Національний університет оборони
Азербайджанської республіки

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

Національний аерокосмічний університет
імені М. Є. Жуковського
"Харківський авіаційний інститут"

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей одинадцятої міжнародної
науково-технічної конференції

16 – 17 листопада 2023 року

Том 2: секції 3, 6

Баку – Харків – Бельсько-Бяла –2023

УДК 004 : 681.3 doi: https://doi.org/10.32620/PI.23.t2

У збірнику подано тези доповідей одинадцятої міжнародної науково-технічної конференції "Проблеми інформатизації". Розглянуті питання за такими напрямами: інформатизація навчального процесу; застосування, експлуатація та безпека функціонування телекомунікаційних систем та мереж; комп'ютерні методи і засоби інформаційних технологій та управління; методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах; цивільна безпека (інформаційна підтримка); сучасні інформаційно-вимірювальні системи.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Azerbaijan National Defence University

National Technical University
Kharkiv Polytechnic Institute

Kharkiv National University
of Radio Electronics

National Aerospace University
Kharkiv Aviation Institute

University of Bielsko-Biala

PROBLEMS OF INFORMATIZATION

Abstracts of reports of the eleventh international scientific and technical conference

16 – 17 November 2023

VOLUME 2: SECTIONS 3, 6

Baku – Kharkiv – Bielsko-Biala –2023

UDC 004 : 681.3 doi: https://doi.org/10.32620/PI.23.t2

The collection presents abstracts of reports of the eleventh international scientific and technical conference "Problems of Informatization". Issues in the following areas are considered: informatization of the educational process; application, operation and safety of telecommunication systems and networks; computer methods and means of information technology and management; methods of fast and reliable data processing in computer systems and networks; civil security (information support); modern information and measurement systems.

ORGANIZING COMMITTEE

Одинадцята міжнародна науково-технічна конференція “Проблеми інформатизації” проводиться 16 та 17 листопада 2023 року в режимі ONLINE.

Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Інформатизація навчального процесу.

Керівник секції: д.т.н. проф. В. М. Рудницький, ДНДІ ВС ОВТ, Черкаси.
Секретарка секції: к.т.н. Н. В. Лада, ДНДІ ВС ОВТ, Черкаси.

СЕКЦІЯ 2. Застосування та експлуатація телекомунікаційних систем та мереж.

Керівниця секції: д.т.н. проф. Н. Г. Кучук, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. С. С. Бульба, НТУ «ХПІ», Харків.

СЕКЦІЯ 5. Методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах.

Керівник секції: д.т.н. проф. В. А. Краснобаєв, ХНУ, Харків.
Секретарка секції: к.т.н. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків.

СЕКЦІЯ 7. Сучасні інформаційно-вимірювальні системи.

Керівник секції: д.т.н. проф. О. В. Коломійцев, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. А. О. Подорожняк, НТУ «ХПІ», Харків.

ТОМ 2

СЕКЦІЯ 3. Безпека функціонування телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків.
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків.

СЕКЦІЯ 6. Цивільна безпека та захист критичної інфраструктури.

Керівник секції: д.т.н. доц. О. В. Третьяков, НАУ, Київ.
Секретар секції: к.т.н. доц. Є В. Доронін, НАУ, Київ.

ТОМ 3

СЕКЦІЯ 4. Комп’ютерні методи і засоби інформаційних технологій та управління.

Керівники секції: д.т.н. проф. І. В. Рубан, ХНУРЕ, Харків.
д.т.н. проф. А. А. Коваленко, ХНУРЕ, Харків.
Секретар секції: к.т.н. доц. О. С. Ляшенко, ХНУРЕ, Харків.

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків

CREATION OF AN EFFECTIVE RADIOLOCATION AREA FOR THE DETECTION OF UAVs

Maharramov R.R.
Military Scientific Research Institute, Baku, Azerbaijan
Hashimov E.G.
Azerbaijan Technical University, National Defense University, Baku, Azerbaijan

The rapid development of unmanned aerial vehicles and their effective use is one of the main challenges for air defense systems. Timely detection of small-sized, relatively silent and low-altitude UAVs by air defense systems becomes difficult. In the development of UAVs, special colors and protective layers are used, which makes it difficult to detect them by visual observation posts or radiolocation stations [1-2].

From the analysis of the local wars and conflicts that have occurred in recent years, the Patriotic war that occurred in 2020, and also the ongoing Russia-Ukraine war, it was determined that in order to fight against UAVs, they must be detected in time. Due to the fact that the detection stations in the armament of the Armenian Army against the modern UAVs used by the Azerbaijani Army in the Patriotic War are old, the number of those stations is small, and as well as the weak combat skills of the personnel, they could not detect in time most of the UAVs used by the Azerbaijani Army. As a result of the correct combat tactics of Azerbaijan in the first days of the war, the locations of detection stations and anti-aircraft missile complexes in the armament of the Armenian Army were quickly discovered and neutralized. As a result, the air superiority in the Patriotic War completely went to Azerbaijan's side [3]. With the emergence of unmanned aerial vehicles, the problem of combating them has become significantly more relevant. After detecting and identifying UAVs by radiolocation stations, it is necessary to take measures to neutralize them. In order to combat UAVs more effectively, it is important to detect them quickly at a long distance as well as in a dead canyon [4].

One of the important factors is the method of formation of the battle position of RLSs for the detection of UAVs and the creation of an effective radiolocation area. The method of forming a battle position consists of several algorithms that include several interconnected stages. The algorithms are follows:

- battle position selection algorithm of RLS;

-algorithm for determining the number of visual observation posts equipped with an electro-optical system in the position area of the RLS;

-algorithm for choosing a rational variant of the battle positioning of RLS, taking into account the results obtained during the solution of the first two algorithms.

When choosing the battle positioning of radiolocation stations and placing them in positions, it is necessary to pay attention to the minimum dead canyon. The minimum dead canyon means that an effective radiolocation area has been created for detecting UAVs.

In this work, the algorithm for determining the number of visual observation posts equipped with an electro-optical system in the position area of the RLS for the detection of UAVs and the creation of an effective radiolocation area was considered.

Taking into account the characteristics of UAVs and the problems of combating them, it is advisable to equip visual observation posts with an automated electro-optical system for timely and effective detection of UAVs in the dead canyon. The use of existing and promising electro-optical systems in the direction of the likely flight of the enemy and in visual observation posts (VOPs) allows timely detection of UAVs in the dead valley, recognition of their class, type and current nature of their movements.

In the future, the mentioned electro-optical systems can be replaced by more improved models. Thus, examples of electro-optical systems have already been developed and can detect UAVs in time. In order to effectively detect UAVs in a dead canyon, when creating a radiolocation area, it is necessary to pay attention to the combat positioning of radiolocation stations, the number of visual observation posts (VOP) equipped with an electro-optical system, and how to place them in the area. As a result, it can be noted that taking into account the viewing angle , the detection distance of the electro-optical system placed on the visual observation post, the direction relatively to the central axis of the RLS, the angle of the dead canyon of the RLS, the height at which the UAV can enter the RLS dead canyon, the number and distance of the electro-optical system for the detection of UAV, it is possible to detect UAVs in the dead canyon through an electro-optical system placed to the visual observation post.

References

1. Bayramov, A.A. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition // Advanced Information Sistems. Volume 1, №2, 2017, p.70-73 . DOI: 10.20998/2522-9052.2017.2.12

2. Hashimov, E.G., Bayramov, A.A., Khalilov, B.M. Terrain orthophotomap making and combat control // Proceeding of İnternational Conf. “Modern Call of Security and Defence”. İ-st. -2016. – Vol.19. –p.68-71.

3. Aliev, F.A. The detection of small unmanned aerial vehicles (UAV) by the radar stations. Proceedings of the 8 th International Conference on control and optimization with industrial applications. 24-26 August, 2022, Baku. –p. 72.

4. Hashimov, E.G., Maharramov, R.R., Sabziev, E.N., Pashaev, A.B. Assessment of dead zone of joıntly operatıng radars. // -Kharkov: Control, Navigation and Communication Systems, -2023. №3, -p.172-175. https://doi.org/10.26906/SUNZ.2023.3.171.

RESEARCHES SOME ASPECTS INFORMATION SECURITY OF WIRELESS COMMUNICATION NETWORKS

Ibrahimov B.G., Abaszada E.I.
Azerbaijan Technical University, Baku, Azerbaijan

Before discussing possible attacks on wireless networks, it is important to realize that the network deployment procedure involves many activities, which in turn already include security and reliability measures.

But at the same time, the difficulty of a number these measures makes wireless networks vulnerable if mistakes are made or something is simply missed when laying out and configuring the network. For many enterprises, data loss in wireless networks is a negative action and therefore many firms have well-designed security policies [1-3].

This paper is a survey on existing wireless networks and the vulnerabilities of hacking a particular wireless network standard. The purpose of the paper is to familiarize and accumulate knowledge on wireless networks, security methods, vulnerability to hacking.

Knowing well the design and configuration of wireless networks, it is easy to see the sides of vulnerability. Any specialist, knowing the communication networks from different sides, tries to find the means of defense, but also, when building up the means of defense, there may be places for attacks by unwanted representatives [1,4,5].

Thus, the paper considers some aspects information security of wireless communication networks from the point view on the characteristics of the information protection system and reliability of the communication network.

Wireless is open to all winds, and in addition to intrusions from the Internet, it is at least threatened by an attempt of "listening" by colleagues from the neighboring office or from the lower floor. And this is no small matter - such actions can not only bring satisfaction from using the wireless network, but also find ways to penetrate it. Accordingly, if security is not given due attention, such a network may well be considered public, which will inevitably affect its functioning in a bad way [1, 2].

Attempts to penetrate a corporate closed network can occur for several reasons. First, a targeted hack to steal confidential information. Most often, this is the reason why it is necessary to take care of the security of the wireless segment of the network, although in fact the percentage of such hacks is quite small.

Much more popular are attempts to penetrate the network to use someone else's Internet connection.

In this case there is also theft, but not of tangible confidential documents, but virtual - theft of the Internet, namely traffic, connection speed.

Based on the research [1, 2, 4] it is established that the key definitions of the content of the wireless network segment is characterized by many important characteristics to ensure their efficiency, reliability and security.

Considering the constituent technical components of the vector quality of functioning of the wireless network segment $M[K(\lambda_i)]$ is functionally described by the following dependence:

$$M[K(\lambda_i,t)] = \mathrm{W}[\mathrm{E}_{\mathrm{EF}}(\lambda_i,t), R_{HF}(\Lambda_i), I_{IS}(\lambda_i,t)], \quad i=\overline{1,k}, \qquad (1)$$

where $I_{IS}(\lambda_i,t)$ – is the function that takes into account the criteria of information security taking into account the intensity of service and useful traffic λ_i at the moment of time t, which is an indicator of the information protection system, $i=\overline{1,k}$;

$\mathrm{E}_{\mathrm{EF}}(\lambda_i,t)$ – the function, taking into account the criteria efficiency of functioning of the wireless network segment in the communication system taking into account the intensity of service and useful traffic λ_i at the moment of time t, which are the network characteristics hardware and software complexes of the system when providing various telecommunication services and application;

$R_{HF}(\Lambda_i)$ – function, taking into account criteria reliability functioning wireless network segment in the communication system taking into account intensity failures Λ_i hardware-software complexes communication systems at the moment of time t, $i=\overline{1,k}$.

Expressions (1) define the essence of the considered new approach to analyze the complex indicators of the quality of functioning of the wireless network segment in the communication system in the provision of telecommunication services and application.

References

1. Bayram G. Ibrahimov, Ramiz T. Humbatov, Rufat F. Ibrahimov. Cryptographic Methods and Means Protection Transmitted Information in Telecommunication Systems // The Proceedings of the 18th -IFAC Conference on Technology, Culture and International Stability. IEEE Explore. ELSEVIER. IFAC-Papers OnLine, (Scopus) Vol. 51, Issue 30, 2018.pp. 821-824.

2. Gordeychik S.V., Dubrovin V.V.Security of wireless networks. 2008 .288 p.

3. Aliyev K.R., Hashimov, E.G., Cyberspace as a fifth domain of military operations // Проблеми інформатизації. Тези доповідей 9- і міжнародної науково-технічної конференції. Том 1. -Черкаси – Харків-Баку – Бельсько-Бяла: 18 – 19 листопада**,** -2021, -с.104-105

4. Kostin D. V. V., Shelukhin O. I. Comparative analysis of machine learning algorithms for the classification of network encrypted traffic // T- Comm: Telecommunications and transport. 2016. № 9. С.46-5.

5. Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p. 96-98. DOI: https://doi.org/10.30837/csitic52021232904

РОЗРОБКА МУЛЬТИМЕДІЙНОГО КУРСУ З КІБЕРБЕЗПЕКИ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ

Муллалієва Д С.
Харківський національний університет внутрішніх справ, Харків, Україна

За даними Звіту про кібербезпеку Verizon за 2022 рік [1], порівняно з 2021 роком кількість атак програм-вимагачів в 2022 році зросла на 13%, що є значним збільшенням, якщо порівняти цей відсоток з останніми 5 роками разом [2]. У цьому контексті розробка мультимедійного курсу з кібербезпеки на платформі вебсайту є актуальним завданням, адже має низку переваг:

1. Збільшення обізнаності: здобувачі вищої освіти можуть швидко ознайомитися зі змінами в кіберзагрозах та відповідних стратегіях захисту.
2. Реалістичне навчання: мультимедійні ресурси на вебсайті дозволяють створити ситуації, що імітують реальні кібератаки, допомагаючи здобувачам вищої освіти розвивати практичні навички в області кібербезпеки.
3. Гнучке навчання: здобувачі вищої освіти можуть навчатися у власному темпі, вибираючи час і місце для навчання.
4. Оновлення змісту: вебсайт можна легко оновлювати, щоб відображати нові загрози та стратегії захисту, забезпечуючи актуальну інформацію.
5. Візуалізація складних концепцій: мультимедійний формат дозволяє візуалізувати складні кібербезпекові концепції, діаграми та графіки, що полегшує розуміння матеріалу і покращує сприйняття інформації.
6. Інтерактивність: мультимедійні курси можуть включати інтерактивні вправи, вікторини та завдання, що допомагають здобувачам вищої освіти активно залучатися до навчання та встановлювати практичні навички.
7. Можливість дистанційного навчання.
8. Персоналізоване навчання: мультимедійні курси можуть враховувати індивідуальні потреби здобувачів вищої освіти, надаючи можливість обирати шляхи навчання та фокусуватися на конкретних аспектах кібербезпеки.
9. Відстеження прогресу: платформа мультимедійного курсу може надавати звіти про прогрес здобувачаів вищої освіти.
10. Ефективне поширення інформації: мультимедійний курс може бути легко поширюваним та доступним для широкої аудиторії.

Отже, розробка та впровадження мультимедійного курсу з кібербезпеки на вебсайті є необхідним етапом для зміцнення знань та навичок у цій надважливій галузі, щоб забезпечити надійний захист від кіберзагроз і зберегти цифрову безпеку в нашому сучасному глобалізованому світі.

Список літератури

1. Джерело: Verizon. (2022). 2022 Data Breach Investigations Report. [Посилання на джерело: https://enterprise.verizon.com/resources/reports/dbir/]
2. https://blog.desdelinux.net/uk/segun-el-informe-de-2022-de-verizon-el-ransomware-aumento-un-13-en-comparacion-con-el-ano-pasado

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ТА МЕТОДІВ РОЗРОБЛЕННЯ БЕЗПЕЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Алекберов І.Е., Ружинський К.А., Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Події останніх років свідчать, що сучасні засоби захисту програмного забезпечення КС неможуть забезпечити необхідний рівень безпеки. Почастішали випадки кібератак на комп'ютерні системи державних об'єктів критичної інфраструктури, на банківські рахунки, на інформаційні ресурси оборонного відомства та інших державних служб. Пов'язано це багато в чому з тим, що масове поширення комп'ютерних мережевих технологій з одного боку істотно розширило можливості зловмисників у використанні методів і засобів несанкціонованого доступу до даних, а з іншого боку фірми-розробники найчастіше нехтують питаннями безпеки програмного забезпечення. Крім того, рівень розвитку методологій розроблення програмного забезпечення не дозволяє акцентовано забезпечити ІТ-фірми необхідним методологічним і практичним контентом, що підвищує рівень безпеки.

В теорії захисту інформації накопичено значний теоретичний матеріал і практичний досвід. Проте динамічний розвиток інформаційних технологій, інтелектуалізація комп'ютеризованих та керуючих засобів, а також різноманітність технологічних рішень сучасного програмування сприяють тому, що постановка завдань підвищення безпеки ПЗКС істотно видозмінюється через необхідність врахування дії нових факторів. У зв'язкт з цим, особливої актуальності набувають питання синтезу моделей та методів розроблення безпечного ПЗКС. При цьому їх ключовою особливістю є врахування і адаптація існуючих гнучких методологій розроблення ПЗ до підвищених вимог безпеки КС з використанням сучасного математичного, методологічного і технологічного апарату ІТ-фірм. Врахування перерахованих особливостей ПЗКС виходить за рамки існуючих моделей та методів розроблення ПЗ і вимагає як модифікації, так і їх перегляду.

У даній роботі проводиться аналіз основних тенденцій розвитку моделей та методів розроблення безпечного програмного забезпечення і вимог до програмних засобів.

Наведено результати досліджень сучасних моделей та методів розроблення безпечного програмного забезпечення і факторів, що впливають на безпеку.

Проведено аналіз і порівняльне дослідження основних підходів математичного моделювання процесу розроблення безпечного програмного забезпечення.

На основі виявлених закономірностей, переваг і недоліків сучасних методологій розроблення безпечного програмного забезпечення виявляються можливості удосконалення безпечного програмного забезпечення.

АНАЛІЗ МЕТОДІВ ДОСЛІДЖЕННЯ ОЗНАК МОНТАЖУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Волос С.Л., Корчак М. О., Можаєв М.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Криміналістика цифрових зображень - це абсолютно нова галузь досліджень, яка спрямована на перевірку справжності зображень шляхом відновлення інформації про їх історію. Вирішуються дві основні проблеми: ідентифікація зображувального пристрою, який захопив зображення, та виявлення слідів підробок. **Мета доповіді:** проаналізувати різні методики з використанням різних засобів виявлення монтажу цифрових зображень для вибору найбільш ефективного методу проведення дослідження. В результаті проведеного аналізу методів підробки цифрових зображень та у порівнянні з результатами практичної роботи експерта встановлено, що кожен з методів має свої плюси і мінуси. Таким чином для досягнення максимальної ефективності у виявленні монтажу цифрових зображень необхідно комбінувати різні методики.

РОЗРОБКА БІОМЕТРИЧНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ

Гараєв Е.А., Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту (СОІБ). Для побудови та ефективної експлуатації СОІБ необхідно: виявити вимоги захисту інформації, специфічні для даного об'єкта захисту; використовувати напрацьовані практики (стандарти, методології) побудови подібних СОІБ; визначити підрозділи, відповідальні за реалізацію та підтримку СОІБ; розподілити між підрозділами області відповідальності; на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту; реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації; реалізувати систему менеджменту (управління) інформаційної безпеки (СМІБ); - використовуючи СМІБ організувати регулярний контроль ефективності СОІБ і при необхідності перегляд і коригування СОІБ і СМІБ. Як показують нижче привид дані, помилки на організаційному етапі побудова СОІБ, можуть привести до некоректної або неправильної роботи системи. В доповіді розглянуті та проаналізовані засоби захисту інформації, як сукупність інженерно-технічних, електричних, електронних, оптичних і інших пристроїв і пристосувань, приладів та технічних систем, а також інших речових елементів, які використовуються для вирішення різних завдань із захисту інформації, в тому числі попередження витоку і забезпечення безпеки захищається інформації.

ЗАХИСТ ІНФОРМАЦІЇ ПРИ ВЗАЄМОДІЇ З МОБІЛЬНИМИ КОРИСТУВАЧАМИ

Гнатюк І.А.
Харківський національний університет внутрішніх справ, Харків, Україна

Атаки на мобільні телефони та інші гаджети знаходяться в топ-3 за поширеністю серед кібератак. Відповідно, захист мобільних пристроїв утворює проблему. Проте, з ростом використання старт-пристроїв зростає і небезпека витоку та втрати даних. Саме тому кожному користувачеві варто подбати про належний рівень безпеки (кібербезпеки) цифрових пристроїв.

Хакери – це електронні "взламники", які проникають в мобільну та комп'ютерну систему, використовуючи особливі уразливі лазівки у програмному забезпеченні. Захиститися від них можна за допомогою особливого додатку – мережного екрану з пакетною фільтрацією, що входить до складу антивірусних програм і робить комп'ютер невидимим для хакерів.

Для захисту від шкідливого коду і хакерських атак треба:

- встановити антивірусну програму;
- встановити оновлення ОС Windows, що відповідає за безпеку;
- не втрачати увагу при роботі зі спамом в електронній пошті і системах миттєвих повідомлень;
- зберігати резервної копії (BackUp) даних.

Мобільні загрози поділяються на 3 типи: на рівні пристрою, рівні мережі та рівні додатків. Кожен вид має свою специфіку і способи попередження.

1. Загрози на рівні пристрою існують через недосконаліть операційних систем і драйверів. В кожному мобільному телефоні є базовий заводський захист і хакери шукають способи злому пристроїв. Для цього хакери залучають експлойти, що використовують уразливі місця в ПЗ смартфона.

2. Загрози на рівні мережі використовують контроль над Wi-Fi, Bluetooth, USB-кабелем, SMS-повідомленнями, голосовими дзвінками. Наприклад, зловмисники можуть використовувати вразливі бездротові точки доступу, стаючи посередником між пристроєм співробітника і сервером.

3. Загрози на рівні додатків, які несуть у собі використання шкідливого програмного забезпечення. Магазини додатків iOS і Android щодня блокують сотні підозрілих додатків для мобільних пристроїв. Крім шкідливого програмного забезпечення, існує ще й так зване сіре ПЗ, яке теж може бути небезпечним для чутливих даних компанії.

Мобільна безпека - це не встановлення однієї програми. Рішення повинно покривати всі рівні, проводячи моніторинг і аналітику пристроїв, своєчасно усувати загрози та попереджати користувачів про потенційно шкідливі об'єкти, веб-ресурси та небезпечні дії. Способів захистити свій мобільний пристрій існує чимало, варто дотримуватися певних правил використання та не залишати гаджети без нагляду. Тоді користування буде безпечним та захищеним і користування пристроями приноситиме лише позитивні враження.

АНАЛІЗ АПАРАТНИХ ЗАСОБІВ ДІАГНОСТУВАННЯ ЦИФРОВИХ І МІКРОПРОЦЕСОРНИХ ПРИСТРОЇВ ЗАХИСТУ ІНФОРМАЦІЇ

Демченко З.А., Сіроус В.С., Можаєв М.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Для визначення місця прояву несправностей з метою їх подальшого усунення застосовують апаратні, програмні або змішані засоби діагностування цифрових і мікропроцесорних пристроїв. Усі вони, залежно від випадку, тією чи іншою мірою придатні для діагностування цифрових і мікропроцесорних пристроїв захисту інформації. Отже, необхідно проаналізувати кожен з них.

Сьогодні важко надати перевагу апаратним або програмним засобам діагностування цифрових і мікропроцесорних пристроїв.

Найкращий результат дає їх комбінація, оскільки програмні засоби діагностування, зокрема діагностичні програми, мають відпрацьовуватись за допомогою апаратних засобів.

Метою доповіді є аналіз сучасних апаратних засобів діагностування цифрових і мікропроцесорних пристроїв, та оцінка їх ефективності.

В доповіді розглянуто засоби автоматичного контролю і діагностування. їх використання дає істотні переваги, а саме: задавши для приладу початкові умови, подальший процес контролю і діагностування обчислювальних пристроїв і систем відбувається автоматично. Це значно спрощує керування ним. Отже, детально розглядати цей вид автоматизації процесу контролю і діагностування немає потреби.

Розмаїття апаратних засобів діагностування дає змогу обрати їх щодо конкретних цифрових і мікропроцесорних пристроїв захисту інформації. При цьому головну увагу звертають на доцільність використання того чи іншого засобу та економічну ефективність процесу діагностування, реалізованого на його базі.

В результаті досліджень отримано:

1. Виконано класифікацію апаратних засобів контролю і діагностування.
2. Визначено тенденції розвитку технологічного устаткування і апаратних засобів діагностування мікропроцесорних пристроїв та комп'ютерних систем.
3. Проаналізовано основні вимоги до систем діагностування цифрових і обчислювальних пристроїв. Визначено пріоритетні засоби забезпечення цих вимог.
4. Проведено аналіз засобів тестування мікропроцесорів.
5. Визначено спосіб оцінки та проведена оцінка ефективності використання апаратних засобів діагностування мікропроцесорних пристроїв та комп’ютерних систем.

АНАЛІЗ ТА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЙНИХ ВИМІРІВ СИГНАЛІВ В КАНАЛАХ ВИТОКУ ІНФОРМАЦІЇ

Демченко Н.А., Тесленко М.О., Можаєв М.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Існує чималий круг завдань, прямо або побічно пов'язаних з розпізнаванням сигналів, які є носієм інформації, про стан об'єктів або процесів.

Найбільш характерними в цьому відношенні є завдання, пов'язані з виміром форми вхідного сигналу, оскільки від цього залежить вибір оптимальних алгоритмів перетворення даних і обчислення саме тих параметрів, які найточніше оцінюють досліджувані властивості об'єкту або процесу.

Тому дуже часто всі класи завдання розпізнавання сигналів зводяться до завдання виміру форми сигналів і їх характеристик. Ці виміри названі ідентифікаційними вимірами.

Метою даної доповіді є аналіз існуючих технологій ідентифікації вимірів сигналів

Проведений аналіз довів, що основним недоліком розглянутих методів є тривалий час експерименту, що витрачається в основному на очікування сталого режиму при динамічних змінах поведінки трафіку в комп’ютерній мережі.

Крім того, необхідність в отриманні достатньої для апроксимації частотних характеристик кількості даних так само приводить до збільшення часу ідентифікації інформаційного потоку.

Тому використання методів ідентифікації по частотним характеристикам трафіку в мультисервісних комп’ютерних мережах з динамічно змінною (флуктуаційним) поведінкою потоку інформації істотно утруднене.

Подальшим розвитком підходу, пов'язаного з ідентифікацією трафіку на основі частотних характеристик є ідентифікація інформаційного потоку спектральними методами.

Проведений аналіз показав, що вказаний вид методів ґрунтується на розкладанні сигналів по ортонормованих функціях, не обов'язково гармонійних.

При цьому результатом ідентифікації є визначення ядра інтегрального рівняння об'єкту

Основним недоліком спектральних методів ідентифікації трафіку є низька точність оцінки досліджуваних параметрів за наявності сторонніх шумів (перешкод).

Так тільки при найбільш сприятливому випадку, коли оцінка відносної погрішності рішення задачі ідентифікації співпадає з оцінкою відносної погрішності початкових даних.

У решті випадків практичне застосування спектральних методів ідентифікації приводить до значних погрішностей оцінки інформаційного трафіку..

МОЖЛИВОСТІ ЩОДО ЗАХИСТУ ТА КОНФІДЕНЦІЙНОСТІ КОРИСТУВАЧІВ У СУЧАСНИХ МЕСЕНДЖЕРАХ

Калужінова А.С.
Харківський національний університет внутрішніх справ, Харків, Україна

Із розвитком інформаційних технологій, спілкування все частіше відбувається у режимі онлайн. Це стає все більш зручнішим завдяки появі та удосконаленню певних апаратних та програмних компонентів, що у поєднанні здатні передавати необхідні об'єми інформації, швидко долаючи дистанцію між співрозмовниками. Окрім функціональних можливостей, що надає прогрес, з'являються відповідні загрози, що становлять особливу небезпеку у контексті збереження, обробки та поширенні чутливих даних. Хоча не для кожного питання безпеки та конфіденційності є першочерговими під час здійснення дій у мережі або на пристроях, оскільки можуть потребувати попереднього рівня обізнаності та навіть ускладнювати процес взаємодії, але іноді користувачі всерйоз готові розглядати альтернативи навіть для зручних та звичних інструментів, якщо виникають підозри у їх ненадійності.

Рівень відкритості вихідного коду часто є однією із перших характеристик, на яку звертають увагу потенційні користувачі при виборі застосунків. Кожен месенджер має свою політику стосовно цього питання: розробники деяких із них надають повний доступ до сирцевого коду всіх компонентів, чим заслуговують напідвищену довіру спільноти, деякі частково, наприклад тільки до протоколу шифрування, деякі притримуються повної закритості, обгрунтовуючи це найкращим варіантом для ускладнення пошуку та експлуатації вразливостей сторонніми особами, або іншими, зокрема юридичними, аспектами. Важливою є можливість активації багатофакторної автентифікації, оскільки наразі, це ефективний спосіб захисту облікових засобів та запобігання втрати даних, що генеруватимуться у процесі спілкування та взаємодії з застосунком чи веб-інтерфейсом. Наявність протоколів шифрування та їх спроможності іноді стають вирішальними під час вибору програмного забезпечення для обміну повідомленнями, оскільки є основним, і за звичай ефективним, щодо звичайного користувача, аргументом, але все менш ключовим у корпоративному середовищі, зокрема завдяки, набираючої популярності, моделі нульової довіри. Наразі переважна більшість месенджерів підтримує наскріз не шифрування, принаймні як опцію секретних чатів, що перешкоджає перехопленню та доступу третіх осіб. Якими б характеристиками не володів той чи інший застосунок, безпека та конфіденційність залежить першочергово від самого користувача, його обізнаності та самоконтролю над даними, які він зберігає, опрацьовує та поширює.Технічні можливості щодо захисту у програмному забезпеченні для обміну повідомленнями постійно удосконалюються, але у випадках компрометації на рівні апаратних компонентів, операційних систем зводять нанівець старання розробників та напряму загрожують, як безпосередньо власникам облікових записів, так і їх контактам.

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ МЕТОДІВ БОРОТЬБИ ЗІ СПАМОМ

Корнієнко К.А., Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Метою робити є розробка методології проектування ефективної системи захисту інформації, що забезпечує фільтрацію спаму ворганізації.

У доповіді виконаний аналіз різних видів спаму з погляду їх загроз захищеності інформації, а також розглянуті переваги і недоліки відомих підходів до протидії цим загрозам. Робиться висновок про необхідність розробки нової архітектури системи протидії розповсюдженню спаму, алгоритмів фільтрації, що дозволяють більш ефективно, в порівнянні з існуючими системами,забезпечувати ФС. Виконаний аналіз основних потоків інформації в системі обробки повідомлень. Проаналізований вплив спаму на доступність і цілісність інформації. Виконаний порівняльний аналіз переваг і недоліків спам-фільтрів, що виконують централізовану ірозподілену фільтрацію. Розглянуто три основні можливі способи формування БЗ корисних повідомлень і спаму для фільтрів, що здійснюють централізовану фільтрацію. Реалізація розробленої концепції в організаціях дозволяє підвищити точність класифікації електронних повідомлень на різних рівнях ієрархії системи фільтрації і забезпечити цілісність і доступність інформації в рамках прийнятої в організації політики безпеки.

