

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2023

Безпека інформаційних технологій

МАТЕРІАЛИ

XII Міжнародної науково-технічної
конференції

2-4 травня 2023
м. Ужгород (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 трав. 2023 р. К.: НАУ, 2023. 141 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека, а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Національний авіаційний університет
- ДВНЗ «Ужгородський національний університет»
- Казахський національний педагогічний університет ім. Абая
- Кафедра безпеки інформаційних технологій НАУ
- Кафедра твердотільної електроніки та інформаційної безпеки УжНУ
- Наукова школа “Кібербезпека” НАУ
- ГО “Асоціація спеціалістів кібербезпеки”
- ТОВ «Безпека інформаційних систем «Дельта»
- Редакція наукового журналу «Безпека інформації»
- Редакція наукового журналу «Захист інформації»

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Співголови

Максим ЛУЦЬКИЙ, д.т.н., проф.,
ректор Національного авіаційного
університету

Володимир СМОЛАНКА, д.м.н., проф.,
ректор ДВНЗ «Ужгородський
національний університет»

Заступники співголов

Олександр Корченко, д.т.н., проф.,
зав. каф. БІТ НАУ

Василь РІЗАК, д.ф.-м.н., проф.,
зав. каф. ТЕІБ УжНУ

Відповідальні секретарі

Юлія ХОХЛАЧОВА, к.т.н., доц.,
доц. каф. БІТ НАУ

Михайло ПРИГАРА, к.т.н.,
доц. каф. ТЕІБ УжНУ

Марина ПОГОРЕЛОВА,
асистент каф. БІТ НАУ

Члени програмного комітету

Микола КАРПІНСЬКИЙ, д.т.н., проф.,
Університет у Бельсько-Бялій (м. Бельсько-Бяла, ПОЛЬЩА)

Станіслав РАЙБА, д.т.н., проф.,
Університет у Бельсько-Бялій (м. Бельсько-Бяла, ПОЛЬЩА)

Бахитжан АХМЕТОВ, д.т.н., проф.,
Казахський національний педагогічний університет ім. Абая (м. Алмати,
КАЗАХСТАН)

Геворг МАРГАРОВ, к.т.н., доц.,
Державний інженерний університет Вірменії (м. Єреван, ВІРМЕНІЯ)

Володимир МОХОР, д.т.н., проф. чл.-кор. НАН України,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, НАН України
(м. Київ, УКРАЇНА)

Олена ТИМОШЕНКО, д.ф.н. проф.,
Європейський Університет (м. Київ, УКРАЇНА)

Євген ВАСІЛУ, д.т.н., проф.,
Державний університет інтелектуальних технологій і зв'язку (м. Одеса,
УКРАЇНА)

Василь ЦУРКАН, ктн. доц.,
Національний технічний університет України «Київський політехнічний
інститут ім. Ігоря Сікорського» (м. Київ, УКРАЇНА)

ЗМІСТ

Akhetov Bakhytzhana, Lakhno Valeriy, Adilzhanova Saltanat	
Dynamic management of cybersecurity resources based on genetic algorithms.....	9
Віталій Біланич, Олег Шиленко, Василь Біланич, Alexander Feher, Vladimir Komanicky, Василь Різак	
Виготовлення захисних елементів на халькогенідних плівках методом електронної літографії.....	15
Володимир Богом'я, Юлія Літвінова, Максим Залевський	
Деякі особливості машинного навчання, як технології бізнес-аналітики.....	17
Анатолій Давиденко, Олена Висоцька, Володимир Щербина	
Фіксація деструктивної дезінформації в кіберпросторі за участі студентів спеціальності «Кібербезпека».....	19
Сергій Гільгурт	
Використання ПЛІС для захисту кіберфізичних систем енергетики.....	22
Володимир Хорошко, Юлія Хохлачова, Наталія Вишневська	
Алгоритм структурної ідентифікації прогнозуючих моделей.....	23
Богдан Маліцький, Олександр Черепов, Василь Буковецький, Василь Різак	
Полігон для проведення комплексних навчань з багаторівневого захисту від кібератак.....	27
Олег Карабан	
Дослідження та порівняння систем моніторингу комп'ютерних систем і мереж.....	28
Аль-Амморі Алі, Сергій Заворотний	
Оцінка ефективності захисту інформації в транспортній галузі.....	30
Микола Карпінський, Олександр Корченко, Юрій Дрейс	
Побудова моделі первинних параметрів оцінки стану охорони державної таємниці.....	32
Віта Каштан	
Алгоритм шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів.....	34
Юлія Мисло, Михайло Пагіря	
Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів	36
Богдан Савенко, Антоніна Каштал'ян, Наталія Петляк	
Розподілені системи виявлення worm-вірусів.....	37
Роман Ситник, Вікторія Гнатушенко	
Забезпечення безпеки доступу до хмарних обчислень за допомогою блокчейн технологій.....	39
Роман Штонда, Юлія Черниш, Ірина Мальцева	
Захист інформації та кібербезпека в радіорелейних лініях зв'язку	41
Ірина Удовик, Володимир Гнатушенко	

Використання квантового машинного навчання при обробці багатоканальних аерокосмічних зображень.....	42
Дмитро Євграфов, Юрій Яремчук	
Енергоощадне придушення каналів витоку інформації з екранів моніторів на рідинно-кристалічних структурах.....	44
Сергій Зибін	
Ризики в апаратному забезпеченні.....	46
Ольга Васильєва	
Імітаційні моделі при моделюванні інформаційних операцій у соціальних мережах.....	48
Віта Каштан, Денис Іванов, Ольга Коробко	
Кібербезпека віртуальних грошей в епоху цифрової економіки.....	50
Олександр Кручинін, Володимир Святошенко, Дмитро Тимофєєв	
Особливості автоматизованих систем управління дорожнім рухом як об'єктів кіберзахисту.....	52
Володимир Святошенко, Олександр Кручинін, Дмитро Тимофєєв	
Порівняльний аналіз відкритих платформ з кібербезпеки.....	54
Дмитро Тимофєєв, Олександр Кручинін, Володимир Святошенко	
Реалізація архітектури нульової довіри в процесі впровадження системи управління інформаційною безпекою закладів вищої освіти України.....	56
Іван Трикур, Михайло Січка, Олександр Чобаль, Галина Різак, Василь Різак	
Багатофункціональні оптичні елементи на основі бактеріородопсину у системах контролю доступу та інформаційної безпеки.....	58
Роман Гамрецький, Костянтин Зандер	
Аналіз метрик кібербезпеки для оцінювання якості програмного забезпечення в інформаційно-комунікаційних системах.....	60
Roman Karpiuk, Petro Venherskyi	
Using machine learning (ml) to detect threat anomalies for reducing false-positives on the daily cybersecurity operation centre routine.....	62
Valerii Kozlovskiy, Svitlana Nimych, Oleksii Komar	
Use of inhomogeneous lines as a filtering element for design of SHF devices.....	64
Михайло Кищак	
Проект пристрою активного захисту мовної інформації на базі генератора шуму.....	66
Kateryna Nesterenko, Oleksii Nimych, Vladyslav Dudnyk	
Determination of a four-pole transmission line matrix based on a nonuniform.....	67
Євгенія Іванченко, Ігор Іванченко, Ірина Лозова, Євгеній Педченко, Марі Петровська	
Архітектура хмарного рішення для централізованого збору та обробки інцидентів інформаційної	

безпеки.....	69
Пішковцїй Марїя-Ольга, Рїзак Василь	
Молекулярна криптографїя в кїбербїобезпецї	73
Сергїй Базарний	
Удосконалення методики оцїнювання ефективностї психологїчного впливу в інформацїйній операцїї.....	76
Любомир Боценюк, Юрїй Матьовка	
Вїдалений контроль і захист персонального комп'ютера вїд несанкцїонованого доступу на основї телеграм бота.....	78
Валерїй Ворожко	
Безпековї ризики пїд час транспортування носїв тасмної інформацїї гужовим транспортом.....	80
Максим Делембовський	
OSINT – елемент розвїдки в умовах кїбервїйн.....	82
Іванов Денис	
Метод двїйного хешування SHA з додатковим перебором.....	84
Павло Ігнатоля, Ярослав Сивохоп, Василь Рїзак	
Класифїкацїя та аналіз загроз в інтелектуальних транспортних системах.....	86
Каблучко Дмитро	
Захист критичної інформацїйної інфраструктури та банків.....	88
Володимир Лужецький	
Псевдонедетермінований пїдхїд до побудови шифрїв.....	90
В.О. Країнов	
Мережево-центрична парадигма інформацїйної безпеки в автоматизованих інформацїйних системах управлїння вїйськового призначення.....	92
Володимир Шиповський	
Порівняльний аналіз логїчних моделей оцїнювання кїберстїйкостї інформацїйних систем об'єктїв критичної інфраструктури.....	95
Наталїя Петляк, Юлія Хохлачова, Юрїй Кльоц	
Пїдхїд до аналізу вихїдного трафїку.....	97
Єгор Шарай, Георгїй Чупрїн	
Приватнїсть та інформацїйна безпека у соцїальних медїа.....	99
Михайло Пригара, Іван Опїрський, Михайло Рїзак	
Оцїнка виявлених ризикїв інформацїйної безпеки в освїтї в умовах надзвичайних ситуацїй.....	105
Вїталїй Тупкало, Сергїй Черепков	
Сигнатурний метод контролю ходу програм цифрових автоматїв.....	109

Анатолій Грицак, Ігор Абрамчук, В. Саврацький	
Підвищення захищеності Web ресурсу від атак типу Cross-Site Scripting.....	111
Богдан Карачун	
Управління інцидентами інформаційної безпеки за допомогою SIEM.....	113
Павло Павловський, Дмитро Присяжний, Віталій Гудзь	
Виявлення радіозакладних пристроїв за рахунок поєднання методів локалізації за рівнем поля та акустичного зв'язування.....	115
Наталія Попович, Наталія Цуд, Катерина Велтруска, Владімір Матолін, Василь Різак	
Виготовлення та властивості наночастинок азотистих основ нуклеїнових кислот для молекулярної криптографії.....	117
Ольга Салієва, Василь Карпінєць, Ірина Бондаренко	
Підвищення захищеності Web-ресурсів стійкими криптоалгоритмами на основі генераторів випадкових чисел.....	119
Анатолій Шиян, Михайло Тюльпін, Яна Яремчук	
Перспективи використання методів розмежування доступу в інформаційному протиборстві.....	121
Василь Буковецький, Юрій Тягур, Тетяна Матьовка	
Інструменти для зневадження клієнт-серверних застосунків.....	123
Марина Саєнко	
Виникнення загроз у кіберпросторі як результат технологічного розвитку суспільства.....	124
Lakhno V., Malyukov V., Akhmetov B., Alimseitova Zh., Ogan A.	
Strategy of countering phishing attacks on the cryptocurrency exchange as part of the endless antagonistic game scheme.....	127
Юлія Хохлачова, Алла Гаврилова	
Проблеми безпеки інформації в сучасних інформаційно-комунікаційних системах та мережах.....	128
Людмила Ковальчук, Роман Олійников, Юрій Беспалов, Ганна Неласа	
Розвиток криптографічних протоколів анонімної маршрутизації в Інтернет.....	130
Dora Sabov, Pavlo Mulesa, Marianna Sharkadi	
The State of Cyber Security of Ukraine During a Full-Scale Intrusion.....	132
Віталій Носов, Василь Лучик, Тетяна Колісник, Сергій Калякін, Віталій Світличний	
Оцінка реалізації розподіленого криптоаналізу в умовах обмежених ресурсів.....	134
Євгенія Галич, Владислав Павленко	
Штучний інтелект Chat GPT: можливості та загрози технологічної новинки.....	138

UDC 32.973.202 (004.8)

**DYNAMIC MANAGEMENT OF CYBERSECURITY RESOURCES
BASED ON GENETIC ALGORITHMS****Akhmetov Bakhytzhana, Lakhno Valeriy, Adilzhanova Saltanat**

Kazakh National Pedagogical University named after Abai¹,
National University of Bioresources and Occupational Sciences of Ukraine²,
Al-Farabi Kazakh National University³

¹b.akhmetov@abaiuniversity.edu.kz, ²lva964@nubip.edu.ua,

³asaltanat81@gmail.com

The report examines methods, models and information technologies for the dynamic management of cybersecurity resources. The relevance of the study is determined by the need to optimize the indicators of information security tools of the object of informatization (OBI) in the conditions of dynamic confrontation with the attacking party. The solution to the problem is seen in the optimal distribution of limited financial resources of the OBI management between the objects of protection, taking into account the actions of the attacker.

The problem of dynamic resource management of the OBI protection side is not only a purely technical task, which is solved by increasing the number of protection components in the cybersecurity circuits (KB) of the OBI. But it's also a management challenge. Moreover, the second component of the tasks is associated with such a concept as information security management (IS) and KB, the main task of which is to optimize not only technical, but also economic indicators of the effectiveness of the functioning of information security tools (SIR) for OBI [1].

The criterion of optimality can be one (or several) indicators of information (cybernetic) security - the amount of damage from the implementation of information threats, total costs, which include damage from information leakage and the cost of its protection, profit from investments in information protection, etc. At the same time, it is quite difficult, and often impossible, to achieve optimal values of various indicators due to the inconsistency of their requirements. As a result, we come to a multi-criteria problem [2].

The solution of the task is complicated by a number of reasons. The main one is due to the fact that the search for the optimal solution is conducted in conditions of uncertainty, when the actions of the opponent can be assumed only with a certain probability, and sometimes it is impossible at all. Under these conditions, the search for the optimal distribution of limited resources between the objects of information protection (IR) is possible through the use of game-theoretic methods and taking into account the dynamics of changes in conditions, which will reduce the vulnerability function of the objects of protection to a minimum [3].

The winnings of each side depend on the opponent's strategies and are determined by the objective function. $o(h, d)$. The objective function for the attacker and the

defense side can be as follows: $o(h_k, d_k) \rightarrow \max$, $o(h_k, d_k) \rightarrow \min$.

The amount of damage caused can be estimated, for example, by the cost of an information resource (IR). The amount of damage will depend on the distribution of the resources of the parties.

The strategy of the attacker (attackers) is to distribute his resources between objects in different ratios:

$$\{h_{ik}\} = (h_1, h_2, \dots, h_l), \sum_{k=1}^l h_k = H, h_k \geq 0, \quad (1)$$

where is k – object number of protection ($k = \overline{1, l}$), h_k – costs (resources) for the implementation of threats at the facility k ; l – is the number of objects of protection, H – is the total number of attack resources; i – the current number of the object of attack.

Similarly, the defence applies its resource allocation strategy:

$$\{d_{jk}\} = (d_1, d_2, \dots, d_l), \sum_{k=1}^l d_k = D, d_k \geq 0, \quad (2)$$

where is d_k – costs (resources) for the implementation of protection on site k ; D – total number of protection resources; j – the current number of the object of protection.

For the selected game model, the target function expresses the damage caused by the implementation of threats and has the form:

$$o(h_k, d_k) = \sum_{k=1}^l o_k(h_k, d_k) = \sum_{k=1}^l g_k p_k v_k(h_k, d_k), \quad (3)$$

where is $k = \overline{1, l}$ – Object number for protection;

h_k, d_k – accordingly, resources of attack and defence;

g_k – relative value of IR on k – object;

p_k – the likelihood of an attack on a IS facility;

$v_k(h_k, d_k)$ – vulnerability k – IR object is considered as a probability of a successful attack and depends on the costs of attackers and the cost of protecting the object.

Values $o(h, d)$, $o_k(h, d)$, g_k are attributed to the entire value of the IR.

The first step is to find the parameter values and the form of the dependencies that are included in the objective function (3).

When establishing dependencies $v(h, d)$ the following considerations were taken into account. The probability of a successful attack is directly proportional to the cost h to carry out the attack and inversely proportional to the costs d to protect the object. Therefore, variables h, d must be included in the expression for $v(h, d)$ as an attitude $r = h/d$.

It is clear that dependencies $v(h, d)$ must meet the following conditions:

$$\text{at } r = \left(\frac{h}{d}\right) \rightarrow 0, v(h, d) \rightarrow 0; \text{ at } r = \left(\frac{h}{d}\right) \rightarrow \infty, v(h, d) \rightarrow \infty.$$

These conditions are satisfied by the power functions of the species:

$$v(h, d) = \frac{r^n}{r^n + a}, \quad (4)$$

where a and n are constants that determine the position and shape of the curves.

The solution of the objective function (3) in the analytical form is very difficult.

Its solution is greatly influenced by vulnerability $v(h, d)$ object, which is considered as the probability of a successful attack and depends on the costs of the attackers and the cost of protecting the object. However, knowing the values of the parameters and the form of dependencies that are included in the expression for vulnerability (4), we can replace the procedure for solving the objective function with finding the parameters a and n .

The task of establishing the form of dependence of the probability of a successful attack on the ratio of attack and defense resources is quite complex and is solved separately for each specific system. In our case, the form of dependence was established on the basis of expert assessment of specialists in the field of information protection of Ukraine and the Republic of Kazakhstan and defined as a power function of the species (4). At $n = 1$ it expresses a fractional-linear dependence, with $n > 1$ – fractional-nonlinear [4].

The following is the initial data for solving this task on the example of a parameter study , which affects the degree of vulnerability of the IR to the OBI.

Consolidated list of works to ensure the protection of information on the OBI (to determine the maximum value of a)

1. Design, development and deployment of an integrated SPI (A).
2. Improvement of the information security system (ISS) (B).
3. Identification of information security incidents, incident response, risk forecasting for OBI (S).
4. Minimization of connections between individual objects of IR and unification of components of IR (D).

5. Development of organizational measures of IR, corresponding to the specifics of the business processes of OBI (E).

Grouping of allocated resources by object of expenditure (types of resource investment in IR and KB)

1. Material and financial costs for IR (MFC).
2. Human resources involved in projects to provide IR and KB OBI (HR).
3. Costs of project management in the field of IR and CC OBI (CM).
4. Other costs for the provision of IR and CC OBI (RS).

Competitive advantages from the implementation of events IR and CC for OIB (optimality criteria)

1. Improving competitiveness and new markets (COP, $k=1$).
2. Development of innovations and introduction of digital technologies in business processes (IN, $k=2$).
3. Reduced IT costs (RI, $k=3$).

The optimality criterion in the process of determining the parameters can be described as:

$$F_k = \sum_i \sum_j I_j \cdot E_{ijk} \cdot X_{ijk} \rightsquigarrow \max,$$

where k is the number of the optimality criterion; $k=1,2,3$;

I_j – priority (importance) in the chosen optimal option for the allocation of resources

of the defense side, $\sum I_j = 1$;

$i = 1(A), 2(B), 3(C), 4(D), 5(E)$ – types of work type from the list of works, may vary depending on the characteristics of the OBI;

$j = 1$ for MFC, $j = 2$ for HR, $j = 3$ for storage, $j = 4$ for RS – types of investment investments (resources);

X_{ijk} – variable, equal to 1, if the work (i) from the list of works is used to implement the investment investment (j) . Otherwise, we accept – 0;

E_{ijk} – work efficiency of the type (i) from the list of works that are performed for the implementation of the investment (j) that provides an optimality criterion;

\rightsquigarrow – non-strict achievement of the optimal parameter value a .

Restrictions on the allocated resources available to the company can be set as follows:

$$Q = \sum_i \sum_j I_j \cdot I_{ijk} \cdot X_{ijk} \leq A_j,$$

where is l_{ijk} – resource costs (j) (or labor intensity), which are associated with the performance of work of the type (i) that provides an optimality criterion k ;
 A_j – resource investment restriction (j) , which are related to the performance of work of the form (i) that provides an optimality criterion k .

The constraints that determine the structure of the solution of the problem (or the arrangement of values 0 and 1 in the decision matrices) are described below.

Restriction $\sum_i X_{ijk} \geq 1.$ means that in the direction of resources, for

At least one of the works of the optimality criterion is used according to the list of works:

Restriction $\sum_j X_{ijk} \geq 1.$ means that in the course of operation of the (j) for k – th criterion of optimality, resources (i) use at least once.

Restriction $\sum_k X_{ijk} \geq 1.$ means that any kind of work of the type (i) in any direction of resource allocation (j) must participate in the formation of at least one k – the optimality criterion [5].

To solve the problem of finding rational parameters a and n that are part of the objective function, it is proposed to use a modified genetic algorithm. This algorithm, along with their known advantages, evaluates the fitness of the chromosome to solve the multi-criteria problem of optimizing the allocation of resources of the defense side with fuzzy relationships (calculates the attractiveness of the solution) based on the Bellman–Zadeh principle. This makes it possible to solve the optimization problem under the condition of the evolution of the system from the current state to some finite one and, accordingly, to move from solving the original multi-step optimization problem to the sequential solution of several one-step optimization problems, for example, by determining the parameters a and n .

Forsituations, where the number of ICS nodes is large enough, it is quite a laborious process to solve in parallel the problem of selecting, optimiRng and redistributing all the resources of the defense side tolassic methods. Therefore, it is proposed to apply a composite genetic algorithm to solve this problem. The essence of its application is that at the first stage a genetic algorithm (GA) is involved in solving the problem, and at the second stage, the solution found with the help of GA can be improved by the method of branches and boundaries (MGA) [6].

In the course of computational experiments, a comparative analysis of the composite algorithm (GA + MGA) with the classical GA, "greedy" and the exact brute force algorithm was carried out. To evaluate the above algorithms, test sets from 5 to 150

items (SIR) in a set were formed. 5 series of 30 experiments per series were conducted, a total of 150 computational experiments. Computational experiments were performed on a PC with an Intel i7 9750H processor (2.6 – 4.5 GHz).

The expected solutions, which were obtained using the exact method of full search, turned out to be more accurate. But the operating time of such an algorithm, even taking into account the use of i7 processors, is 17-25 times greater than for GA or GA + MVG. It was found that the composite genetic algorithm is characterized by a sufficiently high efficiency and speed. The time spent on solving the problem when using it is about 16-25 times less compared to the indicators of the method of branches and boundaries. The greedy algorithm is inferior to both the GA and the method of branches and boundaries in terms of adaptability to solving a multi-criteria optimization problem, taking into account the restrictions imposed and the number of variables.

Literature

1. Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In *Proceedings of the Computational Methods in Systems and Software* (pp. 162–171). Springer, Cham.

2. Sviridov, V. I., & Moiseev, S. I. (2019). Mathematical models of the optimal distribution of protective resources by sources of information threats. *Bulletin of the Voronezh Institute of High Technologies*, (1), 110-112.

3. Grischuk, R. V. (2012). The use of differential games to optimize control in information security systems / Grischuk R.V., Khoroshko V.A., Khokhlacheva Yu.E. *Modern information protection* (2), pp. 21–26.

4. Akhmetov, B. , Lakhno, V. , Yagaliyeva, B. , Oshanova, N. , Adilzhanova, S. Conceptual Diagram of An Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems. *Journal of Theoretical and Applied Information Technology* this link is disabled, 2021, 99(18), pp. 4297–4310.

5. Lakhno, V. , Adilzhanova, S., Kryvoruchko, O., Desiatko, A., Buriachok, V. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. *Lecture Notes in Networks and Systems*, 2021, 228, pp. 41–53.

6. Lakhno, V., Bereke, M., Adilzhanova, S., Desiatko, A., Palaguta, K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. *Journal of Theoretical and Applied Information Technology*, 2022, 100(7), pp. 1693–1705.

УДК 621.395.7 (043.2)

ВИГОТОВЛЕННЯ ЗАХИСНИХ ЕЛЕМЕНТІВ НА ХАЛЬКОГЕНІДНИХ ПЛІВКАХ МЕТОДОМ ЕЛЕКТРОННОЇ ЛІТОГРАФІЇ

**Віталій Біланич¹, Олег Шиленко², Василь Біланич¹,
Alexander Feher², Vladimir Komanicky², Василь Різак¹**

*Ужгородський національний університет¹, vbilanych@gmail.com,
Pavol Jozef Šafárik University, Kosice, Slovakia²*

Використання спеціальних захисних елементів, які наносяться безпосередньо на носій інформації є одним із способів технічного захисту інформації. Створення таких елементів може бути реалізовано літографічними методами: необхідно створити майстер-голограму, тобто записати індивідуальне голографічне зображення - логотип, напис, візерунок тощо. У даній роботі представлені дослідження формування мезо- та наномасштабних структур та зображень захисних елементів на поверхні халькогенідних плівок методом сухої електронної літографії

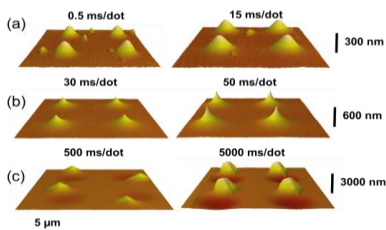


Рис. 1. Зміна форми наведеного рельєфу поверхні плівки

$\text{Ge}_9\text{As}_9\text{Se}_{82}$ товщиною 3 мкм зі збільшенням часу експозиції (а – інтервал малих доз електронного опромінення (б) – інтервал

У даній роботі наведені результати досліджень формування поверхневого рельєфу під час взаємодії електронного пучка (ЕП) з плівками халькогенідів. Плівки опромінювали ЕП за допомогою скануючого електронного мікроскопа (Tescan, модель VEGA) в діапазоні доз $G=9,3 \times 10^3 - 9,3 \times 10^7$ мкКл/см². Рельєф поверхні плівки досліджували за допомогою атомно-силового мікроскопа (Bruker, модель ICON). Показана можливість виготовлення майстер-оригіналів захисних елементів за технологією одноступеневої електронної літографії. Встановлено можливість використання халькогенідних плівок різних складів як позитивних, так і негативних електронних резистів. Реалізовано процес виготовлення оригіналу захисного елемента методом сухої електронної літографії на плівках систем Ge-As-Se та As-Se.

Було виявлено, що в цьому діапазоні доз утворюються три різні типи поверхневих особливостей у вказаних матеріалах. В інтервалі доз $9,3 \times 10^3 - 2,8 \times 10^5$ мкКл/см² ЕП індукує утворення конусів із профілем Гауса (висота 250–270 нм). В

інтервалі доз $5,6 \times 10^5 - 1,9 \times 10^6$ мкКл/см² поверхня конуса загострюється, переходячи в конус Тейлора (висота 380-560 нм). В інтервалі доз $4,6 \times 10^6 - 9,3 \times 10^7$ мкКл/см² формується рельєф комбінованої форми. В цьому інтервалі спостерігається утворення кратера глибиною 530 нм і гігантського конуса Тейлора (750-2510 нм) на краю кожного кратера. Механізм формування такого електронно-індукованого поверхневого рельєфу можна пояснити з допомогою двошарової зарядової моделі. Для реалізації процесу електронної літографії були розраховані параметри цієї моделі для плівок систем Ge-As-Se і As-Se. Виходячи з отриманих результатів були виготовлені зображення певного логотипа шляхом електронного опромінення халькогенідної плівки згідно розробленого літографічного процесу.

У якості ресруючого середовища, тобто, електронного резисту, були взяті плівки системи Ge-As-Se і As-Se товщиною 3 мкм, утворені методом термічного випаровування на сапфірову підкладку. Конвертування файлу зображення програмою DrawBeamAdvanced визначило кількість елементів на зображенні, які необхідно було створити на плівці електронним променем. Перед опромінюванням був проведений аналіз щільності елементів зображення, врахований елемент близькості елементів і були підібрані різні параметри електронного пучка для виготовлення різних елементів зображення, зокрема: прискорююча напруга $U = 30$ кВ, діаметр електронного пучка $B = 640$ нм. У залежності від елемента зображення, струм пучка електронів змінювався від 5 нА до 60 нА. Час експозиції змінювали від 0,5 мс до 10 мс на точку. З рисунка видно, що при роздільному опроміненні окремих елементів якість емблеми задовільна.

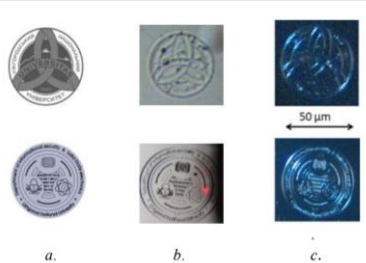


Рис.2. Вид логотипів університету та кафедри ТЕІБ (а) і їх зображення на поверхні плівки As_4Se_96 у відеокамері атомно-силового мікроскопа (б) і після їх металізації (в).

Покращення якості зображення було пов'язане з коректуванням параметрів електронного променя, особливо часу експозиції. Після оптимізації параметрів літографічного процесу, певної кількості спроб запису зображення на плівку на електронному мікроскопі та його огляді в атомно-силовому мікроскопі було отримане зображення емблем прийнятної якості на плівці As_4Se_96 (рис.2). Для створення можливості виготовлення захисних елементів методом холодного тиснення на полімерну основу, на халькогенідну плівку із зображенням логотипів

була нанесена металева плівка з ванадію товщиною 100 нм, яка покрила рельєфне зображення емблеми.

Таким чином, в результаті проведених досліджень встановлена можливість використання даних матеріалів як позитивних так і негативних електронних резистів та розроблено процес створення оригіналів захисних елементів на халькогенідних плівках.

УДК 004.94

ДЕЯКІ ОСОБЛИВОСТІ МАШИННОГО НАВЧАННЯ ЯК ТЕХНОЛОГІЇ БІЗНЕС-АНАЛІТИКИ

Володимир Богом'я, Юлія Літвінова, Максим Залевський

*Київський університет інтелектуальної власності та права
Національного університету «Одеська юридична академія»,
bog2603@ukr.net*

Машинне навчання — це тип штучного інтелекту (ШІ), який дозволяє комп'ютерним системам автоматично навчатися та вдосконалюватися на основі досвіду без явного програмування.

Ключова ідея машинного навчання полягає в тому, щоб комп'ютери могли вчитися та вдосконалюватися з часом за допомогою нових даних. Це досягається шляхом надання комп'ютеру набору навчальних даних, які використовуються для навчання моделі. Потім модель використовує ці навчальні дані для виявлення закономірностей і прогнозування нових даних.

Метою даної роботи є аналіз особливостей використання машинного навчання, а потім використання цих закономірностей для прогнозування або прийняття рішень щодо нових даних, щодо технологій бізнес-аналітики, консолідації інформації та менеджменту знань.

Існує кілька типів алгоритмів машинного навчання, включаючи контрольоване навчання, неконтрольоване навчання та навчання з підкріпленням. Контрольоване навчання передбачає навчання моделі на позначених даних, де вже відомий правильний результат. Неконтрольоване навчання передбачає навчання моделі на немаркованих даних, де алгоритм повинен самостійно ідентифікувати закономірності та зв'язки. Навчання з підкріпленням передбачає навчання моделі методом проб і помилок, коли алгоритм отримує винагороду за прийняття правильних рішень і покарання за прийняття неправильних рішень.

Машинне навчання має широкий спектр застосувань, включаючи розпізнавання зображень і мови, обробку природної мови, системи рекомендацій, виявлення шахрайства та прогнозне обслуговування, моделювання експерименту. Оскільки обсяг доступних даних продовжує зростати, машинне навчання стає все більш важливим у багатьох галузях.

Однією з найпоширеніших пасток у машинному навчанні є перенавчання (overfitting). Вона виникає, коли модель занадто точно підлаштовується під навчальні дані, включаючи шуми та випадковості, що призводить до зменшення її здатності до узагальнення нових, невідомих даних.

В результаті перенавчання модель має дуже низьку помилку на навчальних даних, але погано працює на нових даних. Перенавчання може статися, якщо модель занадто складна або якщо у неї недостатньо даних для навчання.

Існують різні способи запобігання перенавчання, включаючи використання регуляризації, зменшення складності моделі, збільшення обсягу даних для навчання та використання методів валідації для оцінки здатності моделі до узагальнення нових даних.

Існує кілька сучасних методів для боротьби з перенавчанням у машинному навчанні:

Регулювання: це метод додавання штрафу за складність моделі у функцію втрат під час навчання. Це допомагає запобігти моделі від занадто точної відповідності навчальним даним та фокусуватися на більш загальних характеристиках даних.

Виключення (Dropout): це метод, за якого випадково відключаються деякі вузли під час навчання нейронної мережі. Це змушує мережу поклатися на конкретні вузли, що допомагає знизити перенавчання.

Рання зупинка (Early stopping): це метод, коли навчання зупиняється, коли продуктивність моделі на наборі перевірки перестає поліпшуватися. Це допомагає запобігти перенавчанням, оскільки модель не продовжуватиме навчатися, коли її продуктивність на нових даних перестане покращуватися.

Збільшення обсягу даних: більше даних для навчання допомагає запобігти перенавчанням. Якщо модель навчається більшій кількості різноманітних даних, вона може краще узагальнити їх у нові дані.

Методи зниження розмірності: ці методи дозволяють зменшити кількість ознак даних, зберігаючи у своїй найважливіші характеристики. Це допомагає зменшити складність моделі та запобігти перенавчанням.

Крос-валідація: це метод, у якому дані поділяються кілька наборів, і модель навчається одному наборі і перевіряється іншому. Це допомагає оцінити продуктивність моделі на нових даних та запобігти перенавчанням.

Авторами був проведений аналіз літератури стосовно цієї тематиці.

Так, наприклад, у книзі "The Elements of Statistical Learning: Data Mining, Inference, and Prediction" авторів Trevor Hastie, Robert Tibshirani та Jerome Friedman наведено огляд методів машинного навчання та статистичного моделювання, включаючи обговорення проблеми перенавчання та способів її вирішення.

У "Deep Learning" авторів Ian Goodfellow, Yoshua Bengio та Aaron Courville проаналізовано проблема перенавчання та наведено методи боротьби.

"Регуляризація і різновид Selection the Elastic Net" авторів Hui Zou і Trevor Hastie описує метод Elastic Net, який поєднує регуляризацію L1 і L2 для боротьби з проблемою перенавчання.

"Dropout: Simple Way to Prevent Neural Networks from Overfitting" авторів Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever і Ruslan Salakhutdinov описує метод Dropout, який є ефективним способом боротьби з перенавчанням у нейронних мережах.

Також відома "A Few Useful Things to Know About Machine Learning" авторів Pedro Domingos. Ця стаття являє собою огляд методів машинного навчання і містить кілька порад стосовно цієї проблеми.

Найбільший інтерес являє собою "Data Science. Наука о данных с нуля" автора Грас Д., де наведено практичні рекомендації стосовно не тільки проблеми перенавчання даних. Також висвітлені питання вирішення супутньої проблеми недонавчання даних (underfitting), наведені практичні рекомендації покращення моделей із застосуванням мови програмування Python.

Висновок. Автори у своєму дослідженні звертаються до контрольованих моделей (тобто таких, де є сукупність даних, позначена правильними відповідями, на яких відбувається засвоєння); до неконтрольованих моделей (де правильні відповіді відсутні), до напівконтрольованих моделей (де тільки деякі дані позначені правильними відповідями), а також до онлайн-моделей (у яких модель повинна безперервно самоналаштовуватися до даних, що надходять). Інші типи моделей не розглядалися.

Вищенаведені методи можна використовувати як окремо, так і в комбінації один з одним, щоб запобігти перенавчання та покращити продуктивність моделі на нових даних.

УДК 004.056.5

ФІКСАЦІЯ ДЕСТРУКТИВНОЇ ДЕЗІНФОРМАЦІЇ В КІБЕРПРОСТОРИ ЗА УЧАСТІ СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

Анатолій Давиденко¹, Олена Висоцька², Володимир Щербина²

*¹Інститут проблем моделювання в енергетиці ім. Г.С. Пухова НАН
України, davidenkoan@gmail.com,*

²Національний авіаційний університет, lek_yys@ukr.net

В умовах війни актуальними проблемами є виявлення, моніторинг та фіксація російської дезінформаційної діяльності. Ці питання мають політичні, організаційні та технологічні аспекти. Для перемоги на інформаційному фронті принципово важливим є своєчасно виявляти та фіксувати дезінформацію, а також передбачити можливі наслідки для попередження руйнівного впливу цієї дезінформації. Українське суспільство має дуже важливі та необхідні для перемоги властивості самоорганізації, але цілеспрямованість та наполегливість дій принципово залежить від чистоти інформаційного впливу від випадкової або навмисної дезінформації. Необхідною складовою формування суспільства є навчання молоді основам кібергігієни. Студенти та школярі в першу чергу вразливі до інформаційного впливу, тому вони мають бути залучені до процесу виявлення дезінформації, з метою формування у них імунітету до її впливу.

Метою роботи є розробка методичних матеріалів для навчання студентів фіксації деструктивної дезінформації в кіберпросторі.

На останніх курсах бакалаврату студенти технічного напрямку мають достатній досвід використання інформаційних технологій але їм потрібна чітка

фіксація проблеми протидії дезінформації, тому є актуальною задача розробки практичних лабораторних робіт з вияву російської дезінформації.

Розробка лабораторних робіт за тематикою виявлення, моніторингу та фіксації російської дезінформаційної діяльності для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпеки» сприяє залученню молоді безпосередньо до процесу протидії російської дезінформаційної діяльності. Наявність іноземних студентів в групах, які навчаються в рамках навчального курсу Incident Management in Cyberspace (НАУ) робить процес протидії більш публічним та незалежним.

Досвід останніх років показав, що розглядати тільки технологічні аспекти процесу виявлення, моніторингу та фіксації російської дезінформаційної діяльності недостатньо. Крім навчання студентів навичкам пошуку, аналізу та збереження фейкової інформації, необхідним є формування у студентів розуміння ознак фейкової інформації та вміння її виявлення в ручному режимі. Крім того, важливим є навчитись здійснювати пошук першоджерела інформації, визначення головних напрямів інформаційної атаки та вивчення характерних ознак та методів розповсюдження фейкової інформації. Важливим є вмінти своєчасно зафіксувати факт дезінформації. Не менш важливим етапом є навчити студентів навичкам копіювання інформації зі збереженням її автентичності. Це копіювання у вигляді дзеркала веб-сайту з обов'язковою фіксацією дати копіювання та адреси, забезпечення цілісності копії, наприклад за допомогою хешування та накладення цифрового підпису, надійне збереження знайденої інформації в хмарному або грид середовищі.

Але крім цих важливих навичок стандартною помилкою студентів під час виконання лабораторних робіт є помилки при ідентифікації інформаційної атаки. По-перше, це фіксація вторинного джерела дезінформації, по-друге, студенти не завжди відрізняють кібервплив від інформаційного. Тому в цьому році студентам були запропоновані додаткові лабораторні роботи, які наочно показують цю різницю.

Важливим аспектом при проведенні лабораторних робіт є розуміння факту, що інформація це зброя, поводження з якою потребує особливої обмеженості. Намагаючись довести фейковість інформації не можна розкривати критичну інформацію (наприклад ЗСУ має тільки n-NIMARS, а РФ говорить, що знищила їх більше ніж існує насправді). Нажаль невдала спроба протидії може спричинити більше шкоди ніж сама фейкова інформація. Тому важливими є фактори самоцензури та знання наслідків розголошення інформації. Перші місяці війни добре навчили нас, що застосування інформаційних технологій без розуміння що саме вони роблять веде до незворотних втрат.

2023 471_472_Information security inciden... Стрiчка Завдання Люди Оцiнки

Lab_2 Analysis of information attacks on Uk... Дата здачі: 24 бер.

Опубліковано 9 бер.

<p>Var : 1. the banking system as a whole 2. economic relations 3. human rights 4. territorial integrity of the country 5. international relations 6. bank Приват 7. bank Сberбанк 8. ministry of defence 9. government information structure 10. exchange rate 11. energy industry</p> <p>1. describe the problem as a whole 2. formulate the main objectives of the attack 3. find and document fake messages aimed at destabilization (fix the location address (link), download and attach the message image to the work log)</p> <p>Переглянути інструкції</p>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block; margin-bottom: 5px;">6</div> Здали	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block; margin-bottom: 5px;">21</div> Призначено	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block; margin-bottom: 5px;">10</div> Оцінено
---	--	--	---

[Оцінити завдання](#)

Рис. 1. Лабораторна робота Analysis of information attacks on Ukraine з дисципліни «2023 471_472_Information security incident management», НАУ, 2023 рік

Розробка навчально-методичних матеріалів, їх практична апробація та формування групи фахово-підготовленої молоді, вмотивованої на виявлення, моніторинг та фіксацію російської дезінформаційної діяльності є основними результатами цього року.

УДК 004.274:004.056

ВИКОРИСТАННЯ ПЛІС ДЛЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ ЕНЕРГЕТИКИ

Сергій Гільгурт

ІПМЕ ім. Г.Є. Пухова НАН України, hilgurt@ipme.kiev.ua

Цифровізація промислового обладнання та кіберфізичні системи останнім часом все частіше використовуються для підвищення ефективності критичної інфраструктури, зокрема, в енергетичній галузі. Цифровізація електричних підстанцій, які є найпоширенішими об'єктами електроенергетики, відбувається згідно низки стандартів МЕК-61850 «Мережі та системи зв'язку на підстанціях», згідно якого єдиним засобом передачі інформації на всіх рівнях підстанції прийнятий стандарт Ethernet. На жаль, пакетна передача даних і протоколи, що на ній засновані, роблять цифрові підстанції більш вразливими для кібератак. Наявний в ІТ-галузі досвід захисту інформації не може буди безпосередньо застосований до цифровізованих промислових систем, але з низкою поправок його доцільно використовувати. До дієвих засобів протидії загрозам безпеки інформації

відносяться сигнатурні засоби, зокрема, системи IDS/IPS, побудовані за сигнатурним принципом. Прискорити ресурсоємну процедуру множинного розпізнавання патернів в таких системах дозволяють апаратні пристрої на базі ПЛІС.

Метою даної роботи є дослідження можливостей та особливостей використання пристроїв програмованої логіки в якості апаратної платформи для побудови сигнатурних систем технічного захисту інформації в кіберфізичних системах енергетичної галузі.

В результаті аналізу існуючих кіберфізичних систем, знайдено два класи технічних засобів, що містять ПЛІС, на яких можуть бути реалізовані апаратні засоби захисту інформації. По-перше, це системи управління, що використовують такі інтелектуальні технології як нейронні мережі та нечітку логіку, інтелектуальні системи збору даних, частотні перетворювачі для електроприводів тощо. По-друге, деякі "розумні" електронні пристрої (Intelligent Electronic Devices – IED), які також використовуються технологією Smart Grid кіберфізичних систем містять ПЛІС і системи на кристалі. Реконфігурація (оновлення обчислювальної структури) програмованих пристроїв може бути виконано віддалено. Проте даний процес необхідно захистити, оскільки канал зв'язку привносить потенційну вразливість у разі фізичного доступу зловмисника до мережі. В роботі розглянуто безпечний протокол і реконфігуровний модуль на ПЛІС, який використовується для налаштування та моніторингу мережевих IP-адрес. Запропонована полегшена версія протоколу другого рівня, реалізованого повністю апаратно та захищеного криптографічним алгоритмом AES-GCM відповідно до стандарту IEC 61850-90-5.

Висновки. ПЛІС, що задіяні в пристроях промислової автоматки, а також входять до складу інтелектуального цифрового обладнання, можуть бути використані для синтезу в них апаратних систем захисту інформації. Для безпечної віддаленої конфігурації ПЛІС, що використовуються в засобах захисту кіберфізичних систем, необхідно вживати додаткові заходи.

УДК 004.681.3

АЛГОРИТМ СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ ПРОГНОЗУЮЧИХ МОДЕЛЕЙ

¹Хорошко Володимир Олексійович, ²Хохлачова Юлія Євгенівна,

³Вишневська Наталія Сергіївна

Національний авіаційний університет

¹professor@ukr.net,

²yuliiahohlachova@gmail.com, ³nataliia.vyshnevskaya@npp.nau.edu.ua

Прогнозування кіберзахищеності об'єктів є одним із вирішальних наукових факторів формування стратегії та тактики кіберзахисту.

