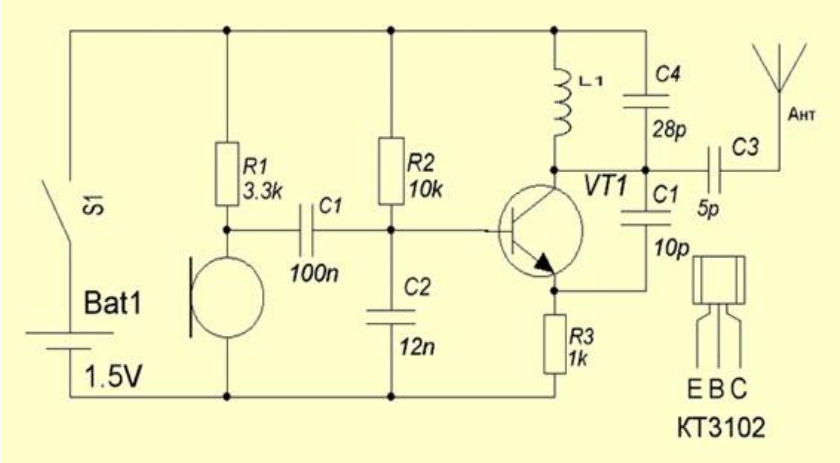


Рис. 1. Електрична схема рідіожучка

Робоча напруга жучка 1.5V, тобто він працює від батарейки типу "таблетка".

Рис. 2. Готовий радіожучок

На рис. 2. зображено радіо жучок, що створений на базі електричної схеми, яка наведена вище. За допомогою даного жучка можна здійснювати підслуховування звукової інформації через FM-хвилю радіоприймача.

Література

1. Веб-сайт РадіоКот. [Електронний ресурс]. Режим доступу з https://radiokot.ru/circuit/analog/receiv_transmit/15/
2. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

МОДЕЛЬ RD-АТАКИ

Олег Вацлавик

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Considerations of RD attacks on implanted medical devices at emergency states of the patient. Consider a new scheme based on the patient's access template to the implanted medical device and uses a vector support machine.

Keywords: information security, RD attacks, implanted medical device, authentication.

Через обмежені ресурси ІМП у термінах споживаної потужності , продуктивності процесора та об'єму пам'яті є досить складно розробити ефективну схему контролю доступу до ІМП.

В ідеальному випадку ІМП повинен би взаємодіяти лише з невеликою кількістю зчитувачів (таких як зчитувач вдома у пацієнта чи кабінеті лікаря). Більше того , комунікація не повинна відбуватися в будь-який час. Для більшості пацієнтів доступ до ІМП демонструє певний тип шаблону. Базуючись на цьому спостереженні , можна побудувати модель нормального доступу пацієнта до ІМП, яка тоді може бути використана для виявлення спроб шкідливого доступу шляхом поєднання моделі та ефективного класифікую чого алгоритму. Якщо ІМП виявляє спробу шкідливого доступу він переходить в режим сну та зберігає енергію. Така схема уникає втрат енергії під час процесу автентифікації, а отже ефективно захищає від RD-атак.

Розглянемо нову схему , яка базується на шаблоні доступу пацієнта до ІМП та використовує Векторизовану машину підтримки (ВМП). В ній використовується мобільний телефон пацієнта для виконання більшості обчислень. Ця схема є першою лінією захисту. Тобто вона запускається перед будь-якою процедурою автентифікації . Якщо будь-яка спроба доступу не пройде нашу схему, автентифікація не здійснюватиметься. Це збереже значну кількість енергії пристрою . Якщо зчитувач пройде нашу схему, далі потрібно буде пройти автентифікацію , яка забезпечує додатковий захист доступу до ІМП.

RD-атака розглядається як атака примусової автентифікації. ІМП взаємодіє через безпровідний канал з зовнішнім зчитувачем. Якщо автентифікацію не пройдено, тоді ІМП розриває взаємодію з зчитувачем. Проте процес автентифікації сам по собі вимагає від ІМП виконання багатьох обчислень та передач іформації , що споживають значну частку енергії. Якщо неавторизований зчитувач постійно намагається з'єднатися з ІМП , це спричиняє виконання ІМП багатьох автентифікацій , що споживає значну частку ємності батареї. На додаток до цього , цей тип атак генерує масив записів про події безпеки , які заносяться в журнал, що також є RD-атакою на ємність пам'яті ІМП.

Атаки примусової автентифікації можуть бути легко здійснені зловмисником через використання технології SDR (Software-Defined Radio) програмно-заданої радіо технології (рис. 1).