РОЗРОБКА СИСТЕМИ ТЕСТУВАННЯ FLASH-НАКОПИЧУВАЧА ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ ІНФОРМАЦІЇ

Курилов Д.О., Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Мета доповіді – детально вивчити види діагностики, відновлення та тестування Flash-накопичувача, зробити відповідні висновки та створити програмну систему тестування Flash-накопичувача. Аналіз методів тестування зовнішніх накопичувачів показав можливість використання різних підходів, що дозволяють в тій чи іншій мірі підвищити ефективність процесу. Наведемо приклади різних підходів тестування флеш-накопичувачів, використовуваних в процесі створення програмної системи тестування. **Лінійне читання**. Тестування поверхні в LBA адресації. Призначено для максимально швидкої і точної діагностики стану поверхні. Під час тестування весь адресний простір розбивається на блоки однакової довжини. **Випадкове читання.** Тестування поверхні, коли адреси блоків видає генератор випадкових чисел. Діапазон можна задати у вигляді кордонів LBA. При цьому також вимірюється час доступу до кожного блоку, але на відміну від лінійного читання, воно буде більше. У доповіді досліджені сучасні програми відновлення Flash-накопичувача та розроблена програма тестування Flash-накопичувача.

ПРОБЛЕМАТИКА ЦИФРОВИХ ДОКАЗІВ В ЕЛЕКТРОННІЙ КОМУНІКАЦІЙНІЙ МЕРЕЖІ

Мерзлікін А.В.
Харківський національний університет внутрішніх справ, Харків, Україна

При роботі з цифровими доказами наступні принципи: законності, цілісності даних, документування процесу, експертної підтримки, відповідної фахової підготовки, розумної обережності.

Окремо слід звернути увагу стосовно дослідження цифрових доказів обґрунтовується тим, що в межах як слідчої, так і судової практики, учасниками кримінального провадження під час підтвердження власного алібі, здійснюється посилання на їх взаємодію з електронними системи, розташування яких є відмінним від місця вчинення конкретного кримінального правопорушення. Серед останнього наводяться випадки користування мобільним телефоном, авторизація у різних електронних системах, потрапляння у зону знаходження камер відеоспостереження, праця з персональним комп'ютером тощо.

Особливість цифрових доказів полягає в тому, що вони можуть змінюватися або бути знищені швидше, ніж традиційні докази.

Робота з доказами в цифровій формі має деякі особливості, порівняно з класичними доказами, такими як паперові документи чи свідчення свідків. Серед них:

- Висока швидкість передачі, копіювання та зберігання інформації.
- Ризик маніпуляцій, зміни та фальсифікації даних.
- Потреба використовувати спеціалізовані технічні засоби та методи для збору, аналізу та оцінки доказів.

Робота з доказами в цифровій формі стає все більш актуальною у сучасному світі.

Це вимагає від правоохоронних органів та судових інстанцій адаптації до нових технологій та особливостей роботи з цифровими доказами. Дотримання принципів законності, достовірності та конфіденційності є ключовими для забезпечення якісного збору, аналізу та використання доказів в цифровій формі.

Список літератури

1. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів: ДСТУ ISO/IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978;

2. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод.реком. за ред. О.В. Корнейка. Вид.2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.;

3. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.*2013.Вип.5.С.256-260.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО СТВОРЕННЯ БЕЗПЕЧНОЇ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ ЗА ТЕХНОЛОГІЄЮ WI-FI

Сімора Ю.В., Можаєв М.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Сьогодення важко уявити без існування безпровідного зв'язку. Сфери діяльності людства дедалі тісніше переплітаються з інформаційними технологіями, зокрема й з засобами безпровідного зв'язку, який, в свою чергу, дає можливість інформаційним технологіям бути мобільними, не залежати від конкретного місця перебування та бути доступними будь-де та будь-коли.

Безпровідне середовище передачі є спільним для усіх вузлів мережі, тому для забезпечення рівноправного доступу до фізичного середовища використовуються конкурентні методи доступу. В умовах конкуренції та використання спільного середовища суттєвий вплив на ефективність роботи безпровідних мереж мають процеси, які відбуваються на підрівні доступу до фізичного середовища. Незважаючи на ряд проблем, таких як недостатня керованість і надійність, складність прогнозування пропускної спроможності, доступної абонентам та інші, бездротовим технологіям немає альтернативи у таких застосуваннях як системи керування бойовими діями, інформаційні інфраструктури при надзвичайних ситуаціях (цунамі й землетрусах) та ін.

Метою даної доповіді є підвищення продуктивності бездротової комп'ютерної мережі підприємства щодо передавання інформації та доставки контенту в умовах збільшення його обсягів на основі вдосконалення методів передавання потоків навантаження в інфокомунікаційних системах.

Один з підходів до проектування бездротових комп'ютерних мереж, розглянутий у цій роботі, базується на апріорно обліку кількості бездротових абонентів і їхніх вимог до пропускної здатності при вирішенні задачі розподілу точок доступу для покриття обслуговується зони.

Запропонований метод проектування враховує такі параметри: площа приміщення; прогнозована кількість користувачів мережі; мінімальна пропускна здатність, яка повинна бути забезпечена для кожного користувача; продуктивність конкретного вузла в мережі; кількість мережевих точок; максимальний потік даних в системі; -швидкість потоку даних для кожної станції в вузлу мережі.

Запропонована програмна реалізація забезпечує можливість розрахунку необхідної кількості точок доступу і радіусу покриття кожної точки, близькі до оптимального, для забезпечення необхідної продуктивності для проектованої бездротової мережі. При цьому забезпечується повне покриття зони обслуговування, що виключає «мертві зони», а також знижує взаємну інтерференцію і перешкоди від сусідніх точок доступу.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОТИДІЇ ФАЛЬШУВАННЮ ІНФОРМАЦІЇ У КІБЕРСФЕРІ

Семко Р.С.
Харківський національний університет внутрішніх справ, Харків, Україна

Фальшування інформації або дезінформація явище доволі старе, яким людство користувалося переважно в військових або політичних цілях. Однак лише з появою глобального павутиння воно змогло набрати такого сильного впливу на повсякденне життя. Стрімкий потік інформації, який щодня, щогодини обрушується на звичайну людину, впливає на її світогляд.

Метою доповіді є розробка рекомендацій, що дозволить виявляти та протидіяти викривленню інформації у глобальній веб-мережі.

В доповіді наводяться аналіз процесів створення і поширення дезінформації та рекомендацій протидії фальшуванню інформації, як на державному рівні, так і на рівні самонавчання , що дозволить підвищити соціальну обізнаність громадян у даній сфері і збереже громадян від можливих інформаційних загроз в кіберсередовищі, що являється доволі актуальним на тлі сучасних подій, де ці знання допоможуть зберегти не тільки фінанси, здоров'я, здоровий глузд, а іноді і життя.

РОЗРОБКА ІМІТАЦІЙНОЇ МОДЕЛІ ДЛЯ ВИЗНАЧЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНИХ СИСТЕМАХ

Зарудняк Д.С.
Харківський національний університет внутрішніх справ, Харків, Україна

Метою доповіді є опис розробленої імітаційної моделі яка містить: блок генерації мережного трафіку, призначений для імітації потоку даних у комп'ютерній системі (КС) як на підготовчому, так і на основному етапі функціонування; імітатори захоплення та фільтрації мережного трафіку – імітують відповідні процедури мережевого аналізатора, тобто, виробляють первинну обробку згенерованих блоком генерації даних; блок статистичної обробки; блок зберігання даних; блок перевірки статистичних гіпотез призначений для обробки статистичних портретів шаблонних даних та потоків даних окремих служб та сервісів КС; блок прийняття рішення на підставі результатів перевірки статистичних гіпотез узагальнює та приймає рішення про наявність чи відсутність шкідливого мережевого трафіку та відповідного вторгнення; блок управління здійснює узгодження роботи інших блоків імітаційної моделі та управління основними обчислювальними операціями.

У доповіді визначено, що розроблена імітаційна модель може адаптивно реагувати на поточну ситуацію та за необхідності блокувати підозрілий трафік та розсилати попередження сусіднім вузлам мережі, робочу станцію мережного адміністратора, сервер протоколювання атак тощо.

АНАЛІЗ СИСТЕМ УБЕЗПЕЧЕННЯ ВІДДАЛЕНОГО ДОСТУПУ В РОЗПОДІЛЕНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Коломацький О.А., Чуєв В.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Метою доповіді є аналіз систем убезпечення віддаленого доступу в розподілених обчислювальних системах.

В доповіді наводяться визначення загальних проблем убезпечення віддаленого доступу в розподілених обчислювальних системах, дослідження доступу до розподілених обчислень на віртуальному кластері та надання рекомендації щодо захисту інформації від вторгнень. Використання додаткового рівня резервування інформації має сенс, ґрунтуючись на попередні твердження, адже це можливість уникнути втрати інформації на кластері даних цілком – чого не передбачає архітектура RAID, зокрема. Окрім того, звертаючи увагу на те, що твердотільним носіям необхідна час від часу процедура поновлення даних, у разі їх втрати, було б логічно в рамках запланованого сервісного обслуговування, або в разі втрати даних робити відповідні поновлення, для всього вузла інформації. У випадку локального катаклізму це також зможе уберегти інформацію від втрати. Наразі відома низка системи віддаленого зберігання даних, які працюють на потенційно ненадійних кластерах даних. Зокрема до таких систем відносять: Facebook‘s codes Hadoop, Google Colossus, Microsoft Azure. Отже, виникає потреба в модифікації існуючих систем резервування та відновлення інформації в віддалених розподілених системах зберігання даних.

РОЗРОБКА КОМПЛЕСНОЇ СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННИХ ВКЛАДЕНЬ В СИСТЕМІ ЕЛЕКТРОННОЇ ПОШТИ

Патьоха П.В.
Харківський національний університет внутрішніх справ, Харків, Україна

Спеціальні рішення захищають комунікацію співробітників та усувають кіберзагрози в системі електронної пошти.

За рахунок впровадження засобів захисту в системі електронної пошти можна досягти таких результатів: знижуються ризики, пов’язані зі збитками для репутації та доходів компанії, атаки на електронну пошту можуть призвести до величезних витрат, збоїв у роботі та інших серйозних наслідків; підвищується продуктивність: надійні рішення для захисту електронної пошти дозволяють компаніям скоротити кількість збоїв у роботі та час простою через кібератаки; забезпечується дотримання законів про захист даних, наприклад, регламенту GDPR.

У доповіді наведено декілька рекомендацій щодо захисту електронної пошти.

АНАЛІЗ ПОШИРЕНИХ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ВЕБ-САЙТІВ ТА МЕТОДІВ ЇХ УНИКНЕННЯ

Сиса А.С., Манжай О.В.
Харківський національний університет внутрішніх справ, Харків, Україна

Веб-сайти стикаються з безліччю загроз в кібербезпеці, які включають, але не обмежуються: атаками розподіленої відмови в обслуговуванні (DDoS), що перевантажують веб-сайт трафіком та роблять його недоступним для звичайних користувачів; SQL-ін'єкціями: зловмисники вводять шкідливі SQL запити, щоб використовувати вразливості в базі даних веб-сайту для отримання несанкціонованого доступу або викрадення конфіденційних даних; Cross-Site Scripting (XSS) атаками, які дозволяють зловмисникам впроваджувати шкідливі сценарії на веб-сторінки, що переглядають інші користувачі; фішинговими атаками, які використовують оманливі електронні листи або веб-сторінки: cross-Site Request Forgery (CSRF) атаками; підробкою запитів на стороні сервера (SSRF) – вразливістю, яка виникає, коли зловмисник може маніпулювати сервером, щоб він надсилав запити до інших ресурсів у внутрішній мережі чи Інтернеті. Щоб підвищити безпеку веб-сайту, вкрай важливо реалізувати комплексну стратегію кібербезпеки, елементи якої наводяться у даній доповіді.

АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ПІДПРИЄМСТВА

Харківський національний університет внутрішніх справ, Харків, Україна

Проблематика застосування методів та систем штучного інтелекту є новим напрямком прикладної науки, який повинен мати ґрунтовну теоретичну деталізацію. Зважаючи на потребу у розвитку інтелектуальних технічних систем, спрямованих на розв'язання найскладніших виробничих завдань, дослідження методів та систем є штучного інтелекту є актуальним напрямом наукових узагальнень та пошуків. **Метою доповіді** є визначення методів оцінки ризиків безпеки підприємства із застосуванням штучного інтелекту та надання практичних рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту. В доповіді розглянуто правові основи застосування технологій штучного інтелекту, проаналізовано методи оцінки стану інформаційної безпеки та надано практичні рекомендації щодо застосування технологій штучного інтелекту для нівелювання ризиків інформаційної безпеки підприємства. Подальші дослідження повинні бути спрямовані на з'ясуванні можливості розподілу методів за напрямками використання та за критерієм ефективності відповідно до пріоритетів, закріплених Концепцією розвитку штучного інтелекту в Україні.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ

Хавіна І.П.
Харківський національний університет внутрішніх справ, Харків, Україна

Захист інформації в автоматизованій системі (АС) – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1].

Метою доповіді є розробка рекомендацій, які дозволять побудувати комплексну систему захисту (КСЗІ) інформації для обробки інформації з різними ступенями захисту, для забезпечення цілісності та конфіденційність в автоматизованій системі громадської організації.

В доповіді наводяться рекомендації щодо створення комплексної системи захисту інформації. Наведена інформація розкриває етапи створення КСЗІ, які розкривають подальшу послідовність дій, для забезпечення безпеки від витоку інформації технічними каналами. Порядок створення КСЗІ в автоматизованій системі громадської організації є єдиним незалежно від того, створюється КСЗІ в АС, яка проектується, чи в діючій АС, якщо виникла необхідність.

Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення АС, визначеними НД ТЗІ 3.7-003-05 [2].

Також перед обранням КСЗІ, слід звернути увагу на комплекс засобів захисту (КЗЗ).

Більш універсальним та доступним КЗЗ, є створення КСЗІ на базі операційної системи Windows 10 Pro. Переваги даного КЗЗ, є бюджетним варіантом та більш легким у налаштуванні та користуванні, як звичайному користувачу так і системному адміністратору. Також використання такого засобу в АС громадської організації є доступним для будь-якого тримача інформації. Але може не задовольнити в надійності захисту інформації з більш високим грифом обмеження доступу.

У разі необхідності КЗЗ для інформації з грифами вище ніж «Для службового користування», рекомендується обрати засоби з підвищеною безпекою, наприклад: Лоза-1 з рівнем підвищеною безпекою [3].

Список літератури

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

2. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

3. Система захисту інформації Лоза™-1, ВЕРСІЯ 4 [Електронний ресурс]. – Режим доступу: http://avtoprom.kiev.ua/avtoprom/ru/content/Sistema-zaschity-informacii-LOZA™-1-versija-4

АНАЛІЗ МОЖЛИВОСТЕЙ ВИЯВЛЕННЯ ФІЗИЧНОГО ВТОРГНЕННЯ ЗЛОВМИСНИКА НА ОБ'ЄКТ ЗАХИСТУ ШЛЯХОМ АНАЛІЗУ WI-FI ПАКЕТІВ

Андреєв І.Ю.
Харківський національний університет внутрішніх справ, Харків, Україна

Важливим аспектом сучасної технології безпеки, а саме можливостями виявлення фізичного вторгнення на об'єкт захисту за допомогою аналізу Wi-Fi пакетів. Зловмисники постійно шукають нові шляхи проникнення в системи безпеки, і Wi-Fi аналіз може стати ефективним інструментом в цьому контексті. Безпека об'єктів захисту стала вкрай важливою в нашому сучасному світі. Фізичне вторгнення на об'єкт захисту може призвести до серйозних наслідків, і саме тому ми маємо знати, як захищати себе від таких подій.

Wi-Fi аналіз – це метод вивчення та аналізу бездротового трафіку, який включає в себе моніторинг радіосигналів та бездротових пакетів даних в Wi-Fi мережах. Wi-Fi аналіз може допомогти виявити фізичне вторгнення на об'єкт захисту на різних етапах. По-перше, він дозволяє визначити незаконний доступ до мережі шляхом аналізу мак-адрес. Такий аналіз дозволяє виявити небажаних користувачів, які намагаються отримати доступ до мережі. Для виконання аналізу Wi-Fi пакетів і виявлення фізичного вторгнення існують різноманітні інструменти і програмні засоби, такі як Wireshark, Aircrack-ng та високоточні аналізатори Wi-Fi трафіку. Вони дозволяють докладно вивчати пакети даних та ідентифікувати аномалії. Аналіз Wi-Fi пакетів дозволяє ідентифікувати підозрілі пристрої та з'єднання, а також виявити аномальні зміни у звичайному трафіку.

Однак важливо не тільки аналізувати пакети даних, але й зберігати журнали аналізу та аналізувати їх вміст. Це дозволяє виявити аномалії в діяльності мережі та швидко реагувати на них. Виявлення інсайдерських загроз Wi-Fi аналіз також може бути використаний для виявлення загроз від власних співробітників. Шляхом моніторингу поведінки пристроїв інсайдерів можна вчасно виявити недоброзичливих діячів і запобігти можливим вторгненням.

І, нарешті, розглянемо переваги і обмеження Wi-Fi аналізу для виявлення фізичного вторгнення. До переваг належать швидке виявлення фізичного вторгнення та можливість реагування в реальному часі. Проте існують обмеження, такі як можливість фальсифікації трафіку та обмежена ефективність в захищених мережах. У заключенні, важливо підкреслити, що безпека об'єктів захисту вимагає постійного моніторингу та покращення методів аналізу Wi-Fi для підвищення безпеки. Зловмисники ніколи не сплять, і ми також повинні бути завжди на сторожі.

Список літератури

1. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко Ш.Д. Телекомунікаційні та інформаційні мережі», 2010. https://ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ З РОЗРОБКОЮ БЛОКУ ЗАХИСТУ

Власенко Т.О., Радіонов Р.О.
Харківський національний університет внутрішніх справ, Харків, Україна

На сьогоднішній день методи перехоплення інформації набули вдосконалення та розширення [1, 2]. Однією з таких загроз є перехоплення даних за допомогою проксі-серверів. Проксі-сервери можуть бути налаштовані для прослуховування мережевого трафіку, і в разі недостатнього захисту можуть надати можливість зловмиснику отримати доступ до конфіденційних даних. Ще однією загрозою є перехоплення даних через використання підписаного сертифікату браузера. Це може виникнути внаслідок компрометації самого сертифікату або атак на центри видачі сертифікатів. Атаки цього типу дозволяють зловмисникам встановити довіру до шкідливого сертифікату та отримати доступ до зашифрованого трафіку. Важливо ретельно аналізувати ці методи перехоплення, оскільки вони можуть мати серйозні наслідки для безпеки конфіденційної інформації.

Ефективний захист від перехоплення інформації вимагає комплексного підходу та використання передових технологій та засобів безпеки. Однією з ключових технологій є шифрування даних. Використання сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), гарантує, що дані залишаються конфіденційними під час передачі по мережі. Важливим компонентом є використання віртуальних приватних мереж (VPN), які створюють шифровану тунель для безпечної передачі даних. Крім того, важливо мати механізми для перевірки аутентичності сертифікатів SSL/TLS та виявлення можливих атак з використанням підписаних сертифікатів браузера. Системи моніторингу та аналізу трафіку можуть виявити надзвичайні події.

Розробка надійного блоку захисту від перехоплення інформації є невід'ємним кроком у забезпеченні безпеки мережевого оточення.

Висновок. Дослідження методів та засобів перехоплення інформації та розробка блоку захисту є ключовими аспектами для забезпечення безпеки мережі та захисту конфіденційної інформації. У світі, де обмін даними відіграє критичну роль, ефективні засоби та технології захисту є невід'ємними для забезпечення безпеки та довіри.

Продовжуючи дослідження та впровадження нових заходів безпеки, ми зможемо створити мережеве середовище, яке залишається надійним та захищеним у цифровій епохі.

Список літератури

1. Комп'ютерні мережі. Таненбаум Е. С., Уезеролл Д. С.792–793.
2. Куперштейн Л. М., Кренцін М. Д. Аналіз тенденцій розвитку пірингових мереж. Вісник Хмельницького національного університету. 2021. № 4. С. 25–29.

ЕВРИСТИЧНИЙ АНАЛІЗ ЯК МЕТОД ВИЯВЛЕННЯ НЕБАЖАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Діденко М.С.
Харківський національний університет внутрішніх справ, Харків, Україна

Традиційні методи виявлення шкідливого програмного забезпечення часто виявляються неефективними проти нових або модифікованих загроз, оскільки зосереджуються на пошуку вже відомих сигнатур шкідливих об'єктів. У таких ситуаціях евристичний аналіз може стати ключовим інструментом або додатковим рубежем захисту. Евристичний аналіз застосовується для пошуку команд та інструкцій, які зазвичай непритаманні етичному програмному коду. Наприклад, він може виявляти команди для доставки корисних даних, які часто маскуються під виглядом троянського коня, або є такими, що використовуються для розповсюдження вірусів [1]. Рішення для захисту від небажаних програм використовують два методи евристичного аналізу [2]: статичний, де здійснюється зворотне проєктування або декомпіляція вихідного коду програми, подальше його зіставлення із раніше відомим програмним забезпеченням у евристичних базах даних; динамічний, де відбувається ізоляція підозрілого виконуваного файлу у окреме контрольоване віртуальне середовище, його запуск та детальне спостереження.

Рішення, що базуються на евристичному аналізі, попередньо потребують детальних налаштувань. Застосування такого захисту у режимі реального часу може суттєво впливати на продуктивність середовища виконання, оскільки, як статичний, так і динамічний, методи потребують накладних ресурсів, особливо це може бути помітним при роботі із файлами великого обсягу або такими, що активно змінюються у розмірах. За можливості та відповідно до наявної політики інформаційної безпеки варто розглядати додавання цих елементів у виключення. Евристичний аналіз є ефективним засобом для виявлення поліморфних вірусів та загроз нульового дня [2] оскільки не спирається на перевірки гешу, що є невідомим у цьому контексті. Важливо регулярно оновлювати евристичні бази аби зменшити рівень хибних спрацювань та отримувати актуальні моделі поведінки загроз.

Хоча переважно сучасні системи захисту містять інструменти із декількома методами одночасно, комбінують їх використання у залежності від конкретних профілів, але все більше уваги приділяється адаптивним аспектам, оскільки складність програмного забезпечення невпинно зростає, а кіберзлочинці знаходять нові способи якнайдовше приховувати свою активність.

Список літератури

1. FORTINET [Електронний ресурс]. – What Is Heuristic Analysis? – Режим доступу: https://www.fortinet.com/fr/resources/cyberglossary/heuristic-analysis.

2. TechGenix [Електронний ресурс]. – What Is Heuristic Analysis and Why Is It Important for Cybersecurity? By Shweta Shetty / November 14, 2022. – Режим доступу: https://techgenix.com/heuristic-analysis-cybersecurity.

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ

Півоварчук О.В., Хавіна І.П.
Харківський національний університет внутрішніх справ, Харків, Україна

Сучасний світ інформаційних технологій та процесів синхронно розширює можливості бізнесового світу, відкриває нові сфери діяльності комерційних підприємств, вдосконалює шляхи їх розвитку, одночасно й збільшуючи їх інформаційну вразливість та, як наслідок з'являються фінансово-економічні ризики.

Збереження інформації від витоку - це невід'ємна умова для стабільного функціонування та розвитку комерційної організації.

Створення комплексної системи захисту інформації є єдиним шляхом для виконання цієї умови.

Комплексна система захисту інформації – сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від витоку, розголошення, несанкціонованого доступу.

Метою доповіді є формування алгоритму дій керівника комерційної організації та/чи осіб, відповідальних за безпеку підприємства, при створенні в організації комплексної системи захисту інформації.

У доповіді визначено структуровану сукупність організаційних та інженерно-технічних заходів, які направлені на забезпечення захисту цінної для підприємства інформації від її знищення, спотворення.

Основними з таких заходів являються такі [1–3]:

- вивчення задач підприємства, сфери та особливостей його діяльності, організаційно-штатної структури;
- формування переліку відомостей, які не підлягають розголошенню, визначення об'єктів захисту;
- розробка моделей загроз, порушника та політики безпеки організації;
- створення та впровадження нормативно-правових, організаційних, інженерних, технічних, програмно-апаратних систем захисту;
- моніторинг та контроль за впровадженими системами захисту, їх обслуговування та корегування відповідно до поточних та прогнозованих змін на охоронюваних об'єктах.

Список літератури

1. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

2. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

3. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

РЕКОМЕНДАЦІЇ ЩОДО ДОТРИМАННЯ ПРАВОВИХ НОРМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Семенов М.В.
Харківський національний університет внутрішніх справ, Харків, Україна

Метою доповіді є наведення рекомендацій щодо дотримання правових норм захисту персональних даних. В доповіді наводяться рекомендації щодо дотримання правових норм захисту персональних даних, а саме: дотримання законодавства; мінімізація даних; шифрування персональних даних; контроль доступу та аутентифікація; антивірусний та антишпигунський захист; навчання та свідомість персоналу; моніторинг та аудит; реагування на порушення; постійне вдосконалення.

Отже, захист персональних даних - це завдання, яке вимагає серйозної уваги та відповідальності. Необхідно пам'ятати, що захищає персональних даних - це не лише правовий обов'язок, але й етична відповідальність перед особами, чиї дані ви обробляєте.

ДОСЛІДЖЕННЯ ПРИНЦИПІВ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ «1» З РОЗРОБКОЮ РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ ПАРОЛІВ ДОСТУПУ

Снігур Ю.Д., Горелов Ю.П.
Харківський національний університет внутрішніх справ, Харків, Україна

Розробка та впровадження комплексної системи захисту інформації в автоматизованій системі класу «1» включає такі основні етапи: обстеження об’єкта інформаційно-телекомунікаційної системи класу «1» (окремий комп’ютер) та формування акту обстеження; розробка технічного завдання на КСЗІ, погодження його з Держспецзв’язку України (у разі необхідності); проектування КСЗІ; розробка організаційних документів та підготовка розпорядчих документів, необхідних для створення та впровадження КСЗІ; впровадження КСЗІ; оцінка захищеності інформації від витоку каналом, розробка програми і методики випробувань КТЗІ, атестація КТЗІ у разі, коли захисту підлягає інформація 2 або 3 категорії; супровід КСЗІ на етапі проведення державної експертизи.

Головна перевага парольної ідентифікації - простота і звичність. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин вразливості комп’ютерних систем до спроб несанкціонованого доступу (НСД).

АНАЛІЗ СИСТЕМ ТА МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ МЕРЕЖІ

Амельницька А.М.
Харківський національний університет внутрішніх справ, Харків, Україна

Система виявлення вторгнень (англ. Intrusion Detection System, IDS) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Їх можна класифікувати таким чином: за характером відповідної реакції: пасивні; активні; гібридні; за методиками аналізу: статистичні СВВ; сигнатурні СВВ; гібридні СВВ; за рівнем виявленням атак: NIDS; GrIDS; OIDS; HIDS. На сьогоднішній день виділяють і рекомендують до застосування, в тому числі, і при побудові системи захисту три групи методів виявлення атак: сигнатурні методи; методи виявлення аномалій; комбіновані методи. Загалом, слід зазначити, що системи виявлення вторгнень допомагають виявити потенційні атаки, які можуть включати в себе вторгнення в мережу, спроби несанкціонованого доступу до системи тощо. Вони відіграють важливу роль у забезпеченні безпеки інформаційних систем та мереж, допомагаючи вчасно реагувати на загрози, попереджати атаки та виявляти їх.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПОБУДОВИ ПРОГРАМНОЇ СИСТЕМИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

Тихоненко В.Д., Волков А.В., Можаєв М.О.
Харківський національний університет внутрішніх справ, Харків, Україна

В доповіді розглянуто алгоритми, які вбудовують приховані дані в області первинного зображення. Їх перевага полягає в тому, що для вбудовування немає необхідності виконувати обчислювально складні і тривалі перетворення зображень. Проаналізована система приховування даних в графічних файлах, як і люба інша система складається з програмної та апаратної частини, при цьому програмна частина за звичай інсталюється в комп'ютерну систему, а апаратна частина може складатися зі звичайних (персональна ЕОМ) обчислювальних пристроїв, та спеціалізованих обчислювальних і периферійних пристроїв (спецпроцесори, принтери, сканери, планшети та інш.).

Однією з основних складових даної системи є підсистема прийому, обробки інформації та формування контейнеру.

В залежності від професійної діяльності абонентів та технічної направленості творчого процесу джерелами даних, які необхідно захищати можуть бути цифрові фотоапарати, відеокамери, сканери та інші цифрові пристрої. Формування контейнеру може здійснюватись по будь якому з алгоритмів створення та обробки зображення, наприклад алгоритму формування зображення формату BMP.

РОЗРОБКА СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ GOLANG

Бездрабко М.С., Можаєв О.О.
Харківський національний університет внутрішніх справ, Харків, Україна

Системи відеоспостереження у теперішній час є досить популярним пристроїм, який забезпечує безпеку будь-якого об'єкту.

Тому забезпечення якісного функціонування таких систем є безумовно актуальною задачею.

Метою даної доповіді – розробка системи відеоспостереження на Golang, а також оголошуються завдання дослідження.

Для досягнення цієї мети у даній доповіді проведено аналіз раціональності вибору мови програмування Golang для розробки системи відеоспостереження.

Аналізуються переваги, цієї мови, такі як висока продуктивність завдяки багатопотоковій обробці, швидкість розробки завдяки простоті мови та зручному стандартному пакету бібліотек, а також масштабованість для розширення системи.

Наводяться результати порівняльного аналізу Golang з альтернативними мовами програмування і наводиться аргументація вибору.

У подальшому був проведений аналіз сучасних рішень у галузі відеоспостереження. В його результаті були виділені сильні та слабкі сторони існуючих систем, щоб визначити прогалини, які наша система може заповнити. При цьому робиться акцент на технологічних тенденціях і можливостях використання нових технологій, таких як штучний інтелект та машинне навчання.

В доповіді запропоновано використовувати архітектура системи відеоспостереження на основі Golang**.** Описується загальна архітектура системи відеоспостереження, включаючи компоненти, їх функції та взаємодію. Пояснюється вибір розподіленої архітектури для високої доступності та масштабованості.

Визначаються методи зберігання відеоданих та система взаємодії з камерами та серверами.

В результаті проведених досліджень, запропоновані реалізації архітектури системи відеоспостереження на основі Golang, що дозволить суттєво покращити якість функціонування таких систем.