Для прогнозування та моделювання процесів кіберзахисту найбільш прийнятними є статистичні методи, що ґрунтуються на існуючих тенденціях у змінах показників кіберзахищеності.

Моделі прогнозування можуть бути як довгостроковими, так і короткостроковими. Внаслідок широкого ступеня невизначеності в отриманні інформації пріоритетне значення надається короткостроковим прогнозам.

Невід'ємною складовою завдань управління (оптимального, автоматизованого чи на рівні прийняття рішень) є побудова моделей, які описують чи прогнозують поведінку об'єкта, процесу системи. У випадку отримання математичної моделі необхідно вибрати її структуру і оцінити параметри, тобто розв'язати задачу структурної ідентифікації.

Структурна ідентифікація сприймається, як завдання перешкоди структури моделі з мінімальною дисперсією помилки прогнозування.

Існують різноманітні постановки завдання структурної ідентифікації, методи її вирішення та варіанти програмної реалізації, розроблені фахівцями у галузях ідентифікації, прикладного регресійного аналізу та пошуку залежностей.

Більшість методів побудовано різних підходах, що ускладнює порівняльний аналіз визначення умов їх ефективного застосування. Оскільки для завдань управління важливо будувати моделі з меншою помилкою прогнозування, це є основою для порівняння ефективності існуючих підходів.

Найбільш поширеними є дві групи методів, на основі яких будують моделі для прогнозування: описання взаємодії процесів кіберзахисту різного рівня на основі вивчення внутрішніх механізмів функціонування процесів, що моделюються, та представлення отриманих знань; отримання моделей за допомогою оцінювання параметрів за вибірками спостережень із застосуванням регресійного аналізу.

У загальному випадку процес вирішення задачі структурно-параметричної ідентифікації включає наступні основні етапи: завдання вибірки даних до апріорної інформації; вибір чи завдання класу базисних функцій та перетворення даних; генерація різних структур у вибраному класі; оцінювання параметрів генерованих структур та формування безлічі моделей F ; мінімізація заданого критерію та вибір оптимальної моделі f ; перевірка адекватності отриманої оптимальної моделі; ухвалення рішення про завершення процесу.

Перелічені етапи описують довільний процес побудови моделей, причому залежно від апріорної інформації та мети моделювання ті чи інші етапи можуть бути відсутніми.

Для складних об'єктів кіберзахисту та процесів типовою є невизначеність інформації щодо механізму їх функціонування, ступеня інформативності вимірних змінних та властивостей. При цьому необхідно застосовувати формалізовані методи та автоматизовані способи моделювання.

Тому актуальною є проблема розробки алгоритму структурної ідентифікації прогнозуючих моделей з метою створення автоматизованих способів оптимального вибору структури моделей складних об'єктів за вибірками обмеженого обсягу в умовах неповної інформації.

Алгоритм складається з наступних кроків:

Крок 1. Вказується початкова матриця приватних описів Z^0 (для неї вважають $s = 0$):

$$Z^0 = [O : o : I : X] = \left[O : \bar{C}^0 \right], \quad (1)$$

де O – нульовий вектор (розмірності N);

O – нульова матриця (розмірності $N \times F$);

I – одиничний вектор (розмірності N);

$X = [x_1 : x_2 : x_3 : \dots : x_m :]$ – матриця спостережень вхідних змінних (розмірності $N \times F$).

Крок 2. Визначається вектор R .

Нехай вектори \bar{Z}^r будуються за правилом:

$$\bar{Z}^r(i) = \bar{a} \cdot \bar{Z}_{j_1}^{r-1}(i) + \bar{b} \bar{Z}_{j_2}^{r-1}(i) \cdot \bar{Z}_{j_3}^{r-1}(i), \quad (2)$$

де $z = 1, 2, 3, \dots$ – номер ітерації;

$i = 1, 2, 3, \dots, N$ – номер спостереження, який для зручності запису взято у дужки;

$j_1, j_2, j_3 = 1, 2, 3, \dots, F + 2 + m + 2s, (j_3 \geq j_2)$ – номери приватних описів із

матриці \bar{Z}^{r-1} ;

\bar{a}, \bar{b} – коефіцієнти, що визначаються на навчальній підвиборці спостережень (A).

Значення коефіцієнтів (\bar{a}) і (\bar{b}) перебувають як розв'язання задачі мінімізації:

$$\bar{a}, \bar{b} = \arg \min_{a, b} \Phi(a, b) \quad \Phi(a, b) = \sum_{i=1}^{N(A)} e_A^2(i), \quad (3)$$

де $e_A(i)$, $i = 1, 2, \dots, N(A)$ – залишки в регресії \mathcal{Y}_A за двома змінними

$$y_A(i) = a \cdot \bar{Z}_{j_1}^{r-1}(i) + b \cdot \bar{Z}_{j_2}^{r-1}(i) \cdot \bar{Z}_{j_3}^{r-1}(i) + e_A(i). \quad (4)$$

З усіх генерованих за правилом (9)-(11) приватних описів відбираються F описів кращих мінімуму квадратичної норми залишків на перевіірочній підвиборці спостережень B :

$$\begin{aligned}
 J &= \frac{1}{N(B)} \sum_{i=1}^{N(B)} \bar{e}_B^r(i), \\
 \bar{e}_B^r(i) &= y_B(i) - \bar{Z}_B^r, \\
 \bar{Z}_B^r &= a \cdot \bar{Z}_{j_1 B}^{r-1}(i) + b \cdot \bar{Z}_{j_2 B}^{r-1}(i) \cdot \bar{Z}_{j_3 B}^{r-1}(i),
 \end{aligned} \tag{5}$$

де $N(B)$ – обсяг перевірконої добірки B .

Відібрані найкращі приватні описи, ранжирувані за зменшенням величини J , використовуються при формуванні матриці

$$\bar{G}^r = \begin{bmatrix} \bar{z}_1^r & \bar{z}_2^r & \dots & \bar{z}_F^r \\ \vdots & \vdots & \ddots & \vdots \end{bmatrix}. \tag{6}$$

Матриця \bar{C}^r не змінюється $\bar{C}^r = \bar{C}^{r-1}$.

Матриця \bar{D}^r формується з урахуванням структури кращого із F відібраних приватних описів (\bar{Z}_F^r). Перші S стовпці матриці \bar{D}^r заповнюються окремими елементами кращого приватного опису за правилом:

$$\bar{d}_h^r(i) = \bar{Z}_{F+2+m+2s}^r(i) = \theta_h \prod_{j=1}^m x_j^{\alpha_{hj}}(i) \tag{7}$$

де $h = 1, 2, 3, \dots, S$ – номер члена у структурі;

S – число членів у структурі кращого приватного опису;

Другі S стовпців матриці \bar{D}^r формуються почерговим винятком окремих членів із структури приватного опису за правилом

$$\bar{d}_{s+h}^r(i) = \bar{Z}_{F+2+m+s+h}^r(i) = \sum_{\substack{q=1 \\ (q \neq h)}}^s \bar{\theta}_q \prod_{j=1}^m x_j^{d_{jq}}(i) \tag{8}$$

Таким чином визначається оператор R перетворення

$$\bar{Z}^{r-1} \xrightarrow{R} \bar{Z}^r.$$

Правило обстановки для ітераційної схеми: обчислення закінчуються на ітерації r^* , якщо виконується умова

$$J(\bar{Z}_F^{r^*-1}) - J(\bar{Z}_F^{r^*}) < \delta_z \tag{9}$$

де $J(\bar{Z}_F^{r*})$ – значення критерію для найкращого приватного опису ітерації r ;
 δ_z – задане число.

Особливістю алгоритму є багатоповерховість. Номер поточного етапу визначає максимально можливу кількість членів у моделях. Синтез моделей починається з етапу з номером $p = 1$ чи з будь-якого заданого номера p^0 . Кожен етап є ітераційною схемою (8)-(16). Початкова матриця приватних описів етапу з номером p задається кінцевою матрицею приватних описів попереднього етапу

$$\bar{Z}_p^0 = \bar{Z}_{p-1}^{r*} \quad (10)$$

а для $p = p^0$ вона збігається з (8). Обчислення закінчується на етапі p^* , якщо виконано умову

$$J(\bar{Z}_{F_1 p^*-1}^{r*}) - J(\bar{Z}_{F_1 p^*}^{r*}) < \delta_p, \quad (11)$$

де $J(\bar{Z}_{F_1 p^*}^{r*})$ – значення критерію для кращого частного опису r -й ітерації етапу p ;
 δ_p – задане число.

Відмінні риси алгоритму: багатоповерховість моделі; пошук моделі, як у класі лінійних, так і в класі нелінійних за вхідними змінними моделями; прийоми виключення окремих членів кращого приватного опису та на основі цього розширення базисного набору аргументів; оптимальність за обчислювальними витратами для ітераційних алгоритмів методу групового обліку аргументу (МГОВА) схеми розрахунку критерію іспиту, що ковзає; можливість оцінювати коефіцієнти у моделях як за методом найменших квадратів, так і за методом найменших модулів.

УДК 004.056:378.16 (043.2)

**ПОЛІГОН ДЛЯ ПРОВЕДЕННЯ КОМПЛЕКСНИХ НАВЧАНЬ З
БАГАТОРІВНЕВОГО ЗАХИСТУ ВІД КІБЕРАТАК****Богдан Маліцький¹, Олександр Черепов²,
Василь Буковецький³, Василь Різак⁴***Ужгородський національний університет,**¹malitskiy.bohdan@student.uzhnu.edu.ua,**²cherepov.oleksandr@student.uzhnu.edu.ua,**³vasyi.bukovetskiy@uzhnu.edu.ua, ⁴vrizak@uzhnu.edu.ua*

Постійне зростання кіберзлочинності, технологічні зміни та загрози, які ставлять безпеку інформаційних систем під удар спонукають шукати нові методи підготовки майбутніх фахівців з кібербезпеки. Ефективним методом навчання є робота на кіберполігонах, які дозволяють студентам набувати практичних навичок та відпрацьовувати різні сценарії кібератак, покращуючи їхню здатність виявляти та відвертати реальні загрози. Такий підхід до навчання сприяє підготовці ефективних фахівців з кібербезпеки, які зможуть адаптуватися до швидко змінюваних умов сучасного кіберпростору.

Використання полігонів з кібербезпеки як навчального середовища лише набирає популярності як в Україні, так і у світі, тому аналогів цієї розробки є небагато.

Метою даної роботи є створення кіберполігону для практичного навчання майбутніх фахівців з кібербезпеки.

Наша розробка являє собою локальну мережу, яка розбита на дві підмережі. Використання однієї підмережі передбачено командою атаки (червона команда), іншої - командою захисту (синя команда). Процес роботи на полігоні відбувається в форматі хакатону, де перед кожною з команд ставиться визначений перелік завдань, які вони повинні виконати для здобуття перемоги.

Полігон виконує наступні завдання: навчання користувачів основам роботи з мережами, мережевими пристроями, їх налаштуванням, конфігурацією та використанням; симуляція проведення процесу кібератак (червона команда) та захисту від них (синя команда); практична демонстрація роботи фахівців з кібербезпеки у режимі реального часу.

Серед основних переваг можна виділити: пристосованість системи для користувачів різного рівня знань у сфері кібербезпеки; різноманітність завдань, які можуть бути поставлені перед представниками обох команд; можливість легкої адаптації системи під нові вимоги, поставлені перед розробкою.

Сфери застосування розробки є дуже широкими: моделювання реалістичних сценаріїв кібератак та захисту в безпечному та контрольованому середовищі; підвищення кваліфікації та компетентності фахівців з кібербезпеки, здобувачів освіти, державних службовців, ветеранів бойових дій, посадових осіб органів самоврядування; проведення науково-дослідної роботи та експерименти з використанням нових технологій та методик з кібербезпеки; сприяння розвитку культури кібербезпеки в суспільстві та популяризації професії кіберексперта.

Полігон протестований та випробуваний під час проведення практичних навчань здобувачів освіти та перших в Україні навчаннях із кібербезпеки Grid NetWars і повністю готовий до використання.

УДК 004.77

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ СИСТЕМ МОНІТОРИНГУ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Олег Карабан

*Харківський національний економічний університет імені Семена
Кузнеця, oleg.karaban034@gmail.com*

Сьогодні інформаційні технології (ІТ) знайшли своє місце практично у всіх сферах людської діяльності. Повсюдне використання ІТ є характерною рисою ведення сучасного бізнесу. Це пояснюється тим, що цифрові технології надають швидкий шлях для виходу продукту на ринок, ефективні зв'язки з постачальниками та клієнтами, засоби комунікації та взаємодії робітників тощо. У своїй більшості мережеві взаємодії та Інтернет стає головною складовою сучасних ІТ. Важливою рисою застосування таких ІТ є забезпечення їх кібербезпеки.

Для ефективної роботи та підтримки безпеки комп'ютерних систем і мереж слід впроваджувати системний підхід та комплекс заходів на рівні окремого комп'ютеру, серверу та мережі. Важливою складовою такого забезпечення безпеки є засоби моніторингу стану ІТ-інфраструктури.

Метою даної роботи є дослідження та порівняння систем моніторингу комп'ютерних систем і мереж шляхом розроблення та впровадження моделей та засобів інформаційних технологій й інструментів керування ІТ-інфраструктурою за умов раціонального використання її інформаційно-обчислювальних ресурсів.

Незалежно від розміру компанії, не можна ігнорувати необхідність моніторингу серверів, баз даних, мережі, безпеки, інфраструктури тощо. При цьому важливо використовувати якісні інструменти моніторингу. Моніторинг необхідний компаніям, щоб бути впевненими, що кожна система працює належним чином. Але процес моніторингу ІТ-інфраструктури буває досить клопітким й іноді викликає труднощі, якщо моніторинг не налаштований належним чином. Також, сама система моніторингу завжди є ціллю для зловмисників як потенційна точка для втручання в певний сервіс, систему тощо.

Чим активніше розвиваються ІТ-технології в окремо взятій компанії, тим виразніше можна визначити коло завдань системних адміністраторів, яким доводиться контролювати все більше процесів і стежити за станом все більшої кількості систем. Поруч з цим, для невеликої компанії, налаштування одного серверу та забезпечення його безпеки може бути досить критичним для ефективного рішення бізнес-завдань. Тому, проблема вибору та впровадження систем моніторингу комп'ютерних систем і мереж буде актуальною незалежно від масштабу ІТ-інфраструктури підприємства чи компанії.

Можна визначити декілька рівнів систем моніторингу за сферою їх призначення та масштабу впровадження. На рівні серверу завжди є примітивні

засоби спостереження за утилізацією процесорного часу, пам'яті, процесів та мережевого трафіку й ін. Ці системи фактично є утилітами операційної системи, які на рівні окремого серверу доцільно розширити на певну кількість основних засобів, що надають дані у реальному часі. Наприклад, для операційних систем Linux є застосунок *htop*, що надає поточні відомості щодо роботи вузла. Наступним за масштабом та кількості спостережених даних є застосування систем моніторингу на основі циклічних баз даних (Round-robin Database, RRD). Такою є система моніторингу *Cacti*, яка дозволяє аналізувати дані про стан вузла та мережі. Також можна відзначити інші системи, що фактично виконують моніторинг вузла.

Для аналізу стану багатьох серверів та мереж на рівні IT-інфраструктури доцільним є впровадження спеціалізованих рішень моніторингу *Nagios*, *Zabbix* та ін. Ці системи не обмежені границями циклічних баз даних, а застосовують рішення, наприклад, реляційних баз даних промислового рівня. Також відповідні системи є модульними, завдяки застосуванню проксі-серверів дозволяють побудувати ієрархічну модель системи моніторингу й тим самим розвантажити головний вузол, що надає агреговані дані по всій мережі підприємства. Поруч з цим, слід розглянути доцільність застосування рішення *Prometheus* та *Grafana*. Фактично, це системи нового покоління, яким характерна модульність, сумісність за протоколами передачі даних, вони дозволяють налаштувати збір необхідних метрик та побудувати персоналізований інтерфейс відбиття даних.

Більшість сучасних систем моніторингу мають модель збору даних на основі залучення агентів, тому важливим є налаштування шифрування трафіку між агентом, який виконується на стороні вузла та системи моніторингу. Також для запобігання несанкціонованому втручанню слід налагоджувати ефективну систему на основі ролей користувачів, які отримають доступ до системи моніторингу та ін.

Поруч з традиційними системами моніторингу комп'ютерних систем і мереж слід враховувати важливу складову безпеки та розслідувань інцидентів – аналіз стану журналів систем та застосунків. Раніше обробку файлів логування можна було виконати тільки вручну, зараз одним з ефективних рішень є впровадження пошукових систем для аналізу текстових даних та систем відбиття результатів у зручній формі таблиць, діаграм, графіків та ін., наприклад, *ELK Stack*.

Для забезпечення безпеки мереж корпоративного рівня доцільно застосовувати не тільки системи моніторингу стану вузлів та складових IT-інфраструктури, а й залучати засоби, що аналізують трафік на схожість до відомих сигнатур атак, аномалії, ін. - системи запобігання вторгненням (*Intrusion Prevention System*, *IPS*) та системи виявлення атак (*Intrusion Detection System*, *IDS*). Наприклад, *Snort*, *Suricata* та ін.

Ключовим завданням систем моніторингу IT є отримання, збереження та аналіз інформації про стан елементів IT-структури компанії. Спеціальні програми моніторингу дозволяють швидко відреагувати на проблеми, що виникають в роботі IT-сервісів, а також ефективно запобігати виникненню неполадок. Від вибору комплексу рішень з моніторингу залежить ефективність та працездатність IT-інфраструктури та загальний рівень кібербезпеки компанії.

Науковий керівник – д.т.н., професор, Алексієв В.О.

УДК 044.56.5 (043.2)

**ОЦІНКА ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В
ТРАНСПОРТНІЙ ГАЛУЗІ****Аль-Амморі Алі¹, Сергій Заворотний²***Національний транспортний університет, ¹ammourilion@ukr.net**²seregazavorotnyi@gmail.com*

В процесі експлуатації інформаційних систем (ІС) транспортної галузі, можливе виникнення умов, які непередбачені розробником, при проектуванні систем захисту інформації (СЗІ). Оцінка ефективності захисту інформації повинна обов'язково мати як розрахунковий так і ймовірнісний характер. Методологія оцінки повинна включати систему нормативних документів, що містять кількісні, вимірювані показники ефективності СЗІ, та забезпечити вимоги як замовників так і проектувальників. Необхідність обґрунтування оптимальних значень показників ефективності, що враховує цільове призначення інформаційної системи транспортної галузі є актуальним та дуже важливим питанням в наукових колах. Для вирішення проблеми пропонується використовувати системний підхід. Саме кількісне визначення ефективності може розглядатися як основа для вирішення проблеми.

Мета дослідження полягає в виконанні аналізу нормативно-методичного забезпечення оцінки ефективності захисту інформації в транспортній галузі.

Статистика атак на ІС в транспортній галузі, вказує на негативну тенденцію вразливості ІС до атак та проникнень в інформаційні бази та системи. Атаки реалізуються на складові автоматизованих систем керування (АСК), системи SCADA та НМІ (людино-машинний інтерфейс).

Засоби захисту інформації (ЗЗІ), відповідно до чинних норм та правил, підлягають обов'язковій сертифікації. Однак, сертифікація не є досконалим інструментом і в кращому випадку перевіряють лише 85% від всіх можливих засобів, а зазвичай навіть 60-70%.

Об'єктивне підтвердження ефективності СЗІ є складним процесом, що може ускладнюватися недосконалістю існуючої нормативної бази, а також принциповій різниці інженерії ІТ від традиційної. Як приклад, фахівцями галузі відзначається недостатність систем нормативних показників інформаційної безпеки та критеріїв ефективності СЗІ.

Нормативні документи щодо оцінки безпеки ІТ практично не містять конкретних методик, внаслідок чого різниця між загальними деклараціями та конкретним інструментарієм щодо реалізації та контролю їх положень достатньо велика. Виходячи з призначення, методична база повинна охоплювати всі критично важливі аспекти забезпечення та перевірки виконання вимог, що висувуються до СЗІ в транспортній галузі. У методичному плані визначення ефективності СЗІ повинно полягати у виробленні висновку щодо придатності способу дій персоналу або пристосованості технічних засобів до досягнення мети захисту інформації на основі вимірювання відповідних показників, наприклад, при функціональному тестуванні.

Відповідно до сучасної теорії оцінки ефективності систем, якість будь-якого об'єкта, у тому числі і СЗІ, проявляється лише в процесі цільового функціонування, тому найбільш об'єктивним є оцінювання ефективності застосування. Процедури випробувань, сертифікації або ліцензування не повністю усувають невизначеність властивостей СЗІ або її окремих елементів і не враховують випадковий характер атак. Тому об'єктивною характеристикою якості СЗІ може бути лише ймовірність, що характеризує ступінь можливостей конкретної СЗІ при заданому комплексі умов.

У сучасних нормативних документах з інформаційної безпеки використовується класифікаційний підхід. Ймовірнісні методи також знайшли широке поширення у практиці забезпечення безпеки інших прикладних областях. Відповідно до цих методів рівні гарантій безпеки СЗІ трансформуються на довірчі ймовірності відповідних оцінок показників.

Узагальнені дані про можливі показники ефективності наведено у таблиці 1.

Таблиця 1

Можливі показники ефективності СЗІ та критерії ефективності СЗІ

Вимоги до СЗІ	Види показників ефективності СЗІ
Початок та закінчення випадків	Ймовірність випадку
Досягнення необхідних характеристик	Ймовірність досягнення результату не менше необхідного рівня
Не встановлені	1. Математичне очікування результату 2. Дисперсія результату
Концепція ефективності СЗІ	Критерії ефективності
Придатність	1. Прийнятний результат 2. Допустимий результат
Оптимальність	1. Найкращий результат 2. Найкращий середній результат

Висновок. Нормативно-методичної бази в сфері інформаційної безпеки, що використовується в транспортній галузі не відповідає сучасним вимогам інформаційної безпеки. Для визначення необхідного рівня безпеки СЗІ, потрібно виконувати оцінку ефективності СЗІ за рахунок показників, які мають ймовірнісний характер.

Змістовні результати з оцінювання ефективності систем захисту, можуть бути отримані при системному підході. Кількісна оцінка ефективності СЗІ є сучасним об'єктивним методом на відміну від якісних методів.

УДК 004.056.5

ПОБУДОВА МОДЕЛІ ПЕРВИННИХ ПАРАМЕТРІВ ОЦІНКИ СТАНУ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Микола Карпінський¹, Олександр Корченко², Юрій Дрейс³

*Гуманітарно-технічна академія¹, Польща, mrcarpinski@gmail.com,
Національний авіаційний університет², Україна isaocentre@nau.edu.ua,
Поліський національний університет³, Україна, dreisyuri@gmail.com*

Захист інформації з обмеженим доступом, особливо державної таємниці (ДТ), є важливим завданням у сфері національної та інформаційної безпеки держави. Для мінімізації можливої шкоди національній безпеці від порушень у сфері охорони ДТ (ОДТ) та зменшення негативного рейтингу на рівні держави необхідно створити спеціалізовані бази даних (СБД), розробити і удосконалити існуючі методи [1-3] і моделі [4-6], що реалізують відповідні оцінювання. Саме тому, теоретико-множинне представлення параметрів Узагальненого звіту та Звіту про стан забезпечення охорони ДТ [7] як на рівні держави так і на рівні окремого суб'єкта режимно-секретної діяльності (СРСД) та режимно-секретного органу (РСО), узагальнених кортежною моделлю є актуальним науковим завданням, що дозволяє вирішити науково-практичну задачу формування СБД стану ОДТ для подальшого створення необхідних статистичних даних і формалізації процесу оцінювання негативних наслідків витоку ДТ, заподіяних її розголошенням або втратою матеріальних носіїв секретної інформації, порушенням режиму секретності тощо.

У зв'язку з цим метою даної роботи є побудова моделі формування СБД первинних параметрів для оцінювання стану забезпечення ОДТ з використання ідентифікаційних, статичних і інших даних щодо негативних наслідків (шкоди) у разі витоку ДТ при порушенні вимог ОДТ, що встановлені законодавством.

Введемо множину всіх можливих ідентифікаторів кортежів **IS** (*Information about the Subject*), за допомогою яких можна відображати відомості про СРСД та використовувати у процесі виявлення і оцінювання наслідків у разі втрати ДТ:

$$\mathbf{IS} = \left\{ \bigcup_{\varphi=1}^z \mathbf{IS}^{\varphi} \right\} = \{ \mathbf{IS}^1, \mathbf{IS}^2, \dots, \mathbf{IS}^z \},$$

де $\mathbf{IS}^{\varphi} \subseteq \mathbf{IS}$ ($\varphi = \overline{1, z}$) – ідентифікатор кортежу параметрів, що характеризують φ -й СРСД. Для φ -го СРСД кортеж параметрів, що його характеризує має наступний вигляд:

$$\mathbf{IS}^{\varphi} = \left\langle \mathbf{IS}^{\varphi}_1, \mathbf{IS}^{\varphi}_2, \dots, \mathbf{IS}^{\varphi}_i, \dots, \mathbf{IS}^{\varphi}_k \right\rangle,$$

де: $\mathbf{IS}^{\varphi}_i \subseteq \mathbf{IS}^{\varphi}$ ($i = \overline{1, k}$) – компонент кортежу, що є підкортежем і відображає i -й ідентифікатор параметру φ -го СРСД, а k – максимальне число таких параметрів.

Зазначимо, що для всіх членів **IS** характерна властивість порядку. Наприклад,

відповідно до Узагальненого звіту та Звіту, при $k = 9$ кортеж (2) визначимо як [7]:

$$\mathbf{IS}^{\varphi} = \langle \mathbf{IS}^{\varphi_1}, \mathbf{IS}^{\varphi_2}, \mathbf{IS}^{\varphi_3}, \mathbf{IS}^{\varphi_4}, \mathbf{IS}^{\varphi_5}, \mathbf{IS}^{\varphi_6}, \mathbf{IS}^{\varphi_7}, \mathbf{IS}^{\varphi_8}, \mathbf{IS}^{\varphi_9} \rangle,$$

де, наприклад, підкортеж $\mathbf{IS}^{\varphi_1} = \mathbf{Розділ\ I}$ («Відомості про СРСД, його підпорядкування та відомчу належність»), а інші компоненти вказані у [7].

Висновок. Побудована кортежна модель, яка за рахунок теоретико-множинного представлення множин кортежних моделей інтегрованого представлення первинних параметрів стану забезпечення ОДТ, що відображають величини звітного періоду, множини, що характеризують СРСД, фінансування заходів з ОДТ, кількість МНСІ та працівників з доступом та допуском до ДТ, режимних приміщень об'єктів інформаційної діяльності, порушення у сфері ОДТ, міжнародне співробітництво тощо, дозволяє відповідно до законодавства визначити необхідну кількість початкових величин для формування бази даних, ведення статистики і удосконалення формалізації процесу оцінювання шкоди (збитків) від втрати ДТ національній безпеці України, як на рівні держави, так і на рівні її окремих областей, територіальних громад.

Література

1. О. Корченко, С. Казмірчук, Ю. Дрейс, Метод аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці. *Захист інформації*, 2012, № 3(56), С. 5–18.
2. О. Корченко, О. Архипов, Ю. Дрейс, Оцінювання шкоди національній безпеці України у разі витоку державної таємниці. *Монографія*. Київ: наук.-вид. центр НА СБ України, 2014, 332 с.
3. S. Falchenko, V. Hrebenuik, A. Hrebenuik, A. Korchenko, I. Manzhul, Y. Dreis, Method of fuzzy classification of information with limited access. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*: Conference Proceedings, 25.11.20-27.11.20 Kyiv, Ukraine, pp. 255-259.
4. О. Корченко, Ю. Дрейс, М. Рощук, О. Романенко, Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави. *Безпека інформації*, 2018, Т. 24 (№ 1), С. 29-35.
5. О. Корченко, Ю. Дрейс, Л. Деркач, Теоретико-множинний підхід до оцінювання шкоди національній безпеці України у разі витоку відомостей, що становлять державну таємницю. *Методичні рекомендації*. Київ, НА СБУ, 2021, 128 с.
6. Ю. Дрейс, Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання. *Безпека інформації*, 2014, Т. 20, № 2, С. 176-184.
7. Про затвердження форм звітів про стан забезпечення охорони державної таємниці та інструкції про порядок їх оформлення і подання, Наказ СБ України №6 від 17.01.2020 року.

УДК 004.056.5

**АЛГОРИТМ ШИФРУВАННЯ ЗОБРАЖЕНЬ ДИСТАНЦІЙНОГО
ЗОНДУВАННЯ ЗЕМЛІ З ВИКОРИСТАННЯМ ДВОКАНАЛЬНОЇ
ПЕРЕДАЧІ КЛЮЧІВ****Віта Каштан***Національний технічний університет «Дніпровська політехніка»,
kashtan.v.yu@nmu.one*

Зображення дистанційного зондування Землі (ДЗЗ) можуть містити військову таємницю, профілі території та інші конфіденційні дані, які забезпечують надійну технічну гарантію сталого розвитку національної економіки кожної країни. Використання зображень ДЗЗ пов'язане з ризиком втрати, крадіжки та перехоплення, особливо якщо зображення зберігаються в хмарному середовищі або передаються через загальнодоступні канали. Тому, шифрування зображень є важливим технічним засобом для запобігання витоку конфіденційної інформації.

Останнім часом розроблено багато ефективних алгоритмів для захисту даних від несанкціонованого доступу, але забезпечення якісного та швидкого шифрування залишається актуальним питанням. Хаотичні системи стали типовим методом шифрування зображень, так як мають складну структуру та високу чутливість до параметрів початкових значень. Передові технології шифрування, які базуються на хаотичній системі, включають такі методи, як кодування DNA, заміну S-box, зигзагоподібне скремблювання, схему підйому, математичні моделі та компресійне зондування. Всі вищевказані алгоритми використовують однакову операцію для шифрування кожного каналу (багатоканального) зображення. Це означає, що коли зловмисник зламує зображення у градаціях сірого (панхромне зображення), то всі інші частини зображення можуть бути легко перехоплені.

Метою даної роботи є розробка алгоритму шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів.

Модель двоканальної передачі ключів (Dual-Channel Key Transmission Model) – це метод передачі ключа шифрування, який використовує два незалежні канали передачі для підвищення надійності та безпеки передачі даних. Структурна схема алгоритму шифрування представлена на рисунку 1. Запропонована модель використовує два незалежних канали: головний канал і канал підтвердження. Головний канал використовується для передачі основного потоку даних на основі симетричного ключа, тоді як канал підтвердження використовує прихований ключ на рівні бітів (це дозволяє додати ключ у зашифроване зображення). Процес передачі ключа в моделі Dual-Channel Key Transmission складається з наступних етапів: 1) Ключ генерується відправником та поділяється на дві частини. Одна частина передається по головному каналу, а інша – по каналу підтвердження. 2) Одержувач отримує дві частини ключа та перевіряє їх цілісність. 3) Якщо ключі виявляються неповними або пошкодженими, вони не оброблюються та процес передачі повторюється. Якщо обидві частини ключа були успішно отримані, вони об'єднуються для створення повного ключа шифрування.

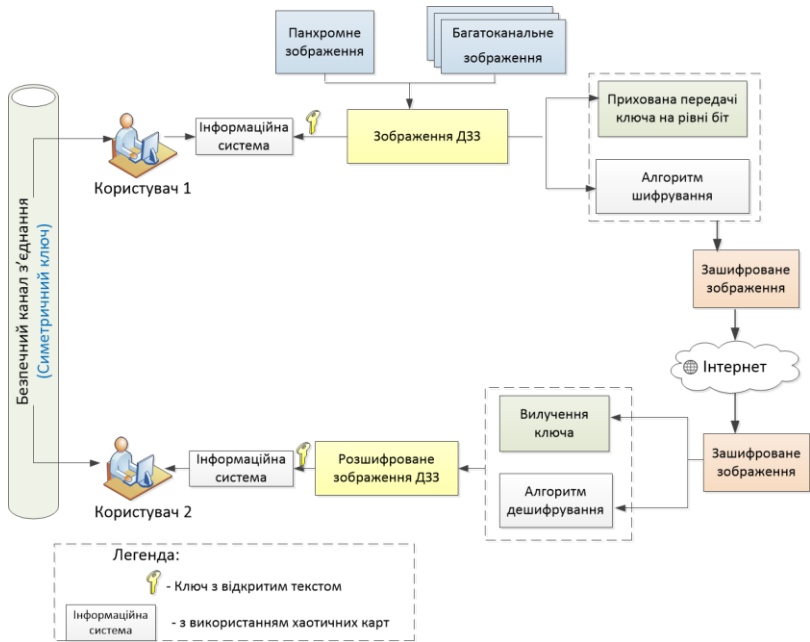


Рис.1. Схема шифрування ДЗЗ зображень

Коли дешифратор отримує зображення з прихованим ключем на рівні біт, він спочатку використовує хаотичну послідовність потоку ключів, щоб визначити приховане положення ключа. Після цього піксельне значення зображення перетворюється на 8-розрядні двійкові числа, останні біти об'єднуються для отримання 32-розрядної двійкової послідовності. Для розшифрування ключа використовується операція XOR порозрядно. Таким чином, два типи ключів взаємодіють у хаотичній системі як ключі шифрування, що ускладнює зловмиснику правильно відновити (дешифрувати) оригінальне зображення, навіть якщо він перехопить один з ключів.

Запропонований в роботі алгоритм шифрування зображень дистанційного зондування Землі з використанням двоканальної передачі ключів через загальнодоступні канали зв'язку, наприклад через Інтернет, пошту або інші канали дозволяє захистити дані від несанкціонованого доступу. Такий підхід дозволяє підвищити безпеку передачі багатоканальних (багатоспектральних) зображення дистанційного зондування Землі через супутникові або військові канали зв'язку.

УДК 003.26:511.41

**КРИПТОАНАЛІЗ АСИМЕТРИЧНИХ КЛЮЧІВ
АЛГОРИТМАМИ ЛАНЦЮГОВИХ ДРОБІВ****Юлія Мисло¹, Михайло Пагіря²***Ужгородський національний університет**¹julia.mislo@uzhnu.edu.ua, ²mykhaylo.pahiryia@uzhnu.edu.ua*

Ланцюгові дроби знайшли своє застосування в багатьох розділах сучасної математики та її застосувань. Використання ланцюгових дробів в теорії чисел служить підґрунтям для аналізу надійності шифрів з асиметричними ключами.

Наприклад, добре відомо [1,2], що коли використовується один із найбільш вживаних алгоритмів з асиметричним ключем алгоритм RSA, то у функції шифрування $E(x)=x^e \pmod n$ модуль n є добутком двох великих простих чисел p та q , $n=pq$, що є таємними. З іншого боку, задача факторизації числа n належить до складних задач теорії чисел і перевершує за складністю задачу перевірки числа на простоту. В свою чергу і секретний ключ d в функції дешифрування $D(c)=c^d \pmod n$ важко знайти, якщо невідоме значення функції Ойлера $\phi(n)$.

Для факторизації числа n на практиці використовують метод пробних ділень, який вимагає $O(n^{1/2})$ двійкових операцій, **ρ -метод Полларда**, який може виявити множник в результаті виконання $O(n^{1/4}(\log n)^3)$ двійкових операцій, **метод Ферма**, який ефективним у випадку близькості співмножників, метод факторних баз, який вимагає виконання $O(\exp(C(r \log r)^{1/2}))$ двійкових операцій. На метод факторних баз спирається спосіб відшукування співмножників числа за допомогою розвинення числа в ланцюговий дріб, який ґрунтується на теоремі Лагранжа.

Ще один метод дослідження стійкості алгоритмів з асиметричними ключами з використанням ланцюгових дробів на прикладі алгоритму RSA розглянуто в роботі [3]. При додаткових припущеннях на складові секретної частини ключа, тобто: $q < p < 2q$, $d < n^{1/4}/3$, $e < \phi(n)$, шукається розвинення відношення складових відкритої частини ключа e/n у правильний ланцюговий дріб і один із канонічних знаменників ланцюгового дроби буде секретним ключем d для RSA шифру. При реалізації алгоритму необхідно здійснити перевірку $O(\ln n)$ підхідних дробів.

Проведено дослідження розглянутих методів факторизації ключів, здійснено порівняння по часу виконання кожного із методів та вироблені рекомендації по формуванню надійних ключів шифрування. Запропоновані деякі модифікації алгоритмів.

Література

1. N. Koblitz *A Course in Number Theory and Cryptography*. 2-nd ed. Springer Science & Business Media, 1994.
2. M. Cozzens & S. J. Miller *The Mathematics of Encryption: an Elementary Introduction*. American Mathematical Society. *Mathematical World* 29, 2013.
3. M. Wiener *Cryptanalysis of short RSA secret exponents*. // IEEE Transactions on Information theory 36.3 (1990): 553-558.

УДК 004.75 (004.5)

РОЗПОДІЛЕНІ СИСТЕМИ ВИЯВЛЕННЯ WORM-ВІРУСІВ**Богдан Савенко¹, Антоніна Каштальян², Наталя Петляк³***Хмельницький національний університет**¹savenko_bohdan@ukr.net, ²antonina@ukr.net, ³npetyak@khmnu.edu.ua*

В комп'ютерних мережах може перебувати різноманітне зловмисне програмне забезпечення. Завдяки технологіям та засобам підтримки функціонування комп'ютерних мереж, крім корисного їх застосування, наявні широкі можливості їх використання зловмисниками. Наприклад, для створення бот-мереж зловмисники можуть використовувати стандартні засоби роботи з пересилання повідомлень та файлів, команди, а також можуть для досягнення своєї мети, щоб приховати свої зловмисні дії, використати мережні віруси для проникнення у вузли в мережах та встановлення в них контролю. Такими вірусами можуть бути worm-віруси.

Метою даної роботи є покращення виявлення worm-вірусів завдяки використанню, крім методу виявлення, особливостей архітектури розподілених систем виявлення, в яку імплементовано метод виявлення.

Розподілена система виявлення зловмисного програмного забезпечення синтезована згідно принципів самоорганізації, адаптивності і часткової централізації. Розглянемо результати її застосування до worm-вірусів. Визначальною їх особливістю є спрямування на інфікування переважно комп'ютерів, а не файлів в них, і цільова функція спрямована саме на досягнення максимізації інфікування кількості комп'ютерів, а не файлів в них. Хоча можуть бути і такі, що додатково спрямовані на інфікування файлів в комп'ютерних станціях, в які отримали доступ. Маючи такий функціонал у worm-вірусах щодо їх поширення і спрямування саме для поширення в комп'ютерних мережах, як локальних так і глобальних, зловмисники можуть їх використати для цілеспрямованого охоплення корпоративної мережі, яка їх цікавить та, як наслідок, навколо якої можуть створити зони поширення таких worm-вірусів. Тому, захищаючи корпоративну мережу частково централізованими системами потрібно імплементувати в них підсистеми та засоби протидії такому зловмисному

програмному забезпеченню, як worm-віруси. Введемо множину W комп'ютерних worm-вірусів так:

$$W = \{w_1, w_2, \dots, w_{N_w}\} \quad W = \{w_1, w_2, \dots, w_{N_w}\}, \quad (1)$$

де w_i - i -ий worm-вірус; N_w - кількість відомих worm-вірусів.

Задамо характеристичні показники worm-вірусів множиною

$$M_W = \{m_{W,1}, m_{W,2}, \dots, m_{W,N_w}\} \quad M_W = \{m_{W,1}, m_{W,2}, \dots, m_{W,N_w}\}, \text{ де}$$

N_w - кількість характеристичних показників, $m_{W,i}$ - i -ий

характеристичний показник, $i = 1, 2, \dots, N_{Wi} = 1, 2, \dots, N_W$. Деталізуємо кожен характеристичний показник з метою подальшого поєднання їх елементів для задання відповідно типу worm-вірусів.

При виборі за характеристичний показник елементу $m_{W,1}m_{W,1}$ можна поділити всю множину worm-вірусів на такі класи: клас, в якому не міститься жодного елементу з характеристичним показником $m_{W,1,j}m_{W,1,j}$ ($j = 1, 2, \dots, 5; j = 1, 2, \dots, 5$), тобто клас, в якому відсутні worm-віруси, і позначимо його $K_W^0 K_W^0$; клас $K_W^j K_W^j$ ($j = 1, 2, \dots, 5; j = 1, 2, \dots, 5$), який визначатиметься характеристичним показником $m_{W,1,j}m_{W,1,j}$ ($j = 1, 2, \dots, 5; j = 1, 2, \dots, 5$), і всього таких класів буде п'ять; клас $K_W^6 K_W^6$, в який будуть віднесені елементи, для характеристики яких буде більше одного характеристичного показника $m_{W,1,j}m_{W,1,j}$ ($j = 1, 2, \dots, 5; j = 1, 2, \dots, 5$). Побудова класу $K_W^6 K_W^6$ може бути здійснена системою SS в процесі її функціонування при виявленні багатовекторних worm-вірусів. Для віднесення об'єкту до класу $K_W^6 K_W^6$ система SS повинна встановити його мінімум в двох класах з класів $K_W^j K_W^j$ ($j = 1, 2, \dots, 5; j = 1, 2, \dots, 5$). Формування класу $K_W^0 K_W^0$ можливе за умови помилкового віднесення worm-вірусів до нього при застосуванні систем виявлення. При правильно здійсненій класифікації worm-вірусів клас $K_W^0 K_W^0$ буде порожнім, тобто $K_W^0 = \emptyset_{K_W^0} = \emptyset$. Наявність елементів в класі $K_W^0 K_W^0$ буде означати помилковість спрацювання відповідного детектора та системи в цілому. Таким чином, всю множину worm-вірусів поділено на шість класів:

$$W = \bigcup_{j=1}^6 K_W^j K_W^j = \bigcup_{j=1}^6 K_W^j K_W^j. \quad (2)$$

З системою, в яку було імплементовано метод виявлення worm-вірусів було проведено експеримент з виділенням класів worm-вірусів та джерел їх поширення. Результати експериментів подано в табл. 1 за типами worm-вірусів та варіантами джерел поширення задано в табл. 1.

Для оцінювання достовірності виявлення worm-вірусів системою S та імплементованим в неї методом, як цілісного бінарного класифікатора, було визначено чутливість та специфічність моделі і обчислено їх значення. У результаті

отримано True Positives Rate - 73,52%, рівень помилкових позитивних результатів - 9,07%, чутливість - 73,52%, специфічність - 90,92%.

Таблиця 1

Результати експериментів

Резу- льтат вия- влен- ня	Клас и worm - віру- сів, $j = 1,2,\dots$	Серії експерименту												Ра- зом
		Екземпляри класу												
		1			2			3			4			
		1	2	3	4	5	6	7	8	9	10	11	12	
<i>FN</i>	$K_w^{0,j}$	34 4	32 0	30 2	37 6	34 5	26 7	30 7	29 8	26 7	34 8	31 7	39 3	3884
<i>TP</i>	K_w^j	91 1	91 5	83 7	89 7	85 3	93 4	89 2	94 6	93 2	97 6	83 1	86 4	1078 8
<i>FP</i>	$K_w^{j,p}$	18 4	19 8	12 9	11 5	12 4	16 0	21 4	25 3	94 2	17 2	20 8	84	1935
<i>TN</i>	$K_w^{j,y}$	15 61	15 67	17 32	16 12	16 78	16 39	15 87	15 03	17 07	15 04	16 44	16 59	1939 3

Оскільки значення специфічності є високим, то система S виявляє негативні випадки краще, ніж позитивні, бо чутливість є меншою порівняно з специфічністю.

Таким чином, застосування розробленого рішення за результатами проведених експериментів підтверджує можливість ефективного його використання при розробці і експлуатації нового типу систем виявлення.