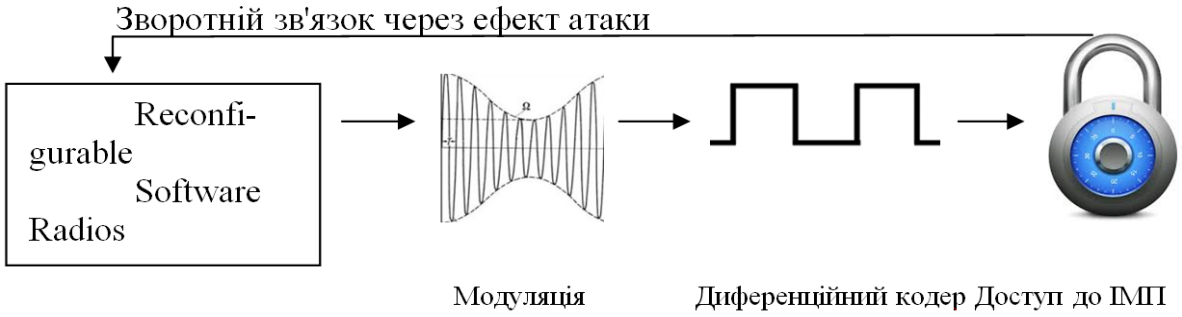


Рис. 1. Атака на ІМП з допомогою SDR

SDR – радіо-телекомунікаційна система , яка може бути налаштована на довільну смугу частот та приймати різні види модульованого сигналу і яка складається з програмованого обладнання з програмним керуванням. SDR виконує значну частину цифрової обробки сигналів на звичайному ПК або на ПЛІС. Метою таких систем , є радіоприймач або радіопередавач довільних радіосистем , який налаштовується шляхом програмної переконфігурації.

Через такі RD-атаки зловмисник може наносити безпосередню шкоду пацієнту розряджаючи джерело енергії ІМП. RD-атаки можуть зменшити ефективний час життя ІМП з декількох років до декількох тижнів, роблячи ІМП некорисним , та створюючи загрозу здоров'ю пацієнта. Тому критично важливим є розроблення легковагових та ефективних схем захисту для ІМП , які можуть протидіяти RD-атаці.

Література

1. В. В. Марков. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види.
2. Яцишин М. Ю. Актуальні проблеми захисту прав людини у кіберпросторі.
3. Орленко В. С. Методи оцінки та підвищення захищеності інформаційних ресурсів систем спеціального призначення. Автореф. Дис. На здобуття наук. Ступеня к.т.н.: 05.13.21 "Системи захисту інформації", Київ, 2009 (ДСК).
4. Avant 4000 bluetooth wireless oximetry: increased safety and accuracy when administering the six-minute walk test, Nonin Medical, Inc., Technical Report, 2008
5. X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices. inProceedings of the IEEE Globecom 2010, 2010, pp.1-5
6. K. Malasri, L. Wang, Securing wireless implantable devices for healthcare: ideas and challenges. IEEE Commun.47, 74-80 (2009)

ПРИНЦИП ДІЇ ТЕХНОЛОГІЇ HONEYPOT ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Валерія Войтович, Марія Шабатура

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

An analysis of existing systems of virtual lures based on honeypot technology. The analysis showed the evolution of honeypot systems from Low-Interaction Honeypots to the most up-to-date Gen III Honeynets and pointed to the disadvantages of existing solutions. In addition, the classification of honeypot-systems has been carried out on a symbolic basis.

Keywords: virtual lure, honeypot technology, intrusion detection, honeynet, a hallmark classification principle.

Honeypot – це комп'ютерна система, яка створена для того, щоб заманювати кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Еволюцію Honeypots можна побачити не озброєним оком, поглянувши на те, як ці системи використовуються разом із IDS для запобігання, виявлення та реагування на атаки. Дійсно, honeypots все частіше знаходить своє місце поряд з мережевими і хост-системами захисту від вторгнень.

Honeypots можуть запобігти атакам кількома способами. Перше – сповільнення або припинення автоматичних атак, таких як хробаки або авторучки [1]. Це атаки, які випадково сканують всю мережу, яка шукає вразливі системи. (Honeypots використовують різноманітні трюки TCP, щоб помістити зловмисника в "холдинг"). Другий шлях – запобігти людським атакам. Тут honeypots прагнуть зіткнутися з нападником, змушуючи його приділяти увагу діяльності, яка не завдає ні шкоди, ні втрати, надаючи організації час відповісти і блокувати атаку.

Виділяють два основних типи реалізацій: адаптовані і реальні. Іноді їх визначають як низько і високоінтерактівні.

Перші здатні емулювати взаємодію від імені певного сервісу, наприклад, прийняти з'єднання на tcp-порт 22, прийняти від атакуючого ім'я користувача і пароль і так далі, при цьому фіксуючи всі дії атакуючого.