В доповіді розглядаються можливості подальшого розвитку системи, включаючи розширення функціоналу та інтеграцію нових технологій.

Список літератури

1. Петров, А. В. Дослідження та розробка системи відеоспостереження за допомогою мови програмування GoLang / А. В. Петров, В. А. Сидоренко, О. М. Пушкар // Вісник НТУ "ХПІ". - 2021. - № 1(147). - С. 153-159.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Кравченко В.В., Хавіна І.П.
Харківський національний університет внутрішніх справ, Харків, Україна

Оцінка ефективності систем захисту інформації (СЗІ) актуальна для порівняльного аналізу та оптимізації цих систем.

Серед показників ефективності СЗІ, виділяють ймовірнісні показники, які описують надійність, та економічні, що оцінюють можливі економічні збитки та витрати [1].

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність завданням на створення системи захисту.

Зараз не існує повноцінної методики, яка б враховувала: важливість ресурсів, що захищаються; інтенсивність та рівень загроз, що впливають на систему; зниження рівня загрози системою захисту; сумарний рівень загрози, що впливає на систему з використанням системи захисту [2].

Метою роботи є ознайомлення з основними підходами для оцінки ефективності систем захисту інформації та визначення їх переваг і недоліків.

В доповіді наводиться методика оцінки ефективності функціонування системи ЗІ за моделлю з повним перекриттям загроз та модель, що заснована на матриці знань інформаційної безпеки та об'єднує складові блоки інформаційної системи за принципом кожен з кожним.

Відзначено, що застосовані методи дозволяють оцінити ризик для інформації без використання СЗІ.

Модель процесу захисту інформації з повним перекриттям загроз потребує опису трьох основних множини: множина елементів ІС, що захищаються; множина механізмів захисту та при цьому кожній уразливості відповідає набір бар'єрів; множина загроз безпеки.

Розглянутий підхід не розкриває зв'язків інформаційної системи, не дає змоги адаптуватися у режимі реального часу.

Використання матриці знань дозволяє локалізувати місця в системі захисту та розробити план заходів по усуненню недоліків систем захисту інформації.

Список літератури

1. Дудикевич В. Б. Проблеми оцінки ефективності систем захисту / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник НУ "Львівська політехніка". – 2015 – № 741. Автоматика, вимірювання та керування. – С. 118-122.

2. Опірский І.Р. Проектне моделювання конфлікту загроз з комплексною системою захисту інформації в інформаційних мережах держави / І.Р. Опірський // // Науковий вісник НЛТУ України. – 2015. – Вип. 25.9 – С. 322 – 327.

ДОСЛІДЖЕННЯ СТРАТЕГІЙ ЗАХИСТУ ІНФОРМАЦІЇ

Задорожний Я.О., Хавіна І.П.
Харківський національний університет внутрішніх справ, Харків, Україна

Захист інформації являє собою складні, але потрібні заходи, які направлені на збереження конфіденційності, цілісності та доступності інформації. В сучасному світі є багато загроз, починаючи від людини закінчуючи стихійними лихами, які можуть дуже сильно нашкодити цифровому світу. Тому потрібно швидко і вдало реагувати на потенційні загрози.

А для того, щоб якомога ефективніше і без особливих наслідків виходити з тієї чи іншої ситуації, у тримача інформації, а це може бути людина, компанія або держава, має бути план. Або, іншими словами, стратегія захисту інформації.

Стратегія захисту інформації – це цілеспрямовані заходи захисту інформації, які передбачають усвідомленість в потенційних загрозах, протидія цим загрозам та наслідкам від них, використовуючи доступні ресурси.

На різні загрози можна і потрібно реагувати по різному. Тому може існувати декілька стратегій захисту.

Метою доповіді є дослідження стратегій захисту інформації, їх огляд, порівняння, ресурсозатратність, результативність в різноманітних викликах інформаційного простору.

В доповіді наводяться приклади стратегій захисту інформації в державному секторі безпеки, як вони формулюється, згідно з економічною та соціальною політикою країни.

Також не забувається геополітична ситуація у світі. Кожна державна установа або країна при складані стратегії враховує власні потреби, ресурси та потенційні загрози.

Вираховуються патологічні втрати, та можливості завадити цьому.

Може розглядатися ситуація, в якій треба протистояти загрозі Нульового дня.

Суть організації стратегії захисту інформації визначається як пошук оптимального компромісу між необхідністю використання конкретних засобів захисту і наявними ресурсами для реалізації цього захисту.[1]

Список літератури

1. Хошаба О. М. Захист інформації в системах електронного урядуван-ня. Електронне урядування та електронна демократія : навч. посіб. 13-те вид. Київ, 2017. Т. 13 : Захист інформації в системах електрон-ного урядування. С. 14. URL: https://old.suitt.edu.ua/wp-content/uploads/2018/05/Part_013_Feb_2018.pdf (дата звернення: 06.10.2023).

ПРЕДСТАВЛЕННЯ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Ковтюх В.А.
Черкаський державний технологічний університет, Черкаси, Україна
Стабецька Т.А.
Черкаський національний університет ім. Богдана Хмельницького, Черкаси, Україна

На сьогоднішній день криптографічний захист інформації залишається одним із найважливіших способів забезпечення безпеки інформації в комп'ютерних системах та мережах. Вчені багатьох наукових досліджень показали, що одним з найперспективніших напрямів розвитку криптографії є поєднання криптології та комп'ютерної інженерії. Він полягає у розширенні спектру спеціалізованих операцій криптографічного перетворення, які формуються з елементарних функцій криптоперетворення. Результати попередніх досліджень [1,2] дали можливість знайти повні набори елементарних функцій та провести розрахунок кількості елементарних функцій в залежності від розрядності. Також в [3], було здійснено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації. Проте в даних роботах відсутній єдиний підхід до представлення знайдених функцій.

Метою доповіді є встановлення оптимального єдиного представлення для груп трирозрядних елементарних функцій, який дозволить використовувати операції, утворені на основі елементарних функцій з різних груп, для криптографічного перетворення інформації.

У доповіді наводиться спосіб представлення елементарних функцій криптографічного перетворення інформації у вигляді поліномів Жегалкіна. На основі такого представлення сформульовано правила синтезу операцій криптоперетворення, які можна використовувати для вдосконалення існуючих криптоалгоритмів [4].

Список літератури

1. Бабенко В.Г., Рудницький С.В., Мельник Р.П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Теоретичний і науково-практичний журнал інженерної академії України «Вісник інженерної академії України»* – К. «Інтерсервіс». 2012. Вип. 3. С. 77–79.

2. Бабенко В. Г., Рудницький С.В., Мельник Р.П. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку.* 2012.Т.2. № 1. С. 170–173.

3. Бабенко В.Г., Мельник О.Г., Стабецька Т.А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації: наук. журнал*. Київ: НАУ, 2014. Т.20. №2. С.143-147

4. Криптографическое кодирование: коллективная монография / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240с.

МЕХАНІЗМИ ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ НЕСИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ СЕТ-ОПЕРАЦІЙ

Лада Н.В., Головняк Д.В., Сапожніков С.К.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

За останні роки все більше наукових досліджень спрямовується на розвиток теоретичних і практичних аспектів розвитку кібербезпеки [1].

Пошук інноваційних рішень для вирішення сучасних проблем криптографічних систем захисту інформації призвів до популяризації теорії СЕТ-шифрування [2].

Однак удосконаленню методів побудови інформаційних систем та інформаційних технологій на основі несиметричних операцій криптографічного кодування, які забезпечать моделювання процесів криптографічного перетворення інформації, а також дослідженню механізмів їх практичної реалізації приділено недостатньо уваги.

Метою доповіді є представлення механізмів практичної реалізації груп несиметричних двохоперандних СЕТ-операцій за рахунок перестановки кортежів несиметричних одноопераднних СЕТ-операцій та перевірка спроможності їх реалізації.

Результати застосування даних механізмів дозволять автоматизувати синтез операцій та груп несиметричних двохоперандних операцій, що в свою чергу забезпечить покращення характеристик криптоалгоритмів.

В доповіді наводяться результати розробки і дослідження моделей несеметричних СЕТ-операцій та методи їх синтезу.

Приводяться алгоритми генерації послідовностей моделей несеметричних двохоперандних СЕТ-операцій.

Проводиться оцінка згенерованих послідовностей.

Отримані і наведені результати забезпечують концепцію реалізації несиметричних двохоперандних СЕТ-операцій на основі генерації псевдовипадкових послідовностей даних операцій.

Список літератури

1. Jancarczyk D, Rudnytskyi V, Breus R, Pustovit M, Veselska O, Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits. 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) [Internet]. IEEE; 2020 Sep 17. DOI: 10.1109/idaacs-sws50031.2020.9297067

2. V. Rudnytskyi, I. Opirskyy, O. Melnyk, M. Pustovit The implementation of strict stable cryptographic coding operations Сучасні інформаційні системи Щоквартальний науково-технічнийй журнал – Х.: НТУ «ХПІ» 2019, Т 3, №4 С. 109-114. DOI: 10.20998/2522-9052.2019.3.15

КЛАСИФІКАЦІЯ СЕТ-ОПЕРАЦІЙ

Рудницький В.М., Лада Н.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Мельник О.Г.
Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля, Черкаси, Україна

В наш час розвитку систем мало ресурсної криптографії приділяється значна увага. Одним із перспективних напрямів розвитку мало ресурсної криптографії вважається СЕТ-шифрування. Перші результати досліджень по класифікації СЕТ-операцій наведені в [1].

Метою доповіді є деталізація класифікації СЕТ-операцій для зменшення обсягів статистичних досліджень при побудові систем СЕТ-шифрування за заданими вимогами.

В доповіді наводяться основні результати класифікації СЕТ-операцій, які реалізують впорядковані набори елементарних функцій криптографічного перетворення інформації.

Класифікація елементарних функцій: в залежності від кількості змінних; в залежності від результатів перетворення (прямі, обернені); в залежності від фізичного змісту перетворення (фізичний зміст перетворення визначається на дослідженням процесу реалізації моделі елементарної функції); в залежності від складності реалізації перетворення.

Класифікація СЕТ-операцій. В залежності від повноти групи СЕТ-операцій діляться на базові операції, поєднання базових операції і операцій перестановки, поєднання базових операції і операцій інверсії; поєднання базових операції, операцій перестановки і операцій інверсії. В залежності від результатів перетворення діляться на прямі і обернені, симетричні і несиметричні, визначені і псевдовипадкові. В залежності від фізичного змісту елементарних функцій можна поділити на матричні операції, розширені матричні операції, операції які керуються інформацією (операції перестановки, що керуються інформацією, операції перетворень що керуються інформацією), операції змішаного фізичного змісту. В залежності від кількості операндів операції діляться на одноопернадні і багатоопернадні. Богатоопернадні операції діляться на операції з постійною, або плаваючою розрядністю перетворення; на симетричні, або несиметричні операції; на операції які дозволяють, або не дозволяють перестановку операндів. В залежності від сфери застосування: для потокового або для блокового шифрування; для мало ресурсної криптографії.

Список літератури

1. Бабенко Віра. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / Віра Бабенко, Ольга Мельник, Руслан Мельник // Безпека інформації: наук. журнал. – Київ : НАУ, 2013. – Том 19. – № 1. – С. 56–59. https://jrnl.nau.edu.ua/index.php/Infosecurity/issue/view/220.

УНІФІКАЦІЯ ОПИСУ МОДЕЛЕЙ ОПЕРАЦІЙ ДЛЯ СЕТ-ШИФРУВАННЯ

Рудницький В.М., Ларін В.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Мельник О.Г.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Черкаси, Україна

Одним з перспективних напрямків розвитку мало ресурсної криптографії є СЕТ-шифрування. Основною перевагою СЕТ- шифрування вважається можливість створення технології побудови шифрів з заданими характеристиками [1]. На сьогоднішній день в теорії СЕТ-шифрування класифіковано лише 3Сі-квантові СЕТ-операції [2]. Слід відмітити, що класифіковані групи операцій, описуються за допомогою різного математичного представлення [3]. Лише застосування дискретно-алгебраїчного представлення [3] забезпечує уніфікований опис СЕТ-операцій, але приводить до збільшення складності моделей, складності реалізації, і ускладнює їх сприйняття.

Метою доповіді є обговорення можних ливості вдосконалення дискректо-алгетраїчного представлення СЕТ-операцій, для уніфікації математично апарату і забезпечення можливості зменшення складності їх опису.

Для уніфікації опису моделей запропоновано використати модифікації ситуаційного опису подій [4], адаптувавши його до дискретних подій. Елементарна функція $f = (f_2)(f_1)(f_3)$ представляє собою дискретне перетворення в якому нульовий результат реалізації f_1 приведе до виконання функції f_2, а одиничний до f_1. Використання заданого опису дозволяє досягти поставленої мети, спростити реалізацію елементарних функцій і СЕТ-операцій.

Список літератури

1. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing symmetric operations of cryptographic information encoding. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021), Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 182–194. ISSN 1613-0073

2. Бабенко Віра. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / Віра Бабенко, Ольга Мельник, Руслан Мельник // Безпека інформації: наук. журнал. – Київ : НАУ, 2013. – Том 19. – № 1. – С. 56–59. https://jrnl.nau.edu.ua/index.php/Infosecurity/issue/view/220.

3. Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабенко, Р. П. Мельник, С. В. Рудницький // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 1 (21), т. 2. – К. : Центр. наук.-досл. ін-т навігації і управл., 2012. – С. 170–173.

4. Поспелов Д. А. Ситуационное управление : Теория и практика / Поспелов Д. А. – М. : Наука, 1986.

МЕТОД ВИЯВЛЕННЯ ВЗАЄМНОГО БЛОКУВАННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Горбачов В.О., Мантуров Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних системах проблема тупиків часто ігнорується, тому що її розв'язання дуже трудомістке або вимагає розробки спеціальних засобів. Це так для більшої частини комерційного ПЗ, де перезапуск системи є найпростішим і швидким рішенням для розв'язування тупика. Але в той же час широко використовуються розподілені, багатопроцесорні, розраховані на багато користувачів системи, в яких проблема тупика не може бути вирішена простим перезапуском, так як такий перезапуск вимагає великих обчислювальних витрат. Отже проблема тупиків в інформаційних системах є актуальною [1].

Основні задачі роботи: аналіз проблеми тупиків в інформаційних системах, розглянути та зробити аналіз існуючих алгоритмів пошуку та вирішення тупиків, використання теорії алгебри процесів для вирішення задач пошуку та усунення тупиків, запропонувати алгоритм вирішення тупиків та перевірки еквівалентності моделей систем до та після усунення тупиків.

В роботі проведено детальний аналіз проблеми взаємного блокування в інформаційних системах.

Були розглянуті існуючі алгоритми вирішення проблеми. Більшість алгоритмів не пропонує універсального рішення проблеми для систем на стадії розробки та виконання.

У роботі пропонується метод пошуку та рішення взаємного блокування, що складається з двох частин. Перша описує пошук взаємного блокування на стадії проектування. Друга частина містить опис алгоритму пошуку взаємного блокування і модуль, що відповідає за їх вирішення в системах, які вже функціонують. Вирішення взаємного блокування може змінити структуру вихідної моделі та її функціональні особливості. Виходячи з цього, метод передбачає перевірку еквівалентності вихідної моделі системи і моделі, отриманої після рішення тупикової ситуації. Досліджено і формально обґрунтовано використання алгебри процесів як засіб аналізу еквівалентності моделей систем.

Практична значущість роботи полягає в тому, що метод може бути застосований при проектуванні сучасних інформаційних систем, таких як системи реального часу.

Список літератури

1. Yaloveha V., Hlavcheva D., Podorozhniak A. Usage of convolutional neural network for multispectral image processing applied to the problem of detecting fire hazardous forest areas. *Сучасні інформаційні системи*. 2019. Т. 3, № 1. С. 116–120. DOI: https://doi.org/10.20998/2522-9052.2019.1.19

ОСНОВНІ ЗАГРОЗИ ВЕБ ЗАСТОСУНКІВ

Куценко Д.О., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді аналіз основних загроз в веб застосунках.

Веб застосунки використовуються для різних потреб суспільства, поступово збільшується використання нових технологій розробки та створення більш масштабних технічних рішень: інтернет магазинів, e-comerce платформ, тощо.

Технічний розвиток веб застосунків у свою чергу зумовлює виникнення нових загроз інформаційної безпеки, саме тому необхідно постійно вдосконалювати методики та алгоритми захисту веб застосунків з метою подальшого виявлення та протидії загрозам.

Серед основних видів загроз особливо необхідно приділити увагу наступним типам загроз на веб застосунки, а саме: міжсайтовий скриптинг, SQL ін'єкції, відмова в обслуговуванні, обхід каталогів, та впровадження команд [1]. Найбільш поширеними серед них у наш час є міжсайтовий скрипінг, SQL ін'єкція, та відмова в обслуговуванні.

Міжсайтовий скрипінг дозволяє зловмисникові впроваджувати шкідливий код через веб-сайт в браузери інших користувачів. SQL-ін'єкції дозволяють зловмисникам виконувати довільний код SQL в базі даних, дозволяючи отримувати, змінювати або видаляти дані незалежно від дозволів користувача. Відмова в обслуговуванні зазвичай досягається за рахунок наповнення цільового сайту підробленими запитами, так що доступ до сайту порушується для законних користувачів [2].

Обхід каталогів зумовлює отримання доступу до частин файлової системи веб-сервера, зловмисником.

Також існує загроза включення файлу, де користувач може вказати файл для відображення або виконання в даних, переданих на сервер. Атаки з впровадженням команд дозволяють зловмиснику виконувати довільні системні команди в операційній системі сервера.

Для протидії загрозам необхідно дотримуватися основних заходів інформаційної безпеки та користуватися інструментами та алгоритмами виявлення загроз. Загалом, регулярна зміна паролів, відмова від використання застарілих протоколів, налаштування і використання HTTPS/HSTS допоможе захистити інформацію в веб застосунках від основних загроз.

Список літератури

1. List of Attacks / Open Web Application Security Project. URL: https://owasp.org/www-community/attacks/.

2. Top 10 Web Application Security Risks / Open Web Application Security Project. URL: https://owasp.org/ www-project-top-ten

ДОСЛІДЖЕННЯ ЗАСОБІВ БЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ

Єфремов Н.С., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні безпроводові мережі стають все більш популярними. Різні компанії використовують їх все частіше через їхні переваги та сучасні умови життя (пандемія, війна тощо). Популярність локальних безпроводових мереж значною мірою виражається в їх перевагах, таких як мобільність користувача, швидка і проста установка, гнучкість, масштабованість і відносно низька ціна. Єдиною суттєвою проблемою безпроводових мереж є безпека даних. Існує безліч методів та атак, які можуть бути використані проти користувачів безпроводових мереж, зокрема глушіння, прослуховування, людина-посередник, підробка даних. Крім того, з поширенням мобільних пристроїв і публічних точок доступу Wi-Fi витік даних та інші загрози кібербезпеці зросли експоненціально [1].

Метою доповіді є дослідження засобів безпеки безпроводових мереж.

Постійне збільшення використання безпроводових інфраструктурних мереж для бізнес-цілей створює потребу в надійних механізмах безпеки. В роботі проведено дослідження різних типів атак, які можуть поставити під загрозу цілі безпеки (автентифікацію, конфіденційність і цілісність), розглянуто основні засоби безпеки безпроводових мереж, технології запобігання витоку конфеденційної інформації з інформаційних систем та мереж Data Loss Prevention (DLP) [2] та виконано аналіз протоколів безпеки безпроводових мереж, зокрема WEP, WPA, WPA2 і WPA3, описано їхні особливості та недоліки в безпеці.

Таким чином, безпроводова мережа надає численні можливості для зручної та швидкої комунікації, підвищення продуктивності та скорочення витрат в сучасних умовах. Але також змінює загальний профіль ризиків інформаційної безпеки компанії.

На даний момент повністю усунути всі ризики, пов’язані з безпроводовою мережею, неможливо, але можна досягти розумного рівня загальної безпеки шляхом застосування систематичного підходу до оцінки та управління ризиками.

Список літератури

1. Baig Anas. 12 Best Practices for Wireless Network Security [Електронний ресурс] / Anas Baig // GlobalSign. – 2022. – Режим доступу до ресурсу: https://www.globalsign.com/en/blog/12-best-practices-wireless-network-security.

2. Аналіз технологій запобігання витоку інформації / С. Є. Пестєрєва, Д. В. Чеботарьова // Тези доповідей дев’ятої міжнародної науково-технічної конференції «Проблеми інформатизації», 18 – 19 листопада 2021 р., Черкаси – Баку – Бельсько-Бяла – Харків. – 2021. – Том 1. – С. 67.

АНАЛІЗ ЗАГРОЗ НА МЕРЕЖІ РОЗУМНОГО БУДИНКУ

Поддельський В.М., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток телекомунікаційних технологій та впровадження їх у побут, навчання, роботу громадян і суспільства в цілому, поставило нові виклики перед вченими та науковцями ІТ-сфери.

Зокрема, популярна наразі мережа Інтернету речей (IoT), інтеграція якої спрощує велику кількість процесів у побуті та людському житті, окрім полегшення та комфорту, принесла також і небезпеку для баз даних та інформаційних програм. Інтернет речей складається з пристроїв, які генерують, обробляють та обмінюються величезною кількістю критично важливих для безпеки даних, а також конфіденційної інформації, і, отже, є привабливими для різних кібератак [1].

Оскільки, безпекові протоколи IoT складаються з захисту і контролю пристроїв, забезпечення безпечного зв'язку та взаємодії між ними, мають бути розроблені ефективні методи забезпечення кібербезпеки у мережах розумного будинку.

Проте, як зазначено у річному звіті Cisco за 2021 рік, спеціалісти, які впроваджують IoT-системи та забезпечують їх захист, на жаль, мало звертають на увагу на ефективність встановленого захисту [2].

Метою доповіді є дослідження складових технології мереж розумного будинку та аналіз загроз для ефективного функціонування мережі.

В доповіді наведені та описані основні складові технології мереж розумного будинку. Проаналізовані найбільш розповсюджені атаки на мережі розумного будинку.

Крім того, наведені методи запобігання кібератак на мережі IoT-технологій та описані методи подолання наслідків подібних атак.

В результаті роботи доведено, що для захисту від атак на мережі IoT важливо дотримуватися загальних принципів кібербезпеки, таких як використання сильних паролів, регулярне оновлення програмного забезпечення, використання шифрованих мереж, встановлення фізичних засобів безпеки та моніторинг активності мережі.

Також рекомендується ретельно вивчати можливі загрози та використовувати безпечні практики керування системою розумного будинку.

Список літератури

1.S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in the Internet of Things: The Road ahead, Computer Networks, vol. 76, pp. 146-164, 2015.

2. Cisco Cybersecurity Report [Електронний ресурс] // Cisco. – 2021. – Режим доступу до ресурсу: https://www.cisco.com/c/en_ca/products/security/security-reports.html.

АНАЛІЗ РЕЙТИНГУ НАЙБЕЗПЕЧНІШИХ МЕСЕНДЖЕРІВ

Маслакова Н.Ю., Золотарьов В.А.
Харківський національний університет радіоелектроніки, Харків, Україна

За допомогою системи миттєвих повідомлень можна обмінюватися не тільки текстовими повідомленнями, але також зображеннями, звуковими сигналами та відеозаписами. Тому гостро постає питання безпеки особистих даних, телефонних дзвінків, текстових повідомлень та іншої інформації, яку пересилають [1].

Метою доповіді є аналіз найбезпечніших сучасних месенджерів.

До найбезпечніших месенджерів, згідно з дослідженням (рис.1), належать Threema, Wickr, Signal і Wire. Було виявлено, що вони мають високу надійність криптографічних протоколів та алгоритмів. Telegram, Viber, Whatsapp, Facebook Messenger та Discord – не є найбезпечнішими для користувачів. Telegram збирає телефонні номери і ID. Whatsapp, Facebook Messenger та Discord зберігають дані без шифрування.

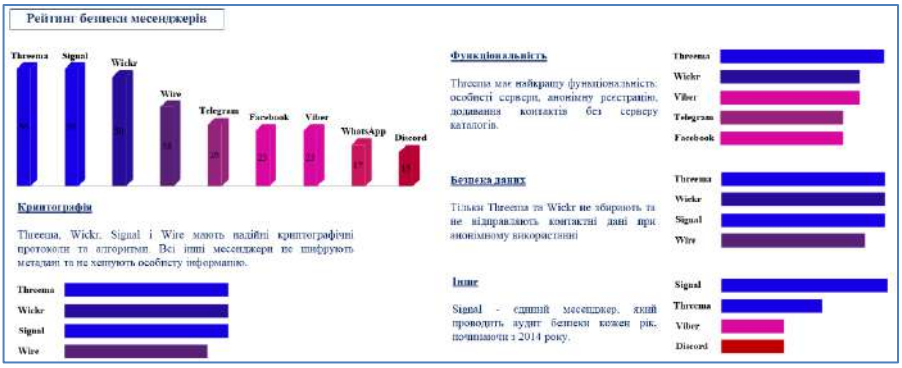

Рисунок 1 – Рейтинг безпеки месенджерів

Згідно з інформацією, найбільш захищеним месенджером у 2023 році є Threema. Він має найкращу функціональність: власні сервери, анонімну реєстрацію та додавання контактів без сервера каталогів. [2]

Список літератури

1. Тетяна Грицик. 11 травня, 2023. Рейтинг найбезпечніших месенджерів [Електронний документ] - Режим доступу: https://ain.ua/2023/05/11/rejtyng-najbezpechnishyh-mesendzheriv-telegram-na-5-misczi/.

2. Маслакова Н.Ю. Дослідження безпеки месенджерів [Електронний документ] Конференція «Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій», Том 4. - Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/d9bf156f-640d-4364-b042-77e4f7ebc832/content.

АНАЛІЗ ВРАЗЛИВОСТЕЙ СУЧАСНИХ МІЖМЕРЕЖЕВИХ ЕКРАНІВ NGFW

Шевчук В.В., Золотарьов В.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні міжмережеві екрани NGFW (Next-Generation Firewalls) необхідні для захисту мережі від вторгнень, атак та несанкціонованого доступу (НСД). NGFW є еволюційним кроком у розвитку традиційних брандмауерів, оскільки надають ширший спектр захисних функцій, зокрема, детальний контроль за даними, що проходять через мережу.

Метою дослідження є аналіз сучасних міжмережевих екранів вразливостей NGFW.

На сьогоднішній день можна виділити наступні основні вразливості сучасних NGFW такі як: DDoS-атаки (Distributed Denial of Service), внутрішні атаки (Insider Attacks), застаріле програмне забезпечення міжмережевого екрану (Outdated Firewall Software), недоліки активації контроля (Failure to Activate Controls), основні протоколи перевірки (Basic Inspection Protocols), неправильна конфігурація обладнання (Improper Configuration).

Аналіз зазначених вразливостей можна здійснити методом оцінювання ризиків NGFW, який включає: ідентифікацію, аналіз та оцінювання потенційних загроз безпеці міжмережевому екрану.

Аналіз допомагає визначити потенційні небезпеки та вразливості, які можуть виникнути: у наслідку неправильної конфігурації; недоліків в проектуванні; атак з боку зловмисників або інших небезпечних факторів.

Оцінити вразливості вручну практично неможливо в сучасних мережевих середовищах, в яких використовується велика кількість типів NGFW.

Отже слід здійснювати їхню перевірку автоматично і періодично.

Під час оцінювання безпеки NGFW слід перевіряти:

контролювання та керування змінами;

фізичну та програмну безпеку пристроїв;

періодичне покращення правил та очищення застарілих політик;

періодичне проведення оцінювання ризиків і вирішення проблем безпеки мережі.

В результаті проведеного аналізу були визначені основні вразливості NGFW екранів, а також виявлені аспекти оцінки аналізу вразливостей та підвищення безпеки цих екранів.

Список літератури

1. Kamara S., Fahmy S., Schultz E.. Analysis of vulnerabilities in Internet firewalls. 2016. Computers & Security 22(3):214-232: https://www.researchgate.net/publication/222543581_Analysis_of_vulnerabilities_in_Internet_firewalls.

2. Rebecca M, Patrick D., National Institute of Standards and Technology // Guide for Conducting Risk Assessments. – 2012. – №1. – С. 17–22.

ЦИФРОВІ АКТИВИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ БЛОКЧЕЙН

Саламатов О.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Цифрові активи стали невід'ємною частиною сучасного цифрового світу. Їх використання надає нові можливості для розробки та впровадження інноваційних рішень в бізнесі та управлінні. Блокчейн-технології відіграють ключову роль в цьому процесі, забезпечуючи безпеку, прозорість та децентралізацію. Цифрові активи – це цифрові ресурси, що мають вартість. Це можуть бути криптовалюти, токени, права на використання певного програмного забезпечення, а також інші види цифрових ресурсів [1]. Вони можуть бути легко передані, збережені або обміняні, що робить їх важливим елементом сучасних інформаційних систем.

Блокчейн – це децентралізована база даних, яка забезпечує високий рівень надійності для транзакцій із цифровими активами [2]. Вона дозволяє користувачам проводити безпечні транзакції без необхідності використання посередників. Блокчейн відіграє ключову роль в управлінні та перевірці прав власності на цифрові активи, що є особливо важливим у світі, де цифровізація постійно зростає.

Метою доповіді є аналіз функціоналу цифрових активів та дослідження інформаційних систем, в яких вони реалізовані. В доповіді наводяться результати аналізу сфер застосування цифрових активів.

Наведені результати показують, що цифрові активи можуть використовуватися в сферах управління, фінансів, права та в IT сфері. Це досягається завдяки властивостям та функціоналу таких активів. Наприклад: наявність усіх даних про актив в базі даних блокчейну забезпечує прозорість при операціях з ним, так як усі дані ще до проведення операції можуть бути перевірені усіма сторонами та блокчейном [2]; можливість реалізувати автоматичні операції з активом в розумних контрактах дає змогу відмовитись від посередників чи інших третіх осіб, задіяних в класичних фінансових чи юридичних операціях [3].

Список літератури

1. Crypto Assets and Cryptocurrency [Електронний ресурс] – URL: https://fcnb.ca/en/investing/high-risk-investments/crypto-assets-and-cryptocurrency.

2. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник у 3 ч. Ч. 1 / П.Кравченко, Б.Скрябін, О.Дубініна – Харків : ПРОМАРТ, 2019. – 452 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/41855.

3. What are Smart Contracts on Blockchain? [Електронний ресурс] – URL: https://www.ibm.com/topics/smart-contracts

ФОРМУВАННЯ СТЕГАНОГРАФІЧНИХ СИСТЕМ НА БАЗІ ДНК ПЕРЕТВОРЕНЬ

Євгеньєв А.М., Савінов Є.І, Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Формування стеганографічних систем на базі ДНК перетворень є актуальним напрямком, який поєднує в собі біологічні та інформаційні технології.