УДК 004.623

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОСТУПУ ДО ХМАРНИХ ОБЧИСЛЕНЬ ЗА ДОПОМОГОЮ БЛОКЧЕЙН ТЕХНОЛОГІЙ

Роман Ситник¹, Вікторія Гнатушенко²

Український державний університет науки і технологій

¹r.sytnyk@outlook.com, ²vvitagnat@gmail.com

Децентралізований механізм контролю доступу до хмарних ресурсів на основі блокчейну та Distributed Ledger Technology забезпечує більшу безпеку хмарних обчислень та можливість прозорого журналювання та моніторингу хмарних систем.

Метою даної роботи є поліпшення механізмів забезпечення безпеки доступу до хмарних обчислень за допомогою технологій блокчейну.

Блокчейн – це розподілена база даних, в якій кожен запис має в собі хеш попереднього, що захищає дані від зміни, таким чином, що зміна одного запису зробить невірним хеш в усіх наступних записах. Технологічною основою блокчейну є Distributed Ledger Technology (DLT). Ця технологія є розподіленою базою даних, яка зберігає записи транзакцій у кількох вузлах мережі, а чи не в

єдиній централізованій базі даних. Розподіленість та безпека технології блокчейну досягається за допомогою технологій консенсусу, криптографічних хеш-функцій та цифрового підпису транзакцій у мережі. Технологія блокчейну створювалася для вирішення проблеми централізації фінансової та банківської сфери.

Для підвищення безпеки хмарних обчислень пропонується впровадити розподілений механізм контролю доступу до хмарних обчислень на основі алгоритмів блокчейну та Distributed Ledger Technology, технології розподіленого реєстру. Цього можна досягти за допомогою механізму смарт-контрактів, програмного забезпечення, що працює у мережі блокчейн і може забезпечити дотримання заздалегідь запрограмованих правил і умов при проведенні транзакцій у блокчейн. Так, наприклад, у мережі Ethereum можливо виконувати запрограмовані інструкції мовою програмування Solidity, які виконуються у мережі блокчейн при виконанні транзакцій.

Запропонований алгоритм забезпечення децентралізованого доступу до хмарних ресурсів працює таким чином, що коли користувач хмарного сервісу хоче отримати доступ до певного ресурсу, наприклад файлу, що зберігається на хмарному сервері, або хмарних обчислень, користувач надсилає запит на доступ до ресурсу (файлу або обчислень) до мережі блокчейн за адресою смарт-контракту, який займається контролем та безпекою дозволів. Смарт-контракт у мережі блокчейн перевіряє запит та дозволи користувача на доступ до ресурсу. Якщо користувач має необхідні дозволи, то смарт-контракт надає користувачеві доступ до ресурсу. Деталі транзакції (особа користувача, доступ до ресурсу, час і дата транзакції) записуються в блокчейн. Кожна транзакція записується в захищений від несанкціонованого доступу децентралізований реєстр транзакцій (Distributed Ledger), що унеможливує зміну чи видалення минулих транзакцій. Кожен новий запит на доступ до ресурсу проходить такий самий процес перевірки та запису в блокчейн.

В прототипному виконанні, такий смарт-контракт забезпечує зберігання у блокчейні списку доступів до ресурсів, з ідентифікатором ресурсу, дозволами та користувачем, доступи якому надані (наприклад, права на читання, на запис, та на виконання), та включає в себе як мінімум дві функції – для зчитування дозволів до ресурсу для якогось користувача, та надання дозволів до ресурсу користувачу адміністратором хмарного сервісу.

Після перевірки прав та дозволів користувача, смарт-контракт, надає користувачеві доступ до ресурсу (файлу або виконання обчислень). Це забезпечує прозорий і перевірний запис усіх запитів на доступ до сервісу і може допомогти запобігти несанкціонованому доступу, витоку даних та поліпшити журналювання та моніторинг хмарної системи.

Ці записи є незмінні, що полегшує відстеження та розслідування будь-яких порушень безпеки або аномалій. За допомогою Distributed Ledger Technology кожна транзакція записується в захищену від несанкціонованого доступу децентралізований реєстр, який унеможливує зміну чи видалення минулих транзакцій, завдяки природі блокчейну. Це гарантує, що всі транзакції є прозорими, перевіреними та захищеними від втручання. Також такі записи забезпечують кращу відповідність нормативним вимогам, таким як збереження даних і зобов'язання щодо звітності. Крім того, децентралізований характер DLT гарантує, що контроль

доступу є розподіленим і захищеним від втручання, зменшуючи ризик несанкціонованого доступу, зміни або витоку даних.

Така інформаційна система захисту хмарних ресурсів дозволяє забезпечити децентралізований механізм контролю доступу до хмарних ресурсів на основі блокчейну та Distributed Ledger Technology, що забезпечує більшу безпеку хмарних обчислень та можливість прозорого та перевіреного журналювання та моніторингу цих систем.

УДК 004.056

ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА В РАДІОРЕЛЕЙНИХ ЛІНІЯХ ЗВ'ЯЗКУ

Роман Штонда¹, Юлія Черниш², Ірина Мальцева³

Військовий інститут телекомунікацій та інформатизації

імені Героїв Криму ¹roman.shtonda@viti.edu.ua,

²yuliia.chernysch@viti.edu.ua, ³iryna.maltseva@viti.edu.ua

Як показує наше сьогоднішнє, застосування радіорелейних ліній зв'язку (далі – РРЛЗ) не втратило своєї актуальності. Із початком повномасштабного вторгнення росії на територію України здійснено ряд кібератак, серед них було запущено шкідливе програмне забезпечення AcidRain, яке вплинуло на роботу станцій супутникового зв'язку Viasat. В результаті чого питома частка передачі даних лягла на РРЛЗ.

Метою даної роботи є доведення дій керівників установ/організацій щодо захисту інформації та кібербезпеки в РРЛЗ.

Радіорелейні засоби зв'язку та побудовані за допомогою них РРЛЗ не є чимось таким новим. Але кіберзагрози та кіберінциденти, що можуть в них виникати по тій чи іншій причині, є актуальним питанням котре потребує глобального вивчення та протидії. Керівники установ/організацій, що експлуатують та надають комунікаційні послуги за допомогою РРЛЗ повинні піклуватись про забезпечення надійного захисту інформації, що в них циркулює, а також здійснювати захист користувачів від кіберзагроз, що можуть проникнути в РРЛЗ із мережі Інтернет чи із-за необізнаного працівника.

Для вирішення даного питання, керівникам організацій/установ, необхідно проводити наступні дії: постійно проводити роботу з підлеглими працівниками з питань додержання кібергігієни; слідкувати за тим щоб працівники ніколи не залишати робочі пристрої (ноутбуки, планшети, накопичувачі тощо) без нагляду; розробляти та впроваджувати заходи додаткової верифікації при вході в мережу або систему; постійно застосовувати двофакторну автентифікацію під час підключення обладнання, яке призначене для роботи/налаштування РРЛЗ; застосовувати відповідні логіни та паролі та постійно проводити системне оновлення паролів доступу; застосовувати паролі із відповідною кількістю символів непов'язаних між собою; мати актуальне антивірусне програмне забезпечення постійно оновлювати його; на обладнанні встановлювати антишпигунське програмне забезпечення; застосовувати на всіх рівнях програмно-апаратні та програмні міжмережеві

екрани/брандмауери; мати в штаті центр захисту інформації та кібербезпеки; проводити систематичний моніторинг доступу до мережі Інтернет.

Підводячи висновок хотілось б зазначити, що для забезпечення розвитку радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання комунікаційних послуг, необхідно постійно приділяти увагу кібербезпеці під час побудови РРЛЗ. Додержання правил та вимог, які ми навели, дозволить будувати РРЛЗ з додержанням правил кібербезпеки та можливістю протидіяти витоку інформації. А також унеможливить проникнення кібершахраїв на робочі пристрої користувачів.

УДК 004.056.5

ВИКОРИСТАННЯ КВАНТОВОГО МАШИННОГО НАВЧАННЯ ПРИ ОБРОБЦІ БАГАТОКАНАЛЬНИХ АЕРОКОСМІЧНИХ ЗОБРАЖЕНЬ

Ірина Удовик¹, Володимир Гнатушенко²

Національний технічний університет «Дніпровська політехніка»

¹ udovyk.i.m@nmu.one, ² vvgnat@ukr.net

Попередня обробка багатоканальних аерокосмічних даних та їх подальший аналіз є важливими задачами в багатьох прикладних областях, зокрема національна оборона та безпека покладаються на супутникові зображення як на важливе джерело інформації. Однак об'єм даних, який генерується за допомогою мульти- та гіперспектральних сенсорів на борту супутників дистанційного зондування Землі (ДЗЗ), а також радіолокаційних датчиків, продовжує зростати, перевищуючи 150 терабайтів на день. Для ефективного дешифрування значущої інформації з такого великого об'єму даних необхідні спеціальні інструменти та методи обробки великих даних. Алгоритми машинного навчання показали великий потенціал при аналізі даних ДЗЗ, проте результати цих технологій обмежені обсягом доступних навчальних даних та обчислювальної потужності. Для подальшого розвитку цих технологій необхідно забезпечити більш ефективну обробку та аналіз великих об'ємів геопросторових даних та використання нових методів машинного навчання, що дозволять отримувати більш точні та швидкі результати. Квантові алгоритми машинного навчання можуть допомогти вирішити зазначену проблему.

Метою дослідження є застосування квантових алгоритмів машинного навчання для аналізу великих об'ємів даних дистанційного зондування Землі. Актуальність даної теми полягає в тому, що ДЗЗ є важливим джерелом інформації для багатьох наукових, екологічних та господарських досліджень, а традиційні методи обробки цих даних є неефективними.

В роботі запропоновано використовувати квантові нейронні мережі з доступом до властивостей проєктованого квантового ядра (Projected Quantum Kernel – PQK) для класифікації зображень, розпізнавання об'єктів та піксельної сегментації.

Квантові комп'ютери з сотнями кубітів вже доступні науковій спільноті. Вони мають потужний потенціал для виконання складних квантових обчислень, що

перевищують обчислювальну потужність будь-якого класичного пристрою. Існуючі схеми квантового машинного навчання можна узагальнити та розділити на три категорії. Перша – заміна складних частин машинного навчання на квантові алгоритми, наприклад, такі як квантові машини опорних векторів. Друга – поєднання динаміки квантових систем з класичним машинним навчанням. І третя – використання фізичних процесів на класичних машинах, наприклад, алгоритм квантового віджигу.

Окремої уваги заслуговують проектовані квантові ядра (PQK) – сімейство ядер, що працюють за допомогою проекції квантових станів на класичне подання. Модифіковане квантове ядро називається проектованим квантовим ядром. Хоча це подання достатньо важко вирахувати за допомогою класичного комп'ютера, воно має ряд практичних переваг, зокрема проекція зменшує велику розмірність навчальної вибірки меншого класичного простору. Проектоване квантове ядро визначено в класичному просторі ознак, щоб уникнути труднощів у навчанні через експоненційну розмірність квантового гільбертового простору.

Існує кілька типів проектованих квантових ядер, але нами використано наступне:

$$K^P(x_i, x_j) = \exp\left(-\gamma \sum_k \sum_{P \in M} \left(Tr(P\rho(x_i)_k) - Tr(P\rho(x_j)_k)\right)^2\right), \quad (1)$$

де $\rho(x_i)_k$ – матриця зменшення щільності кубітів k , M – набір вимірювань на матриці зменшення щільності, $k=0; 1$, $M = \{X, Y, Z\}$ – означає використання вимірювань Паулі для вимірювання кожного окремого кубіта на виході.

В роботі нами використано набори багатоканальних супутникових даних Sentinel-2. Метою експериментів є оцінка впливу PQK-характеристик на точність багатоспектральної класифікації. Для досягнення цієї мети було порівняно результативність різних класифікаторів на створеному датасеті з PQK-векторами ознак та оригінальними спектральними векторами ознак. Також досліджено результативність цих класифікаторів на оригінальному датасеті Sentinel-2, використовуючи оригінальні мітки з PQK-векторами ознак та оригінальними спектральними векторами ознак. Кожен експеримент складався з наступних етапів: підготовка датасетів, підготовка створеного датасету з PQK-векторами та експериментів з класифікації.

Було проведено порівняльне тестування за стандартними метриками, зокрема F-оцінки та точності. Експериментальні результати дозволили дійти висновку, що запропонована квантова нейронна мережа має точність та F-оцінку на рівні понад 95 % в порівнянні з моделлю традиційної повноз'язної нейронної мережі. Нами експериментально доведено, що класичні моделі машинного навчання, зазвичай використовувані для сегментації та/або класифікації фотографічних зображень, показують погані результати на досліджуваному наборі даних, використовуючи стандартні спектральні ознаки. Квантові процедури в поєднанні з класичними методами надають перевагу у завданнях навчання на великих наборах даних ДЗЗ. Точність класифікації значно збільшується, коли модель має доступ до PQK властивостей.

Але на останок слід зазначити, що використання квантових обчислень у машинному навчанні залишається в багатьох аспектах захоплюючою перспективою, оскільки кількісна оцінка квантових переваг таких додатків має деякі тонкі проблеми, що будуть предметом наших подальших досліджень.

УДК 004.2.056.55

ЕНЕРГООЩАДНЕ ПРИДУШЕННЯ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ З ЕКРАНІВ МОНІТОРІВ НА РІДИННО- КРИСТАЛІЧНИХ СТРУКТУРАХ

Дмитро Євграфов, Юрій Яремчук

Вінницький національний технічний університет

yurevyar@vntu.net

Припустимо, що нам необхідно протидіяти витоку інформації з ноутбуку, на якому циркулює конфіденційна інформація, і який експлуатується не на стаціонарному об'єкті з мережевим живленням, а у польових умовах з енергетичними обмеженнями. Екрани моніторів ноутбуків побудовані на рідинно-кристалічних структурах (РКС), а сигнали їх побічних електромагнітних випромінювань і наведень (ПЕМВІН) перехоплюються сучасними спеціалізованими засобами розвідки на відстанях у декілька сотень метрів. Нам необхідно протидіяти витоку інформації з екрану монітору. Подібна задача постає, оскільки не існує енергетичних можливостей ставити суцільну за спектром ΔF шумову заваду: енергії живлення вистачатиме лише на придушення окремих, найбільш інформативних k -х складових спектру ПЕМВІН – Δf_k . Зрозуміло, що у такому випадку контрольована зона, як правило, забезпечується належною організацією охорони і оборони об'єкту, на якому циркулює конфіденційна інформація. Але не розраховуватиме на це і для належної безпеки опиратимемося на технічний захист інформації в активний спосіб.

Метою даної роботи є обґрунтування показника заощадження енергії при застосуванні частотна-вибіркової завади у Δf_k -смугах у порівнянні із широкосмуговою шумовою завадою у спектрі ΔF .

Відомо, що спектри ПЕМВІН з екранів моніторів обчислювальних засобів простягаються від десятків кілогерц до декількох гігагерц, а ширина їх співставна з ΔF . Проте, якщо картинка на екрані монітору тривалий час аналізу T_a статична (незмінна), інформативними гармоніками витоку інформації є частоти $k f_{ver}$, k – номер гармоніки, $k = 1, 2, \dots, K$, f_{ver} – частота вертикальної розгортки екрану монітору, у смугах $\Delta f_k \approx 1/T_a$, для яких $K \approx \Delta F / f_{ver} = \Delta F T_k$, T_k – період кадрової розгортки екрану монітору. При постановці енергоощадної завади замість генерування шумового сигналу у смузі ΔF генеруються шумові сигнали у смугах

Δf_k , $k = 1, 2, \dots, K$, із сумарною шириною шумового сигналу $K\Delta f_k$, які потребуватиме у

$$\eta = \frac{T_a}{T_k}, \quad (1)$$

менше енергії для генерації шуму, ніж при постановці суцільної шумової завади.

При цьому проблема технічної реалізації активного захисту інформації виникатиме:

– під час оцінювання частоти вертикальної розгортки екрану монітору f_{ver} , оскільки неточне оцінювання призведе до неспівпадіння спектральної густини потужності сигналу $S(f)$ з гармоніками витоку інформації, особливо помітні для великих k (див. рис. 1), що робить прицільну за частотою заваду неефективною для великих частот;

– під час оцінювання T_a мінімального значення, для якого визначає мінімальне значення коефіцієнта заощадження енергії – η .

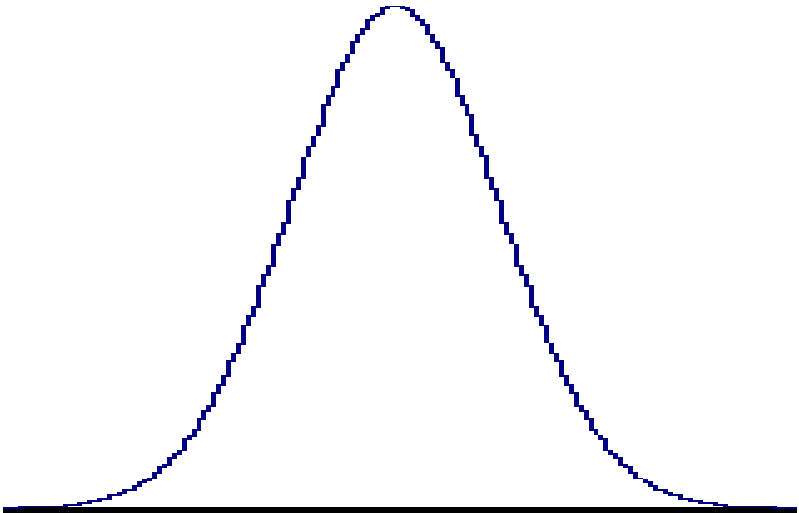


Рис. 1. Накриття спектру ПЕМВІН шумовим сигналом

У табл. 1 подано розраховану відповідно до (1) залежність коефіцієнта η від частоти кадрової розгортки монітору f_{ver} та часу аналізу T_a .

Таблиця 1

Коефіцієнт заощадження енергії шумового сигналу								
f_{ver} , Гц T_a , с	59,9	60,0	60,3	72,8	75,0	85,0	85,1	90
3	179,7	180	180,9	218,4	225	255	255,3	270
5	299,5	300	301,5	364	375	425	425	450
10	599	600	603	728	750	850	851	900
30	1797	1800	1809	2184	2250	2550	2553	2700
200	11980	12000	12060	14560	15000	17000	17020	18000

Як бачимо, у разі незмінного протягом 200 с кадру на екрані монітору з $f_{ver} = 90$ Гц можна у 18000 разів зменшити потужність випромінювання шумового сигналу, щоб ефективно придушити канал витоку інформації.

УДК 004.056

РИЗИКИ В АПАРАТНОМУ ЗАБЕЗПЕЧЕННІ

Сергій Зибін

*Національний авіаційний університет,
zysv@ukr.net*

У інформаційній системі кожна частина обладнання відіграє певну роль. Виходячи з важливості цієї ролі, необхідно вживати відповідних заходів безпеки. З метою зведення до мінімуму ризиків безпеки, застосовуються офіційні політики безпеки, які, як мінімум, повинні включати наступні дванадцять правил.

Правило перше. Ідентифікація підключень.

Кожна частина апаратного забезпечення, яка розглядається як апаратна одиниця, потребує чіткої ідентифікації, обґрунтування та захисту за допомогою спеціальних заходів безпеки. Робочі параметри апаратних одиниць повинні бути чітко задокументовані. Паролі повинні ідентифікувати своїх власників, а також їхніх адміністраторів, де адміністратори призначають паролі, а також політики оновлення, які повинні бути відомі всьому обізнаному персоналу. Непотрібні з'єднання необхідно видаляти, а необхідні підключати по мірі необхідності. Там, де це можливо, слід застосовувати журнали з'єднань, особливо для підключень до Інтернету, інтранету та будь-яких екстранетів.

Правило друге. Оцінювання безпеки.

Заходи безпеки необхідно оцінювати з періодичністю, пов'язаною з розвитком технологій і складністю атак. Оцінювання повинно включати аналіз вразливостей, а також тести на проникнення. Заходи безпеки повинні включати двонаправлені брандмауери в усіх точках входу-виходу, а також систему виявлення та запобігання вторгненням. Користувачам надаються паролі для доступу лише до функцій, для яких вони авторизовані. У будь-який час, 24/7, кожен апаратний блок має відповідальності за його безпеку.

Правило третє. Параметри постачальника.

Усі робочі параметри повинні бути введені обізнаним персоналом, і жодне обладнання не може залишатися з параметрами за замовчуванням, особливо іменами користувачів, паролями та налаштуваннями брандмауера. Існування будь-яких бекдорів, люків або спеціальних точок входу чи інтерфейсів постачальників має бути відоме та запечатане, якщо це можливо.

Правило четверте. Заходи безпеки.

Хоча більшість розробників апаратного забезпечення забезпечують власні заходи безпеки, найчастіше вони базуються на власних протоколах, дотримуючись філософії, що невідомість – це вбудована безпека. Це суперечить фундаментальному принципу безпеки, згідно з яким доступ має бути захищеним, а не прихованим від очей.

Правило п'яте. Виявлення та запобігання вторгненням.

Необхідно використовувати вбудовану, цілодобова систему виявлення та запобігання вторгненням, яка відстежує зовнішні та внутрішні вторгнення та звітує обізаному. Невід'ємною частиною системи виявлення та запобігання вторгненням є попередньо визначена послідовність кроків для обробки вторгнення. У кожній діяльності, пов'язаній із безпекою, має бути залучена команда ІТ-спеціалістів.

Правило шосте. Перевірки.

Часті технічні перевірки є основою будь-якої політики безпеки. Аудит повинен включати відвідування фізичного середовища апаратного блоку з метою можливого виявлення несанкціонованих можливих точок підключення, і для підтвердження дотримання політики фізичного доступу.

Правило сьоме. Команда з оцінювання ("Blue Team")

Метою створення команди являється відповідальність за оцінювання вразливостей, загроз і ризиків. Команда є постійним комітетом з ІТ не-ІТ спеціалістів, який визначає сценарії атак і пропонує захист і протидію.

Правило восьме. Посадові інструкції.

Чіткі посадові інструкції визначають обов'язки та повноваження кожного учасника структури кібербезпеки. Для виконання яких необхідно розробити кроки, яких необхідно вжити у разі кібернебезпечної ситуації.

Правило дев'яте: Критичні функції.

Необхідно розробити ієрархічну структурну діаграму, що ілюструє різні функції системи. Також має бути показано рівень їх відносної важливості разом із відповідними загрозами та відповідними контрзаходами. Враховуючи, що нові загрози з'являються постійно, дана діаграма має постійно переглядатися комітетом з кібербезпеки організації.

Правило десяте. Безперервність.

Необхідно вживати заходи і запроваджувати процедури для відновлення після кібератаки. Це вимагає безперервного та багаторівневого архівування даних, функціонального резервування та ознайомлення персоналу з необхідними процедурами.

Правило одинадцятьте. Керування конфігурацією.

Конфігурація будь-якої системи, а тим більше будь-якої інформаційної системи, ніколи не може бути статичною. Нове апаратне забезпечення, нове програмне забезпечення, нові загрози, нові ринки, нові технології та нові ідеї вимагають від ІТ-стратегів еволюційного переналаштування систем.

Правило дванадцяте. Поглиблений захист.

Це дуже стара оборонна концепція, яку було перенесено в інформаційні системи. Основними принципами якої являються два принципи: пошаровий захист і відсутність єдиної точки відмови. Успішна реалізація цієї концепції вимагає впровадження відповідних заходів протягом усього процесу розробки системи. Такі заходи створюють кілька рівнів захисту між учасником і ресурсом, до якого планується здійснювати доступ і блокують доступ учасника до неавторизованих зон.

Поглиблений захист – це стратегія забезпечення захисту інформації, у якій кілька рівнів захисту розміщено по всій системі. Він усуває вразливі місця в забезпеченні безпеки персоналу, технологій і операцій протягом життєвого циклу системи.

УДК 004.94:316.472.4

ІМІТАЦІЙНІ МОДЕЛІ ПРИ МОДЕЛЮВАННІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

Ольга Васильєва

Національний університет «Чернігівська політехніка»

olga.vasiljeva37@gmail.com

Моделювання можна розглядати як один із способів вирішення проблем, що виникають у реальному світі, зокрема, при плануванні та проведенні інформаційних операцій. Найчастіше моделювання застосовується у випадках, якщо експерименти з реальними об'єктами неможливі або занадто витратні. Моделювання охоплює відображення реальної проблеми у світ абстракції, вивчення, аналіз та оптимізацію моделі й відображення оптимального рішення назад у реальний світ.

Метою даної роботи аналіз імітаційних моделей інформаційних операцій, що проводяться в соціальних мережах.

При моделюванні існує два альтернативних підходи - аналітичне та імітаційне моделювання. Ідеальні аналітичні моделі допускають строге аналітичне рішення, або, щонайменше, постановку, наприклад у вигляді систем диференціальних рівнянь. Однак аналітичні рішення не завжди досяжні. Тому, особливо останнім часом, і особливо при вирішенні завдань із сфери соціальної динаміки все частіше застосовуються методи імітаційного моделювання (англ. - Simulation Modeling). Імітаційне моделювання є могутнім і практично незамінним засобом аналізу соціальних процедур.

Можливість замінити реальну мережу на її модель відкриває перспективи для дослідження поширення інформації в моделі мережі з перенесенням отриманих результатів досліджень на реальну мережу, що надалі дозволяє отримати відомості про топології малих мереж.

Для моделювання інформаційних операцій в соціальних мережах можна використовувати різні імітаційні моделі. Розглянемо деякі з них.

Моделі незалежних каскадів (Independent Cascade Model) належать до моделей так званих систем частинок, що взаємодіють (Interacting Particles Systems). Вузол мережі (агент) визначається аналогічно з моделлю з порогами. Коли агент і стає активним в певний момент часу t , він отримує шанс активувати на наступному (і тільки на наступному) кроці кожного зі своїх сусідів j з імовірністю P_{ji} (причому j можуть намагатися незалежно активувати і інші агенти).

«Теоретико-ігрові» моделі, в яких акцент робиться на інформованість і взаємозв'язок між гравцями (агентами). Виграш, що отримується агентом (гравцем), залежить від дій опонентів (інших гравців). Агент діє так, щоб максимізувати свою вигоду.

Моделі «дифузії інновацій». Динаміка процесу поширення традиційно моделюється логістичною кривою (\wedge -образною), що по суті є характеристикою будь-якого інфекційного процесу або процесу навчання.

За допомогою теорії поширення нововведень (diffusion theory), яку науковці використовують також для моделювання соціальних систем, намагаються пояснити, які умови збільшують або зменшують ймовірність прийняття нововведення членами соціальної системи, з якою швидкістю нововведення розповсюджується в соціальній системі.

Модель Ізінга. Модель Ізінга - математична модель, що описує виникнення намагнічування матеріалу. Передбачається, що конформність або незалежність у великій соціальній групі може моделюватися за допомогою моделі Ізінга; вплив найближчих сусідів є визначальним, а аналогом температури є готовність групи мислити творчо, готовність прийняти нові ідеї. Зовнішнім полем для соціальної групи є вплив «авторитету» або управління.

Моделі на основі клітинних автоматів. Для опису процесів поширення інформації в соціальній мережі останню модель можна розглядати як складну адаптивну систему, яка складається з великої кількості агентів, взаємодія між якими призводить до масштабної, колективної поведінки, яку важко передбачити і аналізувати. Для моделювання та аналізу таких складних систем іноді використовуються клітинні автомати. Клітинний автомат складається з набору об'єктів (в даному випадку агентів), які зазвичай утворюють регулярну решітку. Стан окремо взятого агента в будь-який дискретний момент часу характеризується деякою зміною. Стани синхронно змінюються через дискретні інтервали часу відповідно до незмінних локальних вірогідних правил, які можуть залежати від станів найближчих сусідніх агентів в оточенні даного агента, а також, можливо, від стану самого агента.

Ланцюги Маркова. В даній моделі вивчається вплив в групі агентів. Запропонована модель є динамічною Байєсовою мережею (Dynamic Bayesian Network - DBN) з дворівневою структурою: рівнем індивідів (моделюються дії кожного агента) і рівнем групи (моделюються дії групи в цілому).

У більшості моделей в основному розглядаються правила взаємодії агентів, але що стосується самої мережі впливу в цілому, її властивостей, взаємозв'язків і процесів взаємодії, то наявний аналіз цих моделей надає дуже небагато результатів.

Агентне моделювання - відносно новий напрямок в імітаційному моделюванні, що використовується для дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами і законами

(як в інших парадигмах імітаційного моделювання), а навпаки, коли ці глобальні правила і закони є результатом індивідуальної активності членів групи.

Агента модель являє реальний світ у вигляді багатьох активних підсистем, які окремо специфікуються, та називаються агентами (автономних об'єктів, цілеспрямовано функціонуючих в конкретному середовищі за певним набором правил, що взаємодіють один з одним і адаптуються в процесі функціонування). Зазвичай в таких системах не існує глобального централізованого управління, агенти функціонують за своїми законами асинхронно.

Науковий керівник – д.пед.н., проф. Ткач Ю.М.

УДК 004.092

КІБЕРБЕЗПЕКА ВІРТУАЛЬНИХ ГРОШЕЙ В ЕПОХУ ЦИФРОВОЇ ЕКОНОМІКИ

Віта Каштан¹, Денис Іванов², Ольга Коробко³

Національний технічний університет «Дніпровська політехніка»

¹kashtan.v.yu@ntnu.one, ²ivanov.d.v@ntnu.one, ³korobko.o.v@ntnu.one

З розвитком технологій і зростанням складності систем і технічних механізмів, що лежать в основі функціонування сучасного суспільства, нова форма безпеки є важливою та застосовується до всіх обчислювальних пристроїв. Кібербезпека має як фізичне, так і цифрове значення, а саме як для захисту цілісності обладнання та схем, так і для захисту даних та інформації, що зберігаються, передаються та обробляються обладнаннями. Активне використання комп'ютерних систем у таких сферах як фінансові системи, комунальні послуги, промислове обладнання, персональні споживчі пристрої, ІТ-інфраструктура компаній та навіть Уряд є уразливими до кібератак. Ефективна кібербезпека полягає у здатності захищати комп'ютерні системи від несанкціонованого доступу, змін або знищення обладнання, крадіжки інформації або порушення конфіденційності та цілісності даних.

Метою роботи є огляд моделей виявлення актуальних загроз порушення інформаційної безпеки даних при використанні віртуальних грошей, що враховує склад специфічних загроз, пов'язаних із технологією «блокчейн» (конфіденційність, доступність, цілісність, достовірність).

Стандарт ISO/IEC 27032 визначає кібербезпеку як «збереження конфіденційності, цілісності та доступності інформації в кіберпросторі». У свою чергу, кіберпростір визначається як «складне середовище, що є результатом взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою підключених до нього технологічних пристроїв і мереж, яке не існує в жодній фізичній формі». Тому, із впровадженням криптовалют виникли нові проблеми кібербезпеки.

Стрімке зростання світової вартості криптовалютного ринку привернуло не тільки чесних інвесторів, але й шахраїв. Загалом шахрайство з криптовалютою поділяється на дві різні категорії, а саме: витік даних і дезінформація. За визначенням, порушення даних – це «порушення безпеки, яке призводить до

випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до захищених даних, що передаються, зберігаються або обробляються іншим чином». Рівень безпеки криптовалютного гаманця залежить від його типу з урахуванням схеми управління ключами. Здається раціональним використовувати холодні гаманці, оскільки їх автономний дизайн ефективно захищає збережені активи від крадіжки. З іншого боку, так як кількість гаманців не обмежена, їх активи можна зберігати на різних типах гаманців. Крім того, для забезпечення найвищого рівня безпеки даних слід дотримуватись правил таких як мінімальна довжина пароля, складність і примусове дотримання історії, мінімальний і максимальний вік пароля. Інша головна проблема полягає в розробці резервного копіювання та відновлення даних. Це дозволить швидко відновити дані.

Сьогодні широко використовується технологія блокчейн для цифрових валют. Так як має високий рівень безпеки. Ця ідея відносно нова, але досить популярна серед дослідників у всьому світі, які пропонують модифікації початкової ідеї, щоб подолати дедалі більше виявлених проблем (наприклад, високе енергоспоживання, тривалий час роботи, проблеми з масштабованістю, тощо) і проблеми безпеки (слабкі сторони внутрішньо використовуваних алгоритмічних процедур, підвищена вразливість до атак, викликаних передачами на великі відстані, і проблеми з конфіденційністю користувачів і відсутністю анонімності, тощо).

Кіберзлочинна діяльність зараз спрямована на криптовалюти через псевдонім і конфіденційність, які вони пропонують. Зловмисники продовжують створювати нові кібератаки, незважаючи на те, що розроблена велика кількість методів, методик захисту для запобігання цих дій. Фішингові атаки є одними з найпоширеніших атак соціальної інженерії та можуть використовувати складні методи, такі як, наприклад, атака «Людина посередині» (Man in the middle). Цей вид атаки характеризується тим, що хакери опиняються в центрі цифрового комунікаційного зв'язку між електронним банком і його клієнтами, де ні банк, ні клієнт не знають про атаку, а конфіденційні дані та облікові дані скомпрометовані. Незалежно від обраної техніки атаки, хакери прагнуть отримати дані користувачів електронного банкінгу, щоб здійснювати фінансові махінації та незаконно збирати гроші користувачів на користь хакера.

Щоб протистояти кібератакам, користувачам та співробітникам банку потрібно регулярно проходити онлайн-навчання з безпеки, бути в курсі потенційних загроз і методів атак, використовувати двофакторну автентифікацію (ідентифікацію клієнта за допомогою додаткового компонента у вигляді коду, надісланого на електронну поштову скриньку і/або телефон, підтвердження через дзвінок або додаткові біометричні дані та з використанням додатку Google Authenticator), прив'язка IP-адреси до конкретного пристрою користувача (увімкнути можливість авторизації тільки з довірених IP-адрес), використовувати комплексний підхід у вигляді Internet Security антивірус, що включає в себе антивірус, захист від DDoS атак, фішингу та firewall захист.

Таким чином, для цифрової валюти безпека все ще є основним принципом, включаючи захист від подвійних витрат, підробок, а також витоку облікових записів і даних. В даній роботі представлено узагальнений опис вимог та алгоритмів проведених безпеки даних, з урахуванням нових тенденцій розвитку

інформаційних систем. Обґрунтовано актуальність розробки методу забезпечення безпеки даних при їх обробці в блокчейн-системі, що передбачає безпеку аналізу санкціонованої поведінки користувачів інформаційної системи.

УДК 004.056.5

ОСОБЛИВОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ДОРОЖНІМ РУХОМ ЯК ОБ'ЄКТІВ КІБЕРЗАХИСТУ

**Олександр Кручинін¹, Володимир Святошенко²,
Дмитро Тимофєєв³**

НТУ «Дніпровська політехніка»

¹kruchinin.o.v@nmu.one, ²sviatoshenko.v.o@nmu.one,

³tymofiev.d.s@nmu.one

Згідно з визначеннями, які наведені у законі України «Про основні засади забезпечення кібербезпеки України», автоматизована система управління дорожнім рухом (АСУ ДР) може бути віднесена до об'єктів критичної інформаційної інфраструктури. Таким чином, АСУ ДР є об'єктом кіберзахисту та потребує реалізації відповідних заходів.

Метою даної роботи є аналіз особливостей автоматизованих систем управління дорожнім рухом як об'єкта критичної інформаційної інфраструктури.

Насамперед АСУ ДР призначена для забезпечення ефективного функціонування вулично-дорожньої мережі міста. Але на сьогодні вона може взаємодіяти з іншими системами, які об'єднані у повністю інтегровану інтелектуальну інфраструктуру міста, що дозволяє в режимі реального часу здійснювати збір й аналіз даних і реалізовувати управління всіма процесами діяльності міських служб.

Типова АСУ ДР складається з трьох частин:

- Центральний управляючий пункт. До його складу входять автоматизовані робочі місця для контролю та управління; управляючий обчислювальний комплекс; комплект контрольно-діагностичної апаратури.

- Периферійне обладнання. До його складу входять дорожні контролери; детектори транспорту; вносні пульти керування, покажчики швидкості руху; керовані знаки; табло виклику пішохода; комплекти апаратури пріоритетного пропуску.

- Мережева інфраструктура. Включає мережі зв'язку, які забезпечують передачу даних між фізичними та керуючими компонентами системи.

Але на сьогодні додаткові функції АСУ ДР та швидкий розвиток технологій впливають як на структуру системи, так і на перелік та вид представлення інформації в системі. Наприклад, є перспективним впровадження до таких систем «розумних» автомобілів, технологій ІоТ, використання даних систем міського відеоспостереження для реалізації нових алгоритмів управління, систем трекінгу автотранспорту та інше. Це необхідно враховувати при аналізі загроз, визначенні ризиків та при обґрунтуванні вибору методів та засобів захисту.

В АСУ ДР циркулює інформація різного змісту та виду представлення: алгоритми управління дорожнім рухом, дані та звіти про трафік, інформація про технічний стан елементів системи, відеозаписи дорожнього руху та місць дорожньо-транспортних пригод, база географічна інформація, інформація з трекерів транспортних засобів, статистичні дані, пакети даних керування периферійними пристроями тощо. Частина цієї інформації є з обмеженим доступом, але практично вся потребує захисту.

Основними особливостями АСУ ДР, які необхідно враховувати при забезпеченні їх кіберзахисту, є такі характеристики:

- гетерогенність: інформаційно-комунікаційна система реалізує різні технології; обчислювальна система складається з різноманітного за призначенням, рівнем апаратного та програмного забезпечення;

- система розподілена: периферійне обладнання знаходиться на значних відстанях та підключені через незахищене середовище, у тому числі із використанням радіоканалів. Крім того, живлення цих пристроїв не може бути централізованим;

- обмеження ресурсів: значна частка периферійного обладнання має обмеження щодо параметрів апаратного забезпечення. Це обумовлює наявність обмежень до обчислювальних можливостей та відстані стабільної роботи каналів зв'язку;

- чутливість до затримок: система повинна працювати в режимі реального часу. Це, враховуючи обмеження ресурсів, обмежує використання деяких методів та засобів захисту, у тому числі криптографічних;

- складність системи: велика кількість компонентів системи, їх взаємовплив один на одного, наявність алгоритмів адаптованого управління, спричиняє виникнення труднощів при аналізі захищеності системи.

Додатково слід зазначити, що АСУ ДР є системами, які в процесі експлуатації можуть постійно розширюватися. Тому запропоновані рішення з кібербезпеки повинні бути масштабованими. Також, враховуючи довгостроковий термін експлуатації таких систем, механізми захисту повинні бути динамічними та мати змогу реагувати на зміни вимог щодо рівня кібербезпеки.

Крім цього, наявність незахищених каналів зв'язку та обмеження ресурсів створює додаткові труднощі з розповсюдженням та зберіганням криптографічних ключів.

Ще однією особливістю існуючих АСУ ДР є те, що програмне забезпечення практично всіх рівнів системи не має підтвердженого рівня своєї безпеки. Це може ускладнити проведення випробувань на відповідних етапах впровадження та експлуатації АСУ ДР. Хоча розробники таких систем декларують, що: інформація, яка циркулює у системі, шифрується сучасними методами криптографії; користувачам системи доступні функції, передбачені попередньо встановленими правами доступу до системи; протоколюються та авторизуються всі дії користувачів, а також усі системні події у режимі реального часу. Безумовно, ці твердження розробників потребують незалежної перевірки.

Висновки: зазначені особливості АСУ ДР необхідно враховувати при розробці, впровадженні та експлуатації систем кібербезпеки. Для цього слід використовувати найкращі світові практики, які відображені у відповідних

стандартах та рекомендаціях. Особливу увагу слід приділити обранню та використанню методів та засобів реалізації криптосистем, заснованих на «легковагових» криптоалгоритмах.

УДК 004.942

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВІДКРИТИХ ПЛАТФОРМ З КІБЕРБЕЗПЕКИ

Володимир Святошенко¹, Олександр Кручинін², Дмитро Тимофєєв³

НТУ «Дніпровська політехніка»

¹sviatoshenko.v.o@nmu.one, ²kruchinin.o.v@nmu.one,

³tymofiev.d.s@nmu.one

В сучасному світі кібербезпека стала критично необхідною для бізнесу та державних установ. Навчання студентів у галузі кібербезпеки стає все більш важливим для підготовки майбутніх спеціалістів. Використання відкритих платформ для навчання кібербезпеці може бути ефективним способом підвищення практичних навичок студентів спеціальності кібербезпека.

Метою даної роботи є визначення вимог до оцінки ефективності відкритих освітніх платформ з кібербезпеки.

Однією з переваг використання відкритих платформ є доступність навчальних матеріалів та ресурсів для студентів з усього світу. Це дозволяє студентам отримати доступ до найновіших технологій та інструментів у галузі кібербезпеки та вдосконалювати свої практичні навички. Більше того, використання відкритих платформ дозволяє студентам навчатися у своєму власному темпі та з використанням своїх власних пристроїв.

Іншою перевагою відкритих платформ є можливість співпраці з іншими студентами та експертами у галузі кібербезпеки. Студенти можуть обговорювати свої ідеї та досвід з іншими учасниками платформи та отримувати корисні поради та рекомендації від кваліфікованих фахівців. Це допомагає студентам розвивати свої навички та знання у галузі кібербезпеки та підвищує їх можливості на ринку праці.

Окрім того, відкриті платформи можуть бути ефективним засобом для проведення онлайн-курсів та тренінгів у галузі кібербезпеки. Це може бути особливо корисним для студентів в місцях, де немає можливості залучення кваліфікованих викладачів або недостатньо фінансових ресурсів для організації традиційної освіти у галузі кібербезпеки, зокрема сучасних кіберполігонів.

Однак, використання відкритих платформ також має свої недоліки. Один з головних недоліків полягає у тому, що студенти можуть відчувати недостатній контроль над своїм навчанням та бути менш мотивованими до здобуття знань. Крім того, відкриті платформи можуть мати обмежені можливості для індивідуального налаштування навчального процесу та врахування різних потреб студентів.

Авторами були проаналізовані широковживані платформи призначені як для самостійної підготовки, так і під керівництвом викладача, серед яких:

HackTheBox - платформа для тестування пенетрації, яка дозволяє вчитися у реальних умовах; TryHackMe - платформа з різними викликами, лабораторіями та іграми для навчання кібербезпеки; RangeForce - це платформа для тренування з кібербезпеки, яка надає широкий спектр навчальних курсів та симуляцій з різних аспектів кібербезпеки; Pentester Academy - платформа з курсами з пенетраційного тестування, які можна вивчати онлайн; Subrary - платформа з безкоштовними та платними курсами з кібербезпеки, які допомагають вдосконалити практичні навички.

За результатами проведеного аналізу сформовано основні вимоги до платформ з підвищення практичних навичок з кібербезпеки:

- рівень доступності: платформа повинна бути доступною та зручною для використання студентами з різним рівнем підготовки;

- підтримка траєкторій навчання: можливість студента обрати кваліфікаційну траєкторію;

- актуальність матеріалів: платформа повинна містити оновлені та актуальні матеріали, що відповідають сучасним вимогам та технологіям у галузі кібербезпеки;

- рівень інтерактивності: платформа повинна забезпечувати можливість практичного виконання завдань та інтерактивного взаємодії з іншими студентами та викладачами;

- адаптивності: платформа повинна мати можливість індивідуального налаштування навчального процесу та врахування різних потреб та рівнів підготовки студентів;

- контроль та оцінювання: платформа повинна забезпечувати належний та гнучкий контроль і оцінку знань студентів, а також можливість відстеження прогресу та результативності навчання;

- взаємодія з роботодавцями: платформа повинна забезпечувати можливість практичної взаємодії з роботодавцями, щоб студенти мали можливість здобувати практичний досвід та виконувати реальні завдання у галузі кібербезпеки;

- гнучкість: платформа повинна мати можливість розширення та адаптації до різних потреб користувачів, що включає можливість використання на різних платформах та пристроях;

- підтримка: платформа повинна забезпечувати належний рівень підтримки для студентів та викладачів, що включає доступність технічної підтримки та можливість вирішення будь-яких проблем, що виникають в процесі навчання;

- підтримка контенту різними мовами: платформа за можливості повинна підтримувати контент мовою користувача;

- підтримка гейміфікації: можливість проводити змагання у формі гри як між окремими студентами так і групами;

- рівень ціноутворення: платформа повинна мати належний рівень ціноутворення, щоб студенти або навчальні заклади мали можливість використовувати її без додаткового фінансового навантаження.