Високоінтерактівні honeypot, засновані на застосуванні реальних ОС і реальних сервісів, трохи складніше в застосуванні. Фактично вони являють собою спеціально спроектовані мережеві сегменти, підключені до мереж загального користування. Мережевий трафік між honeypot і зовнішнім світом контролюється і фіксується, щоб повністю зберегти всі дії атакуючих, при цьому не допустивши шкоди для власної інфраструктури.

Типовими прикладами є honeyd і honeynet [2]. Honeyd дозволяє користувачам налаштовувати кілька віртуальних Honeypots з різними характеристиками і послугами на одній машині. Honeynet – це мережа, розміщена за реверсивним мереженим екраном, що фіксує усі вхідні і вихідні дані. Реверсивний файрвол обмежує об'єм шкідливого трафіку, що може покинути Honeynet-мережу. Ці дані зберігаються, фіксуються і контролюються. У середовищі Honeynet може бути розміщена будь-яка система, включаючи такі системи, які уже функціонують у виробничій мережі, яку покликана захищати Honeynet. Honeynet – це мережа, призначена бути атакованою і скомпрометованою для отримання відомостей про наявні та потенційні вразливості і загрози в мережі.

Сьогодні існує три основні архітектури Honeynet-мереж: I-ого покоління (Gen I Honeynets); II-ого покоління (Gen II Honeynets) та III-ого покоління (Gen III Honeynets).

Gen I Honeynets. Honeynet-мережі I-ого покоління обмежені в можливостях контролю та приборкування зловмисників, проте вони демонструють достатню ефективність у виявленні автоматизованих атак і атак початківців. Передусім Gen I Honeynets фокусуються на атаках відповідно можливостей. Такі мережі-приманки достатньо легко ідентифікуються.

Архітектура Honeynet-мереж I-ого покоління досить проста – ізольована мережа розміщується за пристроєм контролю доступу до мережі, найчастіше таким служить мережевий екран (рисунок 1, а). Мета такого розміщення – забезпечити неможливість атаки не honeypot-систем. Часто поряд з Honeynet-мережею знаходиться виробнича ІКС для адміністрування і накопичення зафіксованих даних. Також, можливим є розміщення інших контролюючих пристроїв (наприклад, маршрутизатора) для додаткового контролю [2]. Фіксація активності шляхом комбінації можливостей файрволу, IDS-сенсорів і системних логів забезпечує перехоплення інформації на таких чотирьох рівнях: активність в мережі, системна активність, активність програм та активність користувача. Gen II Honeynets. Технологія Gen II була розроблена в 2002 р. і направлена на усунення недоліків попередньої. Honeynet-мережі II-ого покоління простіші в розгортанні і складніші у виявленні [3]. Як описувалося вище, технологія Gen I виконувала контроль даних за допомогою мережевого екрану, що обмежував кількість можливих вихідних підключень. Незважаючи на свою відносну ефективність таке рішення є недостатньо гнучким і забезпечує легке «зняття зліпку». Honeynet-мережі II-ого покоління вирішують цю проблему шляхом модифікації загальної архітектури (рисунок. 1, б). Перша основна розбіжність – використання єдиного Honeynet-сенсора, що об’єднує функціонал файрвола та IDS. Друга основна відмінність – сама реалізація Honeynet-сенсора, що представляє собою пристрій другого рівня OSI (схожий на міст). Така реалізація значно ускладнює виявлення, так як відсутня маршрутизація пакетів, зменшення TTL і MAC-адреси пристроїв [4]. За рахунок описаних принципів Honeynet-мережа II-ого покоління може бути частиною основної виробничої мережі, а не ізольованою як в технології Gen I.