Завдяки її унікальній структурі, ДНК може зберігати величезні об'єми даних у дуже малому просторі. Послідовності нуклеотидів можуть служити кодами для зберігання інформації, роблячи ДНК ідеальним носієм для стеганографії [1].

Інформація може бути перетворена в послідовності ДНК через ряд специфічних алгоритмів. Наприклад, текст чи бінарні дані можна кодувати у вигляді послідовностей ДНК. Крім того, специфічні ДНК перетворення можуть оптимізувати процес зберігання та відновлення даних.

Метою доповіді є проведення аналізу можливості формування стеганографічних систем на базі ДНК перетворень.

Основні аспекти ДНК-перетворень включають визначення оптимальних способів представлення даних у формі ДНК послідовностей, а також розробка методів для їхнього читання та запису.

Врахування особливостей біологічних систем та їх взаємодія з інформаційними технологіями може допомогти у вирішенні численних проблем, пов'язаних із зберіганням та передачею даних.

Як і в традиційній стеганографії, в ДНК-стеганографії можна використовувати методи криптографії для додаткового захисту. Проте, ДНК також презентує унікальні виклики, такі як стійкість до пошкоджень або втрати інформації через мутації [2].

ДНК-стеганографія може знайти застосування в біомедичних дослідженнях для зберігання даних про пацієнтів без розкриття особистої інформації. Інший потенційний застосунок - зберігання великих об'ємів даних в мінімальному просторі.

З розвитком біотехнологій можливості ДНК-стеганографії будуть лише розширюватися та представляє собою перспективний напрямок, який комбінує біологічні та технологічні засади для зберігання інформації. Важливо розуміти її можливості та обмеження, а також розглядати етичні аспекти її використання.

Список літератури

1. Sievierinov O., Evheniev A. (2018). DNA Cryptosystem Using a Simple Replacement. *«Інформаційні системи та технології» ICT-2018*, 389.

2. L. M. Adleman. Molecular computation of solutions to combinatorial problems (англ.) // Science. — 1994-11-11. — Vol. 266, iss. 5187. — P. 1021—1024. — ISSN 1095-9203 0036-8075, 1095-9203

RESEARCH OF PROBLEMATIC ISSUES IN FEDERATED LEARNING OF NEURAL NETWORKS

Zuikov A.V., Ruzhentsev V.I.
Kharkiv National University of Radio Electronics, Ukraine

With the rapid growth of cloud computing, as it becomes increasingly ubiquitous, security threats and vulnerabilities in cloud services have become a major concern for organizations and individuals alike. Previously, security solutions often relied on rule-based systems or manual analysis, which was time-consuming and ineffective in detecting new and complex security threats. Machine learning (ML) techniques, including neural networks (NN), have shown promise in improving the accuracy and efficiency of security analysis in cloud environments [1]. Combining different data sources to train NNs can improve the accuracy of predictions, as full range of datasets provides a more comprehensive list of threat signatures. According to market research, Distributed learning (DL) and Federated learning (FL) are used to train models for Internet of Things (IoT), healthcare industry, banking services [2]. However, all these cloud-edge collaborative architectures have central cloud servers to keep global aggregation and to provide NN model for all participants of the learning process. Also, there are FL related challenges, such as statistical heterogeneity, system heterogeneity, model heterogeneity and secure management [2].

The purpose of this work is to investigate the mechanisms of FL for NNs that analyzes security threats and vulnerabilities in cloud services. The problem is that cloud providers use complex proprietary models that have different architecture and high heterogeneity. Also privacy and security of the learning process must be taken into an account. This work analyzes the impact of model size and heterogeneity on quantitative measures of the FL process. A described system, consisting of a neural network and a blockchain network, was built. In the course of the research the work is being carried out to collect metrics for learning speed and network traffic, corresponding to different variants of FL. These metrics will be further used to get optimization for the system architecture. The full version of the report will present the models, the dependencies obtained, and recommendations for system optimization.

Conclusions. The process of large model training can be optimized. With incremental learning, when new threats appear, the percentage of new data is insignificant compared to the total database size. FL of a large model while changing a small portion of the training data results in an increased network traffic and in a longer model training time. Partitioning a large model into an aggregation of specialized feature-models can improve the considered metrics.

References

1. Naveed Ahmed and others. Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction, 2022, Sensors.

2. Guanming Bao, Ping Guo. Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. Journal of Cloud Computing. URL – https://doi.org/10.1186/s13677-022-00377-4.

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЇ З МАШИННИМ НАВЧАННЯМ ДЛЯ БЕЗПЕЧНИХ IoT

Просолов В.В., Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Перевагами децентралізованої безпеки IoT [1] є зменшення вразливості від централізованих атак. А інформація, яка записана в блокчейні [2], є незмінною і публічно доступною, що дозволяє легше виявляти аномалії або зловмисну активність. Смарт-контракти можуть автоматизувати процедури безпеки, реагуючи на загрози в реальному часі. Алгоритми машинного навчання [3] можуть вивчати поведінку мережі, щоб виявляти нові або нерозпізнані загрози, підсилюючи системи безпеки IoT. Комбінація блокчейну і машинного навчання забезпечує адаптивність до постійно змінюваних загроз, забезпечуючи оптимальну роботу IoT-систем. Їх інтеграція може вирішити проблеми масштабованості, які часто зустрічаються у великих IoT-мережах.

Метою доповіді є дослідження можливості та переваг інтеграції блокчейн-технології з машинним навчанням з метою забезпечення надійності, безпеки та ефективності систем Інтернету речей, а також визначення основних проблем та обмежень такого поєднання в контексті IoT.

IoT-мережі можуть генерувати великі обсяги даних від численних пристроїв. Блокчейн-системи, зокрема ті, які використовують доказ роботи (Proof-of-Work) [4], можуть бути обмежені у швидкості обробки таких масивних потоків даних. А для створення ефективних моделей машинного навчання [5] потрібно згенерувати та зібрати великі набори даних для їх тренування. Таким чином, блокчейн дозволяє створити децентралізовану, прозору та незмінну систему запису, що може ефективно взаємодіяти з різноманітними пристроями в мережі IoT. З іншого боку, машинне навчання може допомогти у виявленні аномалій, прогнозуванні загроз безпеки та автоматичному реагуванні на потенційні інциденти безпеки.

Список літератури

1. Ten-Nahuang Le, Chintan Bhatt, Mani Madhukar IoT Security and Privacy Preservation. *Wiley Data and Cybersecurity.* 2020. С. 97-111. DOI: https://doi.org/10.1002/9781119593171.ch6

2. Joseph Holbrook Blockchain Security and Threat Landscape. *Architecting Enterprise Blockchain Solutions.* 2020. С. 323-347. DOI: https://doi.org/10.1002/9781119557722.ch11

3. Jingguo Ge, Tong Li, Yulei Wu Intelligent Network Management and Operation Systems. *AI and Machine Learning for Network and Security Management.* 2020. С. 215-256. DOI: https://doi.org/10.1002/9781119557722.ch11

4. Bin Cao, Lei Zhang, Mugen Peng Consensus Algorithm Analysis in Blockchain: Pov and Raft. *Wireless Blockchain: Principles, Technologies and Applications.* 2022. С. 27-72. DOI: https://doi.org/10.1002/9781119790839.ch2

5. Brett Lantz Machine Learning with R: Learn techniques for building and improving machine learning models, from data preparation to model tuning, evaluation, and working with big data. 2023.

SQL-ІН'ЄКЦІЇ ЯК ЗАГРОЗА БЕЗПЕЦІ ДАНИХ

Іващенко М.Д., Петренко О.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

SQL-ін'єкція, також відома як SQLI, є поширеним вектором атаки, який використовує зловмисний код SQL для маніпулювання серверною базою даних для доступу до інформації, яка не призначена для відображення [1]. Ця інформація може включати будь-яку кількість елементів, включаючи конфіденційні дані компанії, списки користувачів або приватні дані клієнтів.

Метою доповіді є узагальнення та систематизація інформації про SQL-ін'єкцію, що представляє собою серйозну загрозу безпеці та полягає у використанні вразливостей веб-застосунку для несанкціонованого доступу до бази даних. В доповіді зазначено, що у процесі SQL-ін'єкції шкідливий код вставляється або «впроваджується» в текстові поля введення, такі як форми на веб-сторінках. Цей код потім виконується безпосередньо в системі бази даних, що дозволяє атакуючим отримати доступ до конфіденційної інформації, модифікувати дані або навіть знищити їх [2].

SQL-ін'єкції зазвичай поділяються на три категорії: In-band SQLi, Inferential SQLi, Out-of-band SQLi [3]. Розглядаючи можливі наслідки SQL-ін'єкцій, насамперед, важливо підкреслити ризик втрати довіри з боку клієнтів та користувачів. В разі несанкціонованого доступу до особистої інформації, такої як номери телефонів, адреси та конфіденційні дані кредитних карт, може виникнути серйозний злам довіри, що може сильно зашкодити репутації організації або платформи. Запобігання SQL-ін'єкціям та використання належних методів захисту даних є надзвичайно важливими завданнями для забезпечення безпеки веб-додатків та збереження довіри користувачів

Отже, SQL-ін'єкції є серйозною загрозою безпеці інформаційних систем, оскільки вони дозволяють зловмисникам несанкціоноване отримувати доступ до баз даних та впливати на дані. Ця атака може призвести до втрати конфіденційної інформації, порушення цілісності даних та впливу на доступність системи. Загроза SQL-ін'єкцій вимагає від розробників та адміністраторів систем надзвичайної обережності та впровадження ефективних заходів захисту, таких як санітаризація та валідація вхідних даних, використання параметризованих запитів та належна настройка систем безпеки. Розуміння різних видів SQL-ін'єкцій та їх можливих наслідків є важливим кроком для запобігання цим атакам і збереження безпеки інформаційних систем.

Список літератури

1. What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva. Imperva. URL: https://www.imperva.com/learn/application-security/sql-injection-sqli/ (accessed: 05.10.2023)

2. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. (2015). Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. *Системи обробки інформації*, (9), 101-104.

3. SQL-ін'єкції - aCode. Acode. URL: https://acode.com.ua/sql-injection/

МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СХЕМ КВАНТОВОЇ СТЕГАНОГРАФІЇ

Федюшин О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Стеганографія - це галузь обробки інформації, що спеціалізується на приховуванні різних типів інформації всередині повідомлень або файлів; квантова стеганографія використовує особливі властивості квантового всесвіту, такі як суперпозиція та заплутаність для досягнення цієї мети.

В своїй основі вона використовує методи як класичної стеганографії, так і захищені протоколи для обміну інформацією розроблені для квантових систем [1].

Метою даного дослідження є аналіз типової структури засобів моделювання квантових систем, які можна використовувати для прикладних досліджень у сфері квантової стеганографії.

Предметом дослідження є програмні засоби для моделювання квантових систем.

Екосистема програмного забезпечення для моделювання, як правило складається з програмних фреймворків, засобів підтримки мов програмування для квантових обчислень, програм-утиліт та бібліотек. Бізнес-логіка містить: програми-симулятори, що використовують набори бібліотек для симуляції квантових перетворень на класичному комп'ютері, компілятори, засоби підтримки доступних мов програмування, засоби підтримки виконання типових операцій з кубітами, бібліотеки та алгоритми для корекції помилок, засоби тестування та відлагодження та колекції квантових алгоритмів доступних для симуляції.

Основними критеріями вибору середовища для моделювання стеганографічних систем на основі протоколів квантових обчислень в роботі були визначені простота використання, документація, підтримка та функціональність. Були проаналізовані додатки Qiskit, Quipper, Cirq, ProjectQ, SimulaQron [2]. З огляду на ці критерії, Qiskit і Cirq можна вважати найбільш функціональними. Перший є фреймворком, що підтримується і розробляється компанією IBM, написаний на мові Python; другий – Cirq пропонує простий інтерфейс та можливість підключення сторонніх бібліотек, і є розробкою Google, що свідчить про його високу якість.

Список літератури

1. Min-Allah, N.; Nagy, N.; Aljabri, M.; Alkharraa, M.; Alqahtani, M.; Alghamdi, D.; Sabri, R.; Alshaikh, R. Quantum Image Steganography Schemes for Data Hiding: A Survey. Appl. Sci. 2022, 12, 10294. https://doi.org/10.3390/app122010294.

2. Pandey, R., Maurya, P., Singh, G.D., Faiyaz, M.S. (2023). Simulating Quantum Principles: Qiskit Versus Cirq. In: Quantum Computing: A Shift from Bits to Qubits. Studies in Computational Intelligence, vol 1085. Springer, Singapore. https://doi.org/10.1007/978-981-19-9530-9_18.

CNN ТА ЇХ ВИКОРИСТАННЯ ДЛЯ КЛАСИФІКАЦІЇ MALWARE

Федюшин О.І., Хижняк К.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Зловмисне програмне забезпечення – це широка категорія програмного забезпечення, яка включає віруси, трояни, програми-вимагачі та інші malware, призначені для нанесення шкоди або проникнення в комп'ютерні системи [1]. Його динамічний характер, який виражається незліченною кількістю нових варіантів, що з'являються щодня, створює серйозну проблему для традиційних антивірусних систем і систем виявлення вторгнень.

Протистояння між професіоналами з кібербезпеки та авторами шкідливих програм призводить до безперервної еволюції методів їх виявлення. Одним із багатообіцяючих підходів, який набув популярності в останні роки, є використання глибокого навчання, зокрема згорткових нейронних мереж (CNN), для класифікації та ідентифікації штамів шкідливих програм [2]. CNN, як тип глибокої нейронної мережі, були особливо успішними в розпізнаванні зображень. Фундаментальна ідея CNN полягає в тому, що вони можуть автоматично вивчати та отримувати релевантні функції з вихідних даних. Дослідники визнали потенціал застосування цих концепцій до проблеми класифікації шкідливих програм.

Критичним кроком у класифікації шкідливих програм є виділення ознак. На відміну від традиційних графічних даних або тексту, зловмисне програмне забезпечення часто представляється у вигляді двійкових файлів [3]. CNN можуть навчитися представляти ці двійкові файли як послідовності даних і витягувати значущі шаблони та ознаки для класифікації.

Метою доповіді є дослідження моделей нейронних мереж та отримання результатів щодо їх ефективності у ролі класифікатора шкідливого програмного забезпечення на основі таких метрик, як precision, recall, F1-Score та інші [4]. В доповіді також надається аналіз результатів роботи навчаних з нуля моделей.

Список літератури

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. (2017). Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка*, (1), 65-68.

2. Makandar, Aziz, and Anita Patrot. "Overview of malware analysis and detection." International Journal of Computer Applications 975 (2015): 8887.

3. Федюшин О. І., Хижняк К. М. Використання методів глибокого навчання для візуалізації та виявлення malware / Матеріали Тринадцятої міжнародної науково-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», м. Харків, 26-27 квітня 2023р. – С. 84.

4. Anandhi, V., Vinod, P., Menon, V.G. et al. Performance evaluation of deep neural network on malware detection: visual feature approach. Cluster Comput 25, 4601–4615 (2022).

АВТЕНТИФІКАЦІЯ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЇ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Федюшин О.І., Хруслов Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті принципи і проблеми використання технології блокчейну для систем автентифікації в мережах інтернету речей (англ. – «Internet of Things», IoT).

Об'єктом дослідження є системи автентифікації на основі технології блокчейну в IoT мережах. **Предметом дослідження** – принципи та проблеми реалізації систем автентифікації на основі технології блокчейну з урахуванням обмежених обчислювальних можливостей пристроїв IoT.

У типовому методі автентифікації пристроїв IoT використовується система залежності від серверів, які обмінюються ключами. Централізований характер цієї інфраструктури створює одну центральну точку вразливості, яка може бути атакована, перевантажена або відключена, що загрожує безпеці, доступності та надійності всієї мережі [1].

Блокчейн, модель якого базується на розподіленому реєстрі, може надати рішення для децентралізованої автентифікації [2, 3]. Його застосування означає використання безпечного цифрового реєстру з криптографічним захистом для підтвердження, збереження та обміну даними в спосіб, який надійно захищає їх від можливої фальсифікації, пошкодження або зміни. Однак слід враховувати, що використання блокчейн-систем може вимагати значних обчислювальних ресурсів, адже вони базуються на складних математичних обчисленнях. Крім того, пристрої в мережах IoT обмежені обсягом доступної пам'яті, що унеможливлює зберігання великого ланцюжка блоків.

Щоб вирішити проблему високих вимог до обробки даних, потрібно використовувати легкий та швидкий алгоритм консенсусу. Для цього можна використати протокол Authentication-Chains [4]. Цей протокол працює шляхом об'єднання пристроїв у кластери з декількома рівнями блокчейнів, що дозволяє створювати таблиці автентифікації на основі хеш-значень блоків. Пропоноване рішення дає змогу пристроям зберігати менше даних, а також швидко обробляти запити на автентифікацію.

Список літератури

1. Hassija V., Chamola V., Saxena V., Jain D., Goyal P., Sikdar B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. // IEEE Access. – 2019. – №7. – С. 82721 – 82743.

2. Fernández-Caramés T.M., Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. // IEEE Access. – 2018. – №6. – С. 32979 – 33001.

3. Власов А.В., Сєвєрінов О.В., Слиш О.В. Впровадження децентралізованої системи ідентифікації. НТУ «ХПІ», 2020.

4. Al Ahmed M.T., Hashim F., Hashim S.J., Abdullah A. Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks. // Electronics 2023, 12(4), 867; https://doi.org/10.3390/electronics12040867.

СТЕГАНОАНАЛІЗ СТЕГАНОГРАФІЇ НА ОСНОВІ РІЗНИЦІ ПІКСЕЛІВ

Федюшин О.І., Фокін Д.Г.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті методи та підходи до стеганоаналізу для виявлення стеганографії, що використовує різницю пікселів.

Об'єктом дослідження є стеганографія на основі різниці пікселів. **Предметом дослідження** – методи для виявлення модифікацій зображень за допомогою методів стеганографії на основі різниці пікселів.

Використання різниці пікселів як методу приховування інформації в зображеннях є відносно новим підходом у сфері стеганографії. Цей метод дозволяє вбудовування великих об'ємів даних без значущого втручання в зовнішній вигляд зображення. Серед основних методів стеганоаналізу, розроблених спеціально для атак на стеганографію різниці пікселів, використовуються регулярно-сінгулярний аналіз, який базується на розпізнаванні регулярних та особливих областей в зображенні, що містять високочастотні деталі, і які може залишати стеганографія на основі різниці пікселів [1], та аналіз зваженого стегозображення, що зосереджується на виявленні зон зображення, де інформація була вбудована, аналізуючи вагові коефіцієнти пікселів [2].

Обидва вищезазначених метода використовують гістограму різниці пікселів для ідентифікації пікселів із незвичайною різницею значень. Переваги гістограми, очевидні лише тоді, коли ємність вбудовування за допомогою методів стеганографії на основі різниці пікселів висока. Нещодавно запропонований статистичний стеганоаналіз в свою чергу використовує ряд статистичних особливостей, таких як середнє значення, дисперсія та інші, для виявлення аномалій в зображеннях, що містять приховану інформацію [3].

Ефективність конкретного методу стеганоаналізу залежатиме від використовуваного алгоритму стеганографії, а також від ємності вбудовування та якості контейнера.

В роботі зроблений порівняльний аналіз та проведена оцінка ефективності методів стеганоаналізу, і запропоновані рекомендації з їх використання.

Список літератури

1. T. Qian, S. Manoharan. A Comparative Review of Steganalysis Techniques. // 2015 2nd International Conference on Information Science and Security. – 2015. – С. 1 – 4.

2. H. Zhang, T. Zhang, H. Chen. Revisiting weighted Stego-image Steganalysis for PVD steganography. // Multimedia Tools and Applications volume 78. – 2019. – С. 7479 – 7497.

3. W. B. Lin, T. H. Lai, K. C. Chang. Statistical feature based steganalysis for pixel value differencing steganography. // EURASIP Journal on Advances in Signal Processing. – 2021. – №87. – С. 18.

ВИЯВЛЕННЯ БЕЗПЕЧНИХ HTTP ЗАГОЛОВКІВ З ВИКОРИСТАННЯМ ТЕХНІК NLP

Федюшин О.І., Кавецький М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З впровадженням все більш широкого використання веб-програм та сервісів, забезпечення безпеки HTTP-запитів стає критичним завданням для захисту конфіденційності та цілісності інформації. Використання прийомів обробки природньої мови (NLP) може значно полегшити виявлення безпечних HTTP-заголовків, що дозволяє ефективно контролювати та уникати потенційних загроз безпеці.

Об'єктом дослідження є HTTP заголовки веб-протоколу. **Предметом дослідження** – використання технік обробки природньої мови (NLP) для виявлення та аналізу безпечних або потенційно небезпечних HTTP заголовків.

До цього часу існують певні техніки перевірки безпеки HTTP-заголовків, але багато з них потребують великого обсягу ручної роботи та експертного втручання. Використання NLP технік дозволяє автоматизувати цей процес, швидко та ефективно аналізуючи текст HTTP-заголовків для виявлення потенційно небезпечних або підозрілих елементів.

Одним із ключових аспектів використання NLP є здатність до виявлення відхилень від типового способу використання HTTP-заголовків. Застосування методів обробки природньої мови дозволяє створювати моделі, які здатні розпізнавати неочікувані або небезпечні комбінації заголовків, що можуть свідчити про атаки або вразливості в системі [1-2].

Для досягнення максимальної ефективності виявлення безпечних HTTP-заголовків з використанням NLP технік, необхідно враховувати широкий спектр можливих загроз та розробляти адаптивні алгоритми, які можуть адекватно реагувати на нові види атак та шахрайства [3].

Результати дослідження показали, що використання NLP технік дозволяє автоматизувати та покращити процес виявлення безпечних HTTP-заголовків, забезпечуючи більш ефективний та надійний захист веб-додатків та сервісів від потенційних кібератак та порушень безпеки.

Список літератури

1. M. Zolotukhin, T. H¨am¨al¨ainen, T. Kokkonen, and J. Siltanen,"Analysis of HTTP requests for anomaly detection of web attacks," in Proceedings 2014 IEEE 12th International Con-ference on Dependable, Autonomic and Secure Computing, Dalian, China, August 2014.

2. Seungyoung Park, Myungjin Kim, and Seokwoo Lee. Anomaly detection for HTTP using convolutional autoencoders. IEEE Access, 6:70884–70901, 2018.

3. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. (2015). Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. *Системи обробки інформації*, (9), 101-104.

ПІДПИС НА ОСНОВІ КРИПТОСИСТЕМ З ЛОГАРИФМІЧНИМ ПІДПИСОМ

Хівренко Г.О., Фроленко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком технологій квантових обчислень та побудовою дослідних образків квантових комп'ютерів відбувається модернізація криптографічних алгоритмів та протоколів на предмет підвищення їх стійкості. Наявність квантових алгоритмів розкладання цілих чисел і дискретних логарифмів ставить під загрозу можливість використання криптографії доквантового періоду.

У кінці 1970-х років Спірос Магліверас розпочав вивчення використання спеціальних факторизацій для неабелевих груп з відомими властивостями, що називаються логарифмічними підписами. Пізніше були опубліковані роботи, що описують створені ним криптосистеми MST1, які ґрунтуються на логарифмічних підписах, та MST2, що базуються на іншому типі множин, відомих як [s,r]-осередки [1]. Нещодавно була розроблена нова криптосистема з відкритими ключами, яка поєднує дві попередні криптосистеми та працює на основі логарифмічних підписів та випадкових покриттів неабелевих груп. Для реалізації цієї системи були введені Судзукі 2-групи

Метою доповіді є розгляд алгоритмів побудови цифрового підпису на основі криптосистем MST3. Розглянута побудова цифрового підпису на основі криптосистеми MST3, яка відносяться до класу квантово-стійкої. MST3 криптосистема будується на основі логарифмічних підписів, а також на Судзукі 2 групі [2, 3]. Актуальним є розвиток криптосистем схожого типу на багатопараметричні групи, що дозволяє зменшити складність обчислень без втрати секретності. Досліджувана область має великий потенціал, оскільки вона відноситься до області, яку називають "післяквантовою криптографією". Серед актуальних завдань у цій галузі можна виділити розробку нових підходів до створення логарифмічних підписів, досягнення більшої продуктивності криптосистем і створення надійних схем захисту даних.

Виконано попередній квантовий криптоаналіз на основі використання алгоритму Гровера, який показує, що складність квантового комп'ютера буде пропорційна кореню квадратному з K, де K - розмір множини ключів. Квантовий алгоритм запропоновано для моделі переборної атаки на ключі.

Список літератури

1. Svaba, Pavol. (2011). Covers and Logarithmic Signatures of Finite Groups in Cryptography.

2. Hong, Haibo & Li, Jing & Wang, Licheng & Yang, Yixian & Niu, Xinxin. (2014). A Digital Signature Scheme Based on MST3 Cryptosystems. Mathematical Problems in Engineering. 2014. 10.1155/2014/630421.

3. Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., Vlasov A. (2021, July). Towards three-parameter group encryption scheme for MST3 cryptosystem improvement. In *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)* (pp. 204-211). IEEE.

АНАЛІЗ МЕТОДІВ ОБХОДУ СУЧАСНИХ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК (EDR)

Шуліка К.М., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні неможливо уявити захист даних без використання комплексних рішень для захисту кінцевих точок: серверів і робочих станцій. Вимоги до подібних рішень включають забезпечення прозорості процесів і автоматизований пошук аномалій в системах, а також можливість реагувати на інциденти безпеки для спеціалістів команд кібербезпеки [1, 2].

EDR (Endpoint Detection and Response) є типом кросплатформеного програмного забезпечення, що наразі найчастіше використовується для моніторингу подій, формування та формалізації інцидентів безпеки та реагування на інциденти на кінцевих точках [3].

EDR часто використовуються в SOC (Security Operational Center) для забезпечення безпеки в масштабі інфраструктури, але і ці комплексні рішення можливо обійти [4, 5].

Метою доповіді є огляд та аналіз широко використовуваних зловмисниками методів обходу комплексних рішень для захисту кінцевих точок (EDR).

В доповіді розглядаються три методи обходу EDR о використовуються найбільш широко: AMSI обхід, «зняття з крючка» (unhooking), та завантаження рефлективної DLL.

Наводиться опис кожного метода, приклад використання в ході атаки на інфраструктуру, а також надаються рекомендації щодо протидії та запобігання використанню зловмисниками такого методу.

Ці рекомендацію можуть бути використані в ході формування процесів в команді з кібербезпеки.

Робляться висновки щодо вірогідності використання наведених методів обходу EDR на основі їх доступності для зловмисника у глобальній мережі.

Список літератури

1. Ушатов В., Сєвєринов О.В. (2019). Проблемы оперативного обнаружения и реагирования на инциденты информационной безответственности.

2. "Кібервійна та безпека об'єктів критичної інфраструктури", Юрій Когут, Україна, Сідконб 2021

3. "Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems", Matt Hand, No Starch Press 2023.

4. Sievierinov O., Ovcharenko M., Vlasov A. Enterprise Security Operations Center. *COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES*, 2021.

5. "Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass, and evade antivirus software", Yehoshua Nir, Packt Publishing 2021

ВДОСКОНАЛЕННЯ АКУСТИЧНОГО МЕТОДА ТА ЗАСОБІВ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ЗАПИСУ МОВИ

Олейніков А.М., Алфьорова М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Жоден з відомих сьогодні методів придушення несанкціонованого запису мови (акустичний, ультразвуковий, електромагнітний) без апріорного знання типу записуючого пристрою, не може забезпечити гарантоване недопущення запису мовної інформації на звукозаписний пристрій.

Метою доповіді є підвищення ефективності протидії несанкціонованого запису мови шляхом адаптації акустичного методу з урахуванням особливостей поширення акустичних коливань в навколишньому просторі, психофізичного сприйняття звуків вухом людини та покращенням технічних характеристик акустичної системи пристроя придушення , а саме :

- оптимізувати відстань між джерелом акустичної перешкоди та місцем передбачуваного розташування диктофона (необхідно звести до мінімуму і зробити його менше, ніж відстань між джерелом мови та диктофоном);
- формувати акустичну перешкоду з мови співрозмовників у вигляді мовного акустичного сигналу (така мовоподібна перешкода не може бути відфільтрована, так як займає ту ж смугу частот, що і сам мовний сигнал);
- суттєво покращити технічні параметри випромінювача мовної перешкоди_ електростатичної акустичної системи (це дозволить максимально наблизити спектральні характеристики мовної перешкод до голосів співрозмовників і збільшити її густину потоку потужності).

У доповіді наводяться результати проведених експериментів, які показали, що запропонований адаптивний акустичний метод є найбільш ефективним, оскільки перешкода формується безпосередньо по функціональному каналу з урахуванням особливостей поширення та сприйняття акустичних коливань вухом людини.

Ефективність методу підтверджується не лише збільшеною дальністю придушення, але й тим, що дозволяє протидіяти будь-яким відомим засобам запису, незалежно від їх типу.

Список літератури

1. Олейніков А.М., Пулавський В.А., Цибулевський П.В. Оцінка ефективності акустичної протидії несанкціонованого запису на диктофон. // Сучасний захист інформації.-Київ: 2010-№1, С. 8-16.
2. Олейніков А.М., Пулавський В.А., Кривенко М.А. Ультразвукові методи захисту мовної інформації // Радіотехніка: Всеукр . міжвід . наук.-техн. сб.-Харків: 2012. Вип . 169. С. 176 – 181.

ОБҐРУНТУВАННЯ МОЖЛИВОСТІ СТАТИСТИЧНОГО ДОСЛІДЖЕННЯ ЧАСТОТ ПЕРЕДАЧІ ДАНИХ, ПРИ ВИЯВЛЕННІ ПРИХОВАНИХ РАДІОЗАКЛАДНИХ ПРИСТРІЇВ

Зайцев С.В., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботах по виявленню радіозакладних пристроїв (РЗП) на об'єктах електронно-обчислювальної техніки (ЕОТ) основну роль грає аналіз електромагнітної обстановки. Прихованість РЗП може досягатися шляхом вибору частоти передачі перехопленої інформації в близькості до смуг роботи радіомодулів, як елементів ЕОТ, так і інших радіоелектронних засобів, що знаходяться поблизу.

При виявленні потенційних шкідливих інцидентів інформаційної безпеки, джерелом яких може бути РЗП, важливими можуть бути і можуть і одиничні сигнали, і параметри їх випромінювань, що виходять за межі контрольованої зони за межі контрольованої зони, наприклад, так як швидкість передачі даних на частотах типових радіомодулів.