Ці вимоги можуть бути розглянуті у якості базових для порівняння різних платформ з підвищення практичних навичок студентів та допомогти обрати найбільш зручну та ефективну платформу для навчання.

При виборі платформи важливо враховувати не лише означені вимоги, але і індивідуальні запити, потреби та рівень знань студента.

УДК 004.77

РЕАЛІЗАЦІЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ В ПРОЦЕСІ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ УКРАЇНИ

Дмитро Тимофєєв¹, Олександр Кручинін², Володимир Святошенко³

НТУ «Дніпровська політехніка»,

¹tymofiev.d.s@nmu.one, ²kruchinin.o.v@nmu.one, ³sviatoshenko.v.o@nmu.one

В умовах продовження кіберагресії проти України та розширення застосування новітніх інформаційно-комунікаційних технологій в освітній та науковій діяльності, забезпечення системного підходу до організації кіберзахисту та інформаційної безпеки є необхідною передумовою сталого розвитку закладів вищої освіти.

Метою даної роботи є підвищення ефективності впровадження системи управління інформаційною безпекою в закладах вищої освіти (ЗВО) за рахунок реалізації принципів архітектури нульової довіри.

Інформація та інформаційні технології стають найважливішими активами сучасної освіти, що сприяють підвищенню її конкурентоспроможності, заклади вищої освіти мають приділяти особливу увагу вирішенню завдань забезпечення інформаційної та кібербезпеки.

Комплексний підхід до вирішення широкого спектру задач реалізує система управління інформаційною безпекою (СУІБ), що використовує досвід кращих практик міжнародних експертних груп відповідного напрямку відображений у стандартах сімейства ISO/IEC серії 27k.

Серед задач, що вирішуються, можна виділити: відповідність діяльності ЗВО вітчизняним та міжнародним регуляторним актам означеного напрямку; регулярне підвищення рівня освіченості працівників у сфері інформаційної безпеки (ІБ); запровадження та впорядкування моніторингу та контролю безпеки і доступу до інформаційно-комунікаційних систем (ІКС); управління інцидентами, категоріювання та забезпечення конфіденційності інформації; антивірусний захист, резервне копіювання, ліцензійна чистота програмного забезпечення, вхідний/вихідний контроль за обміном інформацією в ІКС; впорядкування технічного та криптографічного захисту інформації; забезпечення фізичної безпеки та інших аспектів інформаційної та кібербезпеки, зокрема захисту персональних даних.

Однак, на відміну від широко вживаних та достатньо деталізованих в Україні вимог до комплексних систем захисту інформації, вимоги до СУІБ чітко не визначені. Означене можна розглядати як недолік з точки зору відсутності конкретних проектних характеристик, але дозволяє доповнити базовий для розробки СУІБ ризик-орієнтований підхід застосуванням відомих моделей та принципів проектування безпечних систем. Відповідно до вимог п. 8.27 стандарту ISO/IEC 27001:2022 відповідні принципи повинні бути встановлені,

задокументовані, підтримувані та застосовані до розробки будь-якої інформаційної системи.

Однією з найбільш перспективних та таких моделей забезпечення кібербезпеки що широко впроваджується є модель архітектури нульової довіри (ZTA), яка підтримується найбільшими і технологічно передовими компаніями та організаціями світу, включаючи такі технологічні корпорації як Google, Microsoft, CISCO, а також урядом США для застосування в державних установах. За даними глобальних опитувань відомо, що близько 70% організацій або впроваджують нульову довіру, або планують прийняти це найближчим часом. Нульова довіра має складатися з моніторингу всіх мережевих комунікацій, уникнення конфігурацій за замовчуванням, відстеження всіх пристроїв і реалізації багатофакторної автентифікації. При цьому стандарт ISO/IEC 27001:2022 вимагає забезпечення підтримки з боку керівництва, комунікації, навчання, моніторингу та вимірювання, а також аудиту, що надає переваги процесу інтегрованого впровадження СУІБ та ZTA.

Хоча провідні кампанії ринку послуг з кібербезпеки та інформаційних технологій створюють власні визначення нульової довіри, існує низка стандартів визнаних організацій, які допоможуть відповідальним фахівцям адаптувати у власні рішення складові архітектури нульової довіри, зокрема NIST 800-207. Існують додаткові вказівки, доступні від таких організацій, як The Open Group's Zero-Trust Architecture Working Group і NIST, включаючи нові еталонні моделі, які можуть полегшити перехід до архітектури нульової довіри та її розвиток, зокрема Zero Trust Maturity Model версія 2.0 від Cybersecurity and Infrastructure Security Agency (США).

Можливість та доцільність використання ZTA в процесі реалізації СУІБ ЗВО обумовлена наступними перевагами:

- організаційна система ЗВО є стабільною, ієрархічною за структурою та управлінськими функціями, яка діє на принципах централізованого управління;
- широке використання ЗВО України на поточному етапі розвитку централізованих та уніфікованих хмарних сервісів провідних технологічних провайдерів, з урахуванням пільгових фінансових умов для освітніх установ;
- можливість поступового впровадження основних елементів архітектури в окремих адміністративних або територіальних підрозділах ЗВО;
- наявність детальних інструкцій та підтримки з впровадження основних елементів ZTA зі сторони компаній постачальників послуг;
- зацікавленістю керівництва ЗВО в гарантіях забезпечення ефективної протидії кіберзагрозам.

Основні проблеми впровадження як архітектури нульової довіри, так і в цілому системне забезпечення інформаційної та кібербезпеки в ЗВО України мають загальні причини та обумовлені відсутністю формалізації бізнес-процесів, низьким рівнем фінансування, застарілою та гетерогенною архітектурою ІКС, недостатньою кваліфікацією та/або перевантаженням залучених фахівців з кібербезпеки та інформаційних технологій, неможливістю або небажанням застосування суворих протоколів та політик безпеки.

УДК 539.23, 538.958, 004.056.53

**БАГАТОФУНКЦІОНАЛЬНІ ОПТИЧНІ ЕЛЕМЕНТИ НА ОСНОВІ
БАКТЕРІОРОДОПСИНУ У СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ****Іван Трикур¹, Михайло Січка², Олександр Чобаль³,
Галина Різак⁴, Василь Різак⁵***ДВНЗ «Ужгородський національний університет»**¹ivan.trikur@uzhnu.edu.ua, ²mykhaylo.sichka@uzhnu.edu.ua,
³oleksandr.chobal@uzhnu.edu.ua, ⁴galyna.rizak@uzhnu.edu.ua,
⁵vrizak@uzhnu.edu.ua*

Актуальність проблематики вдосконалення систем інформаційної безпеки важко переоцінити. Одним з невід'ємних елементів розвитку таких систем є розробка та створення їх матеріальної бази. Бактеріородопсин (БР), який володіє рядом цікавих властивостей, є одним з біологічних матеріалів, що можуть бути ефективно використані у даному напрямку. Від більшості білків він відрізняється структурною організацією молекул у вигляді двомірних кристалів, завдяки чому, демонструє набагато більшу, порівняно з іншими білками, фізичну та хімічну стабільність. Завдяки цьому для БР можливі способи практичного використання, які не можуть бути використані для інших білків. Комбінація оптичних властивостей БР з іншими матеріалами дозволяє отримати функціональні елементи, які можуть бути використані у системах інформаційної безпеки.

Метою даної роботи є систематизація, аналіз та узагальнення даних про можливості використання матеріалів на основі БР у багатофункціональних оптичних елементах систем контролю доступу та інформаційної безпеки.

Поглинання одного кванту світла приводить до збудження молекули БР, після чого, через ряд проміжних станів - інтермедіатів, вона повертається у вихідний стан. Інтермедіати відрізняються спектрально і часами життя. Одним з таких проміжних станів є інтермедіат K_{610} , який стабільний при температурах нижче 150 К. Переходи між BR_{570} і K_{610} можуть ініціюватися при опроміненні молекули світлом відповідної довжини, що дозволяє створити бінарну фотохімічну систему на основі даних двох станів. Висока квантова ефективність ($BR \rightarrow K=65\%$, $K \rightarrow BR=80\%$) фотопереходів відкриває можливість створення криогенних запам'ятовуючих пристроїв, які володіють високою швидкодією та ефективністю. Аналогічну систему можна реалізувати на основі переходу $BR_{570} \leftrightarrow M_{412}$. Для даної фотореакції характерний більший спектральний зсув між станами та високі квантові ефективності ($BR \rightarrow M=65\%$, $M \rightarrow BR=65\%$). При температурах вище 240 К інтермедіат M_{412} термічно нестабільний і молекула переходить в основний стан протягом кількох мілісекунд. Високі перерізи двофотонного поглинання роблять можливим 3-D запис інформації, що суттєво збільшує ємність носіїв. Висока роздільна здатність дозволяє реалізувати голографічний посторінковий запис інформації з адресацією за змістом, який не може бути реалізований за допомогою звичайної електроніки. Носії на інтермедіатах K_{610} та M_{412} можуть знайти застосування коли зберігання секретних даних вимагає їх лабільності для

запобігання несанкціонованому доступу. Остання можливість пов'язана з тим фактом, що всі дані, які зберігаються в інтермедіатах К або М, будуть безповоротно втрачені при нагріванні носія вище ніж 150 та 240 К відповідно.

При лазерному опроміненні молекула БР може поглинати два фотони, що призводить до утворення фотопродукту F_{620} , який не повертається у вихідний стан. Поляризований лазерний імпульс при взаємодії з іммобілізованим БР індукує постійну фотоіндуковану анізотропію, що може бути використано для поляризаційного запису. Точки даних можуть записуватися різною поляризацією, наприклад $0^\circ - "1"$, $90^\circ - "0"$. Інформацію, записану у вигляді зміни поляризаційних властивостей середовища, важко скопіювати. Роздільна здатність середовища в поєднанні з наведеним способом запису дозволяє здійснювати кутове мультиплексування, що може суттєво збільшувати густину запису та ускладнювати її копіювання. Крім прямого оптичного запису даних БР дає можливість оптичного шифрування даних. При записі обох видів поляризації в одному місці матеріал втрачає анізотропію. Поляризація в таких точках не може бути зчитана, що, у свою чергу, не дасть можливості інтерпретувати її як «0» або «1». Це означає, що набір двійкових даних, який має бути зашифрований, перезаписується другим набором даних, який служить «ключем» для шифрування. У всіх бітах, де дані та ключ співпадають, накладена точка даних не змінюється. Але в позиціях де значення бітів даних і ключа не співпадають – анізотропія стирається. Інформація може бути відновлена тільки якщо відомий ключ.

Реверсивний фотохромний зсув поглинання у видимій області при переході $BR_{570} \leftrightarrow M_{412}$ під дією освітлення, дозволяє отримувати фотохромні чорнила для захисного маркування та виготовлення фотохромних областей на картах доступу чи перепустках. Реологічні характеристики таких чорнил подібні до комерційних. Реверсивна зміна кольору дозволить унеможливити несанкціоноване копіювання документів або/та верифікувати відповідне маркування продукції. Використання барвників в стехіометричному співвідношенні з молекулами БР дозволяє отримати повний спектр кольорових відтінків при збереженні фотохромності матеріалу. Наявність всього спектру чорнил полегшить інтеграцію елементів захисту в будь-який документ.

Зміну кольору чи наявність поляризаційно записаної інформації можна помітити неозброєним оком. Однак матеріали на основі БР дозволяють створити захисні елементи, які можна проаналізувати лише в лабораторних умовах. Зокрема можна реалізувати можливість відстеження партій товару виготовленого чи маркованого з використанням БР. Для цього нефункціональні частини амінокислотного ланцюга можна модифікувати, наприклад, заміною певних амінокислотних залишків. Така модифікація виявляється лише мас-спектроскопічними методами та дозволяє надійно ідентифікувати походження матеріалу.

Всі перераховані можливості можуть бути реалізовані в багатофункціональних (як видимих так і не видимих) елементах захисту на одній ID-карті. Перераховані вище факти свідчать, що фотохромні матеріали на основі БР можуть ефективно використовуватися у сфері інформаційної безпеки та контролю доступу.

УДК 004.05 (043.2)

АНАЛІЗ МЕТРИК КІБЕРБЕЗПЕКИ ДЛЯ ОЦІНЮВАННЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Роман Гамрецький¹, Костянтин Зандер²

Національний авіаційний університет

¹45391@stud.nau.edu.ua, ²viktor.hnatiuk@npp.nau.edu.ua

Дослідження метрик кібербезпеки для оцінювання якості програмного забезпечення (ПЗ) в інформаційно-комунікаційних системах (ІКС) є дуже актуальним завданням у сучасному цифровому світі. Це зумовлено, насамперед: зростанням кількості кібератак, законодавчими та регуляторними вимогами, розширенням технологій та розвитком застосувань, підвищеною увагою до захисту персональних даних, економічними втратами від кібератак, зростанням комплексності програмного забезпечення, необхідністю відповідності вимогам стандартів безпеки, розвитком штучного інтелекту та Інтернету речей, тощо.

Сьогодні існує низка діючих стандартів та нормативних документів, які описують метрики кібербезпеки для оцінювання якості ПЗ в ІКС. Базові з них:

1. Стандарти серії ISO/IEC 27000. Це серія міжнародних стандартів, що визначають вимоги до систем управління інформаційною безпекою. Зокрема, стандарт ISO/IEC 27001 визначає вимоги до управління кібербезпекою, включаючи метрики та вимоги до оцінювання ризиків та заходів безпеки.

2. Стандарт OWASP Top Ten Project. Це проект, розроблений Організацією відкритого веб-застосування (OWASP), який ідентифікує десять найпоширеніших вразливостей безпеки в веб-додатках. Він надає метрики для оцінювання рівня захисту веб-додатків від цих вразливостей.

3. Нормативні документи NIST (National Institute of Standards and Technology). NIST розробляє ряд публікацій, включаючи Керівництва з кібербезпеки, які містять рекомендації щодо оцінювання кібербезпеки в різних контекстах, включаючи оцінку якості програмного забезпечення.

4. Стандарти CWE (Common Weakness Enumeration) та CVSS (Common Vulnerability Scoring System). CWE визначає спільні вразливості в програмному забезпеченні, а CVSS надає систему оцінки вразливостей з точки зору серйозності та впливу на кібербезпеку, включаючи метрики, такі як вразливість, доступність, конфіденційність та цілісність.

5. Стандарт ISO/IEC 15408 (Common Criteria). Це міжнародний стандарт, який визначає процедури оцінки безпеки і сертифікації продуктів і систем. Він містить метрики та критерії оцінки безпеки для ПЗ та інших компонентів ІКС.

6. Нормативні вимоги регуляторних органів. Ряд регуляторних органів, таких як Національні агентства з кібербезпеки, банківські регулятори, органи державної безпеки тощо, можуть видавати вимоги щодо кібербезпеки ПЗ в певних галузях або секторах.

7. Стандарт MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Це модель, яка описує типові тактики, техніки та знання злочинців, які

можуть використовувати для вторгнення в систему. Вона надає метрики та критерії оцінки захисту систем від таких загроз.

Основні метрики кібербезпеки, які використовуються для оцінювання якості ПЗ в ІКС включають: вразливості (vulnerabilities), тобто потенційні слабкі місця в ПЗ, які можуть бути використані зловмисниками для здійснення атак на систему. Оцінка кількості та серйозності вразливостей є важливим показником якості кібербезпеки ПЗ; відновлюваність (resilience), тобто здатність ПЗ відновлюватися після кібератаки або інших випадків втрати доступності, цілісності або конфіденційності. Оцінка рівня відновлюваності є важливим аспектом оцінки кібербезпеки ПЗ; автентифікація (authentication), тобто процес перевірки ідентифікації користувачів або систем, що забезпечує доступ лише автентифікованим користувачам або системам. Ефективні методи автентифікації, такі як сильні паролі, багатофакторна автентифікація тощо, є важливим аспектом кібербезпеки; конфіденційність (confidentiality), тобто забезпечення захисту від несанкціонованого доступу до інформації. Ефективні механізми криптографічного захисту, контролю доступу та інших заходів щодо конфіденційності є важливими метриками кібербезпеки; цілісність (integrity), це забезпечення цілісності інформації, тобто запобігання несанкціонованим змінам або викривленням даних; ефективні механізми контролю цілісності, такі як цифрові підписи, контрольні суми та інші методи, є важливими метриками кібербезпеки; доступність (availability), це забезпечення доступності системи або сервісу для користувачів відповідно до встановлених вимог. Ефективні заходи для запобігання втрати доступності, такі як резервне копіювання, балансування навантаження, резервування ресурсів та інші, є важливими метриками кібербезпеки; моніторинг (monitoring), це забезпечення постійного контролю за станом безпеки системи, виявлення потенційних загроз тачасна реакція на події безпеки. Ефективні механізми моніторингу, включаючи системи виявлення вторгнень (IDS), системи журналювання (logging), аналізу відхилень (deviation analysis) та інші, є важливими метриками кібербезпеки; політики безпеки (security policies), тобто встановлення правил та регламентів, що регулюють використання системи та взаємодію з нею, з метою забезпечення безпеки. Ефективні політики безпеки, такі як обмеження прав доступу, правила паролів, політики оновлення ПЗ та інші, є важливими метриками кібербезпеки.

Ці метрики можуть варіюватися залежно від конкретних вимог і характеристик системи, але взагалі вони допомагають оцінити рівень кібербезпеки ПЗ та виявляти можливі вразливості та проблеми, що впливають на безпеку ІКС.

Оцінка якості ПЗ в ІКС вимагає врахування аспектів кібербезпеки. Метрики кібербезпеки є важливим інструментом для оцінки рівня безпеки ПЗ, виявлення вразливостей та проблем безпеки, а також встановлення ефективних заходів для їх усунення. Загальні основні метрики кібербезпеки включають конфіденційність, цілісність, доступність, автентифікацію, авторизацію, моніторинг та політики безпеки. Оцінка цих метрик дозволяє виявити можливі ризики, встановити заходи для запобігання атакам та забезпечити адекватний рівень захисту інформації в ІКС. Важливо враховувати, що метрики кібербезпеки мають бути відповідні конкретним потребам та характеристикам системи, а також враховувати змінюються загрози та технічний прогрес.

У висновку, використання метрик кібербезпеки в оцінці якості ПЗ в ІКС є важливим кроком для забезпечення високого рівня безпеки систем та захисту інформації. Врахування різних аспектів кібербезпеки та встановлення ефективних заходів забезпечить надійний захист від потенційних загроз та зменшить ризики кібератак.

Науковий керівник – к.т.н., доцент, Гнатюк В.О.

УДК 004.056(477)

USING MACHINE LEARNING (ML) TO DETECT THREAT ANOMALIES FOR REDUCING FALSE-POSITIVES ON THE DAILY CYBERSECURITY OPERATION CENTRE ROUTINE

Roman Karpiuk¹, Petro Venherskyi²

Ivan Franko National University of Lviv

¹simpplee@gmail.com, ²petro,venhersky@gmail.com

Every day, cybersecurity operation centers face the need to find a balance between the number of professionals who can analyze cybersecurity events to the number of those events.

We will focus on how to reduce the burden on analysts, namely, how to reduce the number of false positives.

What is the main source of input for the analyst? That's right, correlation rules. What does the Threat Detection engineer first face when it wants to improve the response time of a CSOC - by reducing the number of false positives generated by correlation rules. What can be done for this? Give up static thresholds and use statistics instead. The idea is good, but not very effective, because the ecosystem in which cybersecurity operates is extremely dynamic and there is a high probability of "loss from the radar" is something extremely important due to changes in the behavior of one of the controlled objects (end devices, servers, network equipment or other). And when the statistics no longer meet your requirements in that case comes machine learning. Therefore, all improvements and construction of interaction with machine learning (ML) will be carried out based on the security information and event management (SIEM)"Splunk".

One of the most effective algorithms for detecting anomalies is DensityFunction. The implementation of this algorithm allows you to set different parameters on which training may depend and, consequently, the end result. The algorithm also involves estimating the different distribution of events within the sample for training.

So, let's write a correlation rule that will detect an abnormal number of end-user infections with one type of malware. To implement we need input data, in our case, it will be data from the EDR system.

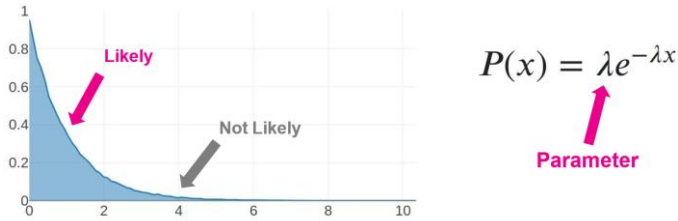


Figure 1 - The parameter that is responsible for the input data on which the training will depend.

To train DensityFunction, we will create a sample 180 days ago, not counting today. We will use the trained algorithm every hour to analyze events for the previous hour and thus we will detect anomalies.

```
Alert Threat - ML Anomaly Detection of Malware Infection by Signature - Rule
Description Optional
Search
| tstats summariesonly=true `els` values(Malware_Attacks.command_line) as
command_line values(Malware_Attacks.file_path) as file_path count
allow_old_summaries=true from datamodel=Malware.Malware_Attacks where
Malware_Attacks.action=blocked by "Malware_Attacks.signature",
"Malware_Attacks.dest", "Malware_Attacks.action", "Malware_Attacks.process"
, "Malware_Attacks.file_name" _time span=1h
| rename "Malware_Attacks.*" as "*"
| search NOT `exclude_malware_signatures`
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=(DayOfWeek="Sunday" OR DayOfWeek="Saturday","Yes","No")
| eval PartOfDay=(HourOfDay>20 OR HourOfDay<7,"Night","Day")
| eval process=(process!="",-,"process)
| stats sum(count) as malware_infections values(dest) as system_list values
(command_line) as command_line by signature action process DayOfWeek
HourOfDay PartOfDay IsWeekend _time
| `ele`
| eval LH=(now()-_time<3600,"1","0")
| apply count_malware_infections_by_signature_1h_with_features threshold=0.01
| search "IsOutlier(malware_infections)=1
| rex field=dest (?<dest>(\w+)?\.\softservecom\.)
| `notable_event_severity_malware_signatures`
| eval urgency=mvdedup(urgency)
| lookup asset_lookup_by_str asset as dest OUTPUT service_importance priority
as host_priority
| fillnull value="--"
| `risk_score_calculation(dest,system)`
```

Figure 2 – use pre-trained ML model (another search) «count_malware_infections_by_signature_1h_with_features» to detect anomalies.

The rule is implemented and works in real conditions. The result of work are 8 alerts in the last 7 days, which is an excellent result in terms of load, as the company has more than 15,000 different types of end-users (servers, laptops, PCs) where EDR is installed.

It’s example of one implementation of 70+ correlation rules for detection different types of cybersecurity anomalies.

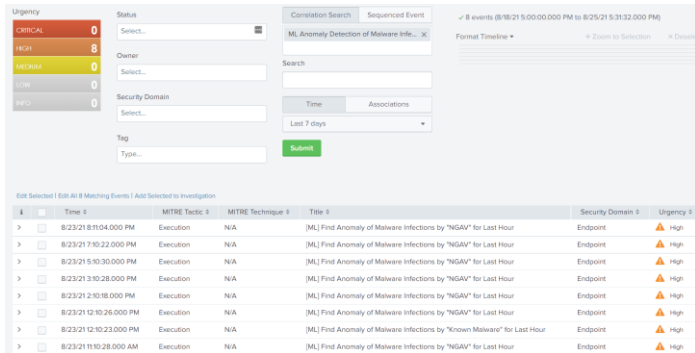


Figure 3 – results

Supervisor - doctor of physical and mathematical sciences, professor, P.Venherskyi

УДК 621.372

USE OF INHOMOGENEOUS LINES AS A FILTERING ELEMENT FOR DESIGN OF SHF DEVICES

**Valerii Kozlovskiy¹, Svitlana Nimych²,
Oleksii Komar³**

*National Aviation University, ¹vvkzeos@npp.nau.edu.ua,
²svt.kovtun@gmail.com*

The problem with the use of homogeneous lines as a filtering element for SHF devices lies in their periodic amplitude-frequency characteristics, which can lead to unwanted parasitic channels. The use of inhomogeneous lines presents a potential solution, but the determination of exact finite expressions for elements of quadrupole matrices based on HL is challenging due to the lack of closed exact solutions. This limitation prevents the full realization of the potential benefits of using inhomogeneous lines as a filtering element in the design of SHF devices.

Recent research has focused on finding accurate solutions to the telegraph equations for inhomogeneous lines to improve the design of SHF devices. While accurate solutions exist for certain types of inhomogeneous lines with exponential, parabolic, and hyperbolic changes in wave impedance, the lack of solutions for other types of lines limits the element base of construction. Numerical methods have been used to study these other types of lines, but the private nature of the results is a disadvantage. There is a need for further research to develop accurate solutions for a wider range of inhomogeneous lines.

Calculation formulas for the scheme of fig. 1:

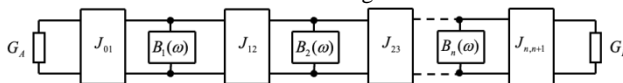


Fig. 1. Generalized schematic of FFT with conductivity inverters

Replace the parallel circuits with irregular transmission lines (fig. 2).

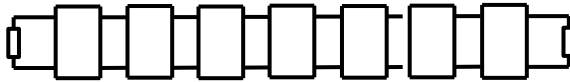


Fig. 2. Generalized FFT scheme on the HL with conductivity inverters

Since J-inverters (conductivity inverters) provide high impedance HL loads, in the area of resonant frequency the "HL-inverter" link has an equivalent circuit of fig.3 [3].

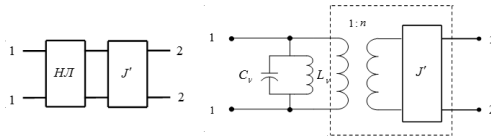


Fig. 3. Equivalent diagram of the "LV-inverter" link in the resonant frequency region

Let's find the circuit matrix of the "ideal transformer - inverter" connection (fig. 3).

$$A = \begin{bmatrix} \frac{1}{n} & 0 \\ 0 & n \end{bmatrix} \begin{bmatrix} 0 & \pm \frac{j}{J'} \\ \pm jJ' & 0 \end{bmatrix} = \begin{bmatrix} 0 & \pm \frac{j}{nJ'} \\ \pm jnJ' & 0 \end{bmatrix}. \tag{1}$$

Therefore, the quadrupole circled by the dotted line in Fig. 3 is an inverter of conductances with the inversion coefficient. Consequently, for the circuits of Fig. 4 and 6 to be equivalent it is necessary to fulfill the condition for all links of HL - inverter. As a result, we get the condition of equivalence of both circuits:

$$J'_{01} = J_{01}, J'_{12} = \frac{J_{12}}{n}, J'_{23} = \frac{J_{23}}{n}, \dots, J'_{n,n+1} = \frac{J_{n,n+1}}{n}. \tag{2}$$

Using the formulas obtained, we synthesized FFT prototypes with two parallel loops based on a closed homogeneous line and one loop based on three HL with wave impedances with the raw data:

- relative bandwidths;
- bandwidth attenuation;
- load conductivity.
- the center frequency of the first parasitic band is 7 times higher than the center frequency of the passband.

In conclusion, the use of inhomogeneous lines as a filtering element for the design of SHF devices offers a number of advantages over the use of homogeneous lines. The selection of the appropriate wave impedance for inhomogeneous lines can significantly reduce the presence of parasitic channels in receiving filters and matching devices. The synthesis of filters based on inhomogeneous lines can be done using existing methods, and the use of inhomogeneous lines as resonators allows for increased band gap in comparison with homogeneous lines.

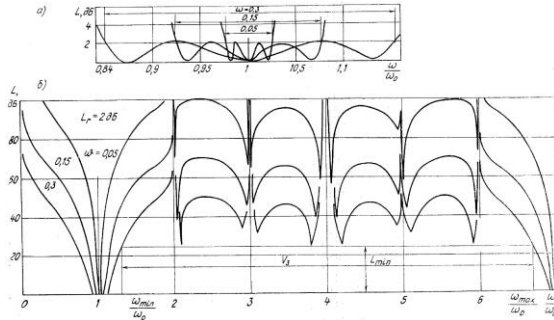


Fig. 4. Amplitude-frequency response of the prototype FFT; ω_0 - central frequency of the passband, V_δ – width of the blocking area, L_{min} - minimum attenuation in the blocking area.

However, the frequency response in the obstruction region is highly indented, which requires the use of resonators with a disjoint spectrum of frequencies to increase the attenuation in this region. Further research is needed to develop accurate solutions for a wider range of inhomogeneous lines and to explore the potential of inhomogeneous lines for other applications.

Supervisor – doctor of technical sciences, professor, Kozlovskiy V.V.

УДК 621.372

ПРОЄКТ ПРИСТРОЮ АКТИВНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА БАЗІ ГЕНЕРАТОРА ШУМУ

Михайло Кищак

ДВНЗ «Ужгородський національний університет»

Актуальність пов'язана з розвитком технологій перехоплення інформації, а також в потребі її захисту. Пристрої захисту весь час вдосконалюються, дорожчають, що також змушує задуматись над питанням, чи доцільно захистити інформацію тим чи іншим методом і чи це економічно вигідно. Тому розробка дешевого і надійного пристрою в наш час буде актуальною темою.

Інформаційна сфера – область діяльності, що відноситься до створення, передачі і використання інформації, включаючи особисту і суспільну свідомість, інформаційну і телекомунікаційну інфраструктуру та власне, інформацію [1].

Використання пасивних методів захисту може з тих чи інших причин не забезпечити необхідну захищеність приміщення від прослуховування. До того ж, більш економічним може бути варіант з придбанням системи віброакустичного шумлення (генератора шуму, вібровипромінювачів та акустовипромінювачів) замість забезпечення звукоізоляції [1].

Технічний захист інформації - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації [2].

Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини). Якщо інформація існує у вигляді акустичних хвиль, які створюються за допомогою голосового апарату людини, вона називається мовною [2].

Принцип захисту простий – потрібно замаскувати акустичні сигнали в приміщенні, яке захищається шляхом збільшення енергії перешкод, тим самим знижуючи рівень розбірливості мови до необхідних значень. Система складається з генератора білого шуму, який відправляє згенерований сигнал на акустичні та віброакустичні випромінювачі. Така система дозволяє запобігти витоку інформації через різні конструктивні компоненти приміщення, а саме через двері, щілини, вікна та труби батарей.

Висновки

- 1) Мій власний пристрій є дешевим відносно пристроїв захисту на ринку;
- 2) Пристрій дозволяє захистити інформацію від витоку акустичними, віброакустичними каналами;
- 3) Подальші вдосконалення пристрою є доцільними.

Література

1. С.О. Іванченко, А.С. Швецов, О.В. Гавриленко, О.А. Липський. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
2. Технічний захист інформації. <https://tzi.ua/ua/tz.html>.

УДК 621.372

DETERMINATION OF A FOUR-POLE TRANSMISSION LINE MATRIX BASED ON A NONUNIFORM

Kateryna Nesterenko¹, Oleksii Nimych², Vladyslav Dudnyk³

National Aviation University

¹*kateryna.nesterenko@npp.nau.edu.ua*, ²*aleksei.nimich@gmail.com*,

³*vb.dudnik@gmail.com*

The problem of determining the quadrupole matrix for nonuniform transmission lines has no closed exact solution, as the processes in homogeneous lines are described by second-order differential equations whose solution is expressed in quadrature only in special cases. This limits the realization of the potential of nonuniform lines in the design of high-speed communication systems. Therefore, developing analytical techniques for determining the quadrupole matrix for nonuniform lines is crucial for realizing the full potential of these lines in practical applications.

Recent research in the field of transmission lines has focused on developing accurate analytical techniques for determining the quadrupole matrix of nonuniform lines.

While exact solutions for a limited number of homogeneous lines exist, such as those with exponential, parabolic, and hyperbolic wave impedance, other types of lines require numerical methods. However, these methods yield private results and lack general applicability. Therefore, researchers have explored various analytical methods, including the method of characteristics and the method of moments, to determine the quadrupole matrix for nonuniform lines.

To determine the quadrupole homogeneous lines (HL) matrices, we propose to use the properties of the line as a quadrupole with compact deduction, whose matrix of resistances and conductivities has no partial poles, and the transfer conductivity and transfer resistance have no zeros. This allows us to find all elements of the resistance and conductance matrix by the input resistance of an open line (input conductance of a closed line).

Let's use this method to determine the HL conductivity matrix with wave impedance, where t - current delay time, a - positive number, ch - wave impedance at the beginning of the line. In this case, the element conductivity matrices Y equals

$$y_{11} = \frac{\sqrt{p^2 + a^2}}{pW_0th\sqrt{p^2 + a^2}t} = \frac{\sqrt{p^2 + a^2}ch\sqrt{p^2 + a^2}t}{pW_0sh\sqrt{p^2 + a^2}t} \tag{1}$$

The elements of the matrix of conductivities (resistances) of lossless circuits are determined by deductions and poles. In particular, if the conductivities have a pole at zero, as in our case, then the elements of the conductivity matrix can be represented as (for different elements P and Q different).

$$y_j = \frac{P(p)}{Q(p)} = \frac{k_j^{(0)}}{p} + \sum_{m=1}^{\infty} \frac{2k_j^{(m)}}{P^2 + \omega_m^2}, \quad i = 1,2; j = 1,2; k_j^{(0)} = \frac{1}{L_{cm}} \tag{2}$$

With this in mind, we find the deductions y_{11} . To do this let's write y_{11} in the form of

$$y_{11} = \frac{P(p)}{Q(p)} = \frac{ch\sqrt{p^2 + a^2}t}{pW_0sh\sqrt{p^2 + a^2}t} = \frac{k_{11}^{(0)}}{p} + \sum_{m=1}^{\infty} \frac{2k_{11}^{(m)}}{P^2 + \omega_m^2}, \tag{3}$$

Thus, the conductivity matrix is completely defined. Knowing the conductivity matrix, you can synthesize different types of filters or matching devices, using known methods.

Consider the synthesis of band-pass filters (BPF). To do this, we first define the equivalent circuits of the HL in the pole area of the elements of the resistance and conductance matrix.

For lossless lines, the impedance matrix can be written in the form

$$[Z] = [Z]_0 + \sum_{v=1}^{\infty} [Z]_v \tag{4}$$

$$[Z]_0 = \frac{1}{pC_{cm}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{5}$$

$$[Z]_v = \frac{2p}{p^2 + \omega_v^2} \begin{bmatrix} k^{(v)} \\ mn \end{bmatrix}, \quad v = 1, 2 \tag{6}$$

$$Z_{11} = \frac{1}{C_v} p, \quad Z_{22} = \frac{n^2}{C_v} p, \quad Z_{12} = \frac{n}{C_v} p. \quad (7)$$

For the proof, let's find the elements of the resistance matrix of the circuit of fig. 1. Let's represent this circuit in the form of a cascade connection of a circuit and an ideal transformer. Then the elements of the resistance matrix of the circuit will be written in the form

The antisonant frequency refers to the frequency of series resonance, that is, when the conductivity of a lossless circuit turns to infinity. In other words, the antisonant frequencies are defined by the poles of the input conduction in the plane of the complex frequency variable.

In conclusion, the presented analytical techniques for determining the quadrupole matrix of nonuniform transmission lines provide a valuable tool for designing high-performance microwave devices with improved amplitude-frequency characteristics. The use of inhomogeneous lines allows for the design of broadband matching devices, and the choice of wave impedance for LP resonators can increase the band gap of FFT. However, the presence of additional transformers in inverters made on HL should be taken into account. The frequency response in the obstruction region of nonuniform lines is highly indented, and the attenuation minimum occurs between the frequencies of series resonance of parallel loops. Therefore, to increase the attenuation in the fence region, resonators with a disjoint spectrum of frequencies of parallel and series resonance can be used. These findings offer opportunities for further research to explore the application of these techniques in designing high-speed communication systems with improved performance.

Supervisor – doctor of technical sciences, professor, Nesterenko K.S.

УДК 004.056.5

АРХІТЕКТУРА ХМАРНОГО РІШЕННЯ ДЛЯ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ ТА ОБРОБКИ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Євгенія Іванченко¹, Ігор Іванченко², Ірина Лозова³,
Євгеній Педченко⁴, Марі Петровська⁵**

Національний авіаційний університет

¹evivancenko@gmail.com, ²igor-p-1@ukr.net, ³illozovaya@gmail.com,

⁴ympedchenko@gmail.com, ⁵pmarisha2004@gmail.com

Для всіх комерційних і некомерційних компаній, що мають хоча б одну інформаційну систему – присутня задача збору та обробки подій з даних систем, а також зберігання зафіксованих подій мінімум на 90 днів для потенційного майбутнього розслідування інцидентів з інформаційної безпеки [1].

Тому, постає проблема, що через високу вартість ліцензій та неможливості компаній підтримувати систему в актуальному стані є необхідність розгортання систем для збору та обробки подій отриманих з інформаційних систем на ресурсах

хмарних провайдерів, оскільки саме в даному випадку, компаніям непотрібно буде перейматися за працездатність рішення та виділення обчислювальних ресурсів, які необхідні для функціонування даного типу рішень [2].

Метою даної роботи є удосконалення архітектури розроблюваного хмарного рішення для централізованого збору та обробки подій з інформаційних систем із кластерним розділенням подій для кожної компанії.

Новизною є удосконалення архітектури збору та обробки подій, за рахунок розробки модулю опрацювання даних отриманих з інформаційних обчислювальних систем, що надасть можливість розміщення компонентів обробки даних на обчислювальних ресурсах хмарних провайдерів, таких як AWS, Google Cloud, Microsoft Azure тощо. Використання даного рішення передбачає зменшення бюджетних витрат компанії на обробку та зберігання подій з інформаційних систем, що можуть бути використаними для майбутнього розслідування інцидентів з інформаційної безпеки.

Опираючись на попереднє дослідження [3], в якому розглядалися основні складові розроблюваного модуля – в даному дослідженні удосконалено представлену деталізовану архітектуру працездатності розроблюваного рішення, що дозволить зрозуміти його взаємозв'язок між різними компонентами та логіку роботи.

HLD архітектура розроблюваного рішення представлена на Рисунок 1 та має такі складові, як: кластер шлюзів, кластер баз даних та сервера управління. Для розуміння взаємодії між собою складових рішення, розглянемо їх більш детально:

1. Кластер шлюзів (Gateways) – це компонент збору та обробки отриманих подій з інформаційних систем. Дана складова побудована з використання кластеру Docker-контейнерів [4], що дозволяє за лічені хвилини масштабуватися (auto-scaling) у випадку фіксування великого потоку даних від інформаційних систем. Також, даний підхід є актуальним у випадках, виявлення DDoS атаки на Gateways, що дозволяє попередити виведення їх з ладу та продовжити отримувати та обробляти події з інформаційних систем.

2. Кластер баз-даних (Databases) – це компонент зберігання оброблених інцидентів на компонентом Gateways, що дозволяє на рівні розділяти події, отримані з різних джерел чи компаній. Даний кластер побудований також із використанням кластеру Docker-контейнерів з використанням бази-даних MySQL [5], що дозволяє об'єднувати декілька контейнерів в єдине середовище і уникати перевантаження тієї чи іншої бази даних.

3. Сервери управління (Management Console) – це компонент (*розроблюваний модуль*), що відповідає на налаштування процедур збору та обробки інцидентів на компоненті Gateways. В даному випадку, для кожної окремої компанії розгортається окремий Docker-контейнер, що дозволяє розділяти системи управління між несуміжними адміністраторами. Також, на даному рівні, є можливість керувати підключеними Gateways до консолі, та, за потреби їх вручну надавати для збільшення обчислювальної потужності.

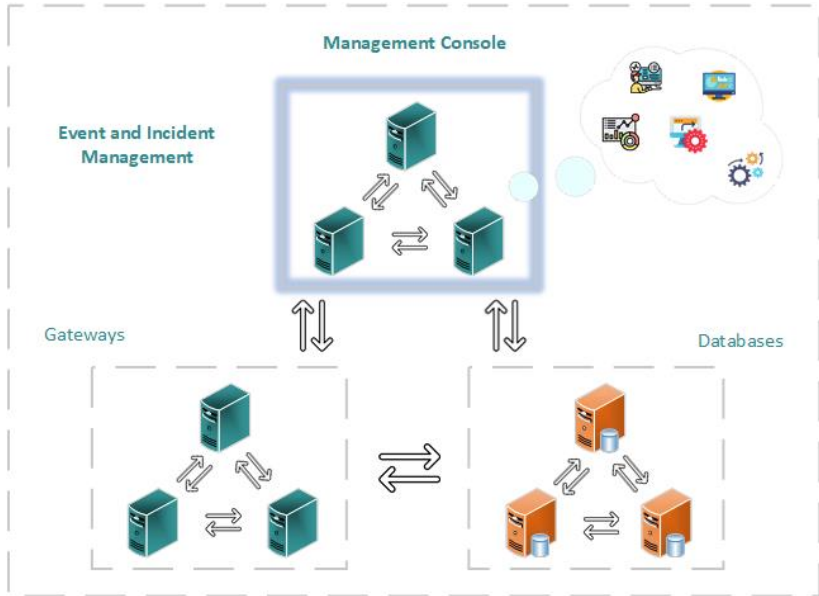


Рис. 1. HLD схема взаємодії компонентів розроблюваного модуля збору та обробки інформаційних подій

Для розробки веб-додатку – використано поєднання декількох мов програмування, а саме:

1. HTML+CSS – поєднання даних двох мов використано для побудови графічної оболонки веб-додатку.
2. JavaScript – використано для побудови логіки веб-додатку та взаємодії з різними компонентами та рішеннями.
3. PHP – використано для побудови зв'язку із базою даних.
4. Фреймворк Node.js – використано для створення запитів до Gateways для обробки отриманих подій від них.

Завдяки даному поєднанню мов програмування та фреймворку вдалося досягти максимальної обчислювальної потужності при отриманні та обробці подій від Gateways та відокремлення подій з інформаційної безпеки, що необхідні для розслідування потенційних інцидентів.

Для того, щоб зрозуміти, про який веб-додаток ми говоримо, рекомендуємо поглянути на Рисунок 2, що представляє візуальне оформлення першої сторінки рішення – вкладки «Dashboard». На даній вкладці відображається наступна інформація про:

- кількість активних Gateways;
- кількість створених джерел отримання, запису та обробки даних;
- загальну кількість отриманих подій;
- 10 останніх подій;
- останні зміни в системі.

4. Swarm mode overview // Documentation : [website]. Palo Alto, California : Docker : Docs, 2023. URL: <https://docs.docker.com/engine/swarm/>.
5. MySQL Cluster CGE // Documentation : [website]. Santa Clara, California : MySQL : Products, 2023. URL: <https://www.mysql.com/products/cluster/>.