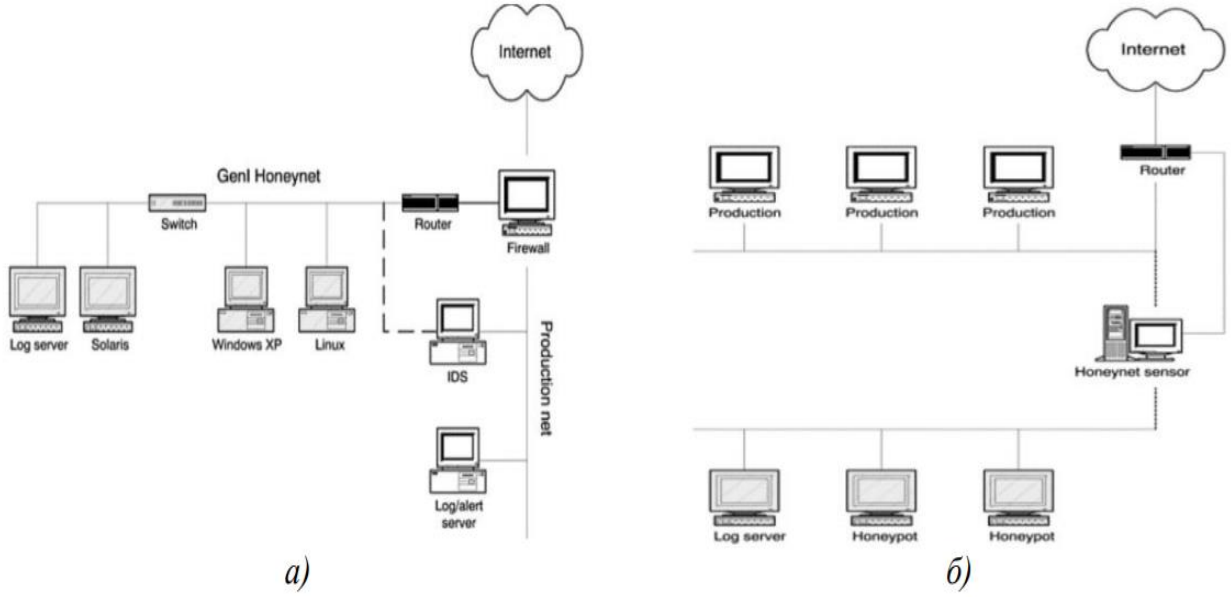


Рис. 1. Типова Honeynet-мережа: а) I-го покоління; б) II-го покоління Gen III Honeynets

Технологія Gen III реалізує подальше удосконалення і розширення можливостей контролю і аналізу даних. Модель аналізу даних базується на таки абстракціях: хости, процеси, мережеві потоки і файли (рисунок. 2). Такий підхід реалізується на основі використання системи Honeywall, розроблений фахівцями проекту Honeynet Project. Для контролю підключень і даних застосовується підхід IP Performance Measerment Working Group, що полягає в моніторингу потоків. У випадку використання Honeywall для цього застосовується система Argus [5]. Іншим удосконаленням є використання засобу пасивного зняття зліпку системи (passive fingerprinting), що ініціює TCP-підключення. Для об’єднання цих двох типів даних (активність в ІКС і процесів на хості) навколо суцільної картини концепції потоків мережі використовують додаткову зв’язуючу ланку. Для цього застосовують систему Sebek, що проводить моніторинг активності в мережі з перспективи

хоста [6]. У роботі виконано моделювання Honeynet Gen III у віртуальному середовищі UML, а праця містить варіант віртуалізації повноінтерактивних приманок.

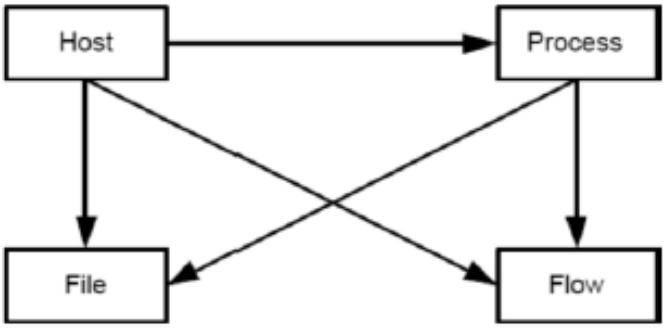


Рис. 2. Модель взаємозв'язків даних у системі Gen III

Висновок: подібно до всіх технологій, у honeypots є свої недоліки, найбільший з них – обмежена сфера їх перегляду. Honeypots захоплюють лише активність, спрямовану проти них, і буде пропускати напад на інші системи.

З цієї причини фахівці з безпеки не рекомендують ці системи, щоб замінити існуючі технології безпеки. Замість цього, вони бачать honeypots як додаткову технологію захисту від вторгнення.

Переваги, які приносять honeypots для захисту від вторгнень, важко ігнорувати, особливо зараз, коли починають розгортатися виробничі honeypot. З часом, коли розгортання розповсюдиться, honeypots можуть стати важливим компонентом операції безпеки на рівні підприємства.

Література

1. Мережні хробаки [Електронний ресурс]. Режим доступу: https://studfiles.net/preview/5206321/page:10/, вільний;
2. Spitzner, L. (2002), Honeypots: Tracking Hackers, 1st edition, Addison-Wesley, Boston, MA.
3. Know Your Enemy: Learning about Security Threats / Honeynet Project. — NY.: Addison-Wesley Professional, 2004. — 800 p.
4. Deal R. Router Firewall Security / R. Deal. — SF. : Cisco Press, 2004. — p. 912.
5. Argus and Infiniband [Електронний ресурс]: (ARGUS – Auditing Network Activity) // QoSient — Режим доступу: http://www.qosient.com/argus, вільний;
6. Balas E. Honeynet data analysis: A technique for correlating sebek and network data / E. Balas // Workshop on Information Assurance and Security US Military Academy, West Point, NY. — IEEE, 2004.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ МЕТОДОМ КОМПЛЕКСНОЇ ЕКСПЕРТНОЇ ОЦІНКИ

Володимир Воскобойник, Іван Лагунов

Запорізький національний технічний університет, м. Запоріжжя, Україна

It is proposed to assess the security of information processing systems using a comprehensive expert evaluation based on metric characteristics. Such an approach will provide an effective solution to the problem of choosing, optimising and evaluating through the integrated use of different methods for quantifying the quality of alternative variants.