При вивченні, стандартних характеристик радіомодулів, можна зробити деякі висновки щодо небезпеки наявності РЗП на об'єкті ЕОТ з такими можливостями передачі великих обсягів інформації. В смугах частот, що належать стандартам LTE (IEEE 802.16m) [1] та Wi-Fi (IEEE 802.11) [2], вже досягаються швидкості понад 50 Мбіт/с. Тобто, якщо РЗП почне передавати документ, що вирушив до принтеру на друк з ПЕОМ, то за межі контрольованої зони, з високою ймовірністю, електронна копія документа потрапить раніше, ніж до користувача ПЕОМ - роздрукована, і це тільки якби в радіозакладних пристроях використовувалися комплектуючі та методи зв'язку, замаскованих під смартфони.

Метою доповіді є твердження, що за винятком проблеми з дальністю передачі, що вирішується установкою несанкціонованих точок передачі інформації, сигнали від закладних пристроїв могли б маскуватися під поширені частоти роботи радіомодулів, і при цьому отримувати серйозні можливості перехоплення даних.

Звичайною, одиничною перевіркою, виявити такі сигнали може бути складно, на відміну від методів пов'язаних зі збиранням та аналізом статистики про навколишню електромагнітну обстановку протягом тривалого терміну, типовим обладнанням радіомоніторингу, що вкотре доводить цю необхідність.

Список літератури

1. OVERVIEW OF IEEE P802.16m TECHNOLOGY AND CANDIDATE RIT FOR IMT-ADVANCED (PDF). https://docbox.etsi.org/3gppETSI/2010-01-13_ITU-R_IMT-Adv_eval_IEEEwkshp/L80216-10_0002.pdf (дата звернення 07.10.2023 р.).

2. IEEE 802.11 Wireless LANs (PDF) https://inst.eecs.berkeley.edu/~ee122/sp07/80211.pdf (дата звернення 07.10.2023 р.).

ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ВІДОМОСТЕЙ З ОБМЕЖЕНИМ ДОСТУПОМ ПРОДУКЦІЇ, ЩО ВИГОТОВЛЯЄТЬСЯ НА ПІДПРИЄМСТВІ

Лучина О.В., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Під час реалізації ефективного та конкурентоспроможного підприємства найбільша увага приділяється створенню надійної системи захисту відомостей з обмеженим доступом продукції, що виготовляється та виробничих технологій. Визначена система захисту відомостей – це сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту від технічних розвідок, несанкціонованого доступу до них [1]. Розроблення такої системи – багатоскладовий, довготривалий процес, під час виконання якого можуть виникати помилки.

У зв'язку з цим, проблема створення ефективної, економічно вигідної та конкурентоспроможної системи захисту інформації на підприємстві залишається актуальною і по наш час.

Особливу увагу під час розробки таких систем приділяють виявленню ознак відомостей для кожної елементарної відомості з обмеженим доступом, так як саме на цьому етапі виникають найбільші втрати через хибні оцінки і результати. Ознаки відомостей – це фізичні поля, явища, характеристики, які піддаються виявленню та аналізу за допомогою розвідувальної апаратури і які можуть бути джерелом інформації про об'єкт [2].

Під час розробки системи захисту відомостей все більше фахівців проявляють зацікавленість до автоматизації певних етапів даного процесу задля їх вдосконалення, пришвидшення роботи, зменшення кількості помилок та зручності оформлення розроблюваних документів.

Метою доповіді є аналіз класифікацій ознак відомостей з обмеженим доступом та дослідження процесу їх формулювання з точки зору семантики. Задля створення програми з автоматизації процесу виявлення ознак відомостей необхідно проаналізувати вимоги до програмного забезпечення на підприємствах.

Результатом роботи є розробка формалізованої схеми пропозицій з виявлення ознак відомостей з обмеженим доступом на основі виявлених закономірностей використовуючи ліцензійне та сертифіковане програмне середовище з наявною можливістю редагування баз даних.

Список літератури

1. Заболотний В.І., Єрмолович А.В. (2017). Методика організації заходів захисту від технічних засобів конкурентної розвідки. *Radiotekhnika*, (189), 23-28.

2. Заболотний В.І., Задорожна Є.В. (2013). Обґрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки.

КОМПЛЕКСНА СИСТЕМА КОНТРОЛЮ ЗА РОБОТОЮ ЗАСОБІВ РАДІЗВ'ЯЗКУ

Голобородько Ю.М., Наконечний М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Широке застосування зв'язку промисловістю, фінансовими та державними відомствами, а останнім часом комерційними фірмами та приватними особами, у тому числі незаконними формуваннями та збройними злочинними групами, ставить:

по-перше, завдання контролю за використанням засобів зв'язку, виявляючи та припиняючи роботу незаконно діючих засобів;

по-друге, використання засобів радіозв'язку кримінальними структурами, у свою чергу, вимагає створення системи радіоконтролю в інтересах силових відомств [1], здатної ефективно вирішувати завдання виявлення роботи в ефірі незаконних формувань, перехоплення повідомлень, що передаються, визначення місцезнаходження радіозасобів, а також визначати боєздатність і можливі напрями їх діяльності [2].

Метою доповіді є обґрунтування необхідності та технічної можливості створення багатоцільової системи радіоконтролю, призначеної для вирішення на користь відомств, як загальних, так і специфічних для кожного відомства завдань [3].

Система складається з:

– стаціонарних станцій радіоконтролю;

– мобільних станцій радіоконтролю, що розміщуються на автомобілях;

– мобільних станцій радіоконтролю, що розміщуються на ЛПА та БПЛА;

– засобів радіоконтролю, що носяться;

– систем зв'язку зі службами кожного із відомств;

– системи управління та обробки інформації.

Таким чином проведені дослідження показали, що наразі силові відомства (СБУ, МВС, НКЕК) мають власні системи радіоконтролю, які вирішують однотипні завдання.

Список літератури

1. Голобородько Ю.М., Кузниченко В.С. Перспективи розвитку засобів радіоконтролю. Збірник тез науково-практичної конференції „Проблеми забезпечення внутрішньої безпеки держави", Харків, 2005.

2. Степовий, В. Б., С. В. Каковкін, and Л. В. Мороз. *Радіоелектронна розвідка збройних сил України*. Diss. ВНТУ, 2020.

3. Гурьєв В.І., Горбачинський І.С., Голобородько Ю.М. Авторське свідоцтво № 210497 від 26.10.84 «Панорамний радіоприймальний пристрій для визначення зони знаходження джерела радіовипромінювання».

РОЗПІЗНАВАННЯ DEEPFAKE ЗОБРАЖЕНЬ НА МОБІЛЬНИХ ПРИСТРОЯХ

Долганенко О.Д., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

Із появою технології ефективної заміни обличчя на фото відео (deepfake), функціонал біометричної автентифікації та підтвердження особистості користувача стає під загрозою [1], особливо в додатках державного та фінансового призначення. Створення швидкого, надійного та захищеного автоматизованого рішення розпізнавання deepfake на мобільному пристрої є актуальною проблемою, яка потребує ретельного дослідження.

Метою доповіді є аналіз предметної області створення та розпізнавання на мобільному пристрої зображень та відео, над якими було здійснено маніпуляцію deepfake. У доповіді наводяться методи створення deepfake: здебільшого це досягається за допомогою глибоких нейронних мереж у поєднанні з методами заміни обличчя та Generative Adversarial Networks (GAN). Також, перераховуються та аналізуються методи розпізнавання deepfake зображень, до яких належать: методи що базуються на статистичних вимірюваннях, методи машинного навчання та глибокого навчання [2]. У результаті порівняння та аналізу існуючих досліджень виявлено оптимальний метод для вирішення цієї задачі – метод глибокого навчання. Наводяться методи створення моделі та аналізуються доступні набори даних, таких як FaceForensics, DFD, Celeb-A та інші.

У доповіді наводяться методи застосування моделей глибокого навчання на мобільних пристроях. Піднімається питання оптимізації моделі шляхом її зменшення, що досягається операцією трасування. Розглядається статистика порівняння точності моделі до та після застосування трасування. Також порівнюються технології PyTorch Mobile та TensorFlow Lite для взаємодії із моделлю на мобільному пристрої. У висновку зазначаються результати дослідження, що включають обрані технології та підходи до розпізнавання deepfake зображень на мобільному пристрої, їх переваги, недоліки та обмеження.

Список літератури

1. Zainab Zahid, Ammar Haider, Nosheen Sabahat, Asim Tanwir . Vulnerabilities in Biometric Authentication of Smartphones. *2020 IEEE 23rd International Multitopic Conference (INMIC)*. 2020. DOI: https://doi.org/10.1109/inmic50486.2020.9318094

2. Hady A. Khalil;Shady A. Maged; (2021). Deepfakes Creation and Detection Using Deep Learning. *International Mobile, Intelligent, and Ubiquitous Computing Conference.* 2021. DOI: https://doi.org/10.1109/MIUCC52538.2021.9447642

АНАЛІЗ КЛІЄНТСЬКОГО ТА СЕРВЕРНОГО ШИФРУВАННЯ

Бєльський О.Ю., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді є дослідження різниці між клієнтським та серверним шифруванням, а також розгляд їх сильних та слабких сторін.

Клієнтське шифрування - це процес захисту даних на стороні користувача (клієнта). У цьому методі дані шифруються на пристрої користувача перед відправкою на сервер. Один із основних прикладів цього - HTTPS (SSL/TLS) шифрування, яке застосовується в браузерах під час з'єднання з веб-сервером [1]. Але на цьому використання клієнтського шифрування не обмежене і може бути використано як основа архітектури проекту.

Серед сильних сторін клієнтського шифрування можна відзначити конфіденційність - дані шифруються ще до відправлення на сервер, що запобігає зловмисним атакам на дані під час передачі. Контроль користувача - користувач має контроль над шифруванням своїх даних, що дозволяє йому забезпечити додатковий рівень безпеки. зменшення обсягу даних - зашифровані дані важко читати для незаконних осіб, що робить їх менш придатними для крадіжки чи зламу [2]. Але подібне шифрування має і свої недоліки: обмежене застосування - клієнтське шифрування не може захистити дані на сервері, коли вони розшифровуються для обробки. Потребує обслуговування на клієнтському боці - підтримка та налагодження шифрування на клієнтському боці може бути складнішою задачею. Серверне шифрування передбачає, що дані надсилаються на сервер у незашифрованому вигляді, і шифруються та розшифровуються лише на стороні сервера [2].

Щодо серверного шифрування то виділяють такі переваги: зручність - всі дані розшифровуються централізовано на сервері, що полегшує обслуговування та моніторинг шифрування. Захист від зловмисних клієнтів - серверний шифр захищає дані від недостовірних клієнтів. Але також очевидні і деякі недоліки: потенційна незахищеність під час передачі - дані надсилаються на сервер у незашифрованому вигляді, що може створювати ризик під час передачі на сервер. Збільшена залежність від сервера - при використанні серверного шифрування, сервер стає однією точкою вразливості.

Обираючи між клієнтським та серверним шифруванням, розробники повинні ретельно розглядати потреби проекту та дотримуватися найкращих практик забезпечення конфіденційності та безпеки даних. Комбінування обох методів також може бути варіантом, щоб забезпечити максимальну захищеність даних в веб-застосунках.

Список літератури

1. Rescorla, E. (2001). "SSL and TLS: Designing and Building Secure Systems." Addison-Wesley Professional.

2. Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company..

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ МОБІЛЬНИХ ПРИСТРОЇВ У КОРПОРАТИВНИХ МЕРЕЖАХ

Сердюков Д.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

З урахуванням зростання мобільності працівників та розповсюдження віддаленої роботи, забезпечення безпеки на мобільних пристроях стає надзвичайно важливим завданням для організацій. Багатофакторна автентифікація допомагає зменшити ризик витоку даних та підвищити загальний рівень безпеки корпоративних мереж у мобільному середовищі.

Метою доповіді є аналіз підходів до автентифікації користувачів на мобільних пристроях, що мають доступ до корпоративної інформації та дослідження тенденцій майбутніх методів автентифікації. Були розглянуті чотири методи автентифікації: на засадах знань, на засадах фізіологічної біометрії, на засадах поведінкової біометрії та багатофакторні методи.

Автентифікація на засадах знань (тобто текстова або графічна) успадковує велику кількість користувачів та має відносно вищу зручність. Вразлива перед різними атакуючими технологіями (наприклад, атаками "перегляд з плеча" та атаками "побічних каналів"), які викрадають або виводять секрети, засновані на знаннях користувачів [1, 2]. Автентифікація на основі фізіологічної біометрії має відносно вищу безпеку, але зазвичай вимагає спеціалізованого обладнання (сканера відбитків пальців, камери глибини та райдужки). Крім того, фізіологічні біометричні дані є не відновлюваними, і вони можуть назавжди втратити ефективність безпеки. Поведінкова біометрія змінюється з часом і стикається з низьким рівнем чутливості сенсорів, що може зменшити продуктивність отримання доступу. Двофакторна автентифікація спрямована на надання найбільш безпечного контролю доступу за допомогою більше ніж однієї метрики [3]. Зокрема, комбінування різних метрик автентифікації без належного підходу обмежує підвищення безпеки, і зручність суттєво погіршується, якщо користувачеві потрібно надати декілька метрик автентифікації окремо. Надійність автентифікації користувача можна значно підвищити, якщо використати два або більше факторів, щоб створити набагато більший виклик для зловмисника. Автентифікація на мобільних пристроях відіграє важливу роль у захисті ІзОД користувача і запобіганні будь-якому несанкціонованому доступу до пристроїв.

Список літератури

1. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів, 2022.

2. R. Saifan, A. Salem, D. Zaidan, and A. Swidan, “A survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices,” Journal of Social Sciences (COES&RJ-JSS), vol. 5, pp. 29–41, 2016.

3. Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu “User Authentication on Mobile Devices: Approaches, Threats and Trends” Computer Networks vol.170, 2020.

АНАЛІЗ ЕФЕКТИВНОСТІ СКАНЕРУ OpenVAS ТА ЙОГО ВДОСКОНАЛЕННЯ

Скляров В.В., Олешко І.В.
Харківський національній університет радіоелектроніки, Харків, Україна

Виявлення несанкціонованого доступу в комп'ютерну мережу або несанкціонованого управління нею мають важливе значення для забезпечення безпеки її функціонування.

, присвячене аналізу ефективності сканера вразливостей OpenVAS та розгляду можливостей для його вдосконалення, відіграє важливу роль в контексті постійного зростання кіберзагроз та вразливостей у програмному забезпеченні та мережах [1, 2].

Метою доповіді є аналіз ефективності сканера OpenVAS та вдосконалення його функціональності для підвищення рівня кібербезпеки.

В доповіді наводяться результати, які показують переваги сканера вразливостей OpenVAS у порівнянні з аналогами. OpenVAS має високу ефективність виявлення вразливостей, open-source формат розробки, а також надає можливість додавання спеціалізованих тестів, які спрямовані на виявлення конкретних загроз.

В ході вдосконалення сканера OpenVAS, були додані нові тести, спрямовані на виявлення вразливостей, які можуть бути використані зловмисником для реалізації мережевої атаки DDoS, а також SQL-ін'єкції [3]. Після отримання результатів дослідження були розроблені стратегії та підходи для оптимізації роботи OpenVAS з метою зменшення помилкових спрацювань та підвищення швидкості виявлення вразливостей.

Наведені дані показують ефективність та актуальність використання сканера вразливостей OpenVAS для аналізу безпеки комп'ютерних мереж та систем.

У роботі надаються рекомендації для подальших кроків у розвитку і вдосконаленні сканера OpenVAS з метою підвищення рівня кібербезпеки в цифровому середовищі.

Список літератури

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Є. Остапов, С. П. Євсеєв, О.Г. \Король. – Львів: «Новий Світ-2020», 2020. - 678 с.

2. Poddubnyi V., Sievierinov O., Pustomelnik, O. Менеджмент вразливостей як складова частина політики безпеки ІТС. *Системи управління, навігації та зв'язку. Збірник наукових праць*, 4(62), 2020. - 55-58.

3. Парасрам Шива, Замм Алекс, Херіянто Теді, Алі Шакіл, Буду Даміан, ЙохансенДжерард, Аллен Лі. Kali Linux. Тестування на проникнення та безпеку. - СПб.:Пітер, 2020. - 448 с.

СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІДПРИЄМСТВА ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ

Гріненко Т.О., Шаповал М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Впровадження нових елементів технологічної інфраструктури має великий спектр ризиків, що пов'язані з обробкою персональних даних. Питання захисту персональних даних постає особливо гостро для державних установ та організацій, які в силу своєї діяльності збирають й обробляють відомості про фізичну особу. Відповідно до Законів України «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах» персональні дані повинні захищатись від несанкціонованого доступу, модифікації та розповсюдження.

Метою доповіді є обґрунтування вимог до систем захисту персональних даних для інформаційних (автоматизованих) систем, порядку проведення робіт з розробки системи захисту персональних даних підприємства та оцінки ефективності такої системи.

Для забезпечення інформаційної безпеки необхідно використовувати комплексний підхід, тобто необхідно систематизувати усі заходи щодо захисту персональних даних у п'ять рівнів захисту: нормативно-правовий, організаційний, інженерно-технічний, апаратний та апаратно-програмний. Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації [1].

Мінімізувати неконтрольоване поширення інформації за межі інформаційних систем, у яких вона обробляється, можна шляхом впровадження систем протидії внутрішнім загрозам чотирьох класів: системи моніторингу та аудиту; системи автентифікації; системи, що реалізує засоби шифрування; системи виявлення і попередження витоку інформації (DLP-системи) [2].

Процес обробки та захисту персональних даних повинен ґрунтуватися на підході, який передбачає систематичне оцінювання ризиків, які можуть виникнути для суб'єктів відносин, пов'язаних з персональними даними. Управління ризиками полягає в описі всіх процесів роботи з даними усередині й ззовні організації, що дозволить проводити пошук найбільш вразливих місць у системі захисту інформації.

Список літератури

1. НД ТЗІ 3.7-003-05 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Електрон. ресурс]: – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

2. Гулак Г.М., Козачок В.А., Складанний П.М., Бондаренко М.О., Вовкотруб Б.В. Системи захисту персональних даних в сучасних інформаційно- телекомунікаційних системах. *Сучасний захист інформації*. 2017. Т. 30. №2. С. 65-70. DOI: http://nbuv.gov.ua/UJRN/szi_2017_2_12.

КЛАСТЕРИЗАЦІЯ СТРУКТУРИ ДНК ДЛЯ ФОРМУВАННЯ ГОМОМОРФНИХ ГРУП

Євгеньєв А.М., Красінська С.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Використання перетворень на основі математичної системи ДНК надає можливість формування комбінованої інформаційної системи у геноміці, біоінформатиці та пов'язаних дисциплінах, оскільки вона допомагає в розумінні функціональних доменів, регуляційних мотивів у генах та інших аспектах генетичної інформації.

Метою доповіді є дослідження кластеризації структур ДНК, яка полягає в групуванні схожих послідовностей або патернів на основі певних критеріїв схожості. Використовуючи різноманітні алгоритми і методи можна ідентифікувати групи, що мають спільні характеристики.

Термін "гомоморфні групи" може вказувати на групи, що містять гомоморфні послідовності ДНК. Гомоморфія в математиці та біології вказує на подібність структур або функцій, яка виникає в результаті подібного розвитку або еволюційних процесів.

Отже, кластеризація структури ДНК для формування гомоморфних груп полягає в тому, щоб групувати послідовності ДНК на основі їх схожості, що може бути визначена за допомогою різних критеріїв, таких як послідовність нуклеотидів, структурні особливості або функціональні властивості [1].

При застосуванні теорії груп до кластеризації структур ДНК основна ідея полягає в тому, щоб розглядати різні послідовності ДНК як елементи групи, а операції над ними (наприклад, мутації, інверсії, вставки тощо) як операції в цій групі.

Комбінування ДНК систем та математичних перетворень в контексті теорії груп дозволяє виділити наступні кластери та групові перетворення:

− групи симетрії: розглядати різні структури ДНК з точки зору їхніх симетрій. Наприклад, паліндромні послідовності в ДНК можуть мати властивості симетрії, які можна описати за допомогою груп;

− дії груп на множині: розглядати як різні операції (мутації, інверсії тощо) діють на послідовності ДНК, та як ці дії формують групу;

− гомоморфізми груп: ідентифікувати структурні або функціональні відповідності між різними послідовностями ДНК, які можна описати за допомогою гомоморфізмів між групами;

− кластеризація на основі групової структури: використовувати властивості груп для кластеризації послідовностей ДНК, враховуючи гомоморфні відносини.

Список літератури

1. Petoukhov, S.V. Genetic coding and united-hypercomplex systems in the models of algebraic biology. *BioSystems*. 2017. Vol. 158. P. 31-46. DOI: https://doi.org/10.1016/j.biosystems.2017.05.002.

МЕТОДИ ЗАХИСТУ СУЧАСНИХ МЕСЕНДЖЕРІВ

Єгорова Н.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні месенджери стали повноцінними комунікаційними центрами, які крім обміну повідомленнями реалізують голосовий та відеозв'язок, обмін файлами чи веб-конференції. Тому безпека та надійність месенджерів є надзвичайно важливими аспектами їх використання. **Метою доповіді** є дослідження та обгрунтування методів захисту сучасних месенджерів. **В доповіді** надані результати аналізу вразливостей сучасних месенджерів, дослідження та порівняльного аналізу існуючих методів та засобів захисту [1]. Найактуальнішими вразливостями месенджерів є такі [2]:

1. Витік даних. Зловмисник отримує максимальний доступ до конфіденційної інформації месенджера шляхом перехоплення відправлених повідомлень, вилучення даних з хмари чи успішної автентифікації.

2. Розкриття місцезнаходження.

3. Вразливість коду або компрометуюче програмне забезпечення. Зловмисник може отримати повний контроль над вашим пристроєм, залишаючись непоміченим.

Безпека месенджерів забезпечується використанням спеціальних методів захисту [2]:

1. Наскрізне шифрування. Забезпечує конфіденційність при передачі повідомлень у месенджері.

2. Відкритий вихідний код. З його допомогою можна проводити комплексний аудит безпеки для виявлення та усунення слабких місць.

3. Шифрування резервних копій у хмарі. Не дозволяє зловмиснику успішно атакувати хмарну інфраструктуру та виток конфіденційної інформації.

4. Підтримка однорангового з'єднання. Ця функція виключає участь третьої сторони, оскільки надіслані повідомлення надходять безпосередньо на пристрій адресата.

5. Використання двофакторної автентифікації.

Для забезпечення високого рівня протидії атакам необхідно використовувати комплексний підхід до забезпечення безпеки, що дозволить корпоративним і приватним користувачам мінімізувати ризики.

Список літератури

1. Арчакова А.І., Сєвєрінов О.В. (2019). Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах. *Комп'ютерні та інформаційні системи і технології.*

2. Jain V., Sahu D.R., Singh Tomar D. An Approach to Identify Vulnerable Features of Instant Messenger. 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP). 2020. P. 71-80. DOI: https://doi.org/10.1109/ISEA-ISAP49340.2020.235003.

3. Найбезпечніші месенджери 2022 року [Електронний ресурс] – URL: https://gloss.ua/ua/lifestyle/139268-najbezpechnishi-mesendzheri-2022-roku.

ШТУЧНИЙ ІНТЕЛЕКТ В КІБЕРАТАКАХ

Ніконенко Д.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки Харків, Україна

Метою доповіді є опис потенційних загроз, які штучний інтелект може становити для кібербезпеки. У галузі кібербезпеки штучний інтелект набирає все більшої популярності, оскільки його можна використовувати для створення нових методів виявлення та протидії кібератакам.

Через те, що штучний інтелект швидко навчається на великих обсягах даних, можна розробляти нові методи атак. Швидкість обробки даних можна використовувати для аналізу великих наборів даних щоб адаптуватись під поведінку користувачів, це допоможе знайти шаблони, які можуть бути використані для розробки фішингових атак та зробити ці програми важчими для виявлення антивірусним програмним забезпеченням [1]. Наприклад, можна зробити програму, яка може шифрувати файли користувача та вимагати викупу.

Штучний інтелект можна використовувати для автоматизації кібератак [2-4]. Це може призвести до збільшення їх частоти та масштабу. Наприклад, коли буде автоматизовано робитись часті масові атаки на цілі, які не мають достатньої захисту, можна буде легко отримати якісь цінні данні, витративши на це менше ресурсів.

Також, його можна використовувати для атаки на критичну інфраструктуру, наприклад, на енергосистеми або транспортну систему. Це може призвести до значних економічних збитків і навіть до людських жертв.

Проведений аналіз показав, що використання штучного інтелекту для реалізації кібератаках є потенційною загрозою. Організації повинні бути готові до цієї загрози та розробляти заходи для протидії новим загрозам. Ці заходи можуть включати в себе:

– впровадження систем виявлення кібератак;

– розробку політик та процедур безпеки;

– підвищення обізнаності співробітників про кіберзагрози.

Список літератури

1. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. DOI: 10.31673/2409-7292.2020.04061

2. Mathew A., Amudha P. and Sivakumari S. Deep Learning Techniques: An Overview. In book: Advanced Machine Learning Technologies and Applications. January 2021. https://www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview.

3. Al Musawi, Ahmad. (2018). Introduction to Machine Learning. https://www.researchgate.net/publication/323108787_Introduction_to_Machine_Learning.

4. Dipankar Dasgupta, Zahid Akhtar, Sajib Sen. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling & Simulation. September 2020.

БЕЗПЕКА ДАНИХ В ВЕБ-ДОДАТКАХ: ЯК ЗАХИСТИТИ ВІД UNION-BASED SQL INJECTION

Ляшко М.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді є розгляд однієї з найпоширеніших форм SQL ін'єкцій - "Union-based SQL Injection," та методів виявлення та запобігання цій загрозі. "Union-based SQL Injection" відноситься до технічних вразливостей, які дозволяють зловмисникам об'єднувати дані з різних таблиць бази даних через SQL-запити [1]. Зловмисники включають операцію UNION у SQL-запит, щоб об'єднати результати свого запиту з результатами легітимного запиту до бази даних. Це може призвести до витоку конфіденційних даних, такі як імена користувачів, паролі, номери кредитних карт, а також іншу конфіденційну інформацію з бази даних. Зловмисники можуть використовувати цю загрозу для незаконного доступу до системи та зміни її функціональності [2, 3].

Для запобігання "Union-based SQL Injection" необхідно вживати низку конкретних заходів безпеки:

– обмеження прав доступу. Користувачі повинні мати доступ лише до даних та функцій, які є необхідними для їхньої роботи, і ні в якому разі не повинні виконувати SQL-запити, які необхідні лише адміністраторам;

– моніторинг безпеки та аудит подій. Система повинна слідкувати за всіма SQL-запитами, що виконуються, та реагувати на незвичайну активність;

– вимкніть виведення помилок – у більшості випадків атакувальники використовують помилки, що відображаються програмою, для перегляду результатів бази даних;

– використання параметризованих запитів – ніколи не долучайте введені користувачем дані у вигляді рядків до SQL-запиту. Замість цього створюйте запит у коді і потім додаєте користувацькі дані як параметри;

– обмеження довжини введення – обмеження довжини полів вводу може запобігти атакам SQL-ін'єкції UNION;

– білий список символів – дані користувачів, які використовуються в SQL-запитах, повинні бути обмежені лише безпечними символами;

– чорний список символів – забороняйте загально вживані символи, які використовуються в SQL-ін'єкційних векторах;

– налаштування аудиту бази даних і встановлення системи виявлення/запобігання вторгнення (IDS/IPS).

Список літератури

1. What is SQL Injection UNION Attacks? GeeksforGeeks.com – URL: https://www.geeksforgeeks.org/what-is-sql-injection-union-attacks/

2. Union SQL Injection: How It Works and 6 Tips for Prevention. Bright – URL: https://brightsec.com/blog/union-sql-injection/

3. SQL injection UNION attacks. PortSwigger.net URL: https://portswigger.net/web-security/sql-injection/union-attacks

АНАЛІЗ XSS–АТАК

Хая А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки Харків, Україна

В епоху інтернет-технологій, коли цифровий світ стає все більш необхідною частиною нашого повсякденного життя, безпека в інтернеті стає питанням критичної важливості. Однією з найпоширеніших та загрозливих атак, з якими стикаються веб-розробники і користувачі, є XSS-атака, або "міжсайтовий скриптінг". Ця атака, відома своєю вразливістю та складністю виявлення, може мати серйозні наслідки, які поширюються від крадіжки конфіденційної інформації до поширення шкідливих програм. Таким чином, зловмисний сценарій може отримати доступ до важливих даних, таких як файли cookie, сесійні маркери та інша конфіденційна інформація. Більше того, ці сценарії можуть навіть змінювати вміст сторінки HTML на вразливому веб-сайті.

Метою доповіді є аналіз XSS-атак, які передбачають вставлення шкідливих сценаріїв на безпечні та надійні веб-сайти. Зловмисники використовують ці атаки для доставки шкідливого коду іншим користувачам через веб-додатки. Враховуючи зростання Інтернет-технологій та їх важливість у повсякденному житті, безпека в Інтернеті є надзвичайно важливою. Виявлення та запобігання атакам XSS вимагає постійного моніторингу та покращення безпеки веб-додатків і веб-сайтів [1, 2].

XSS-атаки стають можливими, коли виконуються дві основні умови:

– ненадійне джерело даних - дані надходять в веб-програму з ненадійного джерела, часто через веб-запит або інші вхідні механізми;

– включення даних без перевірки у вихідні дані - отримані дані включаються в динамічний веб-контент, який потім надсилається користувачеві без належної перевірки на наявність шкідливого вмісту.

Наслідки XSS-атак можуть бути різноманітними, включаючи доступ зловмисника до особистих даних, таких як файли cookie або інформація про сеанс, перенаправлення користувача на контент, контрольований зловмисником, або виконання інших шкідливих дій на комп'ютері користувача під прикриттям вразливого веб-сайту [3].

Отже, зловмисники можуть використовувати XSS для надсилання шкідливих сценаріїв користувачам, які не мають підстав підозрювати небезпеку. Загалом, XSS-атаки є серйозною загрозою і вимагають постійної уваги до безпеки веб-додатків та сайтів для їх вчасного виявлення та запобігання.

Список літератури

1. Cross Site Scripting (XSS). 2023. URL: Cross Site Scripting (XSS) | OWASP Foundation

2. Port Swigger. Cross site scripting. 2022. URL: What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy (portswigger.net)

3. OWASP. Cross Site Scripting (XSS). 2022. URL: Cross Site Scripting (XSS) | OWASP Foundation.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІДЕОКОНТЕНТУ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ

Кібірєв Д.О., Федорченко В.М.
Харківський національний університет радіоелектроніки Харків, Україна

Дослідження у сфері захисту відеоконтенту від несанкціонованого копіювання залишаються актуальними в сучасному світі, оскільки зростає кількість випадків піратства та незаконного копіювання відеоматеріалів. Об'єктом дослідження є конкретні типи відеоконтенту, такі як фільми, телепередачі, відеоролики або стрімінгові послуги.