УДК 621.372

МОЛЕКУЛЯРНА КРИПТОГРАФІЯ В КІБЕРБІОБЕЗПЕЦІ

Марія-Ольга Пішковцїй¹, Василь Рїзак²

Ужгородський національний університет,

¹mariia-olha.pishkovtsii@uzhnu.edu.ua, ²vrizak@uzhnu.edu.ua

Експоненційний ріст світових біонаук та біоекономіки за останні 20 років призвів до прогресу в молекулярній біології, включаючи синтетичну біологію та біотехнологію, а також значні інновації в медицині, охороні здоров'я, енергетиці та обороні. Проте державний та приватний сектори повинні об'єднатися, уможливити подальші законні та міждисциплінарні дослідження та розробки в широкій галузі біології та біоекономіки, також пам'ятаючи про аспекти безпеки, пов'язані з такою діяльністю. Використання перетину таких явищ як цифрові технології та біологія дає значні переваги для здоров'я, економіки та національної безпеки, але також може призвести до збільшення ризиків і вразливості. Досягнення в науці вершин (особливо розробка нових ШІ-технологій і алгоритмів для аналізу та візуалізації даних і розпізнавання нових функцій) і використання біоінженерії для маніпулювання або створення нових біологічних організмів, які мають конкретні нові функції, змінюють здоров'я, енергію, виробництво та екологічні сектори.

Кібербіобезпека є відносно новою сферою, яка прагне захистити цифрові біологічні та медичні дані, щоб захистити індивідуальну, громадську, інфраструктуру охорони здоров'я та розвиток біотехнологічних інновацій. З розвитком технологій та інтернету кіберзагрози стають все більш складними та небезпечними. Одним із способів протидіяти таким загрозам є використання ДНК - молекули, що містить генетичний код живих організмів.

Молекулярна криптографія - це напрям криптографії, що використовує молекули або живий організм, як носії або засоби обчислень для шифрування та дешифрування інформації. Ця галузь може вирішити деякі проблеми традиційних методів, але також створює нові виклики та питання, пов'язані з надійністю, доступністю, стандартизацією та етикою.

Молекулярна криптографія має декілька переваг перед традиційними методами, такими як: висока щільність збереження даних, висока стабільність даних, висока складність атак. Також її можна застосувати, як: 1) створення молекулярних шифрів - це методи шифрування, що використовують молекули як ключі або носії інформації. Наприклад, можна використовувати ДНК-синтез для кодування повідомлень у послідовностях нуклеотидів або використовувати хемосигнали для передачі таємних сигналів. 2) розробка молекулярних протоколів

- це способи взаємодії між молекулярними системами для досягнення певних криптографічних цілей. Наприклад, можна використовувати молекулярну імітацію для моделювання складних криптографічних алгоритмів або використовувати молекулярну комутацію для перемикання станів шифру. 3) застосування молекулярної біометрії - це використання молекулярних особливостей для ідентифікації та верифікації особистостей. Наприклад, можна використовувати ДНК-профайл або антитіла для розпізнавання особи або використовувати ензими або рецептори для перевірки певних ознак.

ДНК - це довгий полімер, що складається з двох ланцюгів нуклеотидів, які утворюють подвійну спіраль. Кожен нуклеотид містить одну з чотирьох азотистих основ: аденін, тимін, гуанін або цитозин. Послідовність нуклеотидів визначає генетичну інформацію, яка кодує будову та функції білків. ДНК можна розглядати як носій інформації, що має високу щільність (один грам ДНК може зберегти до 215 Петабайт даних), стабільність (ДНК може зберігатися протягом тисячоліть) та унікальність (ДНК кожної людини має варіабельні тандемні повтори (ВТП), що роблять її ідентифікатором).

ДНК-криптографія - це використання ДНК як носія інформації та обчислень для шифрування та дешифрування. ДНК-криптографія може застосовувати різні методи, такі як ДНК-шифрування, ДНК-стегаграфія, ДНК-комп'ютери, ДНК-безпека та ДНК-збереження. ДНК-шифрування - це метод перетворення текстової або бінарної інформації на послідовності ДНК за допомогою певного алгоритму. Наприклад, можна використовувати простий правило: A = 00, T = 01, G = 10, C = 11. Таким чином, слово "кріп" можна зашифрувати як ДНК-послідовність "TGTAAGGA". Щоб отримати дешифроване повідомлення, потребується знати ключ - місце початку та кінця прихованого тексту. Перевагами є непомітність даних, можливість використання живих організмів як носіїв інформації та стійкість до знищення. Використання генетичного шифрування має великий потенціал розвитку в споріднених науках до кібербезпеки, об'єднуючи в собі десятки наук, наприклад, біологію, фізику, математику, інформатику, криптографію, кібербезпеку, менеджмент, правознавство. Але як кожне рішення, створює ще більше питань, тому потрібно до цієї теми підходити із викликом. Деякі з них є: - синтез та маніпуляція молекул - це процеси, що вимагають високої точності, складності та витрат. Необхідно розробляти нові методи та інструменти для створення та контролю молекулярних структур та процесів, що можуть служити як надійні криптографічні примітиви; - аналіз та перевірка молекулярних протоколів - це завдання, що потребує глибокого розуміння молекулярної динаміки, хемосигналіну та інших феноменів, що впливають на поведінку молекулярних систем. Необхідно розробляти нові математичні моделі та методи для оцінки безпеки та ефективності молекулярних протоколів у реальних умовах; - сумісність та інтеграція з класичною криптографією - це вимога, що ставиться перед молекулярною криптографією, щоб вона могла співпрацювати з існуючими криптографічними стандартами та системами. Необхідно розробляти нові схеми та алгоритми для перетворення молекулярної інформації в класичну та навпаки, а також для гармонізації молекулярних та класичних ключів, підписів, хеш-функцій.

Це лише деякі з покликів, які стоять перед молекулярною криптографією. Ця галузь науки ще знаходиться на початковому етапі розвитку і потребує багато

досліджень і експериментів для досягнення свого потенціалу. Але цей метод однозначно має переваги порівняно з класичною криптографією, такі як: висока стійкість до квантових атак - молекулярні шифри не базуються на математичних задачах, які можуть бути ефективно розв'язані квантовими алгоритмами, а на фізичних властивостях молекули; велика розмаїтість та гнучкість молекулярних примітивів - молекулярна криптографія може використовувати різні типи молекул та хемосигналів для реалізації різних криптографічних функцій, таких як шифрування, хешування, псевдовипадкова генерація тощо; низька вартість та енергоспоживання - молекулярна криптографія не потребує складного обладнання та високої потужності для своєї роботи, можуть працювати за допомогою хімічних реакцій та дифузії, що забезпечують низьку вартість та енергоспоживання. Це лише деякі з переваг молекулярної криптографії. Ця галузь науки відкриває нові можливості для захисту інформації в різних сферах, особливо в біомедицині та нанотехнологій. може пропонувати нові методи для захисту інформації в умовах зростаючих загроз з боку квантових комп'ютерів та байотехнологій.

Молекулярна криптографія має переваги порівняно з класичною криптографією, такі як: - висока стійкість до квантових атак - молекулярні шифри не базуються на математичних задачах, які можуть бути ефективно розв'язані квантовими алгоритмами, а на фізичних властивостях молекул. Тому вони можуть протистояти загрозам від квантових комп'ютерів; - велика розмаїтість та гнучкість молекулярних примітивів - молекулярна криптографія може використовувати різні типи молекул та хемосигналів для реалізації різних криптографічних функцій, таких як шифрування, хешування, псевдовипадкова генерація тощо. Також можливо створювати гібридні схеми, що поєднують молекулярну та класичну криптографію; - низька вартість та енергоспоживання - молекулярна криптографія не потребує складного обладнання та високої потужності для своєї роботи. Молекулярні системи можуть працювати за допомогою хімічних реакцій та дифузії, що забезпечують низьку вартість та енергоспоживання.

Отже, ця галузь науки є перспективною та інноваційною, оскільки вона поєднує фундаментальні знання з практичною користю. Молекулярна криптографія - це галузь криптографії, що використовує молекулярні структури та реакції для забезпечення безпеки інформації. Молекулярна криптографія може мати декілька переваг перед традиційними методами шифрування, такими як висока щільність зберігання даних, невидимість для звичайних детекторів, висока складність для криптоаналізу та можливість самознищення. Молекулярна криптографія також ставить нові виклики для науковців та інженерів, які повинні розробляти ефективні способи синтезу, кодування, передачі, зчитування та розшифрування молекулярних повідомлень. Цей метод має потенціал стати майбутньою технологією для захисту даних від несанкціонованого доступу та злому. Однак молекулярна криптографія також потребує подальших досліджень та розвитку для досягнення практичної застосовності та надійності.

Науковий керівник – доктор фіз.-мат. наук, професор, Різак В.М.

УДК 355.244.1

УДОСКОНАЛЕННЯ МЕТОДИКИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПСИХОЛОГІЧНОГО ВПЛИВУ В ІНФОРМАЦІЙНІЙ ОПЕРАЦІЇ

Сергій Базарний

Національний університет оборони України

serhii.bazarnyi@edu.nuou.org.ua

В останні роки інформаційні операції стали все більш популярним інструментом в розгортанні інформаційного протиборства. Інформаційні операції використовують різноманітні методи для впливу на громадську думку, військово-політичне керівництво держави та прийняття рішень, такі як розповсюдження дезінформації та маніпулювання емоціями цільових аудиторій. Онлайн-дискусії на форумах, блогах та соціальних мережах є важливими джерелами для розповсюдження дезінформації та проведення інформаційних операцій. Тому моніторинг онлайн-дискусій стає все більш важливим завданням для забезпечення інформаційної безпеки та є складним завданням через великий обсяг даних та різноманітність джерел інформації. Також існує проблема виявлення нових форумів, блогів та авторів соціальних мереж, що створюються для проведення інформаційних акцій в межах проведення інформаційних операцій.

Здійснення моніторингу зорієнтоване на виявлення ключових тем та проблем, які обговорюються в найбільш активних онлайн-дискусіях а також чітко визначений контекст, у якому відбуваються обговорення, включаючи джерела інформації, активність та динаміку взаємодії цільової аудиторії. Основна ідея методу тематичного аналізу полягає в тому, що відбувається процес стандартизації тексту, видалення стоп-слів, лематизацію, а також видалення всіх елементів, які не мають стосунку до тематики тексту. Наступним кроком є розбиття тексту на частини (ключові слова, речення), а потім ці частини групуються в теми або тематичні кластери на основі відповідності слова та контекстуального значення, в якому вони вживаються. Кожен такий кластер відображає тему, яка є предметом обговорення в тексті. Аналіз кластерів на основі їх змісту та контексту, дозволяє встановити, чи є вони пов'язані з метою інформаційної операції та чи відповідають заданим цілям.

Одним з напрямків удосконалення методики є використання аналізу емоційного забарвлення тексту. Емоції можуть впливати на сприйняття інформації та прийняття рішень, тому важливо враховувати їх в оцінці ефективності психологічного впливу. Наприклад, виявлення негативного емоційного забарвлення відгуків про певний інформаційний продукт може свідчити про його низьку популярність серед цільової аудиторії та потребу у вдосконаленні його форми та змісту.

Для визначення показників ефективності психологічного впливу на цільову аудиторію необхідно враховувати різні категорії, такі як кількість переглядів, коментарів, лайків, ретвітів, заклики до конкретних дій, звернення до емоцій, відгуків. Завдяки методу тематичного аналізу можна визначити, які теми та ключові слова найчастіше використовуються в текстах, пов'язаних з певною тематикою. Також можна відслідкувати зміну популярності та актуальності інформаційної тематики в різний час доби, що дає змогу розуміти динаміку зміни активності інтересів цільової аудиторії.

У контексті оцінки ефективності психологічного впливу методом тематичного аналізу моніторингу онлайн-дискусій, форумів, блогів та авторів соціальних мереж, коефіцієнт кореляції Пірсона (r) є статистичною мірою лінійної залежності між двома змінними. Де (r) може набувати значень від -1 до +1. Значення -1 вказує на повну негативну кореляцію, +1 на повну позитивну кореляцію, а 0 на відсутність кореляції може бути використаний для вимірювання ступеня залежності між різними показниками, такими як кількість відгуків на допис, рівень взаємодії користувачів тощо. Наприклад, якщо виявлено позитивну кореляцію між кількістю відгуків та рівнем взаємодії користувачів, це може вказувати на те, що більш активні користувачі мають більший вплив на дискусію.

Формула коефіцієнта кореляції Пірсона (1) містить в собі такі компоненти, як n - кількість спостережень, X та Y - значення двох змінних. Використання цієї формули дозволяє обчислити числове значення коефіцієнта кореляції, що дає можливість кількісно виміряти ступінь залежності між різними показниками та оцінити ефективність психологічного впливу методом тематичного аналізу моніторингу онлайн-дискусій.

$$r = \frac{(n \sum xy - \sum x \sum y)}{\sqrt{((n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2))}} \quad (1)$$

Методи тематичного аналізу такі, як LDA (Latent Dirichlet Allocation) та NMF (Non-negative Matrix Factorization), є потужними інструментами для автоматичної категоризації текстової інформації на основі визначеної тематики.

LDA є статистичною моделлю, яка дозволяє категоризувати тексти за допомогою прихованих тематичних зв'язків. Вона базується на припущенні, що кожен документ складається з декількох тем, які мають різну важливість. Кожне слово може належати до різних тем з різною ймовірністю. Таким чином, LDA дозволяє кластеризувати тексти на основі спільності використовуваних слів та тематики документів.

NMF є іншою методою тематичного аналізу, яка базується на факторизації матриці. Вона використовується для розкладання матриці слів на більш малі матриці, які можуть бути розпізнані як теми. Кожна тема складається з набору слів, які найчастіше використовуються разом у текстах. Цей метод може бути використаний для виявлення тематичних кластерів, які можуть бути пов'язані з конкретними авторами, форумами або блогами.

Тому запропоновані методи обробки мови можуть бути ефективним інструментом для моніторингу онлайн-дискусій під час проведення інформаційних операцій. Зокрема, техніки нормалізації, токенизації та лематизації тексту, які дозволяють автоматично обробляти великі обсяги даних з метою подальшого проведення їх аналізу. Це сприяє своєчасному автоматичному виявленню джерел інформації, що обговорюється а також її авторів, які безпосередньо здійснюють психологічний вплив на дискусію.

Науковий керівник – д.т.н., проф. Прибілєв Ю.Б.

УДК 004.056.53 (043.2)

ВІДДАЛЕНИЙ КОНТРОЛЬ І ЗАХИСТ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ ТЕЛЕГРАМ БОТА

Любомир Боценюк¹, Юрій Матьовка²

Ужгородський національний університет

¹liubomyr.botseniuk@uzhnu.edu.ua, ²yurii.matovka@uzhnu.edu.ua

У сучасному світі, коли майже кожна людина має персональний комп'ютер, захист даних та пристроїв від несанкціонованого доступу є дуже важливим. Злочинці створюють різноманітні програми та алгоритми, які можуть використовуватися для отримання доступу до персональних даних та контролю над пристроєм. Тому розробка захисної системи, яка забезпечує безпеку персонального комп'ютера та захист від несанкціонованого доступу, є дуже важливою задачею.

Одним зі засобів захисту комп'ютера є використання телеграм бота на основі бібліотеки telebot (pyTelegramBotAPI) виконаного на Python. Цей бот забезпечує віддалений контроль та захист персонального комп'ютера, надсилає попередження про включення комп'ютера та надає можливість дистанційного керування ним.

Актуальність даної роботи полягає в тому, що в сучасному світі зростає кількість злочинів, пов'язаних з несанкціонованим доступом до персональних комп'ютерів та крадіжкою важливої інформації. Оскільки багато людей використовують свої комп'ютери для роботи та зберігають на них важливі дані, необхідно забезпечити їх захист від зламу та несанкціонованого доступу. Таким чином, використання телеграм бота на основі мови програмування Python може бути ефективним інструментом для віддаленого контролю та захисту персональних комп'ютерів від потенційних загроз. Дослідження функцій бота та їхнього впливу на захист комп'ютерів є важливим кроком у розробці нових методів захисту персональної інформації та може знайти своє застосування у різних галузях, які вимагають високого рівня безпеки даних.

Метою даної роботи є дослідження можливостей віддаленого контролю та захисту персонального комп'ютера на основі телеграм бота з використанням бібліотеки telebot (pyTelegramBotAPI) на мові програмування Python. Робота спрямована на детальне вивчення функцій бота та їхнього впливу на захист персонального комп'ютера від несанкціонованого доступу та зламу системи безпеки. Під час дослідження будуть розглянуті основні переваги телеграм бота над

іншими методами захисту комп'ютерів та обговорені практичні аспекти його використання.

До основного інструментарію, який використовувався при створенні даного бота, можна віднести високорівневу мову програмування Python та бібліотеку telebot (pyTelegramBotAPI). Python є дуже популярною мовою програмування, особливо в галузях, які пов'язані зі штучним інтелектом, машинним навчанням, науковими дослідженнями, веб-розробкою та іншими напрямками. Основні переваги Python: простота вивчення, велика кількість бібліотек, крос-платформенність, швидкість розробки, відкритий код.

Бібліотека telebot (pyTelegramBotAPI) призначена для розробки ботів для Telegram на мові програмування Python. З її допомогою можна створити ботів із різноманітними функціями, які будуть відповідати на повідомлення користувачів, працювати з файлами та базами даних, обробляти зображення і багато іншого. Бібліотека telebot (pyTelegramBotAPI) має простий і зрозумілий інтерфейс програмування, що дозволяє швидко розробляти ботів для Telegram. Вона також має хорошу і зрозумілу документацію, багато прикладів коду, що допомагає розробникам вивчити її та використовувати для своїх проєктів. Таким чином, бібліотека telebot (pyTelegramBotAPI) є потужним інструментом для створення ботів для Telegram, який забезпечує швидку і просту розробку, а також високу функціональність та можливість взаємодії з користувачами.

Для розширення можливостей дистанційного контролю за персональним комп'ютером, в даній роботі був розроблений телеграм бот на основі бібліотеки telebot (pyTelegramBotAPI) на мові програмування Python. Бот дозволяє віддалено керувати комп'ютером та забезпечує його захист від несанкціонованого доступу.

Однією з основних функцій бота є можливість перетворювати введений дистанційно текст в аудіо файл і програвати відразу на комп'ютері або відтворювати голосове повідомлення, яке власник надіслав у чат боту. Ця функція може бути корисною в ситуаціях, коли необхідно надіслати важливу інформацію на комп'ютер без присутності на місці або повідомити порушнику про його незаконні дії.

Також, бот дозволяє робити скріншоти з екрану комп'ютера та фотографії з камери. Ці функції дозволяють віддалено перевіряти дії користувача на комп'ютері та контролювати простір перед комп'ютером.

За допомогою бота можна також налаштувати рівень гучності на комп'ютері, блокувати або вимикати сам пристрій. Ці функції можуть бути корисними в ситуаціях, коли користувач не зміг виконати ці дії на комп'ютері внаслідок відсутності фізичного доступу до нього.

Крім того, бот дозволяє записувати відео з камери та екрану комп'ютера, символи що введені на клавіатурі та звук із мікрофону. Ці функції дозволяють віддалено перевіряти дії користувача на комп'ютері, а також контролювати дії несанкціонованих користувачів.

Отже, в результаті проведеного дослідження можна зробити висновок, що використання телеграм бота на основі мови програмування Python може бути ефективним інструментом для віддаленого контролю та захисту персональних комп'ютерів від потенційних загроз. Застосування функцій бота, таких як запис символів з клавіатури, фотографії з камери, скріншоти екрану та інші, може значно

збільшити рівень захисту інформації на комп'ютері та дозволити забезпечити безпеку даних. Дана технологія може бути корисною для користувачів комп'ютерів у різних галузях, в тому числі для бізнесу та особистого використання. Проте, необхідно враховувати, що використання даного бота може бути втручанням у приватне життя користувачів, тому необхідно використовувати його відповідально та згідно з законодавством.

Науковий керівник – к.б.н., доц. Суховія М.І.

УДК 623.437-049.5:332.738(043.2)

БЕЗПЕКОВІ РИЗИКИ ПІД ЧАС ТРАНСПОРТУВАННЯ НОСІЇВ ТАЄМНОЇ ІНФОРМАЦІЇ ГУЖОВИМ ТРАНСПОРТОМ

Валерій Ворожко

Національний авіаційний університет, ГДА СБУ,

wp06vv@gmail.com

Нині Україна протистоїть потужним зусиллям своїх ворогів, мета яких – ліквідація української державності та знищення українців. Сучасні політичні виклики зумовлюють необхідність об'єктивного аналізу історичних аспектів функціонування «державного організму» України та його подальшої трансформації в сучасну вільну і демократичну країну.

Метою даної роботи є оптимізація ризик-менеджменту під час транспортування носіїв таємної інформації, недопущення рецидивів минулого.

Функція транспортування носіїв таємної інформації (далі – НТІ) у 1920-30 рр. в межах України покладалася на сформований у 1922 р. Фельд'єгерський корпус (далі – ФК) ДПУ. Між сусідніми обласними і районними центрами, селами та залізничними станціями на невеликі відстані озброєні фельд'єгері перевозили НТІ гужовим транспортом: взимку на санях, в іншу пору на підводах. Доставка НТІ на значні відстані здійснювалася залізницею. Згідно з наказом ДПУ від червня 1923 р ФК зобов'язали доставляти окрім НТІ ще термінову нетаємну кореспонденцію державних органів, пакунки, гроші і цінності. Це призводило до регулярних нападів на фельд'єгерів, яких грабували навіть на багатолюдних вулицях. Так у 1925 р. у центрі Катеринославу був пограбований фельд'єгер Каптель, у якого без спроби спротиву відібрали портфель з грошми та НТІ. Теж саме відбулося і в Умані з фельд'єгером Транченко. Втім фельд'єгерів, які пересувалися другорядними шляхами, іноді через ліси в темряві або степовими шляхами грабували набагато частіше. У жовтні 1928 р. був виданий наказ ДПУ про посилення конспірації в роботі ФК. Саме недостаття конспірація, а не факт перевезення разом з НТІ грошей вважалося керівництвом ДПУ головною причиною чисельних нападів на фельд'єгерів. У наказі пропонувалося: а) відповідним відділам своєчасно попереджувати ФК про прояви бандитизму;

б) направити фельд'єгерів на навчальні бойові стрільби». Під час нападів, фельд'єгері захищали довірені їм НТІ та державні гроші іноді ціною власного здоров'я, а нерідко і життя. Так на фельд'єгерів Дніпропетровського окружного відділу ДПУ Красильникова і Фарятьєва у квітні 1928 р. в районі станції Білі Криниці напала група озброєних грабіжників. У перестрілці з бандитами Красильников загинув. Його напарник удав із себе пораненого, упав, а портфель з НТІ і грішми відкинув від себе. Коли грабіжники кинулися до портфеля, фельд'єгер почав прицільно стріляти по них, одного поранив, інші, підхопивши пораненого, кинулися тікати. У тому ж році неподалік станції Зарудниця Ружинського району було здійснено озброєний напад на фельд'єгера Миронюка. Незважаючи на чисельну перевагу і тяжке поранення правої руки, він вступив в бій з бандитами і, стріляючи з лівої руки, змусив їх тікати. Фельд'єгер зберіг НТІ і гроші. На фельд'єгера Гордона на степовій дорозі у жовтні 1928 р. напала група злочинців. Отримавши поранення правої руки, він відстрілювався лівою. У грудні 1929 р. відбувся черговий напад грабіжників на фельд'єгерів Суровцева та Водяницького у Шполянському районі, які не розгубилися і виявив стрілецькі навички, затримали нападників. За героїзм і збережені карбованці обидва фельд'єгері були нагороджені іменними «маузерами» і місячним грошовим забезпеченням У 1933 р. ДПУ видало наказ про чисельні порушення в роботі фельдз'язку, зокрема у наказі наводився такий випадок: «19 березня 1933 р. фельд'єгера Старобельської експедиції Філатов і Ларін залишили без нагляду на підводі НТІ і гроші, у підсумку зникло, крім грошей і 100 пакетів НТІ, які так і не були знайдені». У квітні 1933 р. був виданий ще один наказ ДПУ УСРР про чергову втрату фельд'єгерами НТІ та пакунка з годинником для начальника прикордонного загону. Такі подарунки для керівництва та інших поважних осіб, реквізовані у «буржуазних спеців» цінні та дефіцитні речі, включно з харчами (найбільш популярним було сало), у багажі фельд'єгерів були майже завжди. У 1933 р. на фельд'єгера Грабова на маршруті Зиньків–Охтирка напали 5 грабіжників, яких, не розгубившись, Грабов розігнав вистрілами з табельної зброї. У травні 1936 р. НКВС було видано наказ про нагородження фельд'єгера Проніна, який на станції Ток, куди він прибув на підводі для зустрічі маршрутних фельд'єгерів, виявив і затримав двох озброєних бандитів – братів Хрюкових. В ніч з 25 на 26 листопада 1937 р. на фельд'єгера Золотоніського райвідділу Недашківського, який слідував за маршрутом із НТІ, три зловмисника здійснили напад із метою пограбування. Фельд'єгер затримав злодіїв, які потім були засуджені. Із наказу НКВС УРСР. нам стає відомо, що «...23 серпня 1938 р. вночі на фельд'єгера Чигиринського райвідділу НКВС Рачинського був здійснений напад невідомих зловмисників. Фельд'єгер відкрив вогонь по зловмисникам і, вирвавшись з їх оточення, зберіг НТІ та цінності. Гроші та пакунки були головною цілью для грабіжників, яких найменше цікавили літерні пакети з НТІ. Фельд'єгерська служба мала значні

безпекові ризики, але бажаних бути фельд'єгером не бракувало. Фельд'єгері мусили добре володіти зброєю, орієнтуватися у просторі, вміти поводитися з кінями, полюбляти ризиковане життя, природу, свіже повітря. Окрім грошового забезпечення вони мали життя повне пригод. Разом з тим зазначимо, що поганий ризик-менеджмент керівників ДПУ регулярно призводив до загибелі фельд'єгерів, життя яких для більшовицької влади нічого не вартувало.

УДК 004.056.5 (355.4)

OSINT – ЕЛЕМЕНТ РОЗВІДКИ В УМОВАХ КІБЕРВІЙНИ

Максим Делембовський

*Київський національний університет будівництва і архітектури
delembovskyi@knuba.edu.ua*

Представлена тема присвячена використанню принципів OSINT (Open Source Intelligence) як елемента розвідки в умовах кібервійни. OSINT - це збір інформації з відкритих джерел, таких як соціальні мережі, веб-сайти, форуми тощо. В контексті кібервійни, OSINT може бути важливим інструментом для отримання інформації про цільову організацію або діяльність хакерів, що дозволяє розкрити слабкі місця і запобігти можливим атакам.

У представлений роботі розглядаються основні методи збору інформації через OSINT, а також приклади їх використання в кібервійні. Також розглянуті техніки захисту від збору інформації за допомогою OSINT. Заключній роботі присвячений перевагам використання OSINT в кібервійні і його місцю в загальній стратегії кібербезпеки.

Ця робота є корисною для кібербезпекових експертів, аналітиків, розвідників, а також будь-якої людини, яка цікавиться кібербезпекою і хоче дізнатися більше про використання OSINT в кібервійні.

Поняття OSINT виникло в наукових і дослідницьких колах ще в 1930-х роках в США, коли військові аналітики стали використовувати відкриті джерела для збору інформації про потенційних ворогів та їх діяльність. Однак, поняття OSINT стало більш популярним після завершення Холодної війни, коли з'явилася потреба в розвідці відкритих джерел, таких як мас-медіа, Інтернет, соціальні мережі та інші джерела відкритої інформації, для збору інформації про тероризм, кіберзлочинність та інші загрози національній безпеці.

У 1992 році в США було засновано Федеральне агентство з відкритої інформації (Federation of American Scientists), яке стало центром дослідження та розвитку методів збору, обробки та аналізу відкритої інформації. Пізніше, в 2001 році, в США було створено спеціальний орган для збору та аналізу інформації з відкритих джерел - Центр національної безпеки відкритої інформації (National Open Source Enterprise), який забезпечував збір, аналіз та передачу відкритої інформації різним агентствам та відомствам США.

У кінці 1990-х - початку 2000-х років з'явилися перші програми та інструменти для збору та обробки відкритої інформації. Наприклад, в 1996 році був

створений програмний продукт NetOwl, який використовується для збору та обробки відкритої інформації.

Станом на сьогодні існує безліч програмних інструментів для збору та аналізу відкритої інформації, а саме:

1. Maltego - це програма, яка дозволяє збирати та аналізувати інформацію про людей, організації та компанії з відкритих джерел.

2. Shodan - це пошукова система, яка дозволяє знаходити відкриті порти на мережі Інтернет та збирати інформацію про пристрої, які підключені до Інтернету.

3. Social Mention - це інструмент для моніторингу соціальних мереж, який дозволяє знаходити та аналізувати згадки про певні ключові слова або бренди в соціальних мережах.

4. Google Alerts - це безкоштовний сервіс від Google, який дозволяє налаштувати сповіщення про нову інформацію з відкритих джерел, яка містить певні ключові слова.

5. Hootsuite Insights - це інструмент для моніторингу соціальних мереж, який дозволяє відстежувати згадки про бренд або ключові слова в соціальних мережах, а також аналізувати поведінку аудиторії.

6. Tineye - це пошукова система, яка дозволяє знаходити зображення в Інтернеті, які мають аналогічний контент.

7. SpyFu - це інструмент для аналізу конкурентів у сфері цифрового маркетингу, який дозволяє дізнатися про платну та органічну пошукову оптимізацію, рекламні кампанії та ключові слова.

Це лише декілька з багатьох програмних інструментів для збору та аналізу відкритої інформації, які можуть бути використані для здійснення OSINT-дослідниками.

В нинішніх умовах військового стану України – це питання є досить актуальним так як постійно потребується робота над пошуком важливої розвідувальної інформації, пошуком колаборантів, військових злочинців та багато іншого. Відповідно цією роботою займаються як військові та правоохоронні органи так і громадські організації.

Для здійснення процесу пошуку інформації можна використовувати різні методи, а саме:

1. Пошук в Інтернеті - це найбільш очевидний метод збору інформації з відкритих джерел. Він може бути виконаний шляхом пошуку ключових слів та фраз в пошукових системах, включаючи Google, Bing, Yahoo! та інші.

2. Моніторинг соціальних мереж - цей метод дозволяє знаходити та аналізувати інформацію, яка опублікована в соціальних мережах, таких як Facebook, Twitter, LinkedIn, Instagram та інші. Це може бути корисним для збору інформації про людей, організації, події та багато іншого.

3. Аналіз відкритих джерел даних - цей метод включає в себе аналіз даних, які доступні з відкритих джерел, таких як газети, журнали, публічні бази даних, офіційні веб-сайти державних установ та інших організацій.

4. Застосування спеціальних програмних інструментів - для збору та аналізу відкритої інформації можуть бути використані спеціальні програмні інструменти, такі як Maltego, Shodan, Social Mention, Google Alerts та інші.

5. Співпраця з іншими джерелами - для збору інформації можна звертатися до джерел, таких як люди, експерти, співробітники організацій, які можуть надати корисну інформацію.

Ці методи можуть бути використані окремо або в комбінації з іншими методами для здійснення OSINT. Важливо також враховувати законодавство та етичний кодекс.

УДК 004.056.5

МЕТОД ДВІЙНОГО ХЕШУВАННЯ SHA З ДОДАТКОВИМ ПЕРЕБОРОМ

Денис Іванов

*Київський національний університет будівництва і архітектури
denys.ivanov20@gmail.com*

Метод двійного хешування SHA з додатковим перебором є ефективним і безпечним способом захисту інформації від несанкціонованого доступу. Даний метод використовує два послідовних хешування з використанням різних алгоритмів SHA, що дозволяє збільшити безпеку процесу.

Для підвищення безпеки методу, можна застосовувати додатковий перебір, який полягає у генерації випадкових значень та їх використанні у якості солі для хешування. Це дозволяє змінювати вихідний результат хешування для однакових даних, що унеможливує зломисникам відновлення вхідних даних.

Ще однією перевагою методу двійного хешування SHA з додатковим перебором є його швидкість та простота використання. Даний метод може бути використаний для захисту даних на різних рівнях, включаючи зберігання паролів та інших конфіденційних даних. Незважаючи на всі його переваги, метод двійного хешування SHA з додатковим перебором не є бездоганним. Існує можливість атаки методу шляхом зламування хеш-функцій, тому важливо регулярно оновлювати алгоритми хешування та солі для максимальної безпеки.

На сьогоднішній день методами локально чутливого-хешування (LSH) використовують майже у всіх сферах ІТ воно є досить актуальними. LSH – це метод, який знижують розмір багатомірних даних. Уявити апаратний або технічний засіб без використання LSH досить складно. Вони допомагають, знаходити дублікати, задіяні у кластеризації та конізації даних, знаходження найближчого сусіда, особливим представлення хешування є те що можна шифрувати в особистому коді інформацію. Для створення рекомендацій можуть використовуватися дані про дії користувача або його характеристики. У роботі розглядається задача кодування текстової інформації у хеш представлення та конізації даних. Представлення набору даних у вигляді LSH дуже важлива тому що саме цю методику використовують у збереженні важливої інформації у базах даних, саме метод чутливого-хешування захищає нашу особисту інформацію від зломисників.

Захист та конфіденційність даних у базах даних одна із головних умов успішного підприємства. Захист паролів та тексту представленого та записаного в базах даних потрібна особливого догляду та контролю. У випадку атаки на систему та втрати даних потягне за собою колосальні збитки та втрати клієнтського базису. Запорукою надійності є повторне хешування даних з використанням солей та повторних алгоритмів cost для надійності та затримання циклу. Швидкість не завжди є добре на живому прикладі з хешуванням даних, можна сказати, що чим швидша хеш функція, тим більш вона вразлива для повного перебору. Всі приклади паролів хешу за алгоритмом MD5 та SHA і зберігаються у вигляді хеш-значень у базі даних.

MD5 – це 128-бітний алгоритм хешування, розроблений професором Рональдом Л. Призначений для створення «відбитків» або дайджестів повідомлення довільної довжини і подальшої перевірки їх достовірності. Широко застосовувався для перевірки цілісності інформації та зберігання хеш паролів у базах даних.

SHA (Secure Hash Algorithm) - це сімейство криптографічних алгоритмів хешування, розроблених Національним інститутом стандартів і технологій (NIST) США. Він використовується для створення унікальних «відбитків» даних, які мають фіксовану довжину. SHA є більш безпечним алгоритмом, ніж MD5, оскільки він використовує більш складні математичні операції та має більшу довжину хешу. Однак, з появою нових технологій і збільшенням обчислювальної потужності комп'ютерів, деякі версії SHA також можуть бути вразливими до атак. Ці алгоритми широко використовуються для перевірки цілісності даних, створення цифрових підписів та збереження хеш паролів у базах даних. У разі крадіжки бази вихідні паролі можуть бути відновлені за допомогою заздалегідь підготовлених райдужних таблиць, так як часто користувачі використовують ненадійні паролі, що легко підбираються за словниками. Якщо ж пароль "посолити", тобто при обчисленні хеш-значень приєднати до вхідних даних рядок з декількох випадкових символів, які будуть значенням солі, то результуючі значення не співпадатимуть з поширеними словниками хеш-значень.

Знання солі дозволяє згенерувати нові словники для перебору, тому значення солі має зберігатись у таємниці. Для солі вірні ті ж рекомендації до складності, що і для складності пароля, тобто значення солі має мати хорошу ентропію і довжину. Використання методу хешування SHA з додатковим перебором та використанням прикладних солей. Аналіз останніх дослідження показали, що із швидким рухом розвитку комп'ютерної індустрії росте потужність апаратної одиниці і постає проблема захищеності даних представлених у хеш значенні, завдяки перебору по алгоритму не постане проблема знайти відповідну колізію до вже отриманого хеш значення.

Алгоритм SHA по собі вже застарілий, але його продовжують активно використовувати і по цей час і саме для нас постає головне питання у використанні алгоритму хешування з додатковим перебором та використання адаптивних солей для надійного шифрування даних, які представляються у базах даних.

Література

1. Next Generation Firewall. URL:<https://www.fortinet.com/ru/products/next-generation-firewall>
2. Top 5 best NGFW vendors of 2021. URL: <https://www.nomios.com/news-blog/top-5-next-generation-firewall-vendors-ngfw-2022/>
3. Finding SHA-1 Характеристики: General Results and Applications (англ.). Дата звернення: 4 жовтня 2017 року. Архівовано 26 липня 2008 року.
4. SHA-1 Collision Search Graz (англ.). - Дослідницький проект технологічного університету Граца . Архівовано з оригіналу 7 листопада 2008 року.

УДК 004.056

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Павло Ігнатолія¹, Ярослав Сивохоп², Василь Різак³

Ужгородський національний університет

¹pavlo.ihnatiolia@uzhnu.edu.ua, ²syvochop@gmail.com,

³editor@physics.uz.ua

Урбанізація та технологічна революція з початку 1990 року спричинила появу концепцій “розумних міст” - населених пунктів, що використовують передові технології та керовані даними рішення для покращення якості життя своїх мешканців, підвищення їх безпеки та оптимізації міських послуг.

Основою функціонування будь-якого міста є його транспортна інфраструктура - це і фізична інфраструктура, така як дороги, мости та тунелі, а також транспортні системи, як-от громадський транспорт, системи спільного використання велосипедів та самокатів та інші автономні транспортні засоби.

Метою даної роботи є встановлення, класифікація та аналіз загроз в інтелектуальних транспортних системах для подальшої розробки комплексної системи захисту (КСЗІ) для інтелектуальних транспортних систем.

Розумна транспортна інфраструктура використовує технології та дані для створення ефективної, безпечної та зручної транспортної системи для жителів міста. Це відбувається шляхом впровадження широкого спектру технологій:

- обладнання для збору інформації - це різні IoT-пристрої, камери відеонагляду, GPS датчики та інші пристрої, що збирають інформацію про поточну завантаженість доріг та транспортних вузлів.

- Технологій для передачі даних (мобільні мережі, WiFi та провідне підключення) та протоколів комунікації (HTTPS, MQTT, LoRa/ZigBee) для доставки зібраних даних до центрів їх обробки.

- Центрів обробки інформації та прийняття рішень, де проводиться аналіз великих об'ємів даних в режимі реального часу та прийняття рішень про оптимізацію трафіку.

Разом з цим виникають нові загрози та виклики, притаманні розумній транспортній інфраструктурі та необхідність впровадження захисту від них.

Виділимо наступні типи загроз для розумної транспортної інфраструктури:

1. Кібератаки - розумна транспортна інфраструктура спирається на взаємопов'язані системи та мережі, що робить їх вразливими до кібератак, які можуть порушити або скомпрометувати систему. До кібератак відносять: - DDoS атаки, - Атака «людина посередині», - SQL ін'єкції та інші. Щоб запобігти кібератакам у розумній транспортній інфраструктурі, необхідно впровадити надійні заходи безпеки, такі як брандмауери, шифрування, засоби контролю доступу та системи виявлення вторгнень.

2. Порушення цілісності даних - збір та обмін даними в інтелектуальній транспортній інфраструктурі може стати мішенню для хакерів, які прагнуть викрасти конфіденційну інформацію, таку як особисті та фінансові дані. Для захисту від такого роду атаки необхідно імплементувати багаторівневу систему авторизації та аутентифікації, для керування доступом до даних, а також використовувати захищені протоколи для доступу до даних.

3. Шкідливе програмне забезпечення - ШПЗ може бути використане для отримання неавторизованого доступу до розумної транспортної інфраструктури та отримання подальшого контролю над системою. Сюди також відносять атаки з використанням програм-шифрувальників, які унеможливають доступ до даних. Для захисту від атак з використанням ШПЗ крім системи розподілення доступу та вищезгаданих засобів захисту, варто мати резервну копію даних та алгоритм швидкого їх відновлення, у разі атаки.

4. Фізичні атаки - розумна транспортна інфраструктура, як-от світлофори, може наражатися на фізичну атаку або вандалізм, що призведе до порушення транспортного потоку та загрози безпеці. Для захисту від фізичних атак, компоненти інфраструктури можуть використовувати спеціальні антивандальні корпуси, а також сповіщати правоохоронні органи про факт вандалізму з наданням власних GPS координат.

5. Внутрішні загрози та соціальна інженерія - співробітники або підрядники, які мають доступ до інтелектуальних систем транспортної інфраструктури, можуть навмисно чи ненавмисно зловживати своїм доступом, що призводить до порушень безпеки або системних збоїв. Найкращим захистом від внутрішніх загроз та соціальної інженерії слугує навчання персоналу та наявність внутрішньої служби безпеки на установі, що ретельно аналізує поведінку працівників та порядок доступу до інформації.

Отже, для усунення вище згаданих загроз потрібне створення та впровадження комплексної системи захисту розумної транспортної інфраструктури з урахуванням особливостей її функціонування.

Крім того, регулярні перевірки безпеки, оновлення програмного забезпечення та профілактичні роботи з персоналом необхідні для забезпечення постійної безпеки та стійкості системи.

УДК 004.56.5(043.2)

**ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ТА
БАНКІВ****Дмитро Каблучко***Державний університет телекомунікацій
info@dut.edu.ua*

У сучасному цифровому світі кібербезпека стає все більш актуальною темою, особливо для країн, які швидко розвиваються в галузі технологій. Україна не є винятком і зазнала багатьох кібератак, що свідчить про необхідність забезпечення кібербезпеки в країні. Ця проблема стає все більш актуальною в контексті ескалації повномасштабної війни з російською федерацією і, відповідно, розвитку кіберзлочинності та активної експлуатації вразливостей в системах безпеки [2].

Кібербезпека є важливою складовою національної безпеки та економіки України, оскільки забезпечення захисту критичних інфраструктур є одним з пріоритетів у діяльності уряду, про що свідчить навіть створення у 2019 році Міністерства цифрової трансформації України (Мінцифри) [5], а також окремі аспекти діяльності Міністерства інфраструктури України (Мінінфраструктури). Крім того, Україна є активним учасником світового інформаційного простору та залежить від інформаційних технологій для розвитку бізнесу та економіки країни. Тому відповідальність за забезпечення кібербезпеки лежить не тільки на уряді, але й на підприємствах та громадянах. Наслідки кібератак можуть бути надзвичайно серйозними, що може призвести до значних втрат для бізнесу та країни в цілому. Забезпечення кібербезпеки в Україні є надзвичайно важливою задачею для всіх стейкхолдерів, які залежать від інформаційних технологій.

Захист критичної інформаційної інфраструктури та банків стає все більш актуальним питанням у світі, оскільки дедалі більше держав та організацій стикаються зі збільшенням кіберзагроз. Це може призвести до крадіжки конфіденційної інформації, порушення фінансової стабільності та інших серйозних проблем.

Проблематика захисту критичної інформаційної інфраструктури та банків полягає в тому, що кіберзлочинці постійно шукають нові способи зламувати системи захисту та отримати доступ до конфіденційної інформації. Водночас, інфраструктура банківської системи постійно розвивається та змінюється, що може призвести до зниження ефективності старих методів захисту. Тобто процес розвитку рівня захисту та кібератак є паралельним та взаємо компенсується [1, 2].

Одним з основних викликів захисту критичної інформаційної інфраструктури та банків є недостатня кількість кваліфікованих фахівців, здатних захистити систему від кіберзагроз. Це може призвести до розповсюдження некомпетентності та вразливостей у захисті систем.

Загалом, є цілий ряд ефективних способів захисту критичної інформаційної інфраструктури та банків, усі вони опираються на активне застосування інформаційних технологій, а також високий рівень цифрової обізнаності громадян.

Щодо методів здійснення кіберзахисту банків та критичної інформаційної інфраструктури, то один із них полягає в регулярному аудиті та моніторингу інформаційних систем, щоб вчасно виявляти та виправляти можливі вразливості. Будь-яка система захисту має свій життєвий цикл ПЗ, і потребує постійної актуалізації безпекових підсистем [5].