Keywords: security of information processing systems, expert estimates, metric characteristics.

Забезпечення системи безпеки інформаційних систем обробки інформації є богато альтернативною та залежить від якості експертної оцінки того, чи іншого критерію. При виборі систем в основному використовуються дві групи методів, заснованих на вирішенні однокритеріальної, чи багатокритеріальної задач.

Серед найбільш застосовуваних методів вирішення цих задач слід виділити:

- неевристичні (формальні) - методи введення метрик в просторі та методи згорток метричних характеристик;
- евристичні (неформальні) - метод безпосередньої оцінки, метод ранжирування та метод парних порівнянь.

Доцільність такої класифікації зумовлена тим, що надається можливість визначення області вибору найбільш прийнятного методу з відомих на даний час, та є можливість сформувати передумови для розробки нових методів (суміщення, модифікації, комплексування і т.п.).

Як показав проведений аналіз, що застосування методів розрахунку комплексної оцінки, які засновані на згортках метричних характеристик, методів введення метрик в просторі нормованих метричних характеристик та методів експертних оцінок перетинаються. Це свідчить про те, що кілька методів можуть бути застосовані до однієї і тієї ж задачі, а це обумовлює невизначеність у виборі методу рішення.

Найбільш доцільним для вирішення даного завдання є "експертний" підхід, який дозволяє проводити оцінку якості систем всіма допустимими методами з розглянутих, і за її результатами сформувати матрицю «вторинних показників», а для її обробки застосувати методи експертних оцінок.

Але, не існує універсального, або найбільш приємного методу для всіх альтернатив безпеки систем обробки інформації.

Зазначені вище методи не дають чіткого розуміння: що і як робити при створенні систем безпеки. Вони мають ряд недоліків, але в цілому призводять до близьких результатів.

Слід відзначити, що методи «вторинних показників» обробки (ранжування, або парні порівняння) пропонується проводити за кількістю оцінюваних систем (об'єктів) і малій відмінності між ними. При цьому, за критерій вибору пропонується брати «число оцінюваних систем (об'єктів)» - *k.* Якщо кількість об'єктів, що ранжуються $n < k$ – метод ранжування, а при $n > k$ – метод парних порівнянь.

Метод безпосередньої оцінки застосовується у випадках, коли об'єкти експертизи, що визначають кінцеві результати, що піддаються безпосередньому порівнянні, так як мають однакову природу, тобто у них є загальний еталон порівняння. Метод безпосередньої оцінки дозволяє врахувати ступінь переваги якого-небудь одного показника по відношенню до інших. При визначенні узагальненого показника ефективності, помилкова оцінка експертом може призвести до значного спотворення кінцевого результату.

Метод ранжирування і його різновиди можуть застосовуватися в разі необхідності впорядкувати будь-які об'єкти або явища в часі, або просторі. Ця ситуація виникає, коли необхідно визначити не ступінь виразності будь-якої їх якості, а лише взаємне просторове, або тимчасове розташування цих об'єктів; при необхідності впорядкувати об'єкти відповідно до будь-якої якості, але при цьому не потрібно проводити його точне вимірювання; якщо яка-небудь якість вимірювальна, але в даний момент не може бути виміряна з причин практичного або теоретичного характеру.

При використанні методу ранжирування на отримання кінцевого результату впливає правильний вибір його різновиди для конкретної ситуації. Точність і надійність процедури ранжирування в значній мірі залежать від кількості об'єктів. Чим більше таких об'єктів, тим нижче їх «розрізнення» з точки зору експерта, а, отже, тим менш надійно можна встановити ранг об'єкта, що є істотним недоліком методу.

До основних недоліків методу ранжирування можна також віднести втрату інформації про оцінювані об'єкти внаслідок впорядкування їх лише за взаємним розташуванням без урахування ступеня виразності будь-якої їх якості. Тому метод ранжирування рідко використовується в «чистому вигляді». Найчастіше він поєднується з іншими методами, що забезпечують більш чітке розходження між об'єктами. Одним з них є метод безпосередньої оцінки і деякі його різновиди (ранжування за порівнянною шкалою).

Метод парних порівнянь застосовується у випадках виявлення переваг для великого числа об'єктів та у випадках, коли відмінності між об'єктами настільки малі, що безпосередня оцінка або ранжування не забезпечують їх розумного впорядкування. Метод парного порівняння без додаткової обробки і ряду обмежень не дає повного упорядкування об'єктів, що є його суттєвим недоліком.