Метою доповіді є аналіз методів, які дозволяють запобігати копіюванню, зламу та незаконному використанню відеоматеріалів. В роботі проведений аналіз існуючих методів захисту відеоконтенту: розгляд і оцінка різних методів та технологій, які використовуються для захисту відеоматеріалів від несанкціонованого копіювання. Це включає огляд технологій цифрових водяних знаків, контролю доступу та інших заходів безпеки [1, 2].

Проведений аналіз показав, що потрібна розробка нових технічних моделей, які забезпечують ефективний захист відеоконтенту. Це може включати розробку алгоритмів цифрового водяного знаку, методів автоматичного виявлення та видалення незаконного відеоконтенту, а також моделей контролю доступу.

Розвиток штучного інтелекту та машинного навчання також може знайти застосування в цій галузі. Наприклад, розробка алгоритмів автоматичного виявлення та видалення незаконного відеоконтенту або розробка моделей, які можуть прогнозувати ризик копіювання на підставі аналізу певних ознак..

Результати проведених досліджень можуть допомогти виробникам відеоконтенту вдосконалити свої заходи захисту для збереження їх інтелектуальної власності. Результати дослідження можуть допомогти провайдерам стрімінгових послуг розробити та впровадити ефективні заходи захисту, які забезпечать безперервну та безпечну доставку відеоконтенту своїм абонентам. Для користувачів: Аналіз та розробка методів захисту може забезпечити кінцевим користувачам безпеку та конфіденційність при споживанні відеоконтенту.

Список літератури

1. Martovytskyi V., Ruban I., Bolohova N., Sievierinov O., Zhurylo O., Permiakov O., Nosyk A., Nepokrytov D., Krylenko I. (2021). Development of Methods for Generation of Digital Watermarks Resistant to Distortion. Eastern-European Journal of Enterprise Technologies, 6(2), 114.

2. Gvozdov R., Poddubnyi V., Sieverinov O., Buhantsov A., Vlasov A., Sukhoteplyi V. (2021, October). Method of Biometric Authentication with Digital Watermarks. In *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 569-571). IEEE.

СЕКЦІЯ 6
ЦИВІЛЬНА БЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Керівник секції: д.т.н. доц. О. В. Третьяков, НАУ, Київ
Секретар секції: к.т.н., доц. Є В. Доронін, НАУ, Київ

Підсекція 1

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Доронін Є.В.
Національний авіаційний університет, Київ, Україна
Бондаренко С.В.
Національна академія Національної гвардії України, Харків, Україна

Критична інфраструктура включає в себе активи, системи, об’єкти, мережі та інші елементи, від яких залежить національна безпека, економічна життєздатність, здоров’я та безпека суспільства. Події останніх років показали, що стійкість об'єктів критичної інфраструктури (ОКІ) в умовах російської загрози є актуальною задачею. Від того, наскільки стійкою будуть ОКІ, настільки міцною буде й економіка та безпека нашої Держави. Однією з найважливіших складових вирішення цієї проблеми є створення системи захисту ОКІ від впливу різних чинників [1–3]. Із завданнями підвищення стійкості ОКІ пов'язана необхідність розробки нових підходів і використання сучасних технологій захисту ОКІ.

Метою доповіді є проведення аналізу сучасних систем захисту ОКІ. В доповіді наводяться результати проведених досліджень систем захисту. Наведені дані вказують на недоліки в існуючих системах, що забезпечують стійкість роботи. Встановлено, що основними завданнями державної системи захисту критичної інфраструктури є: 1) формування та реалізація державної політики у сфері захисту критичної інфраструктури та забезпечення національної системи стійкості; 2) здійснення функціонального управління національною системою захисту критичної інфраструктури та національною системою стійкості; 3) забезпечення координації діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об’єктів критичної інфраструктури. Пріоритетний розподіл наявних ресурсів на відповідну підгрупу інфраструктури може посилити безпеку країни, підвищити стійкість і знизити ризики.

Список літератури

1. Конституція України від 28.06.1996 р. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Закон України Про критичну інфраструктуру від 16.11.2021 р. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Закон України Про правовий режим воєнного стану від 14.04.2022 р. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

ВИЗНАЧЕННЯ ГІГІЄНІЧНИХ ПАРАМЕТРІВ ПОВІТРЯ РОБОЧОЇ ЗОНИ ХІМІЧНИХ ВИРОБНИЦТВ

Доронін Є.В., Вальченко О.
Національний авіаційний університет, Київ, Україна

Гігієнічні параметри робочої зони відіграють важливу роль у забезпеченні нормального здоров'я людини та її функціонування під час виробничого процесу. Так, недопустимі параметри мікроклімату виробничих приміщень можуть привести до хронічних захворювань простудного характеру, висока або низька запиленість робочих місць може привести до хронічних захворювань легенів, підвищена напруженість електричних полів — до захворювань центральної нервової системи і таких прикладів можна приводити нескінченно. У цих випадках необхідно контролювати та регулювати параметри повітря робочої зони. Тобто з метою зниження рівня захворюваності працівників необхідно постійно моніторити усі параметри повітря.

Метою доповіді є дослідження та регулювання параметрів робочої зони виробництв хімічної галузі з урахуванням особливостей організації виробничого процесу.

В доповіді наводяться результати дослідження параметрів робочої зони виробництва мінеральних речовин. Наведені дані показують, що на виробництвах даного профілю основними шкідливими та небезпечними факторами [1, 2, 3] є: підвищена вологість, недостатня освітленість робочих місць, підвищена температура, великий рівень виробничих випромінювань тощо.

При аналізі даних встановлено, що превтщення санітарно-гігієнічних показників на робочих місцях викликані використанням застарілого обладнання, та неправильною організацією робочих місць.

З метою приведення даних факторів у відповідність до вимог нормативних документів рекомендується низка заходів, що дозволить мінімізувати вірогідність ризику травмування та професійних захворювань на робочих місцях потенційно небезпечних підприємств.

Список літератури

1. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. Київ, 1999. 36 с.

2. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. Міністерство охорони здоров'я України. Головний державний санітарний лікар України. Постанова N 37 від 01.12.99. Поточна редакція. URL: https://zakon.rada.gov.ua/rada/show/va037282-99#Text. [дата звернення 17.10.2023].

3. ДСТУ-Н Б А 3.2-1:2007. Настанова зодо визначення небезпечних і шкідливих факторів. Київ : Мінрегіонбуд України. 45 с.

УПРАВЛІННЯ РИЗИКАМИ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ В ЗОНІ ВЕДЕННЯ БОЙОВИХ ДІЙ

Козлітін О.О., Третьяков О.В.
Національний авіаційний університет, Київ, Україна

Одним із перспективних напрямків дослідження в галузі оцінки воєнно-техногенних загроз і ризиків для об'єктів транспортної (ОТІ) інфраструктури в зоні ведення бойових дій є аналіз кризових ситуацій та пов'язаних з ними каскадних («доміно») ефектів, що в подальшому внаслідок техногенної аварії можуть призвести до значних людських жертв серед населення та не бойових втрат серед військовослужбовців.

Метою доповіді є розробка імітаційна модель для оцінювання загрози виникнення каскадних ефектів для різних сценаріїв розвитку подій у зоні впливу на ОТІ для отримання необхідного набору даних системи підтримки прийняття рішень. Математична модель загроз для ОТІ будується на основі фундаментальних положень сучасної теорії графів [1]. Побудова математичної моделі здійснюється шляхом виконання таких процедур:

- визначення подій в сценарії розвитку ситуації (складові елементи сценарію, що здійснюють потенційний вплив на реалізацію загрози);
- визначення множини можливих станів подій, що впливають на рівень загрози.
- формування сценаріїв розвитку загрози (визначення ланок, що складаються з пар: «подія – перехід в заданий стан»), що призводять до реалізації загрози, представлено структурно-логічною моделлю розвитку кризової ситуації, що має складну структуру за різним варіантами розвитку сценарію на прикладі ОТІ [2];
- формування оргграфу сценаріїв загроз (структурно-логічна модель, що включає всі сценарії реалізації загрози);
- оцінка ймовірностей станів подій та їх переходів;
- оцінювання ймовірності реалізації сценаріїв загроз.

Застосування такої імітаційної моделі для каскадних ефектів, дає можливість отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями і дозволяє здійснити оцінювання загроз для ОТІ за величиною імовірності настання подій і переходів між ними.

Список літератури

1. Робін Уілсон. Введення в теорію графів. 2019. 240 с.
2. Чумаченко С.М., Мурасов Р.К., Мельник Я.В. Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для потенційно-небезпечних об'єктів критичної інфраструктури в умовах збройного конфлікту на Сході України. *Сучасні інформаційні технології у сфері безпеки та оборони* 118 № 1 (40)/2021, с. 117-122. DOI: https://doi.org/10.33099/2311-7249/2021-40-1-117-122.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кічата Н.М., Третьяков О.В.
Національний авіаційний університет, Київ, Україна

Побудова сучасної системи захисту критичної інфраструктури (КІ) – це складний та багатоаспектний процес, який вимагає поєднання законодавчо-правових, технічних, організаційних та міжнародних підходів для забезпечення безпеки та стійкості цих важливих об’єктів.

Особливість небезпеки полягає в тому, що коли робота одного об’єкта КІ порушується, це може вплинути на роботу інших об’єктів і систем через їх взаємозалежність, спричиняючи такий ефект, який іноді називають «ефектом доміно» [1].

Але деяким аспектам цієї важливої проблематики, зокрема питанням розробки ефективних стратегій розвитку державного управління для критично важливих об’єктів, приділено не достатньо уваги.

Метою доповіді є розробка рекомендацій щодо підвищення ефективності реалізації державної політики у сфері захисту критичної інфраструктури.

КІ України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких може призвести до значних негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [2].

Забезпечення безпеки і захисту КІ є однією з ключових функцій держави, оскільки недостатність або втрата функціонування таких систем може призвести до серйозних наслідків для економіки, суспільства та національної безпеки.

Система захисту КІ України має взаємодіяти з Єдиною державною системою цивільного захисту (ЄДСЦЗ) в рамках загальної системи безпеки країни. Співпраця між цими двома системами полягає в обміні інформацією, координації дій та спільному вирішенні питань, пов'язаних з захистом національної безпеки та готовності до надзвичайних ситуацій.

Ключовим аспектом співпраці між системою захисту КІ та ЄДСЦЗ в Україні є координація заходів під час надзвичайних ситуацій: Обидві системи повинні працювати разом під час надзвичайних подій, таких як природні катастрофи, техногенні аварії, терористичні загрози тощо. Координація дій дозволяє ефективно взаємодіяти та вирішувати ситуації.

Список літератури

1. Бірюков Д.С. Про доцільність та особливості визначення критичної інфраструктури в Україні: Аналітична записка. [Електронний ресурс]. – Режим доступу :http://www.niss.gov.ua/articles/1026/.

2. Зелена книга з питань захисту критичної інфраструктури в Україні :зб. матер. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. – К.: НІСД, 2016. – 176 с.

ОЦІНКА КОМБІНОВАНОГО ВПЛИВУ НА ВОГНЕСТІЙКІСТЬ ЗАЛІЗОБЕТОННОЇ РЕБРИСТОЇ ПЛИТИ

Васильченко О.В., Рубан А.А.
Національний університет цивільного захисту України, Харків, Україна

Можна очікувати, що на об'єктах підвищеної небезпеки (ОПН) під час комбінованого впливу вибуху і пожежі наслідки для несучих конструкцій каркаса і огороджувальних конструкцій будуть відрізнятися [1].

Якщо несучі конструкції витримають такий вплив, то огороджувальні конструкції, які зазвичай виконуються із залізобетону, що володіють меншим запасом міцності, але обрані за принципом відповідності класу вогнестійкості можуть не витримати комбінованого впливу.

Метою доповіді є вивчення комбінованого впливу вибуху і подальшої пожежі на прикладі залізобетонної ребристої плити не тільки з точки зору умов збереження її стійкості, а й можливості подальшої експлуатації. Для цього оцінювалися втрати міцності, особливості утворення тріщин, розрахунок критичних температур арматури і меж вогнестійкості залізобетонної ребристої плити при комбінованому впливі.

В роботі [2] запропоновано методику дослідження поведінки залізобетонної ребристої плити при комбінованому впливі, яка підходить і для інших згинальних конструкцій.

Оціночні розрахунки показали, що виключення з роботи частини стисненого шару бетону залізобетонної ребристої плити, яке сталося в результаті вибуху через утворення тріщин, сильно позначається на зниженні її вогнестійкості. На підставі цих розрахунків з'являється можливість враховувати необхідні параметри ребристих плит при проектуванні і експлуатації конструкцій ОПН.

Розрахунки за запропонованою методикою дозволяють обґрунтовувати заходи щодо підвищення безпеки огороджувальних залізобетонних конструкцій перекриття каркасних промислових будівель ОПН в разі аварійного вибуху та пожежі. Також вони дозволяють прогнозувати відносно безпечну кількість вибухової речовини в технологічному процесі ОПН, що не приводить до катастрофічних наслідків.

Список літератури

1. Roytman V.V., Pasman H.J., Lukashevich I.E. The Concept of Evaluation of Building Resistance against combined hazardous Effects “Impact-Explosion-Fire” after Aircraft Crash. Fire and Explosion Hazards: Proceedings of the Fourth International Seminar. 2003, Londonderry, NI, UK. P. 283-293.

2. Vasilchenko Alexey, Danilin Olexandr, Lutsenko Tatiana, Ruban Artem (2021) Features of Evaluation of Fire Resistance of Reinforced Concrete Ribbed Slab under Combined Effect "Explosion-Fire". Materials Science Forum, Vol. 1038, pp. 492-499. https://doi.org/10.4028/www.scientific.net/MSF.1038.492.

ПІДВИЩЕННЯ ВОГНЕСТІЙКОСТІ ЗАЛІЗОБЕТОННОЇ ФЕРМИ ПРИ ВИКОРИСТАННІ ФІБРОБЕТОНУ

Васильченко О.В., Царенко Г.Р.
Національний університет цивільного захисту України, Харків, Україна

Відомо, що дисперсне армування бетону сприяє підвищенню межі вогнестійкості конструкції [1]. Однак, вартість фібробетону досить висока (хоча і менша за вартість сталі), і тому використання його для виготовлення ферм вважається неекономічним. Крім того, при всіх перерахованих перевагах виробів з фібробетонів недостатньо дослідженою залишається проблема розрахунку їхньої стійкості при пожежі.

Метою доповіді є вивчення можливості використання фібробетону на основі сталевої фібри тільки в окремих, найбільш напружених елементах ферми, що працюють на розтяг. Тому, основним завданням даної роботи є виявлення розрахунковим шляхом найбільш напружених елементів ферми, що працюють на розтягування, розрахунок напруги арматури в них та меж вогнестійкості, а далі – порівняння отриманих характеристик з характеристиками, розрахованими для заміни в цих елементах звичайного важкого бетону на фібробетон.

Розрахунки проводилися у програмі "SCAD" на прикладі залізобетонної кроквяної ферми з паралельними поясами прольотом 18 м для рівномірно розподілених навантажень 5,50 кПа та 8,50 кПа [2].

На підставі оціночних розрахунків показано, що використання фібробетону на основі сталевої фібри в окремих, найбільш напружених елементах залізобетонної ферми значно збільшує її несучу здатність, а також підвищує межу вогнестійкості. Перевагою цього методу є можливість застосування фібробетону для значного посилення ферм при збільшенні робочого навантаження без зміни їх зовнішнього вигляду і перерізу елементів; підвищення економічності з допомогою зниження ваги робочої арматури і, навіть, забезпечення необхідної межі вогнестійкості ферми з допомогою підвищення меж вогнестійкості її окремих елементів.

Список літератури

1. Vasilchenko Alexey, Doronin Evgeny, Chernenko Oleksandr, Ponomarenko Ivan (2019) Estimation of fire resistance of bending reinforced concrete elements based on concrete with disperse fibers. IOP Conf. Series: Materials Science and Engineering 708 012075. https://doi.org/10.1088/1757-899X/708/1/012075.

2. Васильченко А.В., Хмыров И.М. Оценка огнестойкости железобетонной фермы при использовании фибробетона в ее отдельных элементах. Сб. науч. трудов НУГЗ Украины «Проблемы пожарной безопасности». – Вып.36.– Харьков: НУГЗУ, 2014. – С. 58-62.

ОРГАНІЗАЦІЯ МОНІТОРИНГУ ТРАНСПОРТНИХ ТРУБОПРОВІДНИХ КОМУНІКАЦІЙ ІЗ ВИКОРИСТАННЯМ БЕЗПІЛОТНОЇ АВІАЦІЇ

Федина В.П., Якимець І.В.
Національний авіаційний університет, Київ, Україна

Мінекономіки наказом від 27.04.2023 № 2610 затвердило «Правила безпеки в нафтогазодобувній промисловості», які поширюються на суб'єктів господарювання незалежно від форми власності та організаційно-правової форми, діяльність яких пов'язана з проектуванням, будівництвом, експлуатацією, ремонтом та реконструкцією об'єктів нафтогазодобувної промисловості, а також на діагностичні роботи, та ліквідацію аварій на нафтогазодобувних підприємствах [1].

Метою дослідження є розробка методики моніторингу транспортних трубопровідних комунікацій із використанням безпілотних повітряних суден.

В доповіді наводяться результати дослідження ефективності авіаційного патрулювання трубопровідних мереж за допомогою літаків, вертольотів та безпілотних повітряних суден.

Наведені результати досліджень показують, що найбільш ефективним і економічно вигідним методом обстеження нафто- і газо - трубопроводів є застосування безпілотних повітряних суден (БПС), які в режимі реального часу (FPV-дрони) надають якісні зображення та дозволяють виявляти:

- нафтові розливи,
- звалища,
- врізки,
- проведення робіт в охоронних зонах і т.д.

Для комплексної діагностики трубопроводів необхідно виконати низку дій [4]:

- складання технічного завдання та постановка завдань моніторингу;
- комплектація необхідного обладнання та підготовка до аерофотозйомки, вибір оптимальних камер та складання маршруту для БПС;
- аерофотозйомка місцевості;
- обробка та систематизація знімків та відеоматеріалів. За необхідності – складання 3D моделей місцевості, цифрових карт рельєфу тощо. (5)

Список літератури

1. https://oppb.com.ua/news/zatverdzheno-novi-pravyla-bezpeky-v-naftogazodobuvnij-promyslovosti
2. https://uk.wikipedia.org/wiki/Трубопровідний_транспорт
3. http.ns://buklibet/books/27710/
4. https://def-c.com/ua/services/monitoring-truboprovodiv/

ОЦІНКА ПРАЦЕЗДАТНОСТІ ТРАНСПОРТНОГО ПІДПРИЄМСТВА В УМОВАХ НАДЗВИЧАЙНОЇ СИТУАЦІЇ

Федина В.П., Бойко О.Ю.
Національний авіаційний університет, Київ, Україна

Оцінка та підвищення працездатності транспортного підприємства в умовах надзвичайних ситуацій, особливо техногенних катастроф, та своєчасна розробка планів реагування є надзвичайно актуальними, оскільки це не просто бізнес-міркування, а це фундаментальний компонент громадської безпеки, що безпосередньо впливає на безпеку працівників та оточуючих людей, може забезпечити безперервність роботи транспортного підприємства, до того ж, відіграє вирішальну роль у мінімізації економічних втрат та підвищенні загальної стійкості громади та регіону.

Метою доповіді є розробка рекомендацій для підвищення стійкості транспортного підприємства, яке працює в умовах надзвичайних ситуацій.

В доповіді наводяться результати дослідження діяльності ТОВ «Нова пошта», яке як і будь-який інший бізнес у цій галузі, стикається з низкою загроз і ризиків в надзвичайних ситуаціях, які можуть:

порушити роботу,

вплинути на обслуговування клієнтів,

зашкодити репутації та фінансовій стабільності.

Для забезпечення працездатності в умовах надзвичайних ситуацій, ТОВ «Нова пошта» має розробити і регулярно оновлювати комплексний план готовності до надзвичайних ситуацій та реагування на них, який враховує специфічні загрози та ризики, пов'язані зі стихійними лихами.

Інвестиції в надійну кібербезпеку, аварійне відновлення та страхове покриття можуть допомогти захистити діяльність та фінансову стабільність компанії в надзвичайних ситуаціях.

Наведені результати показують, що оцінка працездатності транспортного підприємства в умовах надзвичайної ситуації та вчасна розробка планів реагування може допомогти останньому пережити надзвичайну ситуацію [3].

Інвестуючи в готовність, навчання, стійкість інфраструктури, а також співпрацю, транспортні підприємства можуть зробити суттєвий внесок у загальну здатність регіону протистояти катастрофам і відновлюватися після них.

Список літератури

1. Електронний ресурс: Про затвердження правил техногенної безпеки у сфері цивільного захисту на підприємствах, в організаціях, установах та на небезпечних територіях https://zakon.rada.gov.ua/laws/show/z1006-07#Text

2.Електронний ресурс: Правила технічної безпеки https://www.sop.com.ua/article/933-pravila-technogenno-bezpeki

ІНФОРМАЦІЙНО-ЕНТРОПІЙНІ МЕТОДИ АНАЛІЗУ РИЗИКІВ ТА УПРАВЛІННЯ НАДІЙНІСТЮ В СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Безсонний В.Л.
Харківський національний економічний університет ім. С.Кузнеця,
Харків, Україна
Третьяков О.В.
Національний авіаційний університет, Київ, Україна

Критична інфраструктура визначається як система об'єктів, служб і активів, від яких безпосередньо залежить національна безпека держави, економічне благополуччя та здатність суспільства функціонувати належним чином. Це включає в себе ключові елементи енергетики, транспорту, зв'язку, охорони здоров'я, фінансів та інших сфер. Багато секторів економіки і безпосередньо залежать від стабільності та надійності критичної інфраструктури. зокрема, електроенергетика впливає на роботу промисловості, транспортних систем, медичних установ та інших секторів.

В сучасному світі критична інфраструктура стає потенційною мішенню для різноманітних загроз, від природних катастроф до кібератак. Зростаюча залежність від цифрових технологій збільшує ризик кіберзагроз, що можуть паралізувати цілі системи.

Принцип максимальної ентропії є фундаментальним методом в статистиці та теорії інформації, що використовується для визначення найбільш "невизначеної" (або найбільш непередбачуваної) розподілу ймовірності, який відповідає певному набору обмежень. У сфері управління ризиками принцип максимальної ентропії є корисним для оцінки ймовірностей різних сценаріїв, в умовах обмеженої інформації.

При застосуванні інформаційно-ентропійного управління надійністю аналізується невизначеність або непередбачуваність у поведінці системи і здійснюється оптимізація роботи на основі цього аналізу. Високий рівень ентропії вказує на нестабільність або велику невизначеність в поведінці системи. За обмеженої інформацію про систему використовується принцип максимальної ентропії для побудови найбільш об'єктивної моделі цієї системи. Інформація про ентропійний стан системи є основою для впровадження змін, які покращать її надійність.

Інформаційно-ентропійне управління надійністю дозволяє розробити більш гнучкі та адаптивні системи, які можуть краще справлятися з невизначеностями та ризиками, що існують у сучасному світі.

Список літератури

1. Cover T.M., Thomas J.A. Elements of Information Theory. Wiley-Interscience. 2006.
2. Безсонний В. Л., Третьяков О.В., Пляцук Л.Д., Некос А.Н. Ентропійний підхід до оцінки екологічного стану водотоку. Вісник Харківського національного університету імені В. Н. Каразіна, серія «Екологія». 2022. Вип. 27. С. 6–19.

ОПТИМІЗАЦІЯ СИСТЕМ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ІНФОРМАЦІЙНОЇ ЕНТРОПІЇ

Безсонний В.Л.
Харківський національний економічний університет імені С.Кузнеця, Харків, Україна
Третьяков О.В., Доронін Є.В.
Національний авіаційний університет, Київ, Україна

Компоненти будь-якої системи можуть мати різну важливість в контексті загальної місії системи або її функціональності. Для критичної інфраструктури, зокрема, деякі компоненти можуть бути набагато важливішими за інші, залежно від ролі, яку вони відіграють у системі.

Інформаційна ентропія використовується як міра невизначеності або непередбачуваності в системі. Цінність окремого компоненту визначається на основі його вкладу в загальну ентропію системи. Врахування залежностей між компонентами дозволяє визначити, які з них є найбільш критичними. Такий підхід базується на теорії графів, де компоненти представлені як вершини, а їх зв'язки — як ребра. При виборі, які компоненти системи необхідно захистити або оптимізувати, використовуються методи оптимізації на основі інформаційної ентропії для максимізації інформативності при обмежених ресурсах.

Завдання систем управління безпекою – забезпечити захист від потенційних загроз та реагування на непередбачені події. Інформаційно-ентропійні методи надають можливість розуміння та моделювання невизначеностей та ризиків, що супроводжують роботу систем.

Інформаційна ентропія дозволяє моделювати невизначеність у системах. Це особливо корисно для систем управління безпекою, де необхідно прогнозувати потенційні загрози та їх вплив. Використання інформаційно-ентропійних методів дає змогу оцінити ймовірність певних небажаних подій та їх наслідки, що дає можливість ефективніше управляти ризиками.

Отже, визначення важливості окремих компонентів системи з точки зору інформаційної цінності вимагає інтеграції підходів з теорії інформації, теорії графів та системного аналізу.

Інтеграція інформаційно-ентропійних методів в системи управління безпекою може допомогти у виявленні, аналізі та управлінні ризиками, надаючи системі засоби для адаптації до змінних умов і викликів.

Список літератури

1. Cover T. M., Thomas J. A. Elements of Information Theory (2nd ed.). 2006.

2. Resnick M. D. Adventures in Modeling: Exploring Complex, Dynamic Systems with StarLogo. Teachers College Press. 2007.

3. Безсонний В. Л., Третьяков О.В., Пляцук Л.Д., Некос А.Н. Ентропійний підхід до оцінки екологічного стану водотоку. Вісник Харківського національного університету імені В. Н. Каразіна, серія «Екологія». 2022. Вип. 27. С. 6–19.

ВИЯВЛЕННЯ, ОЦІНКА ТА РЕАГУВАННЯ НА ЗАГРОЗИ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Халмурадов Б.Д., Сацюк М.В.
Національний авіаційний університет. Київ. Україна

Під час війни критична інфраструктура є фундаментальним компонентом національної безпеки. Його вихід з ладу або значне порушення функціонування матиме масштабні руйнівні наслідки регіонального чи національного значення. Противник зосередив свої ракетні та безпілотні удари саме по об'єктах критичної інфраструктури. В першу чергу вона спрямована на досягнення такого руйнівного рівня своїх ударів, щоб створити екологічну, техногенну та гуманітарну катастрофу в умовах застосування звичайної зброї та обмеження застосування ядерної зброї. [1].

Тому проблема виявлення, оцінка та реагування на загрози об'єктам критичної інфраструктури є ключовими елементами для підтримання безпеки цих об'єктів. Об'єкти критичної інфраструктури можуть включати установи енергетики, охорони здоров'я, транспорту, фінансових систем, телекомунікацій та ін. є актуальною на сьогоднішній день.

На сьогоднішній день існує ряд математичних підходів для експертної оцінки можливих загроз і ризиків у сфері критичної інфраструктури. У країнах Європейського Союзу активно впроваджується системний підхід, заснований на оцінці загроз і ризиків за кількома критеріями [1,2].

Відомо, що методи експертних оцінок базуються на мобілізації професійного досвіду та інтуїції експертів. Такі методи оцінки загроз і ризиків використовують формальну теорію прийняття рішень в умовах невизначеності [2]. У разі виникнення надзвичайної ситуації центральною фігурою та суб'єктом прийняття рішення є особа, яка приймає рішення. Це може бути як одна особа, так і група людей, які виробляють колективне рішення, як правило, особа, яка приймає рішення є керівником або керівним органом, який формулює проблему, відіграє вирішальну роль у виборі рішення проблеми та відповідає за прийняте рішення.

В цілому, виявлення, оцінка та реагування на загрози об'єктам критичної інфраструктури є динамічним і комплексним процесом, який вимагає постійного вдосконалення та співпраці між різними структурами та організаціями. Організації, що відповідають за безпеку об'єктів критичної інфраструктури.

Список літератури

1. V. Popel, N. Zaika, S. M.Chumachenko I. O. General approaches to the assessment of threats to critical infrastructure using the method of expert assessment SWorldJournal Issue 18 / Part 1 DOI: 10.30888/2663-5712.2023-18-01-045

2. Assessment of threats to energy security, analytical report https://doi.org/10.53679/NISS-analytrep.2022.112. Kachynskyi A. B. Safety, threats and risk [Text] : scientific concepts and mathematical methods / A. B. Kachynskyi. K.: 2003. 472 p.

ПОПЕРЕДЖЕННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Халмурадов Б.Д., Манько О.А.
Національний авіаційний університет. Київ. Україна

В даний час у всьому світі, в тому числі в Україні різко загострилося питання забезпечення безпеки у зв'язку з зростаючою загрозою тероризму, що набуває міжнаціонального характеру. Найбільш частими об'єктами атак терористів є місця масового скупчення людей, при цьому однією з найзначніших загроз серед різних проявів тероризму є тероризм на транспорті. Одним з способів реалізації терористичного акту є несанкціоноване втручання в роботу об'єктів критичної інфраструктури. На сьогодні система забезпечення транспортної безпеки України вразлива. У зв'язку з чим потрібен комплексний підхід у вирішенні проблем пов'язаних із забезпеченням безпеки на об'єктах транспортної інфраструктури. Тому забезпечення транспортної безпеки є одним з ключових завдань забезпечення комплексної безпеки країни.

Метою доповіді є побудова математичних моделей, які дозволять ранжувати перелік потенційних загроз щодо масштабності та ймовірності здійснення актів з несанкціонованого втручання у роботу транспортного засобу. У більшості випадків аналіз потенційних загроз скоєння актів з несанкціонованого втручання щодо транспортного засобу проводять методом ранжування потенційних загроз з урахуванням масштабності нанесення ймовірного збитку, а також ступеня ймовірності реалізації актів несанкціонованого втручання за допомогою методу експертних оцінок (метод Дельфі). Після створення матриці за результатами опитування експертів, складаються між собою шляхом складання елементів матриць, з метою отримання результативних матриць парних порівнянь загроз за масштабністю (Р1) і ступеня ймовірності вчинення актів несанкціонованого втручання (Р2) в діяльність транспортного засобу. Значення Рі є числовою характеристикою загрози знаходять шляхом додавання балів по рядку матриці, а значення Рij шляхом додавання балів по стовпцю матриці Рі. Пріоритет загрози за ступенем ймовірності реалізації АНВ (Р отні) розраховується за формулою:

$$P_{\text{отні}}=P_i\Sigma P_{ij}, \quad (1)$$

де ΣPij – сума балів за всіма загрозами.