Іншим широко застосованим способом здійснення кіберзахисту розглядуваної інфраструктури є використання ефективної системи ідентифікації та аутентифікації користувачів задля убезпечення від несанкціонованого доступу [4]. Це цілий спектр науково-технічних, а також програмних засобів, що дозволяють відсіяти потенційних шахраїв, кіберзлочинців, або людей, які видають себе за інших, тому системи активно користуються двухфакторними методами входів, обмеженнями часу на користувацькі сесії, видачами користувачам системних токенів або файлі-ключів, технологіями сканерів відбитків пальців або розпізнаванням облич тощо. Додатковий захист можна забезпечити за допомогою використання сучасних криптографічних методів шифрування даних, в тому числі й невпинно прогресуючого методу шифрування та зберігання конфіденційних даних блокчейн(англ. blockchain) та застосуванням фасерволів для контролю доступу до мережі [1, 3].

Також одним із важливих елементів захисту критичної інформаційної інфраструктури та банків від можливих атак та випадків втрати даних є організація резервного копіювання та відновлення даних [3].

Важливим пунктом кібербезпекового захисту є контроль за використанням пристроїв з доступом до мережі та використанням програмного забезпечення, яке може становити загрозу безпеці систем.

Як вже було сказано вище в тезах, то, окрім розвинутої ІТ-інфраструктури, необхідно мати й високу цифрову обізнаність та надійність персоналу, а тому регулярні навчання й підвищення кваліфікації співробітників з питань кібербезпеки можуть допомогти виявляти та запобігати можливим загрозам та вразливостям в системах безпеки. Важливо забезпечувати високий рівень усвідомленості та культури кібербезпеки серед працівників банків та інших організацій, які залежать від інформаційних технологій, а також зберігати строгу й чітку інкапсуляцію відповідних робітників по відношенню до частин системи [2], якій вони належать, що допоможе попередити про потенційні загрози, які могли би виникнути через людський фактор: недбалість, обман, викриття конфіденційної інформації [5].

Отже, просування сфери безпеки критичної інформаційної та банківської інфраструктури є однією з найбільш важливих задач у сучасному світі. Для досягнення цієї мети необхідно застосовувати сучасні методи захисту, такі як системи ідентифікації та аутентифікації користувачів, криптографічні методи шифрування даних та резервне копіювання та відновлення даних. При цьому не менш важливим є регулярне навчання та підвищення кваліфікації персоналу з питань кібербезпеки та усвідомлення культури кібербезпеки серед співробітників [5].

Література

1. World Investment Report 2007: Transnational Corporations, Extractive Industries and Development. — UNCTAD, United Nations. New York and Geneva, 2007.

2. Концептуальні засади правового забезпечення інноваційної політики України: монографія / Д. В. Задахайло, Г. П. Клімова, Л. С. Шевченко та ін. ; за ред. Д. В. Задахайла. – Х. : Право, 2014. – 464 с.

3. Slyusar V.I. Blockchain technology in future multi-domain operations.// Збірник матеріалів науково-практичної конференції “Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності”.– Львів: Національна академія Сухопутних військ імені гетьмана Петра Сагайдачного. Науковий центр Сухопутних військ. – 18 листопада 2021 року. - С. 210 - 211.

4. Автентифікація (інформаційні технології) // Велика українська енциклопедія : у 30 т. / проф. А. М. Киридон (відп. ред.) та ін. — 2016. — Т. 1 : А — Акц. — 592 с.

5. Управління ефективністю моніторингу банківської системи України: монографія / В. І. Приймак, С. М. Лобозинська, П. В. Приймак; Львів. нац. ун-т ім. І. Франка. — Львів: Растр-7, 2015. — 401 с. — Бібліогр.: с. 304—331.

УДК 004.056.55

ПСЕВДОНЕДЕТЕРМІНОВАНИЙ ПІДХІД ДО ПОБУДОВИ ШИФРІВ

Володимир Лужецький

*Вінницький національний технічний університет
lva.kzi2002@gmail.com*

Теоретичним підґрунтям для побудови шифрів є фундаментальна робота Клода Шеннона «Теорія зв'язку в секретних системах», у якій сформульовано основні вимоги, що висуваються до стійких шифрів. Було показано, що шифр може бути побудований на основі декількох циклів підстановки та перестановки. Тому основна увага криптографів спрямована саме на реалізацію цих операцій. Традиційний (детермінований) підхід до побудови блокових шифрів передбачає детермінованість характеристик використовуваних блоків даних та алгоритмів шифрування. Тобто все відомо як тому, хто шифрує, так і тому, хто дешифрує (зловмиснику). Отже стійкість шифру в основному залежить від секретного ключа.

Метою даної роботи є підвищення ефективності підходу до побудови шифрів за рахунок використання перестановок на етапах зчитування і записування даних та псевдовипадкової послідовності бінарних операцій на етапі перетворення даних.

Пропонується підхід, який названо псевдонедетермінованим. Така назва випливає з того, що зловмиснику не відомо, які саме характеристики блоків даних використано і в якій послідовності, а також в якій послідовності використано набір операцій при реалізації алгоритму шифрування, а, отже, йому буде потрібно здійснити повний перебір усіх можливих значень характеристик і можливих алгоритмів шифрування. Тобто з точки зору зловмисника він має справу з недетермінованим процесом шифрування. Навпроти, той хто шифрує має справу з детермінованим процесом, оскільки використання секретного ключа однозначно

визначає характеристики використовуваних блоків даних та послідовність кроків алгоритмів шифрування.

Узагальнена схема процесу шифрування складається з трьох етапів: зчитування даних, перетворення даних і записування даних. Варто відзначити, що традиційно зчитування та записування даних не розглядають як окремі етапи процесу шифрування. На думку автора, це вносить певні обмеження стосовно підвищення стійкості шифру.

Етапи зчитування/записування характеризується довжиною блоків даних і послідовністю їх зчитування/записування. Детермінований підхід передбачає використання постійної довжини блоку даних ($d=const$). Для сучасних шифрів $d = 64, 128, 256$ біт.

Псевдодетермінований підхід базується на використанні блоків змінної довжини ($d=var$). При цьому числове значення довжини залежить від певної складової секретного ключа: $d = f(k_i)$. Пропонується така довжина блоків $d = 8, 16, 32, 64, \dots$

Детермінований підхід передбачає лише природну (в порядку зростання номерів позицій) послідовність зчитування/записування блоків даних. Саме це і пояснює відсутність уваги до даних етапів шифрування.

Згідно з псевдодетермінованим підходом можливі такі послідовності зчитування/записування блоків даних:

- природна/за правилом;
- за правилом/природна;
- за правилом/за правилом.

Послідовності зчитування/записування блоків даних за правилом формуються згідно з правилами перестановок блоків даних, класифікацію яких наведено на рис. 1.

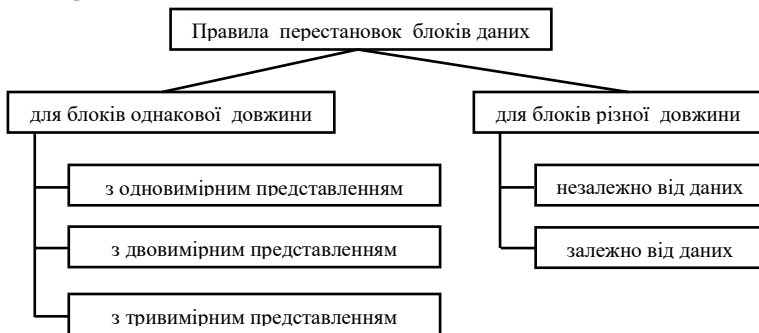


Рис.1. Класифікація правил перестановок

Етап перетворення характеризується набором операцій і послідовністю їх виконання. Пропонується використовувати бінарні операції, що описуються латинськими квадратами. Відомо, що існує велика кількість таких квадратів.

Наприклад, кількість квадратів четвертого порядку $K(4)=576$, а восьмого - $K(8)=108776032459082956800 \approx 10^{20}$.

На перетворення надходять блоки даних у тому порядку, який надає етап зчитування, і блоки гами (псевдовипадкові числа, що формуються залежно від секретного ключа). Нехай послідовність блоків даних, що підлягають перетворенню, має вигляд $\mathbf{M}=\{m_1, m_2, \dots, m_n\}$, а послідовність блоків гами - $\mathbf{G}=\{g_1, g_2, \dots, g_n\}$. Результат перетворення при зашифруванні $\mathbf{C}=\{c_1, c_2, \dots, c_n\}$ визначається як значення функції $c_i = L_j(m_i, g_i)$, де j - номер використовуваного латинського квадрату, що формується псевдовипадковим чином залежно від секретного ключа. Результат перетворення при розшифруванні визначається як значення функції $m_i = \bar{L}_j(c_i, g_i)$, де \bar{L}_j означає латинський квадрат, що описує перетворення, обернене до перетворення латинським квадратом L_j .

Секретний ключ має складові, що визначають правила зчитування і записування блоків даних, генерування гами та вибору латинських квадратів із заданого їх набору.

УДК 004.94.355

МЕРЕЖЕВО-ЦЕНТРИЧНА ПАРАДИГМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В.О. Крайнов

Національний університет оборони України імені Івана Черняховського

Процес впровадження автоматизованих інформаційних систем у військову справу спрямований на підвищення ефективності роботи органів військового управління. Однією з найважливіших функцій у діяльності органів управління є вироблення пропозицій для прийняття обґрунтованого рішення командиром. Основою для виконання цієї функції є інформація про свої війська, війська противника, умови ведення бойових дій та ін. Перш ніж інформацію можна було б використовувати, її необхідно зібрати, систематизувати, обробити і тільки після цього в потрібному вигляді видати користувачу. Для вирішення цих задач у штабах створюються автоматизовані інформаційні системи (АІС). Слід зауважити, що будь-яка АІС для надійного функціонування має бути забезпечена надійною системою інформаційної безпеки.

Проте наявність уразливостей та кіберзагроз породжує кіберінциденти, для локалізації та нейтралізації яких необхідні ефективні методи виявлення, ідентифікації, оброблення та розслідування. Одним із підходів є застосування мережево-центричної парадигми інформаційної безпеки, яка орієнтована на протидію виникненню та ліквідації наслідків кіберінцидентів за допомогою засобів, об'єднаних інформаційними мережами в єдину систему. З огляду на динаміку

розвитку комп'ютерних технологій, пов'язаних з “мережево-центричною” обробкою даних. Маніпуляція і обмін складними даними відбувається в масштабах усе більших і складних неоднорідних мереж, що спонтанно поширюються в неконтрольованому просторі Інтернет. Нова, мережево-центрична (network centric) парадигма інформаційної безпеки, як концептуальна схема (модель) постановки й вирішення проблеми, впливає насамперед з підвищених вимог до живучості АІС, які характеризуються високим ступенем розподілу ресурсів (обслуговуванням, логікою, програмним й апаратним забезпеченням, телекомунікаціями) і практично повною відсутністю централізованого керування. Концептуальна модель ешелонованої багатoshарової системи інформаційної безпеки яка зараз використовується у США, містить у собі набір компонентів, що реалізують функції моніторингу, захисту й адаптації інформаційних ресурсів, які в сукупності дозволяють поетапно запобігти проникненню, виявити факт порушення, локалізувати об'єкт впливу, нейтралізувати й видворити порушника, відновити втрачені функції системи (рис.1). В основі даної моделі системи інформаційної безпеки лежить широке використання пасивних (фільтрів, екранів) і активних (датчиків виявлення вторгнення, розпізнавання аномального поведіння, адаптивних алгоритмів відновлення) технічних засобів захисту. Американський досвід використання технології IDS (Intrusion Detection Systems) у різних галузях говорить про те, що не дивлячись на очевидні

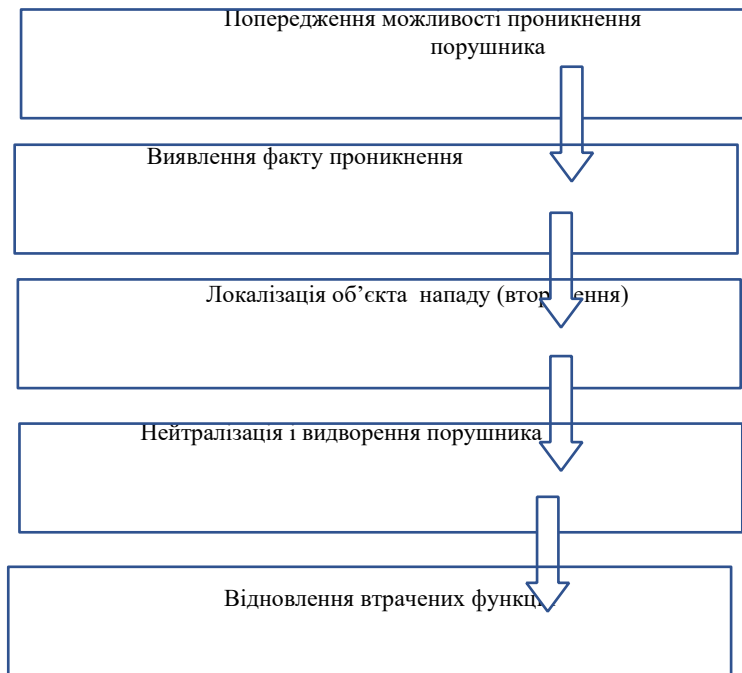


Рис. 1. Концепція ешелонованої системи захисту інформаційних ресурсів

переваги цього напрямку інформаційної безпеки (автономність, гнучкість, адресність, оперативність й ін.) його розповсюдження пов'язане із цілим рядом проблем, як об'єктивного, так і суб'єктивного походження, серед яких можна виділити в якості превалюючих відомчі інтереси й (authentication, non repudiation) і забезпечення надійності (availability) функціонування системи. Закордонний й вітчизняний досвід показує, що це завдання найбільш ефективно вирішується за допомогою методів криптографії в сполученні з використанням перевіреного та ліцензованого програмного забезпечення, а також надійними інтелектуальними носіями ключової інформації (матеріалу ключа) організаційно-технічні експлуатації. У цілому забезпечення інформаційної безпеки сьогодні містить у собі такі поняття як цілісність (integrity) інформації, конфіденційність (confidentiality) і захищеність від несанкціонованого доступу. Забезпечення цілісності інформації й автентичності (особистості) користувача в даний час найбільш ефективно реалізується за рахунок використання електронного підпису на основі несиметричних криптографічних алгоритмів із двома ключами (особистим і загальним) у поєднанні із системою посвідчувальних центрів. У США цей концептуальний підхід до захисту інформаційних ресурсів отримав назву "інформаційної гарантії" (information assurance) який суттєво розширив рамки класичного поняття інформаційної безпеки (INFOSEC). Фактично концепція інформаційної гарантії в США розглядається як оборонна інформаційна операція, в ході якої також при випадковому або навмисному викривленні інформації, несанкціонованому проникненню або навмисному вторгненні в контур управління, втрати частини ресурсів і перевантаження трафіку комплекс організаційно-технічних заходів захисту повинен забезпечити виконання найбільш важливих завдань. Іншими словами, не тільки відмови та збої устаткування, перекручування й витік інформації, але й терористичні акти на об'єктах інформаційної інфраструктури розглядаються вже не як потенційні загрози, а як системотехнічні фактори зовнішнього середовища з усіма впливаючими наслідками.

Таким чином, концепція інформаційної безпеки 21-го століття впливає перш за все із підвищених вимог до живучості інформаційних систем що виходять за рамки підприємств, відомств ті кордонів держав, які характеризуються високим ступенем розподілу ресурсів і практично повною відсутністю централізованого управління. Системи інформаційної безпеки майбутнього повинні не тільки й не стільки обмежувати допуск користувачів до програм і даних, скільки визначати і делегувати їхні повноваження в корпоративному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації й усувати їхні наслідки, гнучко адаптуючи структури в умовах відмов, часткової втрати або тривалого блокування ресурсів.

УДК 338.242(477)

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЛОГІЧНИХ МОДЕЛЕЙ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Володимир Шиповський

Національний університет оборони України імені Івана Черняхівського, v.shypovskiy@nuou.org.ua

Останні події в Україні, зокрема окупація Криму та широкомасштабне вторгнення росії, демонструють важливість забезпечення кібербезпеки об'єктів критичної інфраструктури. Російська Федерація використовує різні методи, включаючи ракетні та кібератаки, для здійснення впливу на інфраструктуру нашої країни та забезпечення своїх військових та політичних інтересів. Ці напади зумовлюють необхідність розвитку та застосування ефективних методів оцінювання кібербезпеки, щоб захистити інфраструктуру від можливих загроз та підвищити рівень безпеки. У даній статті будуть проаналізовані та порівняні різні логічні моделі оцінювання кібербезпеки інформаційних систем, які можуть бути застосовані для захисту об'єктів критичної інфраструктури в Україні.

Метою даної роботи є порівняльний аналіз логічних моделей оцінювання кіберстійкості інформаційних систем, а саме: DREAD, STRIDE, PASTA та CVSS, переваг та недоліків, та вибір оптимальної для загроз та ризиків об'єктів критичної інфраструктури.

Розглянемо найпоширеніші логічні моделі оцінювання кіберстійкості інформаційних систем, деякі з них наведені нижче:

1. Модель дерева загроз: ця модель використовує дерево загроз для оцінювання ризику кібератаки. Кожен вузол у дереві відповідає певній загрозі, а дуги показують ймовірність того, що ця загроза стане реальністю. З цієї моделі можна отримати інформацію про рівень загроз, а також про те, які частини інформаційної системи найбільш вразливі до атак.

2. Модель DREAD: ця модель використовує п'ять факторів для оцінювання ризику кібератаки: Damage, Reproducibility, Exploitability, Affected users та Discoverability. Кожен фактор оцінюється від 0 до 10, і загальний ризик визначається шляхом підрахунку середнього значення.

3. Модель STRIDE: ця модель використовує шість факторів для оцінювання ризику кібератаки: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, та Elevation of privilege. Кожен фактор оцінюється від 0 до 10, і загальний ризик визначається шляхом підрахунку середнього значення.

4. Модель CVSS: ця модель використовує 3 метрики для оцінювання ризику кібератаки: базова метрика, темпоральна метрика, та середовищна метрика. Базова метрика визначає ризик, який може виникнути при використанні вразливості, темпоральна метрика визначає, як швидко вразливість може бути виправлена, а середовищна метрика визначає, як вразливість впливає на систему в цілому.

Порівняльний аналіз моделей за основними характеристиками наведено у таблиці 1.

Таблиця 1

Порівняння характеристик моделей оцінювання

Характеристика	Модель DREAD	Модель STRIDE	Модель CVSS	Модель дерева загроз
Ступінь охоплення	Середній	Високий	Високий	Високий
Точність оцінювання	Висока	Середня/Висока	Висока	Середня/Висока
Швидкість оцінювання	Швидка	Помірна/Повільна	Повільна	Швидка
Розширюваність	Середня	Висока	Низька/Середня	Висока
Придатність до довгострокового використання	Висока	Висока	Висока	Висока
Частота виявлення нових загроз	Низька	Середня/Висока	Низька/Середня	Висока
Вартість розробки та підтримки	Середня	Середня/Висока	Висока/Дуже висока	Середня
Кількість помилок	Середня	Низька/Середня	Середня	Середня
Складність розробки та використання	Низька	Середня	Висока	Середня/Висока

Вибір оптимальної моделі для оцінювання кібербезпеки інформаційних систем саме об'єктів критичної інфраструктури залежить від конкретних потреб та обставин кожної організації. Однак, з урахуванням результатів порівняння чотирьох найбільш популярних моделей (DREAD, STRIDE, Attack Tree та CVSS), можна зробити висновок, що найбільш оптимальним варіантом буде модель CVSS.

Модель CVSS є стандартом, розробленим групою спеціалістів з кібербезпеки та затвердженим міжнародною організацією FIRST. Ця модель оцінює рівень вразливості і потенційну шкоду, що може бути завдана, враховуючи широкий спектр факторів. Крім того, CVSS надає різні метрики, такі як базовий рівень вразливості, вплив та відсутність відповіді на вразливість, що дозволяє оцінювати кібербезпеку з точністю та деталізацією.

Додатково, модель CVSS відрізняється від інших моделей тим, що враховує контекст індивідуального застосування. Це означає, що оцінка кібербезпеки буде більш точною та зрозумілою, оскільки враховується конкретне застосування інформаційної системи.

Отже, модель CVSS є оптимальним варіантом для оцінювання кібербезпеки інформаційних систем об'єктів критичної інфраструктури через її точність, деталізацію та врахування контексту індивідуального застосування

Науковий керівник – д.т.н., проф. Микусь С.А.

УДК 004.77

ПІДХІД ДО АНАЛІЗУ ВИХІДНОГО ТРАФІКУ**Наталія Петляк¹, Юлія Хохлачова², Юрій Кльоц³**¹*Національний авіаційний університет, npetyak@khmnu.edu.ua,*
*2yuliiahohlachova@gmail.com*³*Хмельницький національний університет, klots@khmnu.edu.ua*

Все більше і більше люди стають залежними від комп'ютерів, Інтернету та інших цифрових технологій. Цифровізація проникає в усі сфери життя, включаючи критичну інфраструктуру, бізнес, громадські послуги та інше. Однак, залежність від цифрових технологій також призводить до зростання кіберзлочинності.

Аналіз IPS/IDS систем показав, що вони орієнтовані на захист від зловмисних дій у корпоративних мережах, а самі системи потребують спеціального обладнання та фахівців для налаштування й подальшої підтримки мережі. Тому такі системи, зазвичай, не використовують для загальнодоступних мереж. Для вирішення задач аналізу трафіку застосовують методи параметричного аналізу, нечіткої логіки або штучний нейронний мереж. Однак окреме використання таких підходів має значні недоліки. Відповідно, проблема аналізу вихідного трафіку задля забезпечення безпеки в мережі, захисту її від компрометації та зменшення навантаження на мережу залишається актуальною.

Метою даної роботи є розробка підходу до аналізу вихідного трафіка задля запобігання витоку зловмисного трафіка з мережі та виявлення порушника.

Дослідивши типову поведінку порушників у мережі під час атаки та проаналізувавши пакети можна сформувати набір параметрів, за якими можна виявити зловмисні дії. Задля швидшої роботи системи, яка розроблена на основі вказаного підходу, доцільно обрати параметри з найбільшою ефективністю. На основі оптимізованих параметрів слід сформувати сигнатуру пакета, що використовуватиметься для виявлення зловмисного трафіку:

$$s = \{IPs, IPd, Ps, Pd, Pr, Sd, T\}, \quad (1)$$

де IPs – IP-адреса джерела; IPd – IP-адреса призначення; Ps – порт джерела; Pd – порт призначення; Pr – протокол; Sd – швидкість передачі даних; T – час надходження пакету на перевірку.

Елементи сигнатури IPs , IPd , Ps , Pd , Pr можуть набувати один із трьох станів: заборона, дозвіл та невизначено. Елемент сигнатури Sd може приймати один із трьох станів: низька, середня та висока. Пряме порівняння сигнатур забезпечує максимальну швидкість аналізу, однак, для досягнення необхідної ефективності аналізу трафіку потрібно сформувати словники сигнатур. Однак виникає задача формування словника сигнатур та підтримання його в актуальному стані.

Для аналізу вихідного трафіку та формування словників сигнатур доцільно використати набір правил, що дозволяють провести класифікацію пакетів за критеріями. Задачі такого класу зазвичай вирішуються методами нечіткої логіки. Це дозволить вести аналіз трафіку та будувати словники в режимі реального часу. Перевагою такого підходу є висока достовірність отриманого результату, однак вона досягається за рахунок збільшення часу і ресурсів для аналізу пакету. В умовах

критичного завантаження каналів зв'язку або процесора пристрою, на якому проводиться аналіз доцільно зменшити навантаження на систему за рахунок використання для аналізу попередньо навченої ШНМ.

ШНМ довготривалої короткочасної пам'яті дозволяють знизити навантаження на систему при аналізі трафіку, що дозволяє їх використання в пікових режимах.

З огляду на вищевикладене, для ефективного виявлення порушників у мережі запропонований підхід (рис.1.) складається із трьох методів, що мають різні механізми виявлення.

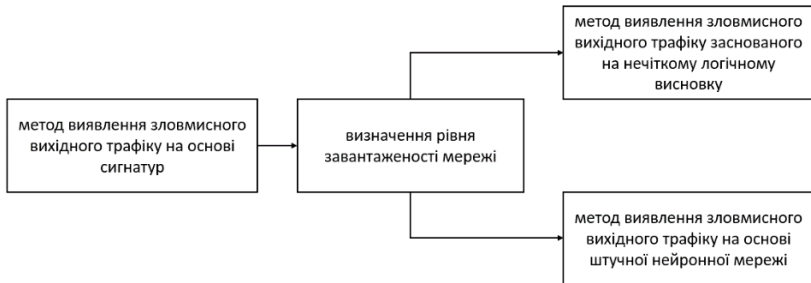


Рис.1. Підхід до аналізу вихідного трафіка

Першочергово має формуватися сигнатура та передаватися на метод виявлення зловмисного вихідного трафіку на основі сигнатур. Даний метод порівнює одержану сигнатуру із сформованими словниками (словник має початкові дані та наповнюється на методі з використанням нечіткого логічного висновку) дозволених та заборонених сигнатур. Якщо сигнатуру класифіковано, то з'єднання дозволяється чи блокується. Якщо сигнатуру не класифіковано, то відбувається перехід до наступного кроку: перевірка завантаженості мережі.

Якщо завантаження мережі та обладнання далеко від пікового, то буде виконуватися метод виявлення зловмисного вихідного трафіку, заснований на нечіткому логічному висновку. Під час виконання буде здійснюватися перевірка сигнатур відповідно до заданого набору правил. Якщо сформована сигнатура пакета відповідає одному з правил, які задовольняють вимогу дозволеного трафіку, то пакету дозволено з'єднання та сигнатура пакета записується в словник дозволених з'єднань. Інакше пакет відкидається та сигнатура пакета записується в словник заборонених з'єднань.

Якщо мережа функціонує в піковому навантаженні, то буде використовуватися метод виявлення зловмисного вихідного трафіку на основі штучної нейронної мережі. Перш ніж даний метод буде функціонувати, він проходить навчання та тестування на попередньо розроблених базах даних. Метод розроблено відповідно до двійкової класифікації довготривалої короткочасної пам'яті.

Запропонований підхід дозволяє класифікувати вихідний мережевий трафік з метою блокування зловмисних дій, що дає змогу запобігти перевантаженню мережевого обладнання та зменшити ймовірність компрометації поточної мережі та її власника.

УДК 004.77

ПРИВАТНІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНИХ МЕДІА

Єгор Шарай, Георгій Чупрін

Державний університет телекомунікацій

Приватність та безпека в соціальних мережах та медіа стали особливо важливими останнім часом, коли багато людей почали турбуватися про те, що їхні особисті дані та конфіденційна інформація можуть бути використані без їхньої згоди. Практично всі соціальні мережі можуть збирати та зберігати інформацію про користувача, таку як особисті дані, контакти, фотографії та розташування. Ця інформація зазвичай використовується для настроювання реклами, створення алгоритмів, але іноді також використовується для нелегального продажу третім сторонам.

Користувачі соціальних мереж повинні розуміти, що інформація, яку вони надають, може бути використана проти них у майбутньому, про що, як правило, дається згода на початку користування. Тому важливо бути обережним при наданні своїх персональних даних у соціальних мережах. Деякі поради, які, на нашу думку, можна дати користувачам, включають:

1. Обмеження доступу до персональних даних: варто бути обережними при наданні своїх персональних даних у соціальних мережах та медіа. Потрібно обмежувати доступ до своїх особистих даних, таких як фотографії, розташування та контактні дані.

2. Використання сильних паролів: користувачі повинні використовувати сильні паролі для своїх соціальних мереж та медіа, щоб запобігти несанкціонованому доступу зловмисників до своїх облікових записів.

3. Використання функції або спеціалізованих застосунків для двофакторної автентифікації: варто використовувати цю функцію для своїх соціальних мереж та медіа, щоб переконатися, що будь-хто інший не отримує доступ до облікового запису.

4. Встановлення оновлень безпеки: користувачі повинні встановлювати найновіші оновлення систем та застосунків, задля того, щоб їх акаунти були захищені від найновітніших кіберзагроз.

Обмеження доступу до персональних даних – це ще одна з основних функцій для запезбечення приватності в соціальних мережах та медіа.

У соціальних мережах та медіа користувачі часто надають свої персональні дані, такі як ім'я, фотографії, місцезнаходження, дата народження, контактні дані та інші. Ця інформація може бути використана як соціальними мережами, так і третіми сторонами для створення профілю користувача та налаштування реклами.

Однак, якщо користувачі не обмежують доступ до своїх персональних даних, це може призвести до витоку особистої інформації і навіть крадіжки особи. Наприклад, зловмисники можуть використовувати ці дані для шахрайства, фішингу та інших видів кібератак.

Варто бути обережними при наданні своїх персональних даних у соціальних мережах та медіа. Слід надавати лише ті персональні дані, які дійсно необхідні для використання соціальної мережі. Деякі соціальні мережі пропонують можливості керувати доступом до особистої інформації, яку користувач надає.

ПОМИЛКИ «СЛАБКИХ» ПАРОЛІВ

1



Використання імен або прізвищ родичів або домашніх улюбленців.

Таку інформацію дуже легко знайти в соціальних мережах та інших відкритих джерелах

2



Використання послідовності цифр, зокрема, 123456 чи 11111, дат народження, комбінації літер, розташованих поруч, наприклад qwerty.

Методом перебору злочинці, легко підберуть такий пароль за тисячні долі секунди

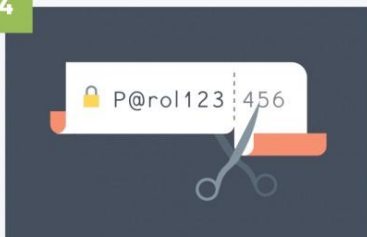
3



Вибір в якості коду слова password, admin або parol. Всі інші варіації банальних слів.

Це просто, але занадто очевидно та не відповідає основним вимогам надійних паролів

4



Використання паролів довжиною менше 8 знаків.

Зверніть увагу, що чим коротше буде ваш пароль, тим простіше його зламати

Один із прикладів того, як користувач може обмежити доступ до своїх персональних даних, це вибір того, хто може переглядати його профіль та публікації. Користувачі можуть вибрати, щоб тільки друзі могли переглядати їх профіль та публікації. Також можна обмежити доступ до інформації, яку бачать треті сторони та рекламодавці, використовуючи конфіденційність.

Крім того, користувачі можуть обмежити доступ до своїх фотографій, розташування та інших особистих даних. Наприклад, програми для соціальних мереж можуть запитувати доступ до розташування користувача, щоб надавати йому інформацію про місцеві події. Але якщо користувач не хоче, щоб його місцезнаходження було доступним для всіх, він може вимкнути цю функцію.

Таким чином, обмеження доступу до персональних даних є важливим кроком для забезпечення приватності та інформаційної безпеки.

Використання сильних паролів є важливим фактором для забезпечення безпеки облікових записів користувачів у соціальних мережах та медіа.

Сильний пароль - це такий пароль, який важко підібрати і має високий ступінь складності. Інакше кажучи, це такий пароль, спроби злому якого займуть занадто багато часу в зловмисників. Такий пароль повинен складатися з літер, цифр та символів, а також мати довжину щонайменше 8 символів. Використання сильних паролів для своїх соціальних мереж та медіа може захистити обліковий запис користувача від несанкціонованого доступу та кібератак.

Необачливі користувачі часто використовують слабкі паролі, такі як «123456», «password» або «qwerty». Ці паролі легко вгадати або підібрати методом грубої сили, так званим «brute force», що робить обліковий запис користувача вразливим для атак. Крім того, багато користувачів використовують один і той же пароль для всіх своїх облікових записів у різних соціальних мережах та медіа, що загрожує одночасною втратою всіх облікових записів, особистої інформації, а також неможливістю їх відновлення.

Також, користувачі повинні регулярно змінювати свої паролі та не ділитися ними з іншими людьми. Це допоможе запобігти доступу до облікового запису, навіть якщо хтось отримає пароль користувача. А також фактично зводитиме нанівець зусилля та витрати часу зловмисників з підбору попереднього паролю.

Насамкінець, використання сильних паролів для своїх соціальних мереж та медіа є важливим фактором для забезпечення безпеки облікового запису користувача та захисту особистих даних.

Використання «двофакторної автентифікації» є додатковим механізмом безпеки для забезпечення захисту облікового запису користувача в соціальних мережах та медіа.

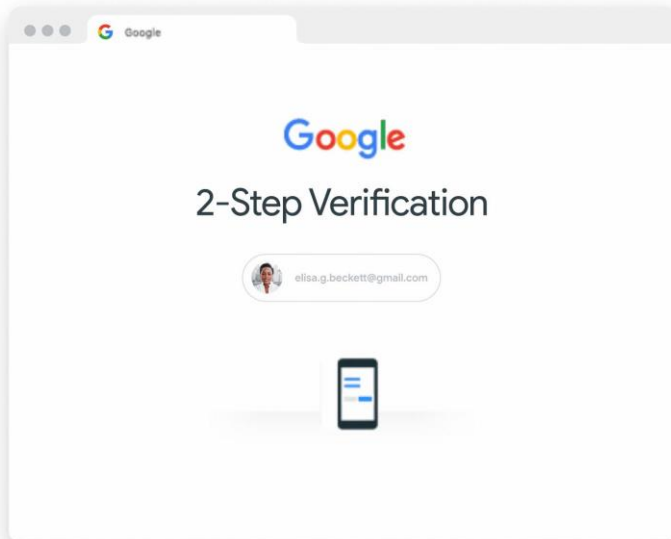
Двофакторна автентифікація (2FA) – це процес автентифікації користувача, який потребує двох незалежних форм ідентифікації. Крім традиційного логіну та пароля, користувачі повинні надати ще один фактор, такий як SMS-код, код від програми автентифікації або відбиток пальця, щоб отримати доступ до свого облікового запису.

Використання 2FA для своїх соціальних мереж та медіа може запобігти несанкціонованому доступу до облікового запису користувача, навіть якщо зловмисник отримає доступ до пароля користувача. У випадку, якщо зловмисник спробує отримати доступ до облікового запису користувача, 2FA захистить

обліковий запис, оскільки зловмисник не зможе надати додатковий фактор ідентифікації.

Користувачі можуть налаштувати 2FA для своїх соціальних мереж та медіа, дотримуючись інструкцій на сайті соціальної мережі або медіа. Більшість популярних соціальних мереж та медіа пропонують власну 2FA як додатковий захід безпеки для своїх користувачів.

Крім того, користувачі мають змогу використовувати програми автентифікації, такі як Google Authenticator або Authy, які генерують тимчасові коди для 2FA. Це дозволяє переконатися, що тільки користувач має доступ до своїх облікових записів у соціальних мережах та медіа.



Хоча двофакторна автентифікація може «зіграти» й проти власника облікового запису, наприклад, при втраті телефону з установленим застосунком 2FA; однак це залишається, напевно найнадійнішим методом захисту власних акаунтів та інформації, що зберігається в них.

Встановлення оновлень безпеки є ще одним важливим механізмом захисту облікових записів користувачів у соціальних мережах і медіа.

Програми соціальних мереж та медіа регулярно випускають оновлення безпеки, які усувають уразливості та запобігають можливим атакам на дані користувача. Користувачі повинні регулярно встановлювати ці оновлення, щоб захистити свої облікові записи від загроз.

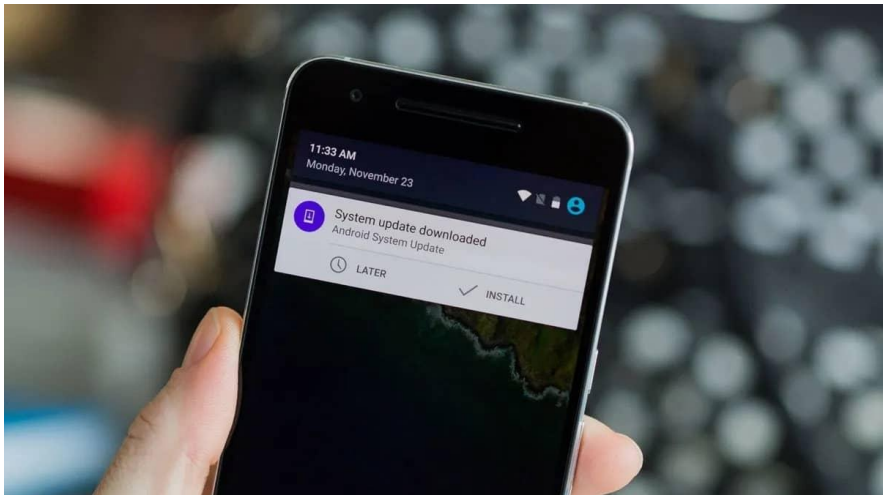
Деякі оновлення безпеки можуть містити виправлення вразливостей, які можуть бути використані зловмисниками для злому облікового запису користувача. Якщо

користувач не встановлює оновлення, вразливості можуть залишатися відкритими, що підвищує ризик зламування облікового запису.

Оновлення безпеки можуть включати нові функції безпеки, які покращують захист облікового запису користувача. Наприклад, оновлення може включати вдосконалений механізм автентифікації, який підвищує безпеку облікового запису користувача.

Для того, щоб регулярно встановлювати оновлення безпеки, користувачі повинні настроїти автоматичне оновлення програм соціальних мереж та медіа. Це дозволяє автоматично оновлювати програми безпеки, коли вони стають доступними.

Насамкінець, встановлення оновлень безпеки є важливим заходом безпеки для захисту облікових записів користувачів у соціальних мережах та медіа. Користувачі повинні регулярно встановлювати оновлення безпеки, щоб усунути вразливості та покращити механізми безпеки своїх облікових записів.



У сучасному світі соціальні мережі та медіа відіграють важливу роль у житті мільйонів людей у всьому світі. Однак використання соціальних мереж та медіа може стати джерелом загроз для приватності та інформаційної або й фінансової безпеки користувачів.

Також, поінформованість – один з видів найкращого захисту. Варто уважно перечитати та запам'ятати всі поради, настанови та правила користування програми електронного листування або соціальними мережами.

Для того, щоб захистити свої дані в соціальних мережах та медіа, користувачі повинні вживати заходів безпеки, рекомендованих розробниками застосунків та систем безпеки, бути обережними при наданні своїх персональних даних, використовувати сильні паролі, двофакторну автентифікацію та регулярно встановлювати оновлення безпеки.

Всі ці заходи безпеки допоможуть користувачам захистити свої облікові записи та персональні дані від загроз. Однак, важливо пам'ятати, що захист даних у соціальних мережах та медіа – це безперервний процес, який потребує постійної уваги та регулярного оновлення заходів безпеки.

Таким чином, використання соціальних мереж та медіа може бути безпечним, якщо користувачі будуть дотримуватися рекомендацій щодо захисту своїх персональних даних та вживати заходів безпеки, які ми описали вище.

Науковий керівник – кандидат технічних наук, доцент, Пена Ю.В.

УДК 654.62-5.007(004.738)

ОЦІНКА ВИЯВЛЕНИХ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОСВІТІ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Михайло Пригара¹, Іван Опірський², Михайло Різак³

ДВНЗ «Ужгородський національний університет»^{1,3}

НУ "Львівська політехніка"²

¹misha_prigara@ukr.net, ²iopirsky@gmail.com,

³rizak.mykhailo@student.uzhnu.edu.ua

Вже більше 3 років освіта в Україні працює в умовах надзвичайної ситуації, спочатку епідеміологічного, а потім і військового характеру, що виявило низку ризиків інформаційної безпеки в галузі освіти на різних рівнях управління та реалізації освітнього процесу.

Умовно можна розділити на дві окремі структури: структура вищої; післядипломної та професійно-технічної освіти; шкільна освіта. Вони мають, як спільні ознаки так і відмінності, але враховуючи, що шкільна освіта має меншу автономію та обмежені ресурси доцільно розглядати її як найбільш ризиковий варіант надання освітніх послуг з врахуванням ризиків вищої та професійно-технічної освіти. На рисунку 1 представлена структура управління освітою в Україні з точки зору прийняття управлінських рішень.

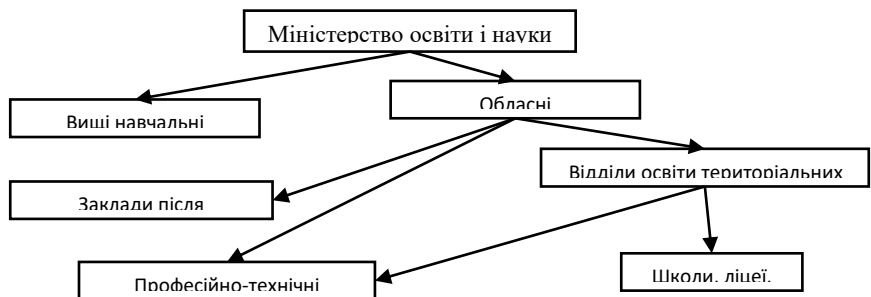


Рис. 1. Структура управління освітою в Україні

Як бачимо з структури управління прийняття рішень на рівні вищої та професійно-технічної освіти вище ніж в шкільній освіті, що зменшує час прийняття управлінських рішень та зменшує час проходження розпоряджень. З цього виходить, що на різних рівнях управління та організації освітнього процесу існує різна ступень зрілості організаційної структури або розвитку організації, наприклад заклади вищої освіти мають відпрацьовані механізми та технології забезпечення різнопланового навчання, що дозволяє зменшити частину ризиків в плані ймовірності їх появи, але не усунуло їх, як такі. Також впровадження дистанційної освіти призвело до виникнення певної групи ризиків.

Більшість документів у галузі захисту інформації датуються 1992 роком і відносяться до інформаційних технологій на базі вже застарілих апаратних засобів. Документи відображають «військову» точку зору на проблеми інформаційної безпеки, відповідно до якої основні зусилля спрямовані на забезпечення конфіденційності (захищеності від несанкціонованого доступу). Іншим аспектам - збереження цілісності і доступності - приділено набагато менше уваги. При цьому особливості сучасних автоматизованих систем цивільного застосування не враховуються. Що приводить до виникнення ще однієї групи ризиків пов'язаних саме з цивільним або комерційним використанням інформаційних ресурсів. Тому відсутність єдиного підходу до інформаційної безпеки, а саме нормативної документації, інструкцій, методів та засобів приводить до виникнення ризиків.

Основні фактори, що вплинули на формування ризиків та самі ризики наведені в таблиці 1.