Розглянуті вище три методи рішення (безпосередньої оцінки, ранжирування і парного порівняння) володіють різними якостями, але призводять до близьких результатів. Тому вибір методу «вторинної» обробки (ранжування, або парні порівняння) пропонується проводити за кількістю оцінюваних об'єктів і малій відмінності між ними. Так як поняття «мала відмінність» не є чіткою фізичною величиною, а її визначення потребує додаткових досліджень, то за критерій вибору пропонується брати «число оцінюваних об'єктів» *(k).* Якщо кількість об'єктів *n*, що ранжуються $n < k$ – метод ранжування, а при $n > k$ – метод парних порівнянь.

Враховуючи вищевикладене, очевидно, що підвищити достовірність та стійкість результату можливо за рахунок отримання комплексної оцінки за результатами розв'язання задачі вибору способу обробки таких результатів.

В якості такого способу і пропонується використовувати метод комплексної експертної оцінки, що забезпечує ефективне рішення за рахунок отримання стійкого результату за сукупністю методів та полягає в наступному.

На начальному етапі проводиться опис порівнюваних систем, кожна з яких представлена вектором характеристик, тобто задається початкова матриця $\boldsymbol{A}\ (m \times n)$, де m – число порівнюваних варіантів систем (рядків матриці $\boldsymbol{A}$), n – число характеристик (стовпців матриці $\boldsymbol{A}$).

Кожен елемент матриці $\boldsymbol{A}$ є значення характеристики $\boldsymbol{X}ji,\ j=1,m,\ i=1,n,$ тобто $\boldsymbol{X}ji$ є значення i-й характеристики j-го варіанту системи.

Далі задається деяке нормуюче відображення безлічі характеристик варіантів систем

$$\{\boldsymbol{X}\,ij\} \xrightarrow{F} \{\boldsymbol{K}\,ij\}\ (i=1,\ n,\ j=1,\ m),$$

де $\boldsymbol{X}ij$ – i -я характеристика j -й системи;

$\boldsymbol{K}ij$-оцінка якості j-ї системи по i-й властивості.

Результатом такого відображення F є матриця $\boldsymbol{A}'(m \times n),$ де m – число порівнюваних варіантів систем (рядків матриці $\boldsymbol{A}'$), n – число показників якості за різними властивостями системи (стовпців матриці $\boldsymbol{A}'$). Таким чином, кожний елемент матриці $\boldsymbol{A}'$

є значення показника якості системи по $\boldsymbol{X}_{ji}$, j=1, m, i=1, n, тобто $\boldsymbol{K}_{ji}$ являється значенням i -го показника j-го варіанту системи.

Запропонований метод комплексної експертної оцінки рекомендується застосовувати в випадках, коли методи згорток, метрик та експертних оцінок в «чистому» вигляді не підходить для рішення даної задачі.

Таким чином, метод комплексної експертної оцінки дозволяє мінімізувати ризик прийняття неправильного рішення при проектуванні систем безпеки інформаційних систем за рахунок комплексного використання різних методів кількісної оцінки якості альтернативних варіантів.

Література

1. Уайдл Д. Оптимальное проектирование: Пер. с англ. – М.: Мир, 1981. – С. 156.
2. Макаров И.М., Виноградская Т.М., Рубчинский А.А., Соколов В.Б. Теория выбора и принятия реений. – М.: Наука, 1982. – С. 328.
3. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. – М.: Статистика, 1980. – С. 263.

ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ І АНАЛІЗУ КОНФІДЕНЦІЙНИХ ДАНИХ В DLP-СИСТЕМАХ

Олег Вацлавик, Христина Явин

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The prevalence of information security (Gartner claims that about a third of companies already use DLP) removes only one part of the problem-random leakage-do not affect malicious behavior. The question here is faster in the perception of DLP-systems as a software capable of independently, without the efforts of the security services of information, to deal with leaks, which is fundamentally wrong.

Keywords: DLP systems, digital imprints, artificial Intelligence, linguistic method.

В DLP-системах зазвичай використовуються три методи ідентифікації: імовірнісний, детерміністський і комбінований. Системи, засновані на першому методі, здебільшого використовують лінгвістичний аналіз контента і «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацьовувань. Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм не вистачає гнучкості. Комбінований підхід поєднує обидва методи з аудитом середовища зберігання і обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації.

У системах DLP застосовуються складні механізми аналізу: порівняння по шаблонах з використанням словників і регулярних виразів, лінгвістичний і контекстний аналіз, цифрові відбитки. Словники і шаблони зручно застосовувати в конкретних областях, наприклад, для контролю номерів кредитних карт і інших персональних даних.