Результуюче значення ступеня ризику є числовим значенням, отриманим шляхом добутку відносних величин Р1 і Р2 за формулою

$$P\text{рез}=P1\times P2\text{отн}i, \quad (2)$$

На підставі проведеного аналізу експертних оцінок, побудови ранжованих переліку загроз за двома основними пріоритетами, що характеризують ступінь ризику, знаходиться результуюче ранжування загроз за ступенем ризику для транспортного засобу, яке показує найбільше значні небезпеки.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ АВТОМОБІЛЬНОГО ТРАНСПОРТУ

Халмурадов Б.Д., Крож Є.Ф.
Національний авіаційний університет, Київ, Україна

Транспортна безпека представляє міждисциплінарний підхід до розуміння та вирішення проблеми глобальної готовності з точки зору транспорту. Мобільність представляє собою культурний життєвий шлях цивілізації протягом всієї історії людства, охоплюючи всі способи транспорту як для економічного, так і для соціального виживання. Це основа, завдяки якій цивілізація підтримувала характер і спосіб життя свого населення, виживаючи та розвиваючись у часі.

Рівень ефективної мобільності безпосередньо пов'язаний із системою транспортного забезпечення. В ідеалі транспортна система базується на безпечному, захищеному, стійкому та ефективному переміщенні людей, товарів та інформації з використанням повітря, землі, моря та космосу. Вона характеризується двома компонентами мобільності: фізичним (наприклад, немоторизований транспорт, авіація, автомобільні шляхи, морський, залізничний транспорт, транзит тощо) та електронним (наприклад, комунальні послуги, супутники, дистанційний зв’язок, інформаційні технології тощо).

Метою доповіді є аналіз сучасних безпекових заходів огляду пасажирів та багажу.

Авіаційна безпека в Україні складається з кількох рівнів і походить з багатьох джерел. Ці різні групи можна розділити на чотири категорії: держава, аеропорт, авіакомпанія та промисловість. Незважаючи на те, що державна категорія набагато більша, ніж інші, кожна з них пропонує важливі аспекти та виклики для мінливого обличчя громадського захисту.

Пристрої для зображення всього тіла: ці пристрої включають технологію зображення міліметрових хвиль і технологію зворотного розсіювання.

Сканери рідин у пляшках: багато версій цього типу пристроїв було випробувано протягом останніх кількох років. Поточні моделі — це портативні пристрої, які виявляють специфічні хімічні пари, що виходять із пляшки чи іншого контейнера.

Перевірка вантажів: вантажі, що перевозяться за допомогою літака, створюють унікальні проблеми перевірки на транспортній арені. Обсяг вантажу разом із розміром і своєчасною потребою у відправленні є перешкодами, які спонукають до потенційних рішень перевірки.

Системи виявлення вибухових речовин для перевірки багажу, розміщені у вантажних приміщеннях разом із розміщенням вантажу в зонах зареєстрованого багажу в аеропортах, є одними з потенційних рішень перевірки.

Крім того, міцні контейнери, здатні протистояти вибухам, оцінюються як потенційні методи пом’якшення катастрофічного інциденту.

ЩО ВИЗНАЧАЄ БЕЗПЕКУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Оксенчук Д.В., Третьяков О.В.
Національний авіаційний університет, Київ, Україна

Безпека об'єктів критичної інфраструктури (ОКІ) може бути визначена як зменшення ризику для критичної інфраструктури від вторгнень, атак або наслідків природних чи техногенних катастроф шляхом застосування фізичних засобів або оборонних кіберзаходів.

Стійкість ОКІ можна визначити як здатність готуватися та адаптуватися до мінливих умов. Це означає здатність протистояти і швидко відновлюватися після збоїв, навмисних атак, аварій або природних загроз чи інцидентів. Відмовостійка інфраструктура такожповинна бути надійною, гнучкою та адаптивною [1].

Ефективна програма безпеки та стійкості критичної інфраструктури ґрунтується на співпраці та обміні інформацією.

Метою доповіді є розробка рекомендацій щодо створення офіційної структуру партнерства у сфері захисту критичної інфраструктури.

Співпраці сприяє створення структур і процесів, необхідних для того, щоб уряд і приватний сектор могли вільно спілкуватися, не розголошуючи службову інформацію і не надаючи несправедливих переваг; підтримувати довірливе середовище обміну інформацією, в якому зацікавлені сторони обмінюються інформацією для зміцнення безпеки і стійкості; забезпечувати справедливе представництво і залучення відповідних зацікавлених сторін на всіх рівнях влади, промисловості, управління в надзвичайних ситуаціях і безпеки.

Успішний обмін інформацією вимагає налагоджених механізмів або каналів для регулярного зв'язку із зацікавленими сторонами, а також до, під час і після інциденту. Обмін інформацією може відбуватися в різних формах, включаючи навчальні заходи, брифінги, сповіщення електронною поштою, конференції, або зустрічі в безпечних місцях для обговорення секретних матеріалів про конкретні загрози та небезпеки, а також документи та форуми, які заохочують до обміну набутим досвідом.

Для сприяння добровільній співпраці та обміну інформацією між секторами критичної інфраструктури та державними установами, а також між ними, необхідно створити офіційну структуру партнерства, що складається з координаційних рад державного та приватного секторів, які будуть проводити окремі та спільні засідання з метою підвищення безпеки та стійкості критичної інфраструктури.

Список літератури

1. Зелена книга з питань захисту критичної інфраструктури в Україні :зб. матер. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. – К.: НІСД, 2016. – 176 с.

ВЗАЄМНИЙ ВПЛИВ ПОВЕРХНЕВИХ ВОДНИХ ОБ'ЄКТІВ З УРАХУВАННЯМ ГЕОЛОГІЧНОГО ВПЛИВУ ОДНІЄЇ РІЧКИ НА ІНШУ (на прикладі річок Ворскла та Самара)

Коваленко С.А., Пономаренко Р.В.
Національний університет цивільного захисту України, Харків, Україна

Вода відіграє важливу роль в житті людини. Її використовують у промисловості (у технологічних процесах), у сільському господарстві (для зрошування сільськогосподарських культур і вирощування тварин), для питного водоспоживання та ін. Науковці акцентують увагу на дослідженні екологічного стану підземних та поверхневих вод України [1-2], а також світу [3]. Проте недостатньо уваги приділяють вивченню питання взаємного впливу поверхневих водних об'єктів з урахуванням наявності ґрунтових вод. Хлориди є найбільш стійкою сполукою, що і дає можливість виконати дослідження.

Метою доповіді є виявлення взаємного впливу поверхневих водних об'єктів з урахуванням геологічного впливу однієї річки на іншу у межах суббасейну за допомогою кореляційних залежностей між вмістом хлоридів у вище та нижчерозташованих притоках.

У доповіді наведено дані спостережень лівих приток річки Дніпро, а саме річок Ворскла і Самара та досліджено кореляційні залежності між вмістом хлоридів вздовж приток. Отримані дані свідчать, що тенденція щодо впливу притоки, яка розташована вище за течією річки на притоку, яка розташована нижче, з урахуванням наявності ґрунтових вод, на якість води поверхневих водних об'єктів зберігається вздовж течії. Для 2020 року найбільший вплив спостерігається на постах, які розташовані найближче до річки Дніпро. Отже, доцільним є дослідити вміст інших домішок, які наявні у поверхневих водних об'єктах, що у подальших дослідженнях наддасть змогу визначити якість води головного джерела водопостачання України – річки Дніпро.

Список літератури

1. Коваленко С.А., Пономаренко Р.В., Третьяков О.В., Титаренко А.В., Іванов Є.В. Екологічна оцінка найбільшої притоки річки Дніпро в межах України. Український журнал будівництва та архітектури. Дніпро. 2022. № 4 (010). С. 65 – 75. DOI: 10.30838/J.BPSACEA.2312.250822.65.879.

2. Шуканова А., Сафронов О. Використання підземних вод Полтавщини та їх характеристика. Освітні й наукові виміри географії та туризму: матеріали Всеукр. науково-практ. інтернет-конф. для студентів, аспірантів, молодих вчен., м. Полтава, 18 листоп. 2020 р. Полтава, 2020. С. 43–42. URL: http://dspace.pnpu.edu.ua/handle/123456789/15654.

3. Groundwater quality in the vicinity of a dumpsite in Lagos metropolis, Nigeria / Carla S.S. Ferreira et al. Geography and sustainability. 2023. URL: https://doi.org/10.1016/j.geosus.2023.09.005.

ПІДВИЩЕННЯ ТЕХНОГЕННОЇ БЕЗПЕКИ АЕРОПОРТІВ ЦИВІЛЬНОЇ АВІАЦІЇ В ЧАСТИНІ ОРГАНІЗАЦІЇ АВАРІЙНО-РЯТУВАЛЬНИХ ЗАХОДІВ З ПОЖЕЖНОЇ БЕЗПЕКИ

Синило К.В.
Національний авіаційний університет, Київ, Україна

Однією з складових авіаційної безпеки аеропорту є проведення регулярних заходів з тренування аварійно-рятувального та протипожежного забезпечення польотів. Зазначені заходи регулюються державними нормами, розпорядженнями Державної авіаційної служби України та стандартами й рекомендованою практикою ІСАО. Планові навчання та тренування пожежників відбуваються відповідно до плану затвердженого керівництвом аеропорту. Організація повномасштабних навчань аварійно-рятувальних служб щодо реагування в умовах надзвичайної ситуації техногенного, природного або військового характеру вимагає залучення: Державної служби надзвичайних ситуацій; Центру екстреної медичної допомоги та медицини катастроф; Національної поліції; Повітряних Сил ЗС України; Державної прикордонної служби України; Товариства Червоного Хреста України. Результати розрахунку викидів та розсіювання забруднюючих речовин дозволяють вдосконалити принципи організації аварійно-рятувальних заходів з пожежної безпеки, а саме:

- узгодження тренувань з аварійно-рятувального та протипожежного забезпечення з графіком обслуговування пасажирів та розкладом авіа руху та іншими заходами на території аеродрому;
- організація тренувань з аварійно–рятувального та протипожежного забезпечення з урахуванням прогнозу несприятливих метеорологічних умов, які призводять до формування високих максимально-разових концентрацій оксидів азоту, оксидів вуглецю та зважених часток, а також несприятливого впливу забруднюючих речовин на здоров'я пасажирів та персоналу аеропорту;
- на етапі проектування аеропорту (реконструкція або розширення інфраструктури) доцільно обґрунтувати ділянку для протипожежних тренувань розрахунками поля концентрацій забруднюючих речовин за несприятливих метеорологічних умов;
- обґрунтування локації автоматизованої системи датчиків для моніторингу місцевої якості повітря та розмірів санітарно-захисної зони аеропорту.

Список літератури

1. ICAO Doc 9889. Airport Ait Quality. – 1st ed. – 2011. – 200 p.
2. FAA EDMS Airport Air Quality Model Development. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142.
3. O Zaporozhets, K Synylo, A Krupko Modelling of local air quality for stationary sources:simple tests//Aviation in the XXI-st Century. Safety in Aviation and Space Technologies: X World Congress, 28-30 September 2022. – K., 2022. – pp. 4.2.20 – 4.2.24.
4. Synylo K., Ulianova K., Zaporozhets O. Air Quality Studies at Ukrainian Airports //International Journal of Aviation Science and Technology, Vol. 2, Issue 1, 2021, 4-14.

ТЕХНОГЕННІ РИЗИКИ АВІАТРАНСПОРТНОЇ СИСТЕМИ

Кажан К.І., Приходько І.С.
Національний авіаційний університет, Київ, Україна

Техногенні ризики авіатранспортної системи - це потенційні загрози та небезпеки, пов'язані з функціонуванням авіаційної галузі і пов'язаними з нею процесами. Ці ризики можуть виникнути внаслідок різних факторів, включаючи технічні, людські, природні і інші обставини. Важливо аналізувати та управляти цими ризиками для забезпечення безпеки авіаційного транспорту. Основні техногенні ризики авіатранспортної системи включають в себе: авіаційні інциденти та аварії; технічні несправності; людські помилки; терористичні акти та військові дії; погодні умови; вибухонебезпечні матеріали; проблеми з інфраструктурою.

Для зменшення техногенних ризиків авіатранспортної системи важливо впроваджувати безпекові стандарти, ретельно навчати персонал, піддавати літаки обов'язковому технічному обслуговуванню, вдосконалювати системи безпеки і вживати інші заходи для забезпечення безпеки пасажирів і персоналу в авіації.

Метою доповіді є відображення результатів аналізу основних джерел техногенних ризиків авіаційних перевезень та формування матриці оцінки ризиків для прийняття рішення про відновлення авіаційних пасажирських та вантажних цивільних перевезень в Україні. В дослідженні удосконалено метод оцінки рівня загрози безпеці цивільної авіації [1] у частині урахування впливу на навколишнє середовища, включаючи персонал та населення, що мешкає неподалік аеродромів та аеропортів цивільної авіації на таких рівнях: збір і аналіз інформації; класифікація рівнів загрози; визначення заходів на рівні загрози; комунікація з населенням та постійне оновлення і вдосконалення системи.

В доповіді наводяться результати застосування методу якісної оцінки техногенних ризиків. Наведені дані показують, що в поточний період військового протистояння техногенні ризики є неприйнятними, а отже, відновлення цивільних авіаційних перевезень, які час від часу обговорюються в суспільстві, вимагатиме істотної зміни вихідних умов.

Список літератури

1. Інструкція з оцінки рівня загрози безпеці цивільної авіації України затв. наказом Міністерства інфраструктури України від 11.06.2020 № 356 URL: https://zakon.rada.gov.ua/laws/show/z0960-20#Text

2. Гусар О.А., Франковська С. Заходи щодо оцінки рівня загрози та ризиків безпеці цивільної авіації // Аеро-2021. Повітряне і космічне право: матеріали Всеукраїнської конференції молодих учених і студентів. - Національний авіаційний університет. – Київ, 2021. – Том 1. – С. 138-140.

ЕКОЛОГІЧНІ ТА ТЕХНОГЕННІ ЗАГРОЗИ НАДЗВУКОВИХ ПОВІТРЯНИХ СУДЕН

Кажан К.І., Назарков Т.І.
Національний авіаційний університет, Київ, Україна

Техногенні загрози для надзвукового повітряного транспорту можуть включати в себе різноманітні ризики, які можуть виникнути в процесі проектування, будівництва, експлуатації і обслуговування таких літаків.

Метою доповіді є аналіз основних джерел екологічних та техногенних загроз при експлуатації надзвукових повітряних суден.

В доповіді наводяться результати моделювання основних техногенних та екологічних чинників, які становлять загрозу для населення та довкілля в цілому під час експлуатації надзвукових повітряних суден. До основних загроз було віднесено [1]:

Аварії та безпека польотів. Надзвукові літаки, особливо під час надзвукового польоту, можуть зіштовхнутися з численними технічними та безпековими проблемами. Аварії надзвукових літаків можуть мати серйозні наслідки для людей та навколишнього середовища.

Знос та старіння матеріалів. Високі швидкості та інтенсивне використання надзвукових літаків можуть спричиняти швидкий знос матеріалів, що може призвести до несправностей і аварій. Надзвукові літаки опиняються під впливом великого робочого тиску та екстремальних умов навколишнього середовища під час надзвукового польоту.

Шум і забруднення довкілля. Надмірні рівні шуму в околиці аеропорті та звуковий удар є потужними екологічними чинниками [2]. Також надзвукові літаки викидають в атмосферу оксиди азоту і вуглеводні, що може спричиняти забруднення повітря і зміну клімату.

Обмеження і регулювання. Багато країн мають обмеження на використання надзвукових літаків через їхній вплив на довкілля та шумове забруднення. Це може обмежувати ринок та розвиток надзвукового транспорту.

Економічні обмеження. Надзвуковий транспорт вимагає значних інвестицій у дослідження, розробку, виробництво та обслуговування. Економічні обмеження можуть впливати на доступність та популярність надзвукових літаків.

Список літератури

1. J. J. Berton, D. L. Huff, K. Geiselhart, and J. Seidel, “Supersonic Technology Concept Aeroplanes for Environmental Studies,” in AIAA Scitech 2020 Forum, American Institute of Aeronautics and Astronautics. https://doi.org 10.2514/6.2020-0263.

2. Akatsuka J, Ishii T. System Noise Assessment and Uncertainty Analysis of a Conceptual Supersonic Aircraft. Aerospace. 2022; 9(4):212. https://doi.org/10.3390/aerospace9040212

ПІДВИЩЕННЯ ТЕХНОГЕННОЇ ТА ПОЖЕЖНОЇ БЕЗПЕКИ АЗС ЗАВДЯКИ МОДЕРНІЗАЦІЇ ПАЛИВНИХ ТЕХНОЛОГІЙ

Халмурадов Б.Д., Жуковський А.Д.
Національний авіаційний університет., Київ, Україна

Автоматизовані заправні станції (АЗС) є ключовою інфраструктурою в енергетичній галузі.

Проте, з розвитком нових технологій та збільшенням обсягів пального, виникає необхідність вдосконалення паливних технологій. Однак, їх експлуатація пов'язана з ризиками, зокрема, можливістю пожеж та інших аварійних ситуацій.

Модернізація паливних технологій може сприяти підвищенню техногенної та пожежної безпеки на АЗС.

Мета дослідження: Метою цього дослідження є розгляд сучасних технологій у сфері паливних систем та їх модернізація для забезпечення вищого рівня техногенної та пожежної безпеки на АЗС. Дослідження також спрямоване на визначення переваг і викликів, пов'язаних із впровадженням сучасних паливних технологій.

Завдання дослідження: Аналіз існуючих паливних технологій: Дослідження сучасних методів зберігання, транспортування та розподілу палива на АЗС. Визначення ризиків та проблем: Аналіз потенційних небезпек та ризиків, пов'язаних з існуючими паливними технологіями, зокрема щодо витоків, вибухонебезпеки та можливості пожеж. Розробка нових технологій: Розроблення та впровадження нових методів та технологій у сфері зберігання та розподілу пального з метою зменшення ризиків пожеж та аварійних ситуацій.

Тестування та валідація: Проведення випробувань та апробація нових паливних технологій з метою перевірки їхньої ефективності та безпеки. Впровадження та моніторинг: Розробка стратегій впровадження нових паливних технологій на АЗС та систем моніторингу для постійного контролю за їхньою безпекою та ефективністю.

Очікувані результати: Це дослідження сприятиме розробці і впровадженню нових технологій, які не лише забезпечать високий рівень техногенної та пожежної безпеки на АЗС, але й сприятимуть зменшенню негативного впливу на навколишнє середовище.

Сприятиме розробці та впровадженню сучасних паливних технологій на АЗС, що сприятиме підвищенню техногенної та пожежної безпеки, зменшенню ризику аварійних ситуацій і покращенню загального рівня безпеки для споживачів пального та персоналу АЗС.

Результати цього дослідження можуть бути корисні для індустрії пального, органів регулювання та громадськості, оскільки вони сприятимуть збільшенню безпеки та стійкості АЗС у майбутньому.

МОДЕРНІЗАЦІЯ СИСТЕМ РАННЬОГО ВИЯВЛЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ТЕХНОГЕННОЇ ТА ПОЖЕЖНОЇ БЕЗПЕКИ АЗС: ШЛЯХ ДО ЕФЕКТИВНОСТІ ТА НАДІЙНОСТІ

Халмурадов Б.Д., Грищенко М.О.
Національний авіаційний університет, Київ, Україна

Автоматизовані заправні станції (АЗС) відіграють ключову роль у сучасному світі, забезпечуючи наші транспортні потреби.

Однак, разом із зростанням технологічних можливостей, збільшується і ризик аварійних ситуацій, пов'язаних з пожежами та іншими техногенними надзвичайними ситуаціями. Відсутність або несправність систем раннього виявлення може призвести до серйозних наслідків.

Мета дослідження: Ця наукова робота спрямована на вивчення сучасних технологій та методів модернізації систем раннього виявлення для забезпечення техногенної та пожежної безпеки на автоматизованих заправних станціях.

Основна мета полягає в з'ясуванні оптимальних шляхів досягнення високої ефективності та надійності цих систем.

Аналіз існуючих систем раннього виявлення: Вивчення сучасних технологій та методів, які використовуються на АЗС для раннього виявлення пожеж та інших аварійних ситуацій.

Ідентифікація недоліків і проблем: Аналіз недоліків і несправностей існуючих систем, їх причин та наслідків для безпеки АЗС та її навколишнього середовища. Розробка пропозицій щодо модернізації: Розроблення конкретних рекомендацій та пропозицій щодо вдосконалення систем раннього виявлення з метою підвищення їх надійності та ефективності.

Експериментальні дослідження та апробація: Проведення практичних випробувань запропонованих рішень для перевірки їх ефективності та можливості впровадження на реальних АЗС.

Оцінка та висновки: Проведення аналізу результатів експериментів, оцінка ефективності модернізованих систем раннього виявлення та формулювання висновків та рекомендацій для подальших заходів.

Очікувані результати:

Ця наукова робота сприятиме розробці та впровадженню нових, надійних і ефективних систем раннього виявлення на АЗС, що значно знижить ризик аварійних ситуацій та сприятиме підвищенню рівня безпеки для споживачів пального та навколишнього середовища.

МОНІТОРИНГ ЯКОСТІ ПОВІТРЯ НАВКОЛИШНЬОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ РОЙОВОГО ІНТЕЛЕКТУ

Гуджуманюк К.С., Подорожняк А.О.
Національний технічний університет «Харківський політехнічний інститут»,
Харків, Україна

Однією з найголовніших екологічних проблем в Україні є погана якість повітря. Це здебільшого спричинено наявністю великої кількості промислових об'єктів, шкідливими викидами від автотранспорту та недотриманням усталених норм та правил.

Першим кроком до вирішення даної проблеми є проведення моніторингу та аналізу якості повітря. Наразі це досягається шляхом використання супутників [1, 2] та спеціальних станцій на місцевості [3]. Проте тут трапляються певні перешкоди: супутники мають певні обмеження, а тому їх використовують для отримання лише допоміжних та непрямих даних. Моніторингові станції мають інший недолік – а саме порівняно невелику ділянку застосування.

В такому випадку, кращою альтернативою є використання системи дронів, що використовує колективний інтелект. Перевагами такого підходу є можливість здійснювати аналіз безпосередньо на необхідних ділянках, проводити виявлення джерел забруднення, охоплювати набагато більші території та може діяти у різних умовах та середовищах [4].

Для проведення моніторингу необхідно зробити певні налаштування та провести постановку задач в залежності від потреб. Після підготовчих робіт здійснюється запуск рою дронів. І відповідно до завдання проводиться збір даних на окремій місцевості. Далі на основі цих даних виконується аналіз та робиться висновок щодо екологічного стану місцевості.

Список літератури

1. Савенець М. В., Осадчий В. І., & Орещенко А. В. Моніторинг якості атмосферного повітря над територією України з деталізацією для міст за даними супутника Sentinel-5P. *Вісник НАН України*, 2021, вип. 3, С. 50–58. DOI: https://doi.org/10.15407/visn2021.03.050.

2. Подорожняк А. О., Любченко Н. Ю., & Лагода О. Д. Метод інтелектуальної обробки мультиспектральних зображень. Системи обробки інформації, 2015, вип. 10 (135), С. 123-125. – Режим доступу: https://scholar.google.com.ua/scholar?oi=bibs&cluster=3970100886242792428&btnI=1&hl=uk.

3. Гударенко В. М., Подорожняк А. О., & Шамаєв Ю. П. Модель точкових забруднень для оцінки якості повітряного басейну. *Стандартизація. Сертифікація. Якість*, 2016, вип. 10 (135), С. 123-125. – Режим доступу: https://scholar.google.com.ua/scholar?oi=bibs&cluster=11502104476153042956&btnI=1&hl=uk

4. Ranganathan R. H., Balusamy S., Partheeban P., Mani C., Sridhar M., & Rajasekaran V. Air Quality Monitoring and Analysis for Sustainable Development of Solid Waste Dump Yards Using Smart Drones and Geospatial Technology. *Sustainability*, 2023, 15, 13347. DOI: https://doi.org/10.3390/su151813347

ФОРМУВАННЯ ІНФРАСТРУКТУРИ РЕСАЙКЛІНГУ БУДІВЕЛЬНИХ ВІДХОДІВ, УТВОРЕНИХ ВНАСЛІДОК БОЙОВИХ ДІЙ

Кікоть М.С., Малєєва Ю.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Розчищення українських міст від руїн стане наймасштабнішою складовою післявоєнного відновлення країни [1]. Проблема полягає у необхідності вирішення критичної ситуації, яка склалася з утворенням, накопиченням, зберіганням, переробленням, утилізацією та захороненням будівельних відходів і характеризується подальшим розвитком екологічних загроз [2]. Вдосконалення системи поводження з таким видом відходів є важливою екологічною проблемою, вирішення якої полягає у ресайклінгу, що дозволяє утилізувати будівельні відходи з мінімальним впливом на навколишнє середовище.

Метою доповіді є аналіз існуючих моделей та стратегій, які сприятимуть ефективнішому впровадженню систем ресайклінгу будівельних відходів в умовах післявоєнного відновлення.

Проекти ресайклінгу мають бути комплексними, що передбачає обов'язкове сортування, повторне використання продуктів переробки, виготовлення з переробленої сировини нових виробів, розщеплювання або дроблення для виділення необхідних компонентів, отримування енергії від спалювання відходів, та обов'язково облаштування очистки викидів від таких установок. Реалізація проектів з мобільної переробки будівельних відходів має ряд переваг: зменшує навантаження на звалища, дозволяє заощаджувати природні ресурси та дає роботу місцевому населенню.

В доповіді наведені результати дослідження підходів до створення інфраструктури ресайклінгу будівельних відходів, утворених внаслідок бойових дій. Ефективне планування та управління процесами ресайклінгу є можливим лише за умови використання інформаційних технологій, які дозволять керувати логістикою в процесі ресайклінгу, вести облік відходів тощо.

Список літератури

1. Mikhno I., Ihnatenko N., Cherniaiev O., Vynogradnya V., Atstaja D., Koval V. Construction waste recycling in the circular economy model. *2nd International Conference on Environmental Sustainability in Natural Resources Management.* Volume 1126. 31 oct. 2022 – 01 nov. 2022. Riga, 2022. DOI: 10.1088/1755-1315/1126/1/012003.

2. Про схвалення Національної стратегії управління відходами в Україні до 2030 року. Розпорядження Кабінету Міністрів України від 8.11.2017 р. № 820-р. URL: https://zakon.rada.gov.ua/laws/show/820-2017-%D1%80#Text. (дата звернення: 25.10.2023).

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ РОЄМ РОЗПОДІЛЕНИХ МОБІЛЬНИХ ОБ'ЄКТІВ

Федорович О.Є., Крицький Д.М.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Сучасні технології управління дронами (наприклад, БПЛА) дозволяють створити комплекси з розподіленими мобільними об'єктами, які інтегруються у рій (зграя). Але виникають труднощі зі створення системи управління роєм, які потребують проведення дослідження для створення інформаційної технології управління на основі штучного інтелекту. Тому, актуальна тема доповіді, в якій розглядаються можливі варіанти управління розподіленими мобільними об'єктами та об'єднання їх у рій [1, 2].

Метою доповіді є створення інформаційної технології моделювання процесу управління розподіленими мобільними об'єктами, які згортаються у рій.

Проведено аналіз проблем організації та управління роєм дронів для виконання різноманітних завдань, у тому числі військового характеру. Виділено можливі варіанти алгоритму управління роєм дронів (централізоване управління, децентралізоване управління з автономними системами, управління зі зміною вожаку зграї, тощо).

Створена оптимізаційна модель для вибору варіанту системи управління роєм в залежності від призначення (аерофотозйомка, баражуючий боєприпас, цілевказівка, тощо).

В якості показників оптимізації використовуються: час польоту, дальність, електроспоживання на борту, ризики загроз. Створена агентна модель для імітації руху дронів за допомогою платформи Anylogic. Використання імітаційної моделі дозволяє формувати плани польотів, оцінювати значення основних показників та формувати відносно безпечні траєкторії руху дронів в умовах військових загроз та використання противником засобів антидронової боротьби.

Запропонований підхід дозволяє обґрунтувати основні технічні характеристики комплексу управління роєм дронів.

Список літератури

1. Modeling of logistics of war reserve stockpiling for successful combat operation / O. Fedorovich, M. Lukhanin, O. Prokhorov, Y. Pronchakov, O. Leschenko, V. Fedorovich // Радіоелектронні і комп'ютерні системи. – 2023. - №1. – С. 183-196. DOI: 10.32620/reks.2023.1.15.

2. Prokhorov, A. Intelligent multi-service platform for building management / A. Prokhorov, Yu. Pronchakov O Fedorovich // IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). – 2020. – P. 62-67. DOI: 10.1109/atit50783.2020.9349312.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ РЕЛОКАЦІЇ ПІДПРИЄМСТВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЇХ СТІЙКОСТІ ДО ЗАГРОЗ

Федорович О.Є., Міланов М.В., Сломчинський О.В.,
Малєєв Л.В., Соловйов В.С.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Мінливі політико-економічні умови існування виробництва високотехнологічних виробів призвели до появи множини загроз та ризиків функціонування підприємств.

Для забезпечення стійкості виробництва до загроз є декілька напрямків, у тому числі, релокація підприємства на нове, відносно безпечне, місце розташування.

Тому, актуальна тема доповіді, в якій представлені результати дослідження дій щодо релокації підприємств на нове місце розташування [1, 2].

Метою доповіді є аналіз можливих напрямків релокації підприємств для забезпечення їх стійкості до можливих загроз.

Однією з проблем глибокої релокації (переміщення підприємства на нове віддалене місце відносно початкового) є формування нових логістичних шляхів постачання та постачальників, які забезпечать не порушення планів роботи підприємства.

Створена оптимізаційна модель для пошуку множини нових постачальників комплектуючих, матеріалів та сировини. Пошук постачальників проводиться з урахуванням показників вартості, часу та ризиків постачання комплектуючих.

Проведено дослідження послідовності логістичних дій щодо переміщення підприємства на нове місце розташування.

Створена імітаційна агентна модель за допомогою платформи Anylogic для дослідження логістичних дій щодо переміщення підприємства на нове місце розташування.

Проведене моделювання релокації підприємства в умовах виникнення військових загроз воєнного стану країни.

Список літератури

1. Modeling of the relocation of high-tech enterprises for the release of innovative products / O. Fedorovych, O. Prokhorov, Y. Pronchakov, A. Popov, M. Momot // Радіоелектронні і комп'ютерні системи. – 2023. – № 2. – С. 180-190. DOI: 10.32620/reks.2023.2.15.