Таблиця 1

Фактори та ризики в освітньому процесі в умовах надзвичайних ситуацій

Фактор	Ризик
Нормативна база	Відсутність процедур забезпечення освітнього процесу
	Відсутність сертифікованих засобів навчання
	Відсутність інструкцій порядку дій у надзвичайних ситуаціях
	Наявність єдиних управлінських рішень для всіх регіонів, без врахування особливостей стану регіону
Введення дистанційного навчання	Відсутність штатних спеціалістів із захисту інформації в закладах освіти
	Відсутність регламентуючих документів на отримання, обробку, збереження, доступ до інформації
	Відсутність ресурсів для реалізації в межах навчального закладу
	Використання сторонніх ресурсів
	Зміна власника даних з навчального закладу на фізичну особу працівника цього закладу
	Фізична відсутність працівників та здобувачів освіти
	Не готовність всіх учасників процесу

Низький рівень інформаційної компетенції працівників	Не використання ІКТ повною мірою
	Використання не надійних засобів ідентифікації та авторизації
	Залежність від кваліфікованих колег
	Використання впливу на формування суспільної думки
	Використання програмного забезпечення, що має сумнівний характер
	Розповсюдження не перевіреної інформації
Відсутність дублюючого каналу передачі даних	Не можливість отримання інформаційних послуг
	Не можливість отримання управлінських розпоряджень
	Відсутність зв'язку із здобувачами освіти
	Відсутність зв'язку з персоналом
	Перевантаження каналів зв'язку
Очікування управлінського рішення від вищого рівня управління	Несвоєчасне прийняття рішення
	Відсутність ініціативи на місцях
	Не дотримання часових рамок виконання
Обмеження в ресурсах освітнього закладу	Не достатнє покриття телекомунікаційною інфраструктурою
	Використання не авторизованих сервісів при наданні освітніх послуг
	Неможливість моніторингу та оцінки якості освітнього процесу
Обмеження в ресурсах здобувача освіти	Відсутність стабільного зв'язку
	Відсутність обладнання для отримання освітніх послуг
Військова	Відсутність електропостачання

агресія РФ	
	Пошкодження каналів зв'язку
	Порушення графіку освітнього процесу із-за повітряних тривог
	Наявність працівників та здобувачів освіти в лавах ЗСУ
	Наявність ВПО та евакуйованих закладів освіти на території області
	Не цільове використання інформаційно-телекомунікаційних ресурсів закладів освіти

Як бачимо ризики в незалежності від факторів перекликаються, тому усунення або зменшення ризиків є комплексним завданням. Для забезпечення якості навчального процесу та усунення ризиків, або зменшення ймовірності їх появи пропонується наступний перелік заходів:

- Приведення нормативної бази до викликів сьогодення;
- Введення штатної посади спеціаліста зі інформаційної безпеки на певному рівні управління;
- Збільшення автономії закладів освіти різного рівня на період надзвичайних ситуацій будь-якого характеру;
- Зменшення ієрархії прийняття рішень;
- Повернення фіксованого телефонного зв'язку у всіх закладах освіти для забезпечення передачі управлінських рішень та постійного зв'язку із закладами освіти;
- Дублювання Інтернет зв'язку в закладах освіти;
- Забезпечення повного покриття Інтернет зв'язку в закладі освіти та забезпечення незалежних місці надання телекомунікаційних послуг;
- Створення єдиного центру надання освітніх послуг в межах області в тому числі з можливістю асинхронного навчання;
- Уніфікація засобів навчання в закладах освіти;
- Проведення тренінгів, курсів, навчань з інформаційної грамотності для здобувачів освіти так і для працівників закладів освіти;
- Приведення у відповідність до чинного законодавства інформаційних ресурсів, які використовують заклади освіти;
- Покращення матеріальної бази закладів освіти для забезпечення надання освітніх послуг з врахуванням потреб дистанційного чи асинхронного навчання;
- Збільшення автономії у прийнятті рішень нижчими ланками управління структурами закладів освіти;
- Забезпечення ВПО та евакуйованих закладів освіти, за потреби, технічними засобами навчання;
- Забезпечення резервними джерелами живлення;
- Забезпечення доступності навчальних ресурсів із закордону;
- Забезпечення можливості отримання освітніх послуг не за графіком освітнього процесу.

Як бачимо частина запропонованих заходів мають потребу у фінансових, організаційних та кадрових ресурсах, що приводить нас до неможливості їх одночасного виконання і потреби в плані реалізації в часі. Створення єдиного центру надання освітніх послуг, який би забезпечував відсутність більшої частини ризиків вважається найбільш оптимальним, тому що він усуне більшість факторів ризику, а саме; введення дистанційного навчання, низький рівень інформаційної компетенції працівників, відсутність дублюючого каналу передачі даних, очікування управлінського рішення від вищого рівня управління, обмеження в ресурсах освітнього закладу. Також буде забезпечено більшість заходів для зменшення ймовірності ризиків чи їх усунення та дасть можливість для впровадження єдиної системи навчання.

Але деякі заходи містять тільки організаційний характер і майже не мають фінансових витрат. Тому пропонується спочатку впроваджувати організаційні заходи і заходи з мінімальним фінансовим навантаженням, а інші з часом та ресурсами.

УДК 658.012.4:621

СИГНАТУРНИЙ МЕТОД КОНТРОЛЮ ХОДУ ПРОГРАМ ЦИФРОВИХ АВТОМАТІВ

Віталій Тупкало¹, Сергій Черепков²

Київський університет інтелектуальної власності та права

¹tvn.prof@gmail.com

Аналіз відомих публікацій зі створення відмовостійких керуючих цифрових автоматів (ЦА) об'єктів критичної інфраструктури показує, що найбільш досліджуваними є тестові методи контролю апаратних засобів ЦА. У той же час, за оцінками експертів, складається ситуація, коли інформаційна стійкість (кіберстійкість) ЦА в значній мірі визначається показниками контролепридатності ходу керуючих програм у реальному часі їх виконання.

Метою даної роботи є підвищення кіберстійкості програмного забезпечення ЦА на основі безперервності сигнатурного контролю адресації множини команд A за всіма шляхами і циклами $K_j(A)$ за умови незмінності правила сигнатурного контролю (sig) по тактам адресації команд програми (мікропрограми) за методом передбачення контрольної сигнатури на кожному наступному такті адресації q_{i+1} відносно його попереднього такту q_i .

Основна частина. В основу розробки авторського метода сигнатурного контролю ходу програм покладено базове концептуальне твердження: основним видом помилок при виконанні програм обчислювальними системами різного призначення є алгоритмічні помилки, пов'язані з управлінням реалізації операційних дій алгоритмів. У цьому випадку найбільш прийнятною моделлю функціонального (у реальному часі) контролю ходу програм (мікропрограм) ЦА є опис їх цільових програм у вигляді кортежів команд K . Слід зауважити, що передумовою забезпечення контролепридатності програмного забезпечення в реальному масштабі часу повинні бути такі відомі принципи синтезу схем алгоритмів програм як модульне структурування і комплексування схем на основі

кінцевої множини елементарних структур (типових обчислювальних процедур). З урахуванням цих принципів контроль ходу програм (мікропрограм) при формальному їх представленні кортежами команд операцій зводиться до контролю деякого детермінованого розгалуженого процесу (кортежу K) адресації команд, кожна гілка $K_j(A) \in K$ якого характеризується своїм оперативним контролепридатним кортежем команд.

Визначення 1. Контролепридатним щодо методу передбачення сигнатур називається кортеж команд $K_j(A)$ (функція адресації), для якого контрольна характеристика (сигнатура) $\text{sig}A_{i+1}$ кожного наступного значення A_{i+1} однозначно визначається безпосередньо попереднім значенням адреси A_i .

Визначення 2. Сигнатура двійкового числа $A(x)$ є його згортка (лінійне перетворення) $\text{sig} A(x)$ за модулем незвідного примітивного полінома $P(x)$:

$$A(x) \equiv \text{sig}A(x) = A(x) \bmod P(x). \quad (1)$$

Визначення 3. Сигнатурно контролепридатна програма (мікропрограма) - це програма (мікропрограма), адресація множини команд A якої здійснюється за всіма шляхами і циклами $K_j(A)$ за умови безперервності контролю кортежу команд по тактам q адресації і незмінності правила контролю методом передбачення сигнатур:

$$\begin{aligned} \text{sig}A_{i+q} &= \text{sig}F_j(A_i); \\ F_k &= \text{sig}F_j(K_j(A)), \end{aligned} \quad (2)$$

де $K_j(A)$ – множина дозволених кортежу j адрес команд контрольованої програми; $F_j(\dots)$ – функція (закон) передбачення (упорядкування) кортежу $K_j(A)$; $\text{sig}F_j(K_j(A))$ – правило сигнатурного контролю; F_k - функція виходу контролюючого пристрою у разі контролю кортежу $K_j(A)$.

У контексті *Визначень 2 і 3* відносно вимоги щодо лінійності оператора sig слід зазначити, що цей оператор може бути лінійним у разі його векторної інтерпретації як унарної операції згортки двійкового числа A довжини n у його контрольну характеристику довжини m по модулю незвідного примітивного полінома $P(x)$ ступеню m на основі рекурентного (последовного тактового у часі), наприклад, алгоритму зсуву регістра із зворотними зв'язками. Але цей алгоритм не дає змогу реалізувати синтез паралельного комбінаційного формувача сигнатур двійкових n -розрядних чисел, що є принциповим для функціонального контролю забезпечення високої оперативності встановлення факту хакерського інциденту при роботі ЦА в реальному масштабі часу. Виходячи з цього зауваження, запропоновано метод синтезу комбінаційного формувача сигнатур паралельного типу на основі використання сигнатурної утворюючої матриці незвідного примітивного полінома $M(\text{sig}A_{[n]})$.

Визначення 4. Утворююча матриця сигнатур $M(\text{sig}A_{[n]})$ полінома $P^m(x)$ - це матриця розміру $(m \times n)$, яка є результатом перемноження по n рядкам матриці вектор-стовпця n -розрядного числа $A_{[n]}$ з n рядками матриці $M(\text{sig}A_{[n]})$ рекурсивної генерації n вектор-рядків m -розрядної сигнатури $\text{sig}\beta_{[n]}$ двійкового числа $\beta_{[n]}$ з одиницею тільки у старшому розряді.

У контексті *Визначення 4*, загальна модель запропонованого формувача сигнатур паралельного типу на основі використання сигнатурної утворюючої матриці незвідного примітивного полінома представлена наступною рівністю :

$$\text{sig}A_{[n]} = a_n \text{sig} \beta_{[n]} \oplus a_{n-1} \text{sig} \beta_{[n-1]} \oplus \dots \oplus a_1 \text{sig} \beta_{[1]}. \quad (3)$$

Висновки. Розроблений метод сигнатурного контролю ходу програм ЦА не потребує зміни існуючої технології структурного програмування та допускає використання різних базисних множин алгоритмів. Метод забезпечує контроль ходу програм безперервно на кожному такті адресації команд без необхідності витрат оперативної пам'яті інформаційних систем для зберігання еталонних сигнатур.

УДК 004.056:004.49

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ WEB РЕСУРСУ ВІД АТАК ТИПУ CROSS-SITE SCRIPTING

Анатолій Грицак¹, Ігор Абрамчук¹, В. Саврацький¹

¹Вінницький національний технічний університет

*¹grytsak.a.v@gmail.com, igrabramchuk@gmail.com,
savratsky9300@gmail.com*

Web-уразливості відіграють важливу роль у сучасних проблемах інформаційної безпеки. Більшість зовнішніх атак на корпоративні інформаційні системи спрямовані саме на вразливості web-додатків.

Порушення інформаційної безпеки можуть бути викликані різними причинами, включаючи вразливість у мережевих програмах або самій операційній системі, помилки в конфігурації або системи політики безпеки.

Метою даної роботи є підвищення ефективності виявлення вразливостей у web-додатках до атак типу Cross-Site Scripting.

За останні роки найбільш поширеним типом вразливості у web-сайтах була атака XSS (Cross-site Scripting), яка становила 19% від усіх знайдених типів вразливостей.

Розробка стратегії захисту web-додатку є нетривіальною задачею.

Предметом покращення та удосконалення є метод знаходження вразливих місць до атак типу XSS у web-додатках.

Загальний алгоритм покращеного методу полягає у тому, що сформується окремий модуль, що буде надсилати запити з «корисним навантаженням», які, у свою чергу, зможуть провокувати видання помилок баз даних у результаті сканування, яке імітує реальну XSS атаку. Інший модуль буде індексувати та виявляти у відповідях усі можливі та типові помилки для баз даних. Перевірка буде реалізована за допомогою методу SQL_check.

Завдяки фреймворку Scrapy павук знаходить URL-адреси, автоматично переслідуючи усі посилання на web-сайті. Після завантаження HTML сторінки сканер автоматично шукатиме на сторінці вразливості XSS.

Це робиться шляхом пошуку декількох загальних точок введення та введення рядка з певною послідовністю символів, а саме «9zqjxel ""() {} <x>: 9zqjxel; 9.». Важливою частиною цього рядка є «" () {} <x>;».

Дані рядки містять "небезпечний" символ. Якщо HTML виводиться без уникнення цих символів, швидше за все, є вразливість XSS.

Можливість здійснення XSS-атаки виникає, коли додаток приймає ненадійні дані і відправляє їх в браузер без належної перевірки або екранування.

XSS дозволяє зловмисникам виконувати скрипти у браузері жертви, здатні захоплювати сесії користувачів, спотворювати web-сторінки або перенаправляти користувача на шкідливі сайти.

Автоматизовані інструменти можуть знайти деякі уразливості XSS автоматично.

Однак кожен додаток будує сторінки по-різному і використовує різні інтерпретатори на стороні браузера.

Для знаходження вразливостей для кожного посилання потрібно модифікувати запит та перевірити чи присутній запит у чистому виді або в структурі додатку. Для кожного посилання буде додаватись корисне навантаження, тобто payload. Він, у свою чергу, генеруватиметься наступним чином: `payload = delim_str + self.test_str + delim_str + ';9'`, де `delim_str` – це рандомна послідовність символів, а `self.test_str = "\"(){}<x>:/\"` – загальні точки введення та введення з певною послідовністю символів. Отже, якщо HTML виводиться без уникнення цих символів, то, швидше за все, є вразливість XSS. Можливість здійснення XSS-атаки виникає, коли додаток приймає ненадійні дані і відправляє їх в браузер без належної перевірки або екранування.

Існує залежність між небезпечними символами XSS та небезпечними символами введення SQL ін'єкції, а саме одинарними та подвійними лапками.

Завдяки виявленню помилок SQL у відповіді вірогідність знаходження вразливостей значно збільшується.

Тому при генерації “корисних даних”, тобто payload буде надсилатись додатковий запит із значенням у “тілі” “d'z”0”, що має викликати SQL помилку у відповідь. Також варто додати параметр, за яким можна буде визначити кількість одночасних з'єднань із сайтом за одиницю часу. Оскільки часто брандмауери та системи IDS можуть визначити сканування як атаку, та блокувати усі запити з IP-адресою, які надсилаються від сканера.

Зменшуючи значення, а саме `-c / -connections`, ймовірність забезпечення стабільної роботи сканера буде збільшена.

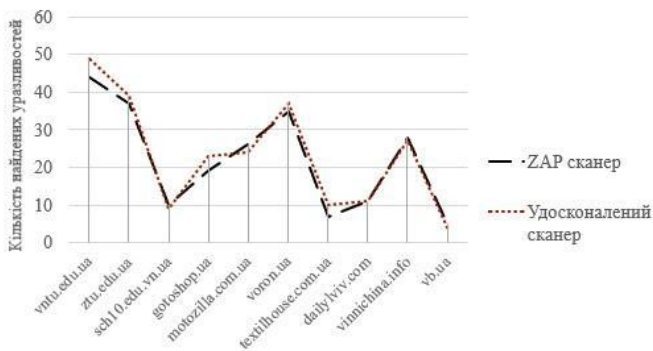


Рис. 1. Порівняльний графік кількості знайдених вразливостей у web-додатках

Таким чином, порівнявши кількість знайдених випадків вразливих місць коду (рис. 1). видно, що сканер, розроблений на основі удосконаленого методу, показав кращий результат, ніж аналог ZAP.

Отримані результати сканувань можна легко використати для покращення роботи просканованих web – сайтів, оскільки вони уже містять опис причин вразливостей та шляхи боротьби з ними. Усунення знайдених вразливостей неодмінно підвищить рівень безпеки перевірених сайтів.

УДК 004.56.5(043.2)

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ SIEM

Богдан Карачун

*Державний університет телекомунікацій
info@dut.edu.ua*

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

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

Розглянемо декілька визначень понять події та інциденту ІБ:

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

2. Подія інформаційної безпеки – це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки. Інцидент інформаційної безпеки відповідно – це одинична

подія або ряд небажаних та непередбачених подій інформаційної безпеки, із-за яких велика ймовірність розкриття конфіденційної бізнес-інформації.

Розглянемо SIEM (Security Information and Event Management) для попередження та фіксування інцидентів:

SIEM-система може виявити можливу загрозу безпеки навіть якщо ця загроза добре замаскована під звичайну подію. Зробити це дозволяє те, що система аналізує не кожен окрему подію, а всі події в комплексі та та-ким чином може «побачити» повну картину подій зі сторони. Ця властивість може бути дуже корисною коли мова йде про систему аналізу загроз конфіденційній інформації користувачів відкритих соціальних мереж.

Така система призначена для аналізу інформації, що надходить від різних інших систем, таких як DLP, IDS, антивірусів і подальшого вияв-лення відхилення від норм за якимись критеріями. Як тільки виявлено від-хилення – генерується інцидент. В основі роботи SIEM лежить, як не див-но, майже гола математика і статистика. Будь-яких захисних функцій «го-ла» SIEM в собі не несе.

SIEM потрібна саме для збору та аналізу інформації. Інформація на-дходить з різних джерел – таких, як DLP-системи, IDS, маршрутизатори, міжмережні скрани, АРМ користувачів, серверів...

Досить клопітно вручну переглядати логи з великої кількості джерел. До того ж бувають ситуації, коли зовні нешкідливі події, отримані з різних джерел, у сукупності несуть у собі загрозу. Припустимо, коли відбувається посилання листа з чутливими для компанії даними людиною, що має на це право, але на адресу, що знаходиться поза його звичайного кола адрес, на які він відправляє. DLP система цього може не відловити, але SIEM, вико-ристовуючи накопичену статистику, на підставі цього вже згенує інци-дент. Аналогічно, якщо один з працівників ІТ відділу відкритої соціа-льної мережі почав проводити листування та повідомляти третім особам, що не мають допуску до інформації, відомості про користувачів, структу-ру соціальної мережі чи програмне та технічне забезпечення, що викорис-товується для забезпечення роботи мережі, то це відразу буде помічено си-стемою SIEM та адміністратори отримають відповідне сповіщення.

Система SIEM може виконувати такі основні функції:

- аналізувати події та створювати оповіщення при якихось ано-маліях: мережного трафіку, несподіваних дій користувача, невідомих пристроях і т. д.;
- перевірити на відповідність стандартам безпеки;
- створити красивий звіт. У тому числі налаштований безпосере-дньо для ваших потреб. Наприклад, щоденний звіт про інциденти, щотиж-невий звіт TOP-10 порушників, звіт з працездатності пристроїв і т. д.;
- відстежувати події, що спровоковані пристроя-ми / серверами / критично важливими системами, створювати відповідні оповіщення для зацікавлених осіб;
- зібрати доказову базу з приводу інцидентів;
- надати звіт про події в мережі без надання доступу до самої мережі, тобто адміністратор з відділу захисту інформації може відстежува-ти поведінку користувачів при тому, що не матиме ніякої можливості ознайомитися з конфіденційною інформацією власника аккаунту.

Загалом може скластися таке хибне враження, що SIEM-система є панацеєю для запобігання будь-яких загроз, але це не так. Ця система мо-же відстежувати всі

події в мережі, проте не може виконувати якихось дій крім створення попередження для адміністраторів цієї мережі, а адміністратор вже спираючись на отриманий звіт приймає рішення про подальші дії. Та все ж такі ця система може відстежувати поведінку користувачів та спираючись на статистику подій вирішити, чи потрібно адміністратору звернути більше уваги тому чи іншому користувачу. Причиною тому може бути як нетипова для користувача поведінка, так і певні маркери в повідомленнях, що можуть вказувати на можливу діяльність користувача, що пов'язана з тероризмом, розповсюдженням наркотичних речовин тощо.

До того ж система SIEM лише аналізує отримані дані і працює тим краще, чим більше до неї надходить інформації з різних джерел (IDS/IPS, DLP, маршрутизатори, сервери тощо) в вигляді логів.

Література

1. Кримінальний Кодекс України, ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах(комп'ютерах), автоматизованих системах, комп'ютерних мережах, або зберігається на носіях такої інформації, вчиненні особою, яка має право доступу до неї».
2. <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/Slyusar> V.I. Blockchain technology in future multi-domain operations.
3. Методи виявлення інцидентів/Ukrainian Information Security journal. <http://jrn1.nau.edu.ua/index.php/ZI/article/view/8798>.
4. Кассето О. What is UBA, UEBA, & SIEM? Security Management Terms Defined [Електронний ресурс] / Опіон Кассето. <https://www.exabeam.com/siem/uba-ueba-siem-security-management-terms-defined-exabeam/>.
5. Incident Response Automation and Security Orchestration with SOAR. <https://www.exabeam.com/siem-guide/incident-response-and-automation/>.

УДК 004.056.53

ВИЯВЛЕННЯ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ЗА РАХУНОК ПОСДНАННЯ МЕТОДІВ ЛОКАЛІЗАЦІЇ ЗА РІВНЕМ ПОЛЯ ТА АКУСТИЧНОГО ЗВ'ЯЗУВАННЯ

Павло Павловський, Дмитро Присяжний, Віталій Гудзь

Вінницький національний технічний університет

prepod@vntu.net, dimpris@gmail.com

Проаналізовано існуючі методи захисту інформації від витоку акустичним каналом, а також методи та засоби захисту від закладних пристроїв. Доведено доцільність посднання методів локалізації за рівнем поля та акустичного зв'язування з метою мінімізації часових витрат на виявлення радіозакладних пристроїв. Обґрунтовано необхідність розроблення пристрою, який буде виконувати функції кількох пристроїв водночас, що визначає не лише його функціональну, але й економічну доцільність.

Найпоширеніший метод витоку інформації – через технічні канали витоку інформації (ТКВІ). Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки. Тобто, технічним каналом витоку інформації є фізичний шлях носія інформації від його джерела до противника. Одним із найбільш поширених ТКВІ є акустичний. Акустичний канал витоку інформації вважають найпоширенішим, тому що у будь-якій ситуації, чи то під час проведення нарад, переговорів, чи то інших подій, люди природнім способом, а саме вголос, висловлюють свої думки, ідеї чи просто важливу інформацію. Разом із цим, завжди існувало поняття конкурент чи опонент, тобто ті особи, яким знання цієї інформації може принести користь. Одним із способів підслуховування розмов – є встановлення у приміщенні, де буде відбуватись розмова, закладних пристроїв (ЗП). Такий тип ТКВІ є найбільш «простим», саме тому він дуже часто використовується. Тому актуальним є розроблення пристрою, який буде здійснювати захист від витоку інформації таким каналом.

Один із таких засобів є пристрій, що здійснює пошук радіозакладних пристроїв. Принцип його роботи базується на пошуку радіовипромінювань та реагуванню на них. Пропонується покращити можливості виявлення радіозакладних пристроїв шляхом поєднання трьох пристроїв у один, що, у свою чергу, дозволяє не лише більш точно локалізувати несанкціонований пристрій, але й отримати певну інформацію про нього. Для досягнення цієї мети пропонується поєднати в один пристрій індикатор поля, частотомір та демодулятор. Частотомір – це електровимірвальний прилад, що призначений для вимірювання частот різних періодичних коливань, електричних або механічних. Такі пристрої поділяються на вібраційні, електромеханічні, резонансні та цифрові. Принцип дії цифрових частотомірів полягає в підрахунку кількості періодів вимірюваних коливань за певний проміжок часу. Цифровий частотомір складається з формуючого пристрою, що перетворює синусоїдальну напругу вимірюваної частоти у послідовність однополярних імпульсів; тимчасового селектора імпульсів, що відкривається на певний проміжок часу; електронного лічильника, який відраховує кількість імпульсів на виході селектора; та цифрового індикатора. Демодуляція сигналу – процес, виділення інформаційного сигналу з модульованого коливання високої частоти. Демодулятор – пристрій, що здійснює розподіл сигналу на інформаційний та несучий (які утворюються у процесі модуляції сигналів). Це дає змогу відкинути несучий сигнал і працювати лише з інформаційним, тобто процес демодуляції сигналу, який передає закладний пристрій, дозволить отримати детальну інформацію про закладний пристрій, та яку інформацію він передає. Пропонується комбінувати ці всі пристрої у одне технічне рішення. Таке поєднання дозволяє мінімізувати час, оскільки для пошуку закладних пристроїв потрібно буде використовувати лише один пристрій, який виконуватиме функції трьох пристроїв.

Запропонований пристрій дозволяє здійснити пошук закладних пристроїв, частотомір відобразити користувачеві частоту, на якій працює даний «шпигунський» пристрій, а демодулятор зчитати та відфільтрувати інформацію, що випромінює закладний пристрій.

Такий підхід уможливує не лише отримання синергічного ефекту від застосування такого комплексного пристрою, а також знизити його собівартість порівняно з ринковою вартістю трьох окремих його складових-пристроїв. Базою для запропонованого пристрою пропонується мікроконтролер Arduino UNO, оскільки дана платформа є найбільш гнучкою, зручною у використанні та має невелику вартість.

Пошук здійснюється шляхом планомірного обходу приміщення з рухом уздовж стін і обстеженням меблів та інших розташованих у ньому предметів. При обході антену необхідно орієнтувати у різні площини, роблячи плавні, повільні повороти основного блоку для пошуку максимального рівня сигналу. Антену приладу доцільно тримати на відстані не більше 20-25 см від обстежуваних поверхонь та предметів. При відсутності обмежень на використання методу акустичного зв'язування динамік вбудованого гучномовця приладу слід орієнтувати у бік обстежуваних поверхонь і предметів.

УДК 544.171.44:004

ВИГОТОВЛЕННЯ ТА ВЛАСТИВОСТІ НАНОШАРІВ АЗОТИСТИХ ОСНОВ НУКЛЕЇНОВИХ КИСЛОТ ДЛЯ МОЛЕКУЛЯРНОЇ КРИПТОГРАФІЇ

Наталія Попович¹, Наталія Цуд², Катеріна Велтруска²,
Владімір Матолін², Василь Різак¹

*¹Ужгородський національний університет
nataliyai.porovych@uzhnu.edu.ua,*

*²Карлов університет в Празі (Чеська Республіка)
veltrusk@mbox.troja.mff.cuni.cz*

Криптографія - одна з найстаріших наук, які займаються вивченням методів захисту даних від несанкціонованих доступу та дій, які можуть призвести до порушення їх цілісності і доступності. Одним із перспективних напрямів сучасної криптографії є ДНК-криптографія. Зазвичай під ДНК-криптографією розуміють або безпосереднє використання ланцюжків ДНК для запису, зберігання та передачі інформації (для чого необхідно високотехнологічне обладнання), або використання в процесі шифрування алфавіту ДНК-нуклеотидів (аденіну, тиміну, цитозину та гуаніну). Актуальність криптосистем, які в тому чи іншому вигляді включають в себе ланцюжки ДНК, також пов'язана з активними дослідженнями в області запам'ятовуючих пристроїв, які використовують ДНК. Подібні пристрої зможуть зберігати обсяг інформації на кілька порядків більший (при компактніших

розмірах), ніж дозволяють сучасні технології. Крім того, термін служби подібних пристроїв зберігання інформації помітно вищий.

Однак, у ДНК-шифрів є певні недоліки в порівнянні з іншими методами захисту даних. Практична реалізація таких шифрів потребує більше обчислювальних ресурсів та затрат часу, ніж для традиційних. Також фізична реалізація шифрів передбачає наявність високотехнологічного біомолекулярного обладнання. Окрім цього, немає єдиної теорії ДНК-криптографії, а практичні реалізації процесів шифрування-дешифрування є поодинокими.

Метою даної роботи є розробка механізму взаємодії ДНК-нуклеотидів з модельними поверхнями та трансформації відповідного інтерфейсу нагріванням для пошуку нових підходів до практичної реалізації криптографічного захисту з використанням ДНК шифрів.

Для досягнення поставленої мети розроблено технологію одержання наночарів аденіну А, тиміну Т та гуаніну G на модельних поверхнях полікристалічного та монокристалічного (110) окису титану методом термічного випаровування у надвисокому вакуумі. Поверхневий шар полікристалічного TiO_x був отриманий нами на поверхні попередньо очищеної титанової фольги відпалом при температурі 650 К в атмосфері кисню при тиску 1×10^{-7} торт протягом 120 хв. Модельна поверхня монокристалу TiO_2 перед осадженням біомолекул ретельно очищалися від домішок, адсорбованих з повітря, кількома циклами бомбардування іонами аргону та наступним відпалом при $T=850$ К. Товщина осаджуваного шару молекул визначалася температурою їх випаровування та тривалістю процесу напilenня.

Механізм взаємодії нуклеотидів А, Т та G з поверхнями досліджувався методом рентгенівської фотоелектронної спектроскопії (РФС) з використанням Al K α рентгенівської трубки. Для ідентифікації зв'язків, які утворюються при взаємодії осаджених молекул з поверхнями, вимірювалися спектри основних рівнів кисню O1s, вуглецю C1s, азоту N1s, що утворюють відповідні хімічні сполуки аденіну, тиміну та гуаніну, й основного рівня Ti 2p $_{3/2}$ титану модельної поверхні.

Аналіз вимірних РФС спектрів основного рівня нітрогену N1s аденіну показує присутність азоту з ненасиченими хімічними зв'язками -N= і NH+NH $_2$. Спектри основного рівня C1s шару аденіну містять дві компоненти, які можна віднести до вуглецю в групах CC/CH і до зв'язків CN-вуглець аденінових кілець. Після нагрівання у вакуумі товщина шару аденіну зменшується; після відпалу при $T=250^\circ\text{C}$ на поверхні полікристалічного окису титану залишаються лише поодинокі молекули нуклеотиду. Зображення поверхні TiO_x після відпалу при температурі 250°C були одержані за допомогою атомно-силового мікроскопа.

РФС спектри наночару тиміну на модельних поверхнях окису титану показали, що пік основного рівня нітрогену N 1s зміщується в бік нижчих енергій на $\Delta E_{\text{зв}} = -(0.3 + 0.7)$ eV відповідно після відпалу при $T > 100^\circ\text{C}$. Такі енергетичні зсуви в органічних багатошарових покриттях пояснюються утворенням хімічних зв'язків між молекулами та підкладкою (хемосорбцією). Пік основного рівня C 1s плівки тиміну містить чотири компоненти, які відповідають карбону з вуглеводними зв'язками C-C, C-H; карбону, зв'язаному з азотом C-N, N-C-N; амідному карбону N-C=O; уреа карбону N-C(=O)-N з енергіями зв'язку 285, 285, 7;

286,5 та 289,2 eВ відповідно. Для плівки тими́ну пік основного рівня С 1s поступово зміщується в бік нижчих значень енергії зв'язку на 0.7-0.4 eВ після відпалу при $T > 100-120^{\circ}\text{C}$. При цьому товщина шару тими́ну в результаті відпалу при температурах до 200°C не змінювалася.

Наношар гуаніну на поверхні монокристалічного (110) TiO_2 виявився стійким до відпалу при температурах до 450°C .

Висновок: результати дослідження фотоелектронних спектрів наношарів азотистих основ ДНК на модельних поверхнях показали широкий спектр особливостей геометричної та електронної структури досліджуваних матеріалів, які можуть бути використані при розробці методів ДНК-криптографії та визначити галузі їх використання. Для розробки теоретичних основ застосування ДНК та її основ у молекулярній криптографії, а також чіткого механізму взаємодій та перетворень, які цих об'єктів під впливом сторонніх факторів предметом наших подальших досліджень є характеристики цитозину на модельних поверхнях, а також поведінка шарів окремих нуклеотидів при тиску повітря, близькому до атмосферного, тобто в умовах, максимально наближених до умов функціонування майбутніх пристроїв на основі ДНК.

УДК 004.421.5.052

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ WEB-РЕСУРСІВ СТІЙКИМИ КРИПТОАЛГОРИТМАМИ НА ОСНОВІ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

Ольга Салієва¹, Василь Карпінєць¹, Ірина Бондаренко¹

*¹Вінницький національний технічний університет
salieva8257@gmail.com, karpinets@gmail.com,
fm.ub15b.bondarenko@gmail.com*

Широке впровадження Web-технологій в усі сфери людської діяльності обумовлює вагомість вирішення питань щодо їхньої безпеки. Адже на сьогодні безліч Web-застосунків мають загальновідомі вразливості, за допомогою яких можна успішно проводити атаки на Web-ресурси.

З метою підвищення захищеності Web-інфраструктури використовують різні методи і засоби, зокрема стійкі криптографічні алгоритми на основі генераторів випадкових чисел (ГВЧ), які поділяються на: апаратні, програмні та табличні. Останні мають багато переваг, зокрема видають істинно випадкову послідовність, не потребуючи фізичної наявності модуля генерації у системі. Проте для зберігання таблиць потрібний великий обсяг пам'яті ЕОМ. Для вирішення даної проблеми у роботі пропонується використати ентропію поведінки користувача в якості Seed даних табличного ГВЧ, оскільки таке джерело ентропії є швидкодіючим та фактично нескінченим.

Метою даної роботи є підвищення захищеності Web-ресурсів за рахунок стійких криптографічних алгоритмів на основі ГВЧ, що враховують ентропію поведінки користувача у багатокористувацькому середовищі.

Для досягнення мети досліджено алгоритм надійного джерела ентропії на основі поведінки користувача Web-ресурсу та об'єднано окремі модулі ГВЧ, а саме алгоритм заповнення буфера табличного ГВЧ та алгоритм вибору з нього випадкового числа.

Розроблений алгоритм умовно розподілено на два етапи.

Етап 1. Заповнення буфера табличного ГВЧ.

Крок 1. В якості показників ентропії обираються координати курсора користувача X та Y .

Крок 2. Обчислюється $Z_n = X_n \oplus Y_n$, яке є результатом ентропії поведінки користувача.

Крок 3. Перевіряється рівність Z_n та Z_{n-1} .

Крок 4. Надсилається Z_n з клієнтської частини на сервер.

Крок 5. На стороні сервера розраховується $Q = Z_{An} \oplus Z_{Bn}$, де Z_{An} – значення ентропії користувача A , а Z_{Bn} – значення ентропії користувача B .

Крок 6. У комірку таблиці з індексом i записується Q .

Крок 7. Інкрементується та записується i .

Крок 8. Здійснюється перевірка: якщо i більше розміру таблиці, то йому присвоюється значення 0.

Етап 2. Вибір випадкового числа.

Крок 1. У модуль передається бажана довжина послідовності n .

Крок 2. З комірки таблиці з індексом i вибирається число X_i .

Крок 3. Інкрементується та записується i .

Крок 4. Перевіряється чи довжина числа X_i задовольняє бажаному n .

Крок 5. Якщо довжина X_i менша n , то вибирається наступне число X_{i+1} (повторюються кроки 2, 3) та конкатинуються до $X_i X_{i+1}$.

Числа вибираються та конкатинуються до тих пір, доки довжина числа X_i не задовольняє бажаному n .

На основі запропонованого алгоритму роботи ГВЧ було розроблено пакет програм криптографічної підсистеми захисту інформації, зокрема, здійснено програмну реалізацію серверної частини алгоритму табличного ГВЧ для платформи ASP.NET Core та клієнтської для Angular2.

Крім того, було здійснено статистичне тестування згенерованої послідовності за допомогою пакету NIST.

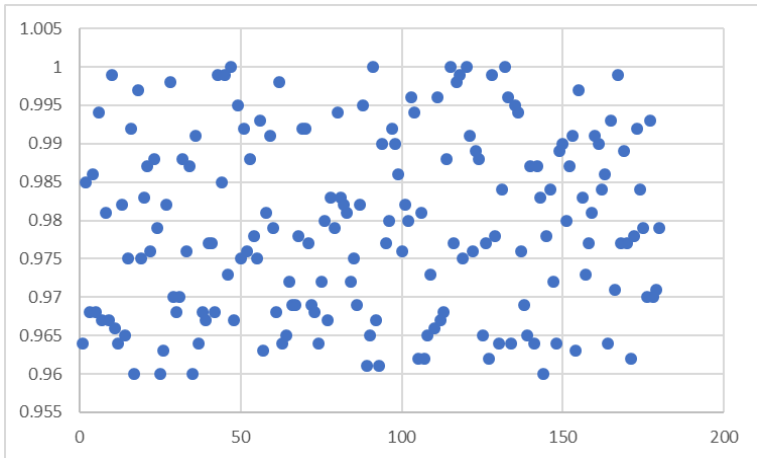


Рис. 1. Результати тестування послідовності згенерованої розробленим ГВЧ

На рис. 1 представлена діаграма, що характеризує попадання частки послідовностей, що пройшли кожен тест у довірчий інтервал $[0,96; 1]$.

Отриманий результат підтвердив, що дана послідовність задовольняє відповідним критеріям випадковості.

Таким чином, за рахунок використання розробленого табличного ГВЧ, який враховує ентропію поведінки користувача, можна підвищити стійкість криптографічних алгоритмів, що, у свою чергу, сприятиме підвищенню захищеності Web-ресурсів.

УДК 004.056.52

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕТОДІВ РОЗМЕЖУВАННЯ ДОСТУПУ В ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

Анатолій Шиян¹, Михайло Тюльпін¹, Яна Яремчук¹

¹*Вінницький національний технічний університет,*

¹*anatoliy.a.shiyan@gmail.com, mtyulpin@gmail.com,*

yanunova@hotmail.com

Інформаційне протиборство в глобальній мережі Інтернет зростає з кожним роком. З одного боку, економічне зростання йде за рахунок впровадження інновацій. З іншого боку, цінність конфіденційної інформації весь час зростає, що залучає до вимог отримати до неї несанкціонований доступ все більшу кількість зловмисників. Існує також і такий ускладнюючий фактор, що практично будь-яка інновація є результатом досить великого колективу. При цьому кожна людина із складу колективу є носієм певної частини конфіденційної інформації. До того ж,

доступ до конфіденційної інформації локалізований на членів колективу первинно.

Таким чином, з точки зору доступу до конфіденційної інформації, в загальному випадку колектив є ієрархічною структурою. На вищих ієрархічних рівнях цієї структури знаходяться люди, які володіють більшим об'ємом інформації. У результаті цього захист інформації від несанкціонованого доступу вимагає використання спеціальних методів розмежування доступу.

Метою даної роботи є аналіз перспектив використання методів розмежування доступу в інформаційному протистоянні.

Методи розмежування доступу базуються на моделях керування доступом (Model Access Control). Вони описують в абстрактній формі способи розмежування доступу з фіксованим набором повноважень, враховують можливість видачі офіційних дозволів (допуску) суб'єктам до інформації різного рівня конфіденційності. Такі моделі поєднують захист з обмеженням прав на знайомство з певною інформацією та призначені для формування умов для протидії небажаному використанню інформації.

Моделі керування доступом мають такі обмеження:

- необхідність класифікації суб'єктів та об'єктів за рівнями безпеки, а це не завжди можливо у деяких системах;
- крім конфігурації розмежування доступом, також потрібна узгоджена політика безпеки, в якій має бути описано які об'єкти є захищеними об'єктами та які суб'єкти мають права доступу;
- користувачі системи не можуть одноосібно визначати доступ суб'єктів до об'єктів;
- серед параметрів керування доступом до об'єкту доступні лише категорії можливостей і мітки можливостей, котрі з ними пов'язані;
- доступом суб'єктів до об'єктів керують лише користувачі з правами адміністраторів;
- оскільки моделі керування доступом використовуються в поєднанні з іншими моделями контролю доступу, то часто важко з'ясувати, на якому «рівні» системи заборонено доступ, що вимагає більш тонкого налаштування усіх рівнів захисту.

Прикладом останнього обмеження є моделі дискреційного контролю доступу (Discretionary Access Control), які контролюють доступ до даного фрагменту інформації на основі політики, встановленої групою власників та/або уповноваженими членами колективу.

Перехід від абстрактних моделей до методів їх застосування завжди є одним із найважливіших етапів реалізації заходів інформаційного протистояння. На цьому етапі здійснюється імплементація теоретичної схеми, пристосовуючи її до умов реальної ситуації. Це можна здійснити, розробивши такі методи, які враховують специфічні особливості функціонування інформаційної системи того об'єкту, який потрібно захищати. Методи розмежування доступом орієнтовані перш за все на те, щоб захистити потрібну інформацію та інформаційні ресурси «зсередини» від власних співробітників.

Методи розмежування доступу, які впроваджені в організації, повинні враховувати не тільки існуючі на даний момент структури інформаційних процесів

та інформацію, яка локалізована на певних співробітниках. Ці методи повинні бути орієнтовані на ті зміни, які виникають як при діяльності організації, так і виникають внаслідок зовнішніх причин.

До перших можна віднести те, що інформація може «дрейфувати» з часом, зменшуючи вимоги до свого рівня допуску. Наприклад, спочатку організація розробляє певний план дій. На початку, на рівні ідеї, цей план має найвищий рівень допуску. А коло людей, які мають доступ до відповідних документів, є вкрай обмежене. З часом ідея обростає документами, які розробляє досить велика кількість працівників. Ці документи вже будуть мати, як правило, менший рівень допуску. Нарешті, на етапі соціалізації ідеї, з результату розробки організації та її супровідних документів не тільки знімаються всі можливі рівні допуску, а й навіть створюються умови для максимально широкого розповсюдження інформації.

Зовнішні причини, які потрібно враховувати при імplementації моделей розмежування доступу та, розробляючи відповідні методи, методики та технології, мають високий рівень різноманітності та широке коли причин.

Наприклад, сторонні особи можуть впливати на співробітників організації різними способами. Найвідомішими прикладами є підкуп чи шантаж співробітників. Також сюди необхідно віднести і корупцію, яку часто намагаються відносити до внутрішніх причин, забуваючи, що при корупції співробітник організації може отримати зиск чи вигоду тільки і тільки за межами своєї організації. Тому зовнішні причини можуть просто полягати в тому, що сторонні особи будуть створювати умови для отримання зиску та/чи вигоди від порушення існуючого в організації розмежування прав доступу. Такий вплив, на відміну від підкупу чи шантажу, є передовсім виключно інформаційним, бо тут потрібно просто донести до співробітника організації ту інформацію, користуючись якою він може отримати певну вигоду.

Враховання перерахованих та інших умов і причин вимагає побудови спеціалізованих інформаційних технологій, які дозволять інформувати відповідні структури організації про порушення правил розмежування доступу. Такі інформаційні технології повинні стати невід'ємною складовою інформаційних потоків організації.

УДК 004.4.233 (043.2)

ІНСТРУМЕНТИ ДЛЯ ЗНЕВАДЖЕННЯ КЛІЄНТ-СЕРВЕРНИХ ЗАСТОСУНКІВ

Василь Буковецький¹, Юрій Тягур², Тетяна Матьовка³

Ужгородський національний університет

¹bukovetsky@outlook.com ²yurii.tjahur@uzhnu.edu.ua

³rtanyusha17@gmail.com

Розвиток технологій доступу до мережі інтернет дозволив створювати веб-застосунки, які по складності не поступаються повноцінним класичним програмним пакетам. Розробка застосунків, які виконують постійний обмін даними

із сервером є нелегкою задачею, адже потребує використання додаткових інструментів для аналізу інформації, яку отримує та відправляє застосунок.

Метою даної роботи є аналіз наявних рішень для зневадження клієнт-серверних застосунків.

Найпопулярнішим варіантом для зневадження є веб-проксі — це програмні інструменти, який дозволяють перехоплювати та аналізувати HTTP(S) трафік між застосунком та веб-сервером. Вони дозволяють знаходити та усувати помилки у веб-застосунках, перевіряти заголовки, куки, кешування, шифрування та інші аспекти веб-комунікації.

Fiddler — проксі для MacOS, Windows та Linux. Він дозволяє ефективно ділитися своїми висновками та додавати контекст з вбудованою командною співпрацею. Він також дозволяє налаштовувати, зберігати та ділитися правилами для обробки складних запитів. Відрізняється високою ціною, від 10 доларів в місяць за одного користувача.

Charles — дозволяє перегляд всього HTTP та SSL/HTTPS трафіку між своїм комп'ютером та Інтернетом. Він включає запити, відповіді та заголовки HTTP (які містять куки та інформацію про кешування). Дозволяє перехоплювати та змінювати запити, емулювати повільну мережу. Програмне забезпечення є платним, та коштує 50 доларів за одну ліцензію.

Proxman — простий застосунок, який дозволяє швидко перехоплювати обмін даними застосунків. Має простий інтерфейс та має можливість перехоплювати також HTTPS з'єднання. Підтримує як Windows так і MacOS. Також доступні варіанти для мобільних операційних систем Android та iOS. Продається за ціною 69 доларів.