У лінгвістичному і контекстному аналізі використовуються морфологія і статистичні моделі, враховується контекст, характер відправника і одержувача інформації. Цей метод хороший для динамічних даних. Цифрові відбитки (аналогічні сигнатурам в антивірусних продуктах) підходять для контролю статичних даних, наприклад, для захисту інтелектуальної власності.

Через DLP-систему проходять всі інформаційні потоки підприємства, і система повинна визначати, чи відноситься інформація, що передається до тієї, що захищається. Для цього використовують наступні технології:

− Сигнатури – пошук в потоці даних "заборонених" слів, послідовності символів ("стоп-слів");

− Лінгвістичні методи – працюють із словоформами, аналізують весь текст (наприклад, визначення частоти зустрічальності термінів);

− Цифрові відбитки – хеш-функції зразків конфіденційних документів;

− Регулярні вирази – дозволяють знаходити збіги за формою даних (а не за самими даними), типу номерів кредитних карток;

− Мітки – установка на файли, що містять конфіденційну інформацію, спеціальних «міток»;

− Штучний інтелект – самонавчальний алгоритм аналізу даних "Vector Machine Learning".

Методом аналізу є пошук в потоці даних деякої послідовності символів («стоп-слів»). У переважній більшості випадків сигнатурні системи налаштовані на пошук декількох слів і частоту зустрічальності термінів.

Метод аналізу масок є розширенням функціонала пошуку сигнатур і є пошуком такого змісту, який неможливо точно вказати в базі "стоп-слів", але можна вказати його елемент або структуру. До такої інформації слід віднести будь-які коди, які характеризують персону або підприємство: ІНН, номери рахунків документів і так далі. Шукати їх за допомогою сигнатур неможливо.

Лінгвістичний метод аналізу тексту несе на собі характеристику всього класу методів аналізу вмісту. З погляду класифікації хеш-аналіз, аналіз сигнатур, аналіз масок – є "контентною фільтрацією", тобто фільтрацією трафіку на основі аналізу вмісту.

Технологія лінгвістичного аналізу дозволяє автоматично визначати тематику і ступінь конфіденційності аналізованого фрагмента інформації на підставі термінів, що зустрічаються в ньому, і їх поєднань. Лінгвістичний аналіз виконується на основі заздалегідь створеної бази контентної фільтрації (БКФ).

База контентної фільтрації – це база даних, яка представляє собою виділений на основі імовірнісних і математичних методів ієрархічно організований список (дерево) категорій з довільною кількістю вкладених рівнів, і що містить слова і вирази, наявність яких в документі дозволяє визначити тематику і ступінь конфіденційності інформації.

БКФ не тільки описує категорії інформації, яка циркулює в компанії, але і враховує різні атрибути її конфіденційності, в т.ч. специфіку діяльності компанії, її вимоги до безпеки.

Результатами проведення лінгвістичного аналізу тексту автоматично привласнюються ті або інші категорії, відповідні його тематиці і змісту. У аналізованій інформації можуть зустрітися терміни (слова і словосполучення) з різних категорій, тому вона може бути віднесена до однієї або декількох категорій БКФ.

База контентної фільтрації і точність детектування конфіденційної інформації

Надійність і точність ідентифікації конфіденційних даних в корпоративних інформаційних потоках за допомогою технології лінгвістичного аналізу залежать від бази контентної фільтрації, на основі якої здійснюється аналіз.

Тому важливо створити базу, яка забезпечить надійні результати фільтрації інформації за категоріями. Основним методом лінгвістичного аналізу за допомогою БКФ є пошук в аналізованому фрагменті інформації слів і словосполучень, що описують конфіденційні дані і структурованих за категоріями.

Література

1. В. Мирошниченко, Д. Ходоров, Е. Щеглова DLP-решения: Как помешать торговле корпоративными секретами [Електронний ресурс] // Інвестгазета №14 10.05.2011 – Режим доступу: https://investgazeta.delo.ua/ praktika/dlpreshenija-kak-pomeshat-tor-273582/
2. DLP-решения - информационная безопасность – Режим доступу: http://securitysoftline.ru
3. А. Прозоров ALL ABOUT DLP [Електронний ресурс] – Режим доступу: http ://bis-expert.ru/blog/ 2560/51911
4. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с.

ДЕЯКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Анатолій Костенко, Василь Плеша, Володимир Бабич

Львівський торговельно-економічний університет, Львів, Україна

Summary. In this article the author describes the technology of cloud computing, analyses the main tasks and the principles of its informational safety, defines the perspective of the development of this technology and the safety's options.

Keywords: cloud computing, informational safety, technology, infrastructure.

Інтенсифікація інноваційних процесів, розвиток інформаційних технологій, їх проникнення в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Проблеми захисту інформації потребують комплексного підходу, тобто створення системи інформаційної безпеки (ІБ).

Сучасні підприємства знаходяться під постійним впливом факторів, пов'язаних із розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, проте, з іншого – зумовлюють проблеми, пов'язані насамперед з інформаційною безпекою.

У разі виникнення ризиків у роботі проблема інформаційної безпеки в системі хмарних обчислень перетворюється в критичний елемент системи. Розглянемо деякі аспекти інформаційної безпеки «хмар».

Управління проблемами безпеки за допомогою віртуальної пам'яті.

Технологія віртуальних машин демонструє очевидні переваги, вона сприяє роботі сервера, який залежить не від фізичного пристрою, а від віртуальних серверів. У віртуальних машинах зміна фізичних параметрів або їх переміщення не впливають на надані постачальником послуги. Якщо користувачеві необхідно більше послуг, постачальник може задовольнити потреби користувачів без втручань в устаткування. Існує можливість взаємної атаки, що веде до загрози захисту віртуальних серверів.

Аутентифікація користувачів та параметрів доступу.

Концепція хмарних обчислень побудована на новій конфігурації.

Вимоги до безпеки на основі аналізу HDFS.

Принципи захисту даних.

Модель захисту даних.

У моделі використовується тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях «хмари».

Надійність.

Перехід до хмарних технологій вимагає значного підвищення вимог до якості надання послуг доступу до Інтернет, які стають критично важливими. Найбільше в цьому питанні розвинулись американські провайдери. В американській практиці прийнято публікувати у відкритому вигляді деталізовані зобов'язання з дотримання якості надання послуг, які прописані в угодах про рівень обслуговування (Service Level Agreements). У випадку, якщо оператор не виконує своїх зобов'язань, він несе за це фінансову відповідальність.

Перегляд законодавства.

Інтернет став платформою для розподілених додатків: компанія може вести конфіденційний внутрішній документообіг на чужих потужностях, уклавши контракт зі стороннім SaaS-постачальником, який, своєю чергою, буде обробляти отримані дані на обчислювальних потужностях інших постачальників послуг IaaS і/або PaaS. Існуюче законодавство (і зарубіжне, і вітчизняне) практично зовсім не передбачає таких ситуацій.

Регулювання відносин у галузі хмарних технологій – складне завдання ще й тому, що інтереси користувачів, зацікавлених у збереженні контролю над своїми даними, та інтереси постачальників хмарних послуг, зацікавлених у максимальній свободі під час експлуатації та розвитку своїх сервісів, розходяться у протилежних напрямах. Майбутнє хмарних технологій багато в чому залежатиме від розумного компромісу обох сторін.

NIST запропонував набір із десяти базових принципів безпеки для хмарних обчислень:

1. Прозорість. Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність.
2. Обмеження за сферами використання. Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників.
3. Розкриття. Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство.
4. Система управління безпекою. Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002).
5. Додаткові можливості у сфері безпеки. Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних
6. Розміщення даних. Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані
7. Повідомлення про витоки інформації. Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних
8. Аудит. Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам від- повідних стандартів
9. Переносимість даних. Компанії надають замовникам можливість вивантаження даних у стандартному форматі, придатному для передавання через Інтернет
10. Звітність. Компанії співпрацюють із замовниками в адекватному розподілі обов'язків під час складання звітності «Про приватність і безпеку»

Отже, незважаючи на те, що зазначені пропозиції не набули широкої підтримки з боку учасників галузі, найімовірніше, в майбутньому дискусія призведе до вироблення загальногалузевих правил – спочатку в США і Європі, пізніше, а, можливо й одночасно, в інших країнах. Це сприятиме регулюванню інтересів користувачів і постачальників хмарних послуг, та в цілому забезпечуватиме високий рівень безпеки для хмарних обчислень.

Література

Бондар Є. С. Хмарні обчислення та їх застосування / Є. С. Бондар, М. М. Глибовець, С. С. Гороховський // Вісник КНУ ім. Т. Шевченка. – Вип. № 1. – К.: КНУ, 2011. – С. 74–82.

Гриджук Г. С. Систематизація методів інформаційної безпеки підприємства / Г. С. Гриджук. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

Гудзовата О. О. Хмарні сервіси: можливості, безпека, перспективи: колективна монографія: у 4 т. / О. О. Гудзовата // Теоретичні та прикладні аспекти підвищення конкурентоспроможності підприємств. – Дніпропетровськ:«Герда», 2013. – Т. 1 – 352 с. (Розділ 1.12). – С. 102–110.

ПОКАЖЧИК АВТОРІВ

МАТЕРІАЛИ

ІІІ Міжнародної науково-технічної конференції

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СУСПІЛЬСТВІ

29-30 листопада 2018 р.

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

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

Підписано до друку 18.11.2018 р.
Формат 60x84/16. Гарнітура Times New Roman.
Наклад 40 прим.