2. Modeling of Technological Process in Nanoelectronic Production / O. Prokhorov, Y. Pronchakov, O. Fedorovich, N. Kunanets // 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 – Proceedings, 2020, 1, pp. 324–327, article no. 9321926. Available at: http://elartu.tntu.edu.ua/bitstream/lib/33074/2/Стаття%20CSIT%20IEEE.pdf.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ СТІЙКОСТІ ПІДПРИЄМСТВ В УМОВАХ ВОЄННОГО СТАНУ

Федорович О.Є., Момот М.О., Попов А.В.,
Поліщук Є.В., Федорович В.А.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Глобалізація економіки призвела до створення розподілених виробництв, в постачанні яких використовується довгі логістичні ланцюги. Зросла кількість загроз, які впливають, як на логістику постачання так і на виробництво високотехнологічної техніки.

Тому, актуальна тема доповіді, в якій наведені результати дослідження суттєвих факторів, які впливають на стійкість підприємств в умовах воєнного стану [1, 2].

Метою доповіді є моделювання стійкості підприємств в умовах військових загроз.

Проведено аналіз множини загроз, які призводять до ризиків функціонування підприємств.

Проява загрози призводить до збудження множини вразливостей розподіленого виробництва та виникненню збитків. Виділені, за допомогою оцінок експертів та менеджерів підприємства, суттєві фактори, які впливають на стійкість підприємства.

Створена оптимізаційна модель, яка дозволяє підвищити стійкість підприємства до проявлення загроз за допомогою проведення превентивних дій. При цьому враховується величина можливих збитків, витрати та час проведення превентивних дій. Велику увагу приділено підвищенню стійкості підприємства в умовах військових загроз, шляхом аналізу логістичних ланцюгів постачання та вибору множини дій, які нейтралізують або мінімізують дію військової загрози. Створена агентна імітаційна модель для моделювання логістики постачання – виробництво – збут.

Запропонований підхід доцільно використовувати для аналізу стійкості виробництв та для зменшення збитків від прояви військових загроз.

Список літератури

1. Modeling of the relocation of high-tech enterprises for the release of innovative products / O. Fedorovych, O. Prokhorov, Y. Pronchakov, A. Popov, M. Momot // Радіоелектронні і комп'ютерні системи. – 2023. – № 2. – С. 180-190. DOI: 10.32620/reks.2023.2.15.

2. Modeling of Technological Process in Nanoelectronic Production / O. Prokhorov, Y. Pronchakov, O. Fedorovich, N. Kunanets // 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 – Proceedings, 2020, 1, pp. 324–327, article no. 9321926. Available at: http://elartu.tntu.edu.ua/bitstream/lib/33074/2/Стаття%20CSIT%20IEEE.pdf.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЛОГІСТИКИ ФОРМУВАННЯ ЗАПАСІВ КОМПЛЕКТУЮЧИХ В УМОВАХ ВОЄННОГО СТАНУ

Федорович О.Є., Пісклова Т.С., Беберіна К.О.,
Шишков Д.М., Громенко А.І.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Сучасні високотехнологічні підприємства функціонують в умовах множини існуючих загроз (політико-економічні, кліматичні, терористичні, військові). Це потребує формування планів виробництва та постачання комплектуючих з урахуванням запасів для забезпечення планової роботи підприємства. На формування запасів впливає рівень стійкості виробництва, при створенні комплектуючих, та формування, відносно безпечних, логістичних ланцюгів постачання в умовах воєнного стану.

Тому, актуальна тема доповіді, в якій наведені результати дослідження логістики формування запасів для високотехнологічного виробництва, в умовах військових загроз [1, 2].

Метою доповіді є дослідження логістики формування запасів за допомогою оптимізаційної та імітаційної моделей. Аналізується множина імовірних виробників комплектуючих для забезпечення потрібного рівня запасів.

При цьому враховуються обмежені можливості постачальників, час для формування запасів та логістичні ланцюги постачання.

Створена оптимізаційна модель для оцінки рівня запасів. Вибір величини запасів комплектуючих здійснюється у діапазоні від страхових до максимально можливих, що пов’язано з обмеженими можливостями постачальників та планами виробництва. Оцінюється вплив ризиків на функціонування постачальників з урахуванням ланцюгів постачання. Особливу увагу приділено ризикам військового характеру.

Створена агентна імітаційна модель для дослідження логістики формування запасів комплектуючих в умовах довгих ланцюгів постачання в різнорідному транспортному середовищі.

Список літератури

1. Modeling the impact of threats and vulnerabilities in transport logistics of a developing enterprise / O. Fedorovich, Yu. Pronchakov, Yu. Leshchenko, A. Yelizieva // Радіоелектронні і комп’ютерні системи. – 2021. – № 3. – С. 29-36. DOI: 10.32620/reks.2021.3.03.

2. Моделювання транспортної логістики військових вантажів з урахуванням збитків, які виникають у зоні бойових дій через запізнення у постачанні / О. Є. Федорович, О. С. Уруський, І. Б. Чепков, М. І. Луханін, Ю. Л. Прончаков, К. О. Рибка, Ю. О. Лещенко // Радіоелектронні і комп’ютерні системи. – 2022. – № 2. – С. 63-74. DOI: 10.32620/reks.2022.2.05.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ДОВГИХ ЛОГІСТИЧНИХ ЛАНЦЮГІВ ПОСТАЧАННЯ В УМОВАХ ЗАГРОЗ

Федорович О.Є., Прончаков Ю.Л., Лещенко Ю.О.,
Єременко Н.В., Коновалова О.В.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Логістика постачання високотехнологічних виробництв є однією з важливих проблем розподіленого виробництва. Глобалізація економіки та поява довгих ланцюгів постачання ускладнює організацію та планування виробничих процесів.

Тому, актуальна тема доповіді, в якій представлені результати дослідження довгих логістичних ланцюгів постачання та оцінка їх впливу на функціонування високотехнологічних виробництв [1, 2].

Метою доповіді є дослідження довгих логістичних ланцюгів постачання в умовах прояви загроз.

Проведено аналіз довгих ланцюгів постачання в різнорідному транспортному середовищі з урахуванням перевалок вантажів з однієї транспортної мережі на іншу.

Виділені критичні місця та можливі вразливості в різнорідній транспортній мережі постачання.

Створена системна модель для типових структур постачання з урахуванням логістичних шляхів та послідовності транспортних дій.

Створена оптимізаційна модель для вибору раціональних логістичних шляхів постачання з урахуванням часу, витрат та ризиків постачання.

Розроблена імітаційна агентна модель з використанням оригінального алгоритму моделювання руху вантажів, яка заснована на розповсюджуванні клонів заявок (вантажів) в різнорідній транспортній мережі.

Проведено моделювання довгих логістичних ланцюгів постачання в умовах виникнення можливих загроз, у тому числі, військового характеру.

Список літератури

1. Modeling the impact of threats and vulnerabilities in transport logistics of a developing enterprise / O. Fedorovich, Yu. Pronchakov, Yu. Leshchenko, A. Yelizieva // Радіоелектронні і комп'ютерні системи. – 2021. – № 3. – С. 29-36. DOI: 10.32620/reks.2021.3.03.

2. Pronchakov, Y. Concept of High-Tech Enterprise Development Management in the Context of Digital Transformation / Y. Pronchakov, O. Prokhorov, O. Fedorovich // Computation. – 2022. – Vol. 10, Iss. 7. – Article No. 118. DOI: 10.3390/computation10070118.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ВСТАНОВЛЕННЯ ВІЙСЬКОВОГО ПАРИТЕТУ СИЛ В ЗОНІ ВОЄННОГО КОНФЛІКТУ

Федорович О.Є., Смідович Л.С., Кулик Ю.О.,
Андрєєв В.Р., Жирко К.В.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Сучасна стратегія проведення бойових дій заснована на використанні різноманітних видів озброєння та військової техніки. Це пов'язано з існуючим характером війни, яка є гібридною. При використанні різноманітного озброєння, в локальних зонах бойових дій, необхідно враховувати боєздатність окремих видів озброєння.

Тому, актуальна тема доповіді, в якій розглядається питання встановлення військового паритету сил за рахунок використання сучасного озброєння з підвищеними характеристиками боєздатності (дальність, точність, розмір зони ураження, тощо) [1, 2].

Метою доповіді є представлення результатів дослідження встановлення військового паритету сил з урахуванням боєздатності сучасних видів озброєння.

Розроблена комбінаторна модель для оцінки множини варіантів розподілу різних видів озброєння за локальними зонами проведення бойових дій. За допомогою методу теорії перерахування оцінюється кількість варіантів та формується їх множина.

Розроблена оптимізаційна модель для розподілу озброєння за локальними зонами бойових дій, з урахуванням боєздатності окремих видів озброєння та військового потенціалу, який має противник.

Розроблена імітаційна модель логістики постачання озброєння та військової техніки за локальними зонами бойових дій.

Список літератури

1. Modeling of supply logistics and training of military personnel for the successful use of weapons in a combat area / O. Fedorovich, Igor Chepkov, Mikhail Lukhanin, Yurii Pronchakov, Kseniia Rybka, Yuliia Leshchenko // Радіоелектронні і комп'ютерні системи. – 2022. – № 3. – С. 33-46. DOI: 10.32620/reks.2022.3.

2. Моделювання комплексного формування запасів військової техніки в зоні воєнного конфлікту з використанням компонентного методу / О. Є. Федорович, Л. М. Лутай, Ю. А. Малєєва, Я. О. Замірець, Т. С. Пісклова // Авіаційно-космічна техніка та технологія. – 2023. – № 2. – С. 56-66. DOI: 10.32620/aktt.2023.2.06.

СИСТЕМА АКУСТИЧНОГО МОНІТОРИНГУ ДЖЕРАЛ НЕБЕЗПЕК ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ МІСТА

Тютюник В.В., Усачов Д.В.
Національний університет цивільного захисту України, Харків, Україна
Тютюник О.О.
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна

Метою доповіді є розвиток науково-технічних основ створення в моделі «SAFE CITY» системи «SMART CITY» підсистеми наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпек, з подальшим отриманням й обробкою інформації, а також прогнозування виникнення на території міста НС різного характеру та розробкою ефективних управлінських антикризових рішень [1]. В доповіді за стандартом IDEF0 розроблено структурно-функціональну модель стратегічного розвитку в загальній системі «SMART CITY» підсистеми «SAFE CITY», з урахуванням керуючих потоків нормативно-правової бази України та наявності в державі відповідних механізмів (ресурсів). В процесі моделювання показано, що процес реєстрації загроз для життєдіяльності міста включає організацію фінансового аудиту, моніторингу соціального стану та довкілля, відеоспостереження, радіаційного, хімічного та біологічного моніторингу, а також спектрального аналізу випромінювань від джерел небезпек. Запропоновано системний підхід та принципи використання спектрального аналізу акустичного простору міста, для реалізації безперервного та тривалого у реальному масштабі часу оперативного моніторингу за місцем виникнення та динамікою розвитку ідентифікованих джерел небезпек для об'єктів критичної інфраструктури. При цьому, встановлено, що основним показником ефективності функціонування підсистеми оперативного акустичного моніторингу зони НС на території міста є достовірність ідентифікації джерела небезпеки за видом та місцем виникнення, яка залежить від факторів, які характеризують безпосередньо динаміку зміни показників розвитку джерела небезпеки, від факторів, які характеризують тактико-технічні показники засобів контролю акустичного простору, а також від факторів, які характеризуються географічними та фізико-хімічними показниками місця виникнення джерела небезпеки та середовища розповсюдження інформаційного акустичного сигналу.

Список літератури

1. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. *Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони"*. Київ. Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52. URL: http://repositsc.nuczu.edu.ua/handle/123456789/15894

Підсекція 2

STUDY OF THE RELIABILITY COMMUNICATION NETWORKS IN CRITICAL INFORMATION INFRASTRUCTURES

Mammadov I.A., Sadigov U.K.
Azerbaijan Technical University, Baku, Azerbaijan

This paper examines the task of studying the reliability indicators of servers multiservice networks NGN/IMS (Next Generation Network/Internet Protocol Multimedia Subsystem) to ensure security and reliable communication in critical information infrastructures in order to obtain analytical expressions of reliability indicators of IMS session monitoring and management systems [1].

Monitoring and management systems for critical objects such as IMS multimedia communications are subject to requirements for the reliable operation of multiservice network servers [2, 3].

Taking into account the above, we will consider the functioning of the server management system in the conditions failures in the IMS core. At the initial stage operation, the server management system is in a fully functional initial state [4].

After the first failure, the control system, let's say, goes into a state in which it searches for a fault in the IMS servers. If a malfunction is detected in the IMS system and the protection is triggered with a probability

$$1-q_1 = p_1 \ .$$

In this case, we assume that in the absence of a second failure during the period of its recovery, the faulty communication channel is excluded from operation without loss of functionality.

Let us assume that after recovery from the consequences of a failure, the server transitions to its original state. In the absence of protection, it is likely

$$q_1 = 1 - p_1$$

The latter means that even the first failure is considered dangerous for multiservice NGN/IMS networks in critical information infrastructures.

Taking into account the above, a structure of graph circuits has been proposed that describes transition states based on absorbing homogeneous Markov chains with continuous time [3].

Here is a graph of state transitions that reflect changes associated with failures and restoration of the server hardware and software systems, and the transitions are determined by the intensity failures λ_i and restorations μ_i, $i = \overline{1,n}$.

We assume that the system input has a failure intensity flow λ_i with duration T_0 and recovery speed μ_i with duration T_b recovery and accept it as the simplest failure flow [3]. We believe that all these random variables are independent of each other and have the same distribution:

$$F(t,\lambda_i) = P\{\eta < t\} \ , \quad G(t,\mu_i) = P\{\xi < t\} \ . \qquad (1)$$

Based on reliability theory for an object with a finite recovery time and on the basis of (1), we can determine the probabilistic characteristics of the IMS multimedia communication subsystem [3]:

● The mathematical expectation T_0 – is the mean time between failures, which is an indicator of the failure-free operation of restored objects of critical information infrastructures and is equal to:

$$T_0 = E[\eta, \lambda_i] = 1/\lambda_i \quad , \quad i = \overline{1,n} \tag{2}$$

● The mathematical expectation T_b – of the average recovery time, as an object with a finite recovery time of the IMS core, is an indicator of maintainability and is equal to:

$$T_b = E[\xi, \mu_i] = 1/\mu_i \quad , \quad i = \overline{1,n} \tag{3}$$

Expressions (1), (2) and (3) are the probabilistic characteristics processes of homogeneous Markov chains with continuous time, allowing to evaluate the components of the reliability of monitoring and control systems for IMS platforms.

These are necessary to ensure maintenance critical information infrastructures, including non-stationary availability $K_H(\lambda, t, \mu)$.

It is worth noting that the latest indicators of the system are new components reliability in international documents such as the provision maintenance and repair.

It is known [2-4] that the IMS platform is designed to manage sessions while ensuring information security and reliable communications in critical information infrastructures that form the basis of the information and communication technology environment.

In addition, the IMS platform serves for session management when providing any multimedia services to users of fixed and wireless networks.

Since the critical information infrastructure as a whole now includes multi-service telecommunication networks based on the NGN and FN (Future Network) architectural concepts.

References

1.Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. doi:https://doi.org/10.30837/csitic52021232904

2.Erokhin S.D., Petukhov A.N., Pilyugin P.L. Security management of critical information infrastructures. – M.: Hotline - Telecom, 2021. 240 p.

3.Mamedov T.H. Study of the effectiveness special-purpose service communication networks//Materials of the XXVII-International Scientific and Technical Conference on “Modern Communications”, BGAS, Minsk . 2022. pp.122-124.

4. Ibrahimov, B.G., Hashimov, E.G.,Talibov, A.M., Hasanov, A.H. Research and analysis indicators fiber-optic communication lines using spectral technologies // -Kharkov: Advanced information systems, -2022. Т. 6, № 1, - стр.61-64. doi: https://doi.org/10.20998/2522-9052.2022.1.10

ПЕРЕМОГА АЗЕРБАЙДЖАНУ У ІІ КАРАБАХСЬКІЙ ВІЙНІ – ЯК ПОЧАТОК НОВОГО ГЕОПОЛІТИЧНОГО БАЛАНСУ У РЕГІОНІ

Алієв Н.А.
Військовий науково-дослідний інститут, Баку, Азербайджан

Аналіз Армяно-Азербайджанського конфлікту показав, що він відіграв вирішальну роль у новій геополітичній структурі Євразії і став джерелом регіональної безпеки та стабільності всього Кавказу та Близького Сходу. У питанні вирішення вірмено-азербайджанського конфлікту керівництво Азербайджанської Республіки відстоювало вирішення проблеми на основі норм міжнародного права за умови збереження територіальної цілісності нашої країни [1]. Однак, неконструктивна позиція керівництва Вірменії та небажання Ради Безпеки ООН виконувати ухвалені ним резолюції щодо вірмено-азербайджанського конфлікту дали керівництву Азербайджану право перетворити військово-політичний шлях вирішальним у врегулюванні Вірмено-Азербайджанського конфлікту [2]. Здійснюючи цей крок, Азербайджанська Республіка діяла на основі положень Статуту ООН, які передбачають захист суверенітету та територіальної цілісності кожної окремо взятої держави-члена.

Вищеперелічені обставини зробили неминучою війну між Вірменією та Азербайджаном, яка розпочалася 27 вересня 2020 року. Збройні сили Вірменії, грубо порушивши режим припинення вогню, навмисно, цілеспрямовано та інтенсивно обстрілювали позиції Збройних Сил Азербайджанської Республіки, що розташовані в прифронтовій зоні. Вірменські озброєні формування під приводом завдання ударів по військових об'єктах зазнавали важких артилерійських обстрілів райони та населені пункти з компактним проживанням цивільного населення [3-4]. В результаті дій у відповідь, заснованих на міжнародному праві та продуманій військовій стратегії, Азербайджанська Армія в ході проведення бойової операції завдала нищівних ударів по ворогові, звільнила землі від 30-річної окупації та здобула історичну перемогу.

Військові дії на вірмено-азербайджанському фронті тривали 44 дні і завершилися 10 листопада 2020 року підписанням Вірменією Акту про фактичну військову капітуляцію. Локальні антитерористичні заходи, проведені Азербайджанською Армією 19-го та 20-го вересня 2023 року, стали логічним наслідком військово-політичної поразки Вірменії [5]. З підписанням Заяви (10-го листопада 2020-го року) і роззброєнням озброєних формувань (20-го вересня 2023-го року) незаконно розташованих у Карабаху завершився 30-річний конфлікт між Вірменією та Азербайджаном, що є частиною складної політичної боротьби на геополітичній арені. де шляхом визволення земель у Карабаху, окупованих озброєними підрозділами Республіки Вірменія, Азербайджану вдалося відновити свою територіальну цілісність. Геополітичні підсумки Перемоги Азербайджану у Другій Карабахській війні:

1. Азербайджан, відновивши свою територіальну цілісність, звільнив свої землі, які перебували під окупацією майже 30 років, та повністю забезпечив свій суверенітет.

2. Азербайджан гарантував повернення на батьківщину понад мільйон вимушених переселенців.

3. Азербайджан «покарав» Вірменію, яка була втягнута у геополітичні ігри регіональних центрів влади.

4. «Розробники гри» зіткнулися з ситуацією, на яку вони не очікували: вони були змушені піти на компроміс з регіональною владою, яка могла б відіграти важливу роль у майбутньому Південного Кавказу – Азербайджан забезпечив входження Туреччини в політичне життя регіону.

5. Азербайджан добився важливого історичного успіху, що викликав підтримку в глобальному масштабі: Баку запобіг непрямому втручанню іноземних сил у процеси, встановивши мир і стабільність у регіоні. Азербайджан водночас є «геосинхронною брамою» до Центральної Азії, яка не має альтернативи для Заходу. Після перемоги у Другій Карабахській війні вплив Туреччини та Азербайджану на Євразійському просторі значно зріс.

6. Азербайджан, приречений на роль «жертви» на початку конфлікту, через 30 років вийшов переможцем з протистояння провідних держав у геополітичній грі, зміцнивши свою незалежність і суверенітет. Війна посилила залежність Вірменії від Росії у сфері безпеки та економіки.

Таким чином Вітчизняна війна відкрила нову сторінку в історії Азербайджану. Вироблена правильна стратегія у військовій політиці сприяла забезпеченню Великої Перемоги Азербайджанської Армії у 44-денній війні, а також дозволило Азербайджану домогтися відновлення своєї суверенної території та тектонічних змін у співвідношенні геополітичних сил на Південному Кавказі. Азербайджан фактично розірвав лінію конфронтації у геополітичному аспекті, створивши в регіоні атмосферу довіри та дружби, співробітництва та безпеки.

Список літератури

1. Nurulla Aliyev. "Victory of Azerbaijan in the Civil War". Baku, 2021. 1096 p.
2. Выступление президента Азербайджанской Республики Ильхам Алиева в видеоформате на 5 сессии Ген. Асс. ООН, 24.09.2020, https://ru.president.az/articles/40937
3. Обращение Ильхама Алиева к Азербайджанскому народу от 27-го сентября 2020-го года, https://ru.president.az/articles/40968
4. Piriyev, H.K., Hashimov, E.G. The Second Karabakh War: military-political and military-technical aspects // - Baku: Proc. of the Military Institute, 2023. No. 1 (40). - p. 7-16. URL: https://mod.gov.az//images/pdf/a5fd996e70a2e325b03dca58256c5c92.pdf
5. Aliyev N.A., Mammadzade V.M.. Geotechnical environment in the South Caucasus and Azerbaijan in the post-war period. -Baku: "AFpoligrAF", -2023, -112 p.

THE EFFECTIVE APPLICATION OF STRATEGIC COMMUNICATION IN THE FIELD OF NATIONAL SECURITY

Orujov R.Q., Mammadzada V.M.
National Defense University, Baku, Azerbaijan

The effective application of Strategic Communication in the field of National Security is essential to achieving national security objectives. Several areas in the concept of general communication began to develop in the last two decades. In

particular, at present, we come across acronyms such as Information Operations (IO) and Psychological Operations (PSYOPS) and Public Affairs (PA). The development of communication was carried out by allocating integrated communication technologies for use in implementing elements of the national strategy. Thus, the regular use of the terms IO, PSYOPS and PA in the field of national security began to popularize the concept of "strategic communication." For example, we can show the period after the terrorist attacks in the USA in 2001.

The term "strategic communication" has become a trend in recent years. Before starting the main body of the topic, we must begin clarifying what we mean by strategic communication. Strategic communication means synchronizing words and actions and how selected audiences will receive them. It also includes programs and activities to communicate and engage with a targeted audience. Strategic communications are essential for countering hostile narratives and engaging with the global community. Therefore, strategic communication is viewed as something that should be used to support national interests and be synchronized with national power. The majority of the country's political and public spheres have developed strategic communication. Every government organization has a unique method of strategic communication. As a result, its inappropriate application has become widespread and needs to be clarified. Strategic Communication is one of the main tools for pursuing and maintaining permanent national objectives for National Security. Regarding national security, strategic communication is a definitional draft devoid of any theoretical or methodological underpinnings and a logical practice entangled in a battleground of disciplines and professions that intend to adopt the idea in one way or another without considering the intellectual ramifications. Therefore, despite the mutilation of the lexicon, they need to recognize the significance of the strategy concept and attempt to accommodate it [1]. Implementing strategic communications in national security is an integral part of the state's efforts to achieve political and defense objectives. Strategic communication efforts should reinforce key themes and messages and be constantly measured against defined objectives. As a result, adjustments must be made, and those responsible for implementation must be held accountable. Strategic communications efforts are an essential component of any country's national security. The successful application of strategic communication is critical for national security during times of War. It helps to shape public perception, gain international support, and control the narrative of the conflict. Strategic communication's practical application in the area of national security depends on the mutual study of its guiding principles and the lessons learned from its use during the Second Karabakh War. In the Second Karabakh War, Azerbaijan used strategic communication to its advantage, and the effectiveness of its communication strategies influenced the outcome of the conflict. Azerbaijan's national security strategy during the Second Karabakh War heavily relied on the use of strategic communication. By portraying itself as a victim of aggression and framing the conflict as a war against terrorism, Azerbaijan was able to advance its national security interests, control the narrative of the conflict, and win international support.

References

1. Cristian E. Guerrero-Castro. Strategic Communication for Security & National Defense: Proposal for an Interdisciplinary Approach. Connections, Vol. 12, No. 2 (Spring 2013): 27-52. (26 p.). https://www.jstor.org/stable/26326320

METHODS OF CONDUCTING CHEMICAL EXPLORATION

Akhundov R.G.
Military Research Institute, Baku, Azerbaijan

Chemical weapons should be understood as toxic substances and the means in which they are used (ammunition, special machines and devices).

Toxic substances (TS) are such chemicals that, when used in combat, can affect people and animals. Toxic substances have the property of infecting air, soil, water sources, foodstuffs, items of equipment and weapons of troops, engineering structures, buildings, etc. [1].

Toxic substances are different in their physicochemical nature and therefore cause human damage of varying nature and severity. The use of toxic substances by the enemy extremely complicates the combat operations of troops and requires the immediate use of special protective equipment.

In all cases of massive artillery-mortar and enemy air raids, observation posts (observers) should pay special attention to the nature of ammunition bursts, since external signs of a rupture can facilitate the detection of the beginning of an enemy chemical attack. Chemical bombs, shells and mines, when exploded, form a creeping gas cloud, which in some cases has a characteristic color.

Chemical reconnaissance must promptly establish: the beginning of an enemy chemical attack; the presence of contaminated areas in the zone of operations of troops; boundaries of contaminated areas and bypass routes or favorable directions for creating passages; the type of toxic substance used by the enemy; the state of the NBC protection of enemy troops; the presence of local agents that can be used for chemical protection.

Detection and determination of the degree of contamination with toxic and highly toxic substances of air, terrain, structures, equipment, transport, personal protective equipment, clothing, food, water, fodder and other objects is carried out using chemical reconnaissance devices or by sampling and subsequent analysis in chemical laboratories.

The principle of detection and determination of TS by chemical reconnaissance devices is based on a change in the color of indicators when they interact with TS. Depending on which indicator was taken and how it changed color, the type of TS is determined, and a comparison of the intensity of the obtained color with a color standard allows us to judge the approximate concentration of TS in the air or the density of infection [2].

Chemical exploration relies on a diverse array of methods to investigate and understand the composition, properties, and behaviors of chemical compounds. This thesis provides an overview of the key methods employed in chemical exploration, including analytical techniques such as spectroscopy, chromatography, and mass spectrometry, which aid in compound identification and quantification. Additionally, it discusses computational modeling and simulation as valuable tools for predicting molecular interactions and behavior. Furthermore, the thesis examines fieldwork and laboratory experiments as essential methods to gather empirical data, as

well as interdisciplinary collaboration to leverage expertise from various scientific disciplines.

Through these multifaceted methods, chemical exploration advances our understanding of matter and fuels innovation in a multitude of industries.

Chemical reconnaissance following the use of chemical weapons and during emergency situations is crucial for the prompt and effective response to chemical threats. This thesis explores the specialized methods employed in chemical reconnaissance during and after such incidents, including:

1. **Deployment of Specialized Teams**: Trained personnel equipped with personal protective gear and specialized detection equipment are dispatched to assess the affected area.
2. **Mobile Laboratories**: Mobile labs are used to conduct rapid on-site analysis of samples, identifying the specific chemical agents involved.
3. **Air and Ground Sampling**: Sampling devices, both in the air and on the ground, are employed to collect air, soil, and water samples for analysis.
4. **Remote Sensing Technologies**: Satellite imagery and unmanned aerial vehicles (UAVs) equipped with sensors can provide critical data on the extent of contamination and identify hotspots.
5. **Chemical Sensors and Detectors**: Portable and fixed chemical sensors and detectors are used to identify the presence of chemical agents in the atmosphere.
6. **Decontamination Procedures**: Reconnaissance teams assess the level of contamination and plan decontamination procedures to make the area safe for responders.
7. **Real-time Data Analysis**: Rapid data analysis and communication of findings to decision-makers are essential for immediate response and mitigation.
8. **Environmental Monitoring**: Continual monitoring of the affected area and its surroundings to track changes in chemical agent concentrations and environmental impact.
9. **Intelligence Gathering**: Leveraging intelligence sources and networks to gain information about potential threats and perpetrators.

This thesis delves into the role of these methods in ensuring the safety of responders and the protection of affected populations during and after chemical incidents. It emphasizes the need for rapid, well-coordinated, and technologically sophisticated chemical reconnaissance to mitigate the impact of chemical threats and emergencies effectively.

References

1. Axundov R.Q. Radiasiya və kimyəvi təhdidlərdən mühafizənin vəziyyəti və inkişaf perspektivləri. Milli təhlükəsizlik və hərbi elmlər. 2022. T. 8, № 1. C.68-77. https://mod.gov.az//images/pdf/f9d7e2abe8147ef65ba96f405a7f857d.pdf
2. Akhundov R., İbadov P. Problematic issues and prospects for the development of airborne radiation, chemical and biological reconnaissance systems. Milli təhlükəsizlik və hərbi elmlər. 2023.T.9, №2. C.68-77. https://mod.gov.az//images/pdf/fd2b946777d5b1f20d25e071a455c2bd.pdf

PROFESSIONAL MILITARY DEVELOPMENT IN THE CONTEXT OF MENTAL PREPARATION

Imamverdiyev E.R., Mammadzada V.M.
Military Scientific Research Institute, Baku, Azerbaijan

Preparation for war (political, economic, military, security and etc.) should be implemented comprehensively. This preparation does not include only a nation's military, but also its political apparatus, its economy, and its people. The military preparation for war involves many important things, such as the organization of the Armed Forces, manpower, defense spending, development of a national defense industry, defense cooperation with foreign countries, and its mental preparation and training. When conducting a military analysis of the Second Karabakh War is analyzed from a military point of view, it is concluded that the victory was not easily won. According to the famous military theorist and Prussian general C. V. Clausewitz, *"The main purpose of war is to destroy the enemy's army, to break the determination and will of the enemy country, and to bring the enemy to a level where he accepts political goals"* [1]. The Azerbaijani side also broke the determination and will of the enemy country, forced Armenia to accept its will, and forced it to sign the tripartite statement. The ultimate goal (strategic goal) delivered by the Azerbaijan in political leadership was the *"liberation of territories occupied in the First Karabakh War."* The operational goal for the Azerbaijani Armed Forces was "destroying the combat power of the enemy." Both of these goals were achieved.

Additonallly, it should be emphasized that after the liberation of the cultural capital of Azerbaijan, Shusha, the determination and will of the Armenian Armed Forces was broken. The districts of Kalbajar, Lachin and Aghdam were returned to Azerbaijan without ~~a~~ fight. The signing of the Bishkek Protocol, which formed the legal basis for the end of the First Karabakh War and the establishment of a ceasefire between Azerbaijan and Armenia in May 1994, was never digested by the Azerbaijani people. As 20% of its territory was lost, thousands of people were martyred and injured in the war, as well as the expulsion of approximately 