WireShark — безкоштовне програмне забезпечення для аналізу різних видів мережевого трафіку. Має дуже широкі можливості для аналізу пакетів різних протоколів. Може перехоплювати та аналізувати навіть низькорівневі повідомлення мережі. Через свою широку направленість не є зручною для зневадження HTTP-обміну.

Застосунки для зневадження є корисними інструментами для розробників, які допомагають ефективно виявляти та усувати помилки у програмному кодї. Однак, вибір такого застосунку може бути складним, оскільки багато з них мають високу вартість або недостатню функціональність. Тому розробникам слід уважно порівнювати різні варіанти застосунків для зневадження та обирати той, який найкраще відповідає їх потребам та бюджету.

УДК 004.946.5:005.334

**ВИНИКНЕННЯ ЗАГРОЗ У КІБЕРПРОСТОРИ ЯК РЕЗУЛЬТАТ
ТЕХНОЛОГІЧНОГО РОЗВИТКУ СУСПІЛЬСТВА****Марина Саснко***Полтавський державний медичний університет**saenkomarina89@ukr.net*

Кібербезпека – це важливий пріоритет системи української національної безпеки, яка може бути забезпечена завдяки посиленню можливостей системи кібербезпеки у процесі її протидії кіберзагрозам, що можуть бути характерними для сучасного безпекового середовища. У процесі формування сучасної української Стратегії кібербезпеки враховуються світові тренди, які присутні у глобальному кіберсередовищі як фактори, які мають вплив на процес розбудови державної системи кібербезпеки XXI століття. При цьому суспільство зустрічає низку ризиків, які є пов'язаними із застосуванням сучасних технологій, зокрема у кіберпросторі. Стратегією кібербезпеки в Україні визначено головні пріоритети, цілі та завдання по забезпеченню кібербезпеки для того, щоб створити умови для такого функціонування кіберпростору, який би був безпечним як для конкретної особи, так і для суспільства та держави в цілому.

Метою даної роботи є дослідження виникнення загроз у кіберпросторі як результату технологічного розвитку суспільства.

Загальна кількість кіберзагроз, які можливі у спектрі загроз національній безпеці країн, поступово збільшується. Дана тенденція і надалі буде посилюватися через те, що інформаційні технології бурхливо розвиваються, відбувається конвергенція з технологіями штучного інтелекту (ШІ). У результаті того, що такий вплив на діяльність національних та транснаціональних структур управління збільшується, формується абсолютно нова безпекова ситуація, пов'язана із викликами нового технологічного рівня. Протягом останнього часу можна спостерігати, що у кіберпросторі відбувається розподіл сфер впливу. Завдяки такому поділу реалізується прагнення людства реалізувати геополітичні інтереси, які постійно зростають.

Вважається, що кіберпростір у поєднанні з іншими фізичними просторами є одним із можливих сценаріїв, за яким відбуватиметься розгортання військових дій. Через це здатність держави захищати національні інтереси є надзвичайно важливою складовою кібербезпеки. Актуальним питанням за сучасних умов є створення нового війська – кібервійськ. Основне їхнє завдання полягає у тому, щоб забезпечити захист критичної інформаційної інфраструктури від можливих кібератак. Проте, крім цього, вони також відповідають за здійснення превентивних наступальних операцій у кіберпросторі, які направлені на те, щоб знищити

обчислювальні мережі та інформаційні системи збройних сил противника. Їхнім завданням є також порушення нормальної роботи об'єктів противника, які є критично важливими. Це можливо досягнути, зруйнувавши інформаційні системи, які забезпечують управління таких об'єктів.

На думку експертів, поступово у кіберпросторі інтенсивність протистояння і розвідувально-підривної діяльності буде лише зростати. Ці явища будуть проявлятися, перш за все, у тому, що буде розширюватися кількість країн, які докладатимуть зусиль для того, щоб організувати діяльність своєї кіберрозвідки, опанувати сучасні технології розвідувально-підривної діяльності у кіберпросторі, сприяти збільшенню державного контролю за національними сегментами всесвітньої мережі. За таких умов більш поширеним буде розробка такого інструментарію, який буде здатним передбачати нагромадження значних інформаційних масивів, які відображатимуть особливості людської поведінки та різних груп у соціумі. При цьому буде використовуватися досвід у сфері ШІ.

На даний момент присутнім є такий розвиток технологій, який пов'язаний із надзвичайно швидким поширенням цифрових технологій, поступово розширюється Інтернет-середовище. Проте цей процес володіє негативною ознакою, яка полягає у тому, що технічний рівень інструментарію реалізації кіберзагроз критично збільшується. У результаті цього такі загрози все більше поширюються на різні сфери життєдіяльності. Кібератаки та їхні різновиди стають все більш інтелектуальними та небезпечними, при цьому вони створюють реальну загрозу для критично важливої інфраструктури. Увага зловмисників зосереджується на тому, щоб знайти вразливі місця активів (систем управління). Для цього розробляються багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети. Враховуючи темпи розвитку технологій ШІ, у найближчі роки розміри та наслідки таких втручань будуть лише збільшуватися.

Все більш глобальним стає використання кіберпростору терористичними організаціями, тобто будемо говорити про кібертероризм. На це впливає цифрова трансформація систем управління та життєзабезпечення, яка постійно розширює цільову аудиторію кібертероризму та спектр потенційних об'єктів кібератак. До пріоритетних об'єктів терористичних кібератак відносять об'єкти атомної енергетики, системи, які відповідають за управління електропостачання, авіа- та залізничного транспорту, системи постачання водою, хімічні та біологічні об'єкти.

У результаті поширення ймовірних загроз та ускладнення інструментарію їх реалізації уряди провідних країн світу змушені були удосконалювати архітектуру національних систем кібербезпеки, змінювати стратегію і тактику протидії кіберзагрозам. При цьому вдосконалюються моделі протидії кіберзагрозам. Ці зміни пов'язані з тим, що має місце розуміння того, що ті можливості, які є на сьогоднішній день, є недостатніми для того, щоб побудувати такі системи захисту, які були б абсолютно невразливими. Як показує досвід, кібератаки можуть бути

здійснені на будь-які інформаційно-комунікаційні системи незалежно від того, який рівень захисту у них присутній. З огляду на це більш значимим стає те, щоб найбільш швидко виявити кібератаки, зреагувати на них та поширити інформацію про такі випадки, щоб мати можливість мінімізувати їх можливу шкоду.

Отже, світ цифрових технологій, який швидкими темпами змінюється, вимагає того, щоб була сформована збалансована та ефективна національна система кібербезпеки, яка була б здатною до гнучкої адаптації до тих змін, які мають місце у безпековому середовищі. Таким чином, вона б гарантувала громадянам країни те, що національний сегмент кіберпростору буде безпечно функціонувати, а також передбачала б нові можливості цифровізації усіх сфер суспільного життя.

УДК 32.973.202 (004.8)

STRATEGY OF COUNTERING PHISHING ATTACKS ON THE CRYPTOCURRENCY EXCHANGE AS PART OF THE ENDLESS ANTAGONISTIC GAME SCHEME

**Lakhno V.A.¹, Malyukov V.P.¹, Akhmetov B.S.²,
Alimseitova Zh.K.³, Ogan A.³**

*National University of Life and Environmental Sciences of Ukraine¹,
Kazakh National Pedagogical University named after Abai²,
Satpayev University³*

¹lva964@nubip.edu.ua, ¹volod.malyukov@gmail.com,

²bakhytzhan.akhmetov.54@mail.ru, ³zhuldyz_al@mail.ru, ³atkeldi@mail.ru

As the scale of the use of various Internet technologies develops, the number of cybernetic threats, as well as all kinds of attacks aimed at computer systems, also increases. Computer attackers are not only inventing new ways and scenarios of conducting cyber attacks, but also improving old proven schemes. For example, despite the rapid development of various intrusion detection systems, the threat of phishing, which occupies a significant share among computer attacks, has not disappeared anywhere. These attacks make it possible for cybercriminals to steal user account data from various Internet sites. At the same time, attackers do not particularly bother to develop new phishing attack scenarios [1]. And, indeed, such methods of phishing are still effective for attackers, such as: sending fake emails, faking websites, etc.

Phishing has not bypassed such a popular type of commercial activity in recent years as trading in digital cryptocurrencies and, accordingly, affected online exchanges engaged in such transactions. With the development and growing popularity of exchanges engaged in trading digital cryptocurrencies, the problem of detecting and predicting the consequences of such attacks, including those based on phishing, remains relevant. In [1], examples of a number of fraudulent attacks aimed at the digital cryptocurrency exchange are considered. Information security specialists are looking for ways to ensure the interaction of all interested parties in order to counter fraud using phishing attack techniques and increase privacy for individual citizens and businesses. However, many

issues still need to be studied in more detail, in particular, relying on game-theoretic methods of analyzing situations that may arise as a result of a phishing attack. For example, when such an attack is aimed at customers of trading platforms engaged in the purchase and sale of digital cryptocurrencies. That is why in this publication we have tried to present our vision of this issue. The solution involved the apparatus of game theory, which made it possible to mathematically consider the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session for the purchase and sale of digital cryptocurrencies.

That is why in this publication we have tried to present our vision of this issue. The solution involved the apparatus of game theory, which made it possible to mathematically consider the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session for the purchase and sale of digital cryptocurrencies.

In the course of research, a mathematical model has been developed for the computational core of the decision support system made during the exchange's trading session on the sale and purchase of digital cryptocurrencies. The model promotes the adoption of rational decisions to ensure the information security of players who may face the threat of a phishing attack against them. The model is developed on the basis of an endless antagonistic game and is designed to find optimal strategies for players. The solution of such a problem contributes to the analytical search not only for the meaning of the game for the interested party, but also makes it possible to find the characteristics of the degree of risk of achieving the goal by players when they use optimal mixed strategies. In particular, such a solution contributes to the analysis of the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session on the purchase and sale of digital cryptocurrencies.

Computational experiments were conducted using the Anaconda distribution kit (PyChar Professional programming environment), which made it possible to visualize the results of the game and will be useful for analysts dealing with information security issues of trading platforms specializing in buying and selling digital cryptocurrencies and countering such threats as phishing attacks.

References

1. Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). Characterizing cryptocurrency exchange scams. *Computers & Security*, 98, 101993.

УДК 004.056

ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Юлія Хохлачова¹, Алла Гаврилова²

Національний авіаційний університет

¹yuliiahohlachova@gmail.com, ²alla.havrylova@khipt.edu.ua

До передових інформаційних технологій сьогодення проявляється інтерес не тільки із наукової зацікавленості чи у пошуках вирішення найважливіших задач людства, а й через пошук шляхів швидкого збагачення за рахунок фізичних осіб, різного рівня бізнес-структур, для проведення дистанційного шпіонажу та для нанесення збитків через несанкціоноване отримання доступу до критично важливої інфраструктури, даних, а також спотворення та крадіжки інформації.

Метою даної роботи є проведення аналізу існуючих загроз сучасним інформаційно-комунікаційним системам та мережам у постквантовому періоді.

При аналізі загроз інформаційній безпеці щодо систем та мереж, необхідно враховувати не тільки методи реалізації кіберзагроз, але й мотиваційну складову їх виникнення та й існуючі дієві інструменти протидії їм (рис. 1).

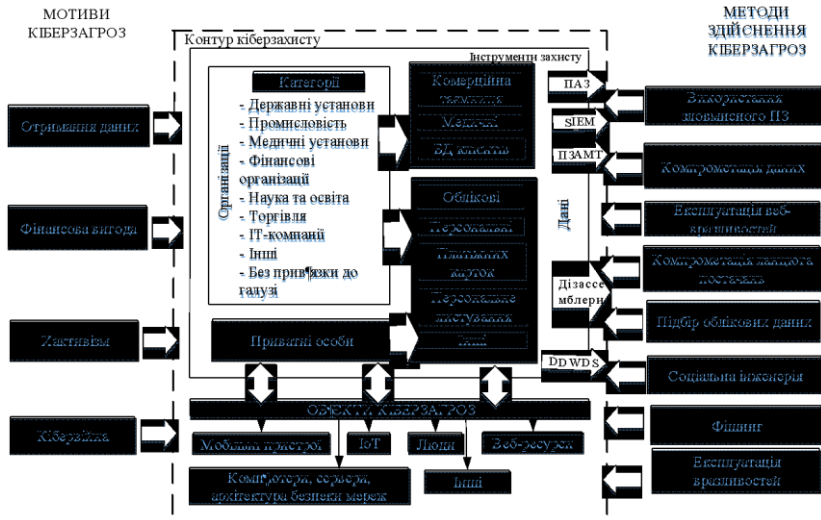


Рис.1. Структурна схема кіберсередовища загроз інформаційної безпеки в інформаційно-комунікаційних системах згідно із мотиваційною складовою

Такий комплексний підхід дозволить спрогнозувати різні режими кібератак, які кіберзлочинці можуть застосувати проти певних систем та підготувати необхідні цифрові системи безпеки при реалізації майбутніх загроз.

Зі схеми видно, що, в залежності від мотиваційної складової кіберзагроз, зловмисники використовують ряд методів здійснення кібератак. Так, мотив щодо отримання даних реалізують в основному за допомогою використання зловмисного програмного забезпечення, фішингу, експлуатації веб- й інших видів вразливостей та методів соціальної інженерії, отримання фінансової вигоди – за допомогою методів соціальної інженерії та компрометації даних й ланцюга постачань, хактивізм – використання веб-вразливостей, підбору облікових даних та фішингу, мету мотива «кібервійна» реалізують за допомогою – зловмисного програмного забезпечення.

На рис. 1 також наведені дієві інструменти підтримання контуру кібербезпеки, за допомогою яких можна визначити й попередити кіберзагрози ще до їх виникнення. Цій перелік на сьогодні представлено інструментами інтелектуального аналізу кіберзагроз: інструменти SIEM, дізасемблери зловмисного програмного забезпечення, платформи аналізу загроз (ПАЗ), програмне забезпечення для аналізу мережевого трафіку (ПЗАМТ), Deep and Dark Web Data Scrubbers (DDWDS).

Згідно із проведеними дослідженнями (на базі матеріалів Державної служби спецзв'язку та захисту інформації) щодо сфер діяльності, на які були спрямовані кіберзагрози та частоти використання методів реалізації цих загроз за період з початку 2022 р., було виявлено наступне:

1) найбільша кількість методів реалізації загроз інформаційній безпеці була спрямована на такі сектори, як медицина, наука та освіта, а також торгівля; найменша кількість була характерна для держорганів, приватних осіб, промисловості та фінансових установ – це пояснюється насамперед тим, що у кіберзлочинців зростає зацікавленість у реалізації своїх мотивів через системи кіберзахисту з менш захищеними периметрами, а тому й дешевою реалізацією;

2) за частотою використання методів реалізації кіберзагроз перше місце займають зловмисне програмне забезпечення та методи соціальної інженерії. Метод компрометації ланцюга постачань використовувався найменше.

З врахуванням обставин, що склалися, безпека об'єктів критичної інфраструктури виходить на перше місце. Тому необхідно не тільки захищати їх з фізичної точки зору, але й розглядати можливості підвищення безпеки передачі інформації незахищеними каналами за допомогою криптографічного захисту.

УДК 004.75

**РОЗВИТОК КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ АНОНІМНОЇ
МАРШРУТИЗАЦІЇ В ІНТЕРНЕТ****Людмила Ковальчук¹, Роман Олійников²,
Юрій Беспалов³, Ганна Неласа⁴***¹Інститут проблем моделювання в енергетиці ім. Г.С. Пухова НАН
України, lusi.kovalchuk@gmail.com,**²Харківський національний університет ім. В.Н. Каразіна,
roliyukov@gmail.com,**³Інститут теоретичної фізики ім. М.М. Боголюбова Національної
академії наук України, yu.n.bespalov@gmail.com,**⁴Національний університет “Запорізька політехніка”
annanelasa@gmail.com*

Із розвитком сучасного суспільства базові послуги безпеки інформації при користуванні Інтернет стають дедалі важливішими. При цьому важливим є не тільки забезпечення цілісності та конфіденційності передачі критичної інформації по телекомунікаційним каналам, а й збереження анонімності абонентів, які є учасниками взаємодії. Стрімкий розвиток децентралізованих систем в останні роки приділяє особливу увагу наявності властивості анонімності суб'єктів криптографічних протоколів.

Метою даної роботи є розробка алгоритму децентралізованого сліпого порогового перешифрування для створення криптографічного протоколу анонімної маршрутизації в Інтернет.

Порівняння технологій Proxu, VPN та Tor приводить до висновку, що Proxu-сервер зручно використовувати для захисту локальної мережі від зовнішнього доступу, в роботі VPN головне – приватність, а при використанні Tor головне – анонімність. Tor зашифрує трафік тричі, ніби створюючи три шари цибулини. Щоразу користувач потрапляє до Інтернету за допомогою випадкового комп'ютера-волонтера, шлях постійно змінюється, а сам браузер за замовчуванням не зберігає історію.

В [1] було представлено методи аналізу трафіку, які дозволяють зловмисникам, які лише частково бачать мережу, визначати, які вузли використовуються для ретрансляції анонімних потоків, і в такий спосіб створюють загрози анонімності користувачів мережі Tor. До того ж, якщо зловмисник контролює достатньо велику частину вузлів Tor мережі, існує не нульова ймовірність, того, що трафік саме того учасника, який цікавить атакуючого, пройде через ці вузли.

Ми пропонуємо підхід, який дозволяє для переадресації між мережами використовувати порогове сліпе перешифрування, яке базується на схемі шифрування Ель-Гамала в групі точок еліптичної кривої, зокрема на її властивостях гомоморфності. Також для побудови протоколу ми використовуємо порогову схему генерації ключів [2] і децентралізовану схему використання шар відкритого ключа

та (NIZK) доведення без розголошення рівності дискретних логарифмів. Також ми вважаємо, що існує деякий децентралізований *комітет*, який виконує певні дії у цьому протоколі. Зазначимо, що існування такого комітету не порушує децентралізацію протоколу, оскільки всі дії комітету є децентралізованими і єдиною вимогою до нього є наявність чесної більшості.

Цей протокол працює коректно з будь-якою кількістю децентралізованих учасників за єдиною умовою, що кількість учасників більша за певний поріг. Алгоритм сліпого перешифрування подібно до алгоритму сліпого підпису працює наступним чином: той, кому адресоване зашифроване повідомлення, використовуючи децентралізовану схему генерації ключа і інші вказані нами протоколи, комітет [3] перешифровує повідомлення з використанням відкритого ключа іншого абонента, не розшифровує його і не читаючи його вміст. Тобто тут суть в тому, що він перешифровує на іншому відкритому ключі, не розшифровуючи, тобто не бачачи вміста цього повідомлення.

Для підгрупи \mathbf{E} великого простого порядку q групи точок еліптичної кривої та фіксованої базової точки $G \in \mathbf{E}$, визначимо *ElGamal* перетворення:

$$E_{r,H} : \mathbf{E} \times \mathbf{E} \rightarrow \mathbf{E} \times \mathbf{E},$$

в залежності від параметра $r \in \{2, \dots, q-2\}$ та $H \in \mathbf{E}$, як зсув на елемент $(rG, rH) \in \mathbf{E} \times \mathbf{E}$.

$$E_{r,H}(V_1, V_2) = (V_1 + rG, V_2 + rH) = \left(E_r^{(1)}(V_1), E_{r,H}^{(2)}(V_2) \right). \quad (1)$$

При використанні Тор-браузера анонімність забезпечується наявністю трьох шарів маршрутизації, тобто є лише один проміжний вузол, який розділяє вхід і вихід. Відповідно, якщо злочинець контролює цей проміжний вузол, він може деанонімізувати абонентів на вході та виході.

Основна ідея протоколу, що пропонується, полягає в заміні цього проміжного вузла комітетом, який і виконує сліпе порогове перешифрування з використанням порогової схеми. В цьому випадку для того, щоб зв'язати конкретного користувача з конкретним виходом, зловмиснику необхідно контролювати більшість вузлів мережі. Ця схема дійсно буде працювати повільніше, ніж Тор-браузер, та не може бути використаною для взаємодії реального масштабу часу (відео, аудіо). Але вона є ефективною саме для маршрутизації приватних повідомлень, якщо потрібен високий рівень анонімності.

Література

1. Steven J. Murdoch and George Danezis Low-Cost Traffic Analysis of Tor, 2006, <https://murdoch.is/papers/oakland05torta.pdf>.
2. Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, Tal Rabin, Secure Distributed Key Generation for Discrete-Log Based Cryptosystems, 2006, <https://link.springer.com/article/10.1007/s00145-006-0347-3>.

3. Bingsheng Zhang, Roman Oliynykov, Hamed Balogun A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence, Network and Distributed // System Security (NDSS) Symposium 2019, https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-2_Zhang_paper.pdf.

УДК 004.056

THE STATE OF CYBER SECURITY OF UKRAINE DURING A FULL-SCALE INTRUSION

Dora Sabov¹, Pavlo Mulesa², Marianna Sharkadi³

¹ Uzhhorod National University, szabodora20@outlook.hu

² Uzhhorod National University, pavlo.mulesa@uzhnu.edu.ua

³ Uzhhorod National University, marianna.sharkadi@uzhnu.edu.ua

Over the course of the past decade, Ukraine has unfortunately been subjected to a persistent and alarming pattern of cyberattacks, with a significant number of these incidents being attributed to Russia. In fact, recent statistics indicate that the Ukrainian state has endured a staggering total of 397,000 separate attacks in the year 2020 alone, with a similarly high number of approximately 280,000 attacks occurring within the first 10 months of 2021.

It is important to recognize that the impact of these cyberattacks extends far beyond the immediate security implications for the Ukrainian state itself. The use of digital means to target critical infrastructure, financial institutions, and government entities in Ukraine represents a serious threat to regional and global stability, with the potential to inflict harm and disrupt operations far beyond Ukraine's borders.

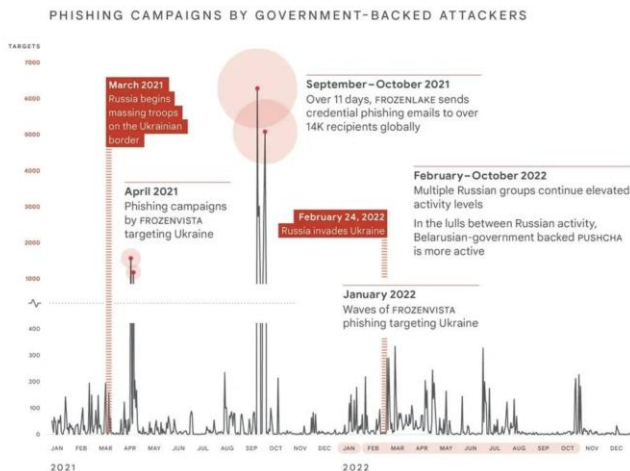


Figure 1. Phishing campaigns by government-backed attackers

In the period leading up to the invasion of February 2022, the intensity and severity of Russian cyberattacks targeting Ukraine reached a disturbing new level. Indeed, during this critical juncture, Ukrainian entities across a wide range of sectors experienced significant disruptions and setbacks due to these malicious activities.

Specifically, the public sector, energy industry, media outlets, financial institutions, commercial enterprises, and nonprofit organizations all found themselves particularly vulnerable to the impacts of these cyberattacks. The scope and scale of these disruptions were unprecedented, posing significant challenges for the resilience and stability of Ukrainian society and the broader region.

The time after Russia's takeover of Crimea in 2014 was marked by persistent cyberattacks targeting important Ukrainian infrastructure by organizations with ties to Russia. An estimated 230,000 consumers in Western Ukraine were left without power for as long as six hours in November 2015 when the Ukrainian power infrastructure was allegedly breached by parties supposedly affiliated with Russia. After the successful attack in 2015, the NotPetya ransomware attack in 2017 followed it, with an estimated total cost of close to \$10 billion worldwide. The strikes were described as the "most destructive and expensive cyber-attack in history" by the White House. The National Cyber Security Centre (NCSC) in the UK issued a statement to this effect in 2018. The 'NotPetya' attack was also the first time Western officials explicitly connected a cyber-strike to organizations tied to the Russian government.



Figure 2. Phishing campaigns targeting Ukraine

As the conflict between Ukraine and Russia rages on, cyberattacks are frequently launched on Ukraine's infrastructure, banking industry, government, and energy sector.

Attackers seek to take advantage of the victims' preoccupation and stress during such moments of fear and disturbance by taking advantage of them. I advise everyone to exercise caution as the attacks go on. As the most likely targets for the assaults, government and defense workers are recommended to exercise extreme caution.

References:

1. The Economist, Cyber-attacks on Ukraine are conspicuous by their absence, March 2022.
2. NCSC, Russian military 'almost certainly' responsible for destructive 2017 cyber-attack, February 2018.
3. The Guardian, Ukraine hit by 'massive' cyber-attack on government websites, January 2022.
4. Carnegie, Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications, December 2022.

УДК 004.056.55

ОЦІНКА РЕАЛІЗАЦІЇ РОЗПОДІЛЕНОГО КРИПТОАНАЛІЗУ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

**Віталій Носов, Василь Лучик, Тетяна Колісник,
Сергій Калякін, Віталій Світличний**

*Харківський національний університет внутрішніх справ
vitnos@univd.edu.ua*

Широке використання криптографічних систем спеціальними службами іноземних держав, злочинними організаціями і окремими правопорушниками зумовлює постійну потребу у розвідувальних, контррозвідувальних і правоохоронних оперативних підрозділах відповідних органів державної влади при здійсненні своїх повноважень проводити криптоаналіз отриманих зашифрованих даних.

Проте, на практиці оперативне криптографічне розкриття таких даних зазвичай має дві суттєві обставини: відсутність спеціалізованих обчислювальних ресурсів та наявність лише обмеженої кількості персональних комп'ютерів з ОС Windows. В таких умовах одним з актуальних способів підвищення ефективності криптоаналізу є реалізація паралельних розподілених клієнт-серверних обчислень на базі локальної мережі персональних комп'ютерів з ОС Windows, де сервер через деякий інтервал часу розподіляє виділені підмножини простору можливих ключів шифрування між агентами в локальній мережі, які в свою чергу передають задачу перебору ключів відповідній локальній програмі.

В [1] з точки зору оперативності і наявних обмежень застосовності для системи розподіленого криптоаналізу було сформульовані такі вимоги:

- максимальна універсальність до типів зашифрованих даних;
- відкриті вихідні коди і ліцензія вільного програмного забезпечення;
- функціонування на різних платформах;
- обчислення як на центральних, так і на графічних процесорах клієнтських персональних комп'ютерів;

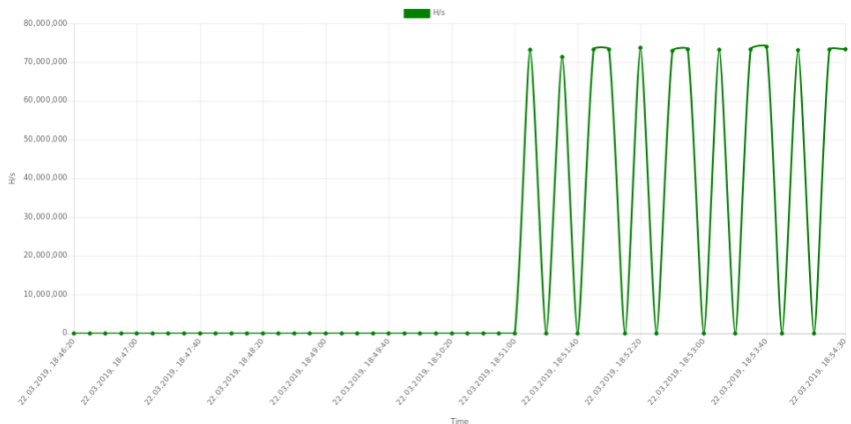
- ОС Windows на клієнтських персональних комп'ютерах;
- необмежена кількість клієнтів.

Найбільш універсальним методом криптоаналізу різних типів зашифрованих даних є вилучення гешу ключа шифрування із різних об'єктів зашифрованих даних (*.pdf, *.7z, *.zip, *.rar, *.docx, і ін.) та обчислення гешу від імовірних ключів для порівняння його із вилученим.

Вищенаведеним вимогам відповідають такі локальні програмні інструменти перебору ключів, як Hashcat [2] і John the Ripper jumbo release (JtR) [3]. Для них розроблені взаємно сумісні скрипти вилучення гешу ключа із великої кількості типів зашифрованих даних [4, 5]. В [1] зазначено, що інструментами розподіленого криптоаналізу, які сумісні з Hashcat або JtR і задовольняють встановленим вимогам, є: Hashtopolis [6], Fiterack [7], Cracklord [8], GoCrack [9].

Загальною метою комплексного дослідження є практична оцінка ефективності зазначених застосунків розподіленого криптоаналізу, яка досягається через послідовну оцінку реалізації кожного застосунку, вибір критерію ефективності і їх взаємного порівняння за обраним критерієм.

Task Speed



Assigned agents

ID	Name	Benchmark	Speed	Keyspace searched	Time spent	Cracked	Last activity	Action
5	HP-01	4096:56429.63	0.00 H/s	566163 (0.70%)	00:03:24	13	22.03.2019, 18:54:33	Unassign

Assign Show all Assignments

Dispatched chunks (showing active only - show latest 100)

ID	Start	Length	Checkpoint	Progress	Agent	Dispatch time	Last activity	Time spent	State	Cracked	Action
21	566163	43551	566163 (0.00%)	0.00%	HP-01	22.03.2019, 18:54:33	(no activity)		New	0	Abort

Рис. 1. Швидкість виконання завдання агентом

Першим для оцінки було обрано застосунок Hashtopolis, який складається з двох частин: клієнтського агента, що написаний на C# або Python та PHP/CSS серверу, який надає графічний інтерфейс управління адміністратора і керує

з'єднанням із клієнтськими агентами. На стороні клієнта Hashtopolis-агент керує запуском із необхідними параметрами утиліти Hashcat, яка дає змогу реалізовувати атаки перебору ключів на більш ніж 200 алгоритмів гешування.

Для реалізації атаки криптоаналізу попередньо з використанням скриптів [4, 5] видобувається геш ключа шифрування з блоку зашифрованих даних.

Практична оцінка реалізації застосунок Hashtopolis здійснювалась на базі локальної комп'ютерної мережі з 21 персонального комп'ютера, які мали такі основні параметри:

- Операційна система: 64-bit Windows 7 Professional Service Pack 1;
- Процесори: Intel® Core™ i5-4590 CPU @ 3.30 GHz 3.30 GHz;
- Оперативна пам'ять: 4,00 ГБ.

Після встановлення сервера та клієнта Hashtopolis на сервері у розділі Task/New task було створено нове завдання для агентів з такими параметрами: “Attack command: -D 1 -a 3 #HL# ?a?a?a?a?a”, “Is CPU only task: Yes” (рис. 6), які задають для утиліти hashcat-5.1.0: використовувати центральний процесор, тип гешів - MD5, перебирати ключі завдовжки 6 символів з алфавіту.

Деталі виконання завдання агентом були відображені на сервері у вигляді графіка, де видні часові паузи в обчисленнях, що пов'язані з отриманням агентом нової підмножини (chunk) простору можливих ключів (рис. 1).

По мірі призначення завдання агентам підсумкова швидкість перебору ключів зростала та стабілізувалась при включенні всіх агентів (рис. 2).

Task Speed

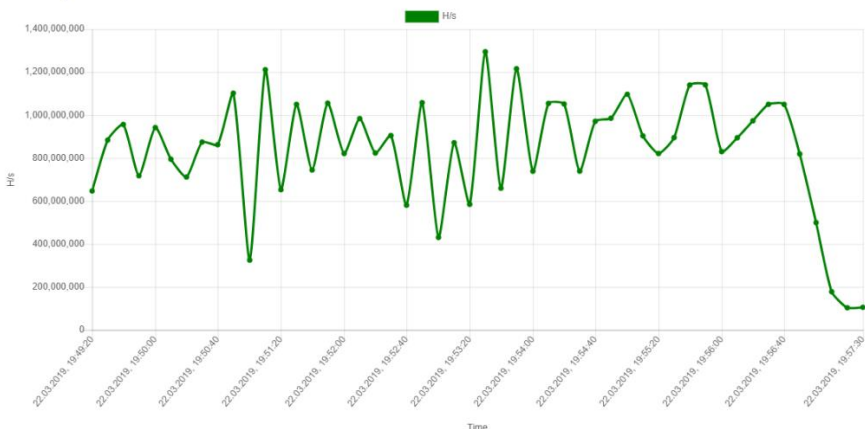


Рис. 2. Стабілізація підсумкової швидкості перебору ключів

Усереднення за 380 секунд роботи підсумкової швидкості перебору ключів розподіленої системи з 21 агентом (табл. 1) дозволило отримати значення швидкості 895 MH/s.

Отже, застосунок Hashtopolis є працездатним у локальній мережі персональних Windows- комп'ютерів, може бути використаний на практиці. Крім цього, зростання швидкості паралельних обчислень не є прямо пропорційним

кількості агентів, що відповідає очікуванням, оскільки витрачається час на формування підмножин простору ключів, їх доставки агентам та отриманням результатів перебору ключів.

Таблиця 1

Зафіксовані підсумкові швидкості перебору ключів на протязі 380 секунд з інтервалом 10 с

Time	19:49:20	19:49:30	19:49:40	19:49:50	19:50:00	19:50:10	19:50:20	19:50:30
Speed, MH/s	647	884	957	718	942	795	712	875
Time	19:50:40	19:50:50	19:51:00	19:51:10	19:51:20	19:51:30	19:51:40	19:51:50
Speed, MH/s	862	1102	325	1211	653	1050	745	1056
Time	19:52:00	19:52:10	19:52:20	19:52:30	19:52:40	19:52:50	19:53:00	19:53:10
Speed, MH/s	821	984	824	905	580	1058	431	872
Time	19:53:20	19:53:30	19:53:40	19:53:50	19:54:00	19:54:10	19:54:20	19:54:30
Speed, MH/s	584	1295	660	1216	739	1055	1052	739
Time	19:54:40	19:54:50	19:55:00	19:55:10	19:55:20	19:55:30	19:55:40	19:55:50
Speed, MH/s	971	985	1097	903	821	895	1140	1141
Time	19:56:00	19:56:10	19:56:20	19:56:30	19:56:40	19:56:50	19:57:00	
Speed, MH/s	830	895	973	1050	1050	819	500	

Практична оцінка Hashtopolis потребує подальшого дослідження зростання продуктивності його роботи у залежності від кількості агентів, інших типів гешів і типів криптоаналізу (за словником, комбінований) та контролю температури процесорів на агентських машинах. Необхідне вирішення задачі оптимального вибору для агентів розміру підмножини простору можливих ключів (chunk) в залежності від кількості агентів, їх поточної швидкості перебору, алгоритму гешу і типу перебору.

Література

1. Носов В.В. Розподілений криптоаналіз при обмежених ресурсах для потреб правоохоронних органів // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків нац. ун-т втур. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020, с. 117-119.

2. Hashcat advanced password recovery [Електронний ресурс]. URL: <https://hashcat.net/> (дата звернення: 18.04.2023).

3. John the Ripper password cracker [Електронний ресурс]. URL: <https://www.openwall.com/john/> (дата звернення: 18.04.2023).

4. Hashstack-server-plugin-hashcat. Scrapers at master. Stricture/hashstack-server-plugin-hashcat. GitHub [Електронний ресурс]. URL: <https://github.com/stricture/hashstack-server-plugin-hashcat/tree/master/scrapers> (дата звернення: 18.04.2023).

5. John/run at bleeding-jumbo. Openwall/john. GitHub [Електронний ресурс]. URL: <https://github.com/openwall/john/tree/bleeding-jumbo/run> (дата звернення: 18.04.2023).

6. GitHub - hashtopolis/server: Hashtopolis - A Hashcat wrapper for distributed hashcracking [Електронний ресурс]. URL: <https://github.com/s3inlc/hashtopolis> (дата звернення: 18.04.2023).

7. GitHub - nesfit/fitcrack: A hashcat-based distributed password cracking system [Електронний ресурс]. URL: <https://github.com/nesfit/fitcrack> (дата звернення: 18.04.2023).

8. GitHub - jmmcatee/cracklord: Queue and resource system for cracking passwords [Електронний ресурс]. URL: <https://github.com/jmmcatee/cracklord> (дата звернення: 18.04.2023).

9. GitHub - mandiant/gocrack: GoCrack is a management frontend for password cracking tools written in Go [Електронний ресурс]. URL: <https://github.com/fireeye/gocrack> (дата звернення: 18.04.2023).

УДК 044.56.53(043.2)

ШТУЧНИЙ ІНТЕЛЕКТ СНАТ GPT: МОЖЛИВОСТІ ТА ЗАГРОЗИ ТЕХНОЛОГІЧНОЇ НОВИНКИ

Галич Євгенія¹, Павленко Владислав²

Національний авіаційний університет

¹ 7405781@stud.nau.edu.ua, ² 7328430@stud.nau.edu.ua

18 лютого 2023 року найгарячіша технологічна новинка світу – чат-бот на основі штучного інтелекту ChatGPT (Generative Pre-trained Transformer) – стала доступною для реєстрації в Україні. Минуло всього декілька місяців відтоді, як ChatGPT з'явився у відкритому доступі, а хвиля новин навколо нього не вщухає, підвищуючи його актуальність серед користувачів.

Метою даної роботи є розбір новітньої технології – чату GPT, аналіз його принципу роботи та ризиків використання.

Додаток, розроблений компанією Open AI – це роботи, призначені для спілкування. Вони автоматично відповідають на письмові запитання, часто у подібній до людської манері. Однак за шоком від можливостей машин, що замінюють людей у різних формах дискусії ховається багато загроз, які будуть описані нижче.

ChatGPT швидко набув шаленої популярності: 1 млн користувачів за п'ять днів, в той час, як соціальна мережа Instagram йшла до таких показників охоплення 2,5 місяці, Facebook – 10 місяців, Netflix – 3,5 роки. GPT Chat працює з великим обсягом наданих даних. Платформа використовує сотні гігабайт тексту, які вона обробляє в режимі реального часу для створення нового контенту. В результаті GPT Chat може імітувати стиль і тон раніше введеного контенту, дозволяючи створювати зв'язні та логічні речення. Можливості використання штучного інтелекту досить масштабні. Наприклад, одним із основних вмінь технологічної

новинки є обробка природної мови. Використання методів машинного навчання для розпізнавання та аналізу текстових даних; виявлення теми, відношення між словами та іншими мовними структурами є фішкою чату GPT. Крім того, машинне навчання можна використовувати для вирішення різних завдань, таких, як прогнозування часових рядів, класифікація зображень і кластеризація даних. Для цього додаток використовує штучні нейронні мережі, щоб навчитися розпізнавати та аналізувати вхідні дані. Ще одне використання GPT Chat – автоматична генерація відповідей на запитання користувачів. Відповіді можуть стосуватися різних сфер, таких, як здоров'я, фінанси, мода, кулінарія тощо.

Головною перевагою GPT Chat є його ефективність і швидкість. Платформа може обробляти великі обсяги даних і виконувати завдання швидше, ніж людина, та працювати без втоми і помилок, що характеризує роботу застосунку як надійну і точну. Використовуючи штучний інтелект, компанії та інші організації можуть скоротити витрати на робочу силу, оскільки він виконує багато рутинних і повторюваних завдань, які раніше виконувала людина.

Незважаючи на те, що ChatGPT є найбільш "просунутою" технологією з використанням штучного інтелекту на сьогоднішній день, вона далека від досконалості.

Застосунок також має свої недоліки та обмеження. Наприклад, обмеженість у прийнятті рішень та недостатній контроль. Хоча чат може дуже ефективно виконувати рутинні та повторювані завдання, все ж таки існує обмежена здатність при вирішенні складних проблем, які вимагають значного розуміння контексту та досвіду. Також, у роботі штучного інтелекту, може бути складно контролювати та розуміти його дії та рішення. Це може становити проблему у випадку, коли рішення мають серйозні наслідки.

Як і будь-який технологічний продукт, використання штучного інтелекту не є повністю безпечним. Наведемо декілька ризиків, пов'язаних з використанням ChatGPT:

1. *Поширення дезінформації*: GPT-розмови можуть давати неправдиві або оманливі відповіді, які можуть бути неправильно інтерпретовані або використані для поширення дезінформації.

2. *Підтримка упередженості*: оскільки модель навчається на великій кількості даних, навчальні дані можуть містити поширені упередження та патерни дискримінації. Якщо ці шаблони не виявити і не виправити, Chat GPT може увічнити негативне ставлення до певних груп.

3. *Вразливість до хакерських атак*: Chat GPT може бути вразливим до різних видів хакерських атак, зокрема атак типу "відмова в обслуговуванні" (DoS), спроб злому та крадіжки даних.

4. *Загроза конфіденційності*: GPT може зберігати персональні дані користувачів. Це може призвести до порушення конфіденційності або використання цих даних сторонніми особами чи організаціями.

Перспективи використання ChatGPT є дуже високими. Технології штучного інтелекту постійно розвиваються, що дозволяє застосунку вдосконалюватись та надавати більше корисної інформації та рішень, розглядатись у контексті спрощення і пришвидшувати деякі процеси нашого життя. ChatGPT, безсумнівно, стане в нагоді маркетологам при написанні рекламних текстів, інфлюенсерам при підготовці контенту для соціальних мереж і власникам бізнесу при веденні необхідної документації. Чат-боти значно спрощують процес пошуку інформації, надаючи користувачам розгорнуті відповіді замість переліку посилань. У майбутньому ChatGPT та інші розробки на основі штучного інтелекту можуть замінити людину у виконанні багатьох завдань. Однак, для того, щоб сформулювати правильні вимоги, вибрати найбільш задовільне рішення та оцінити, чи відповідають результати певним очікуванням, потрібні люди з високим рівнем експертизи та глибоким розумінням конкретної сфери спеціалізації. Також застосунок може допомогти у покращенні освіти, надавати корисні ресурси для навчання та підтримувати сам процес для студентів та вчителів, що є особливо важливим в будь-які часи. Загалом, існує великий потенціал для використання штучного інтелекту, його розвиток може значно покращити якість нашого життя та забезпечити розвиток різних галузей науки і технологій. Однак, важливо, щоб штучний інтелект використовувався етично і відповідально для надання безпеки, конфіденційності і довіри його користувачам.

Перевіримо штучний інтелект у дії. За допомогою сервісу було змодельовано принцип роботи атак на конфіденційні дані користувачів методом SQL ін'єкцій. Для цього було зроблено запит до чату GPT - "Принцип роботи атак на конфіденційні дані користувачів методом SQL ін'єкцій". Отримали наступне.

Розглянемо більш детально, як саме працює атака методом SQL-ін'єкцій. Зловмисник може використовувати SQL-ін'єкції для виконання інших зловмисних дій, таких як вставка, оновлення або видалення даних з бази даних. Наприклад, він може ввести наступну послідовність символів у поле логіну мовою CSS: `' ; DROP TABLE users;--` . Цей запит викличе помилку в базі даних та видалить всі дані з таблиці "users". Щоб запобігти атакам методом SQL-ін'єкцій, необхідно правильно валідувати вхідні дані та коректно оброблювати запити до бази даних. Крім того, рекомендується використовувати параметризовані запити, які дозволяють окремо вказувати дані та запит до бази даних, що допоможе уникнути можливих атак методом SQL-ін'єкцій.

В ході дослідження прийшли до висновку, що користувач, не маючи кваліфікацію, за допомогою ChatGPT може отримати доступ до будь-якого ресурсу шляхом експлуатації певних уразливостей в системі.

Науковий керівник – к.т.н., доцент Хохлачова Ю.С.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ

XII Міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій»

2-4 травня 2023 року

м. Ужгород (Україна)

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних (у тому числі класифікаційного індексу УДК) уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі
безпеки інформаційних технологій
Національного авіаційного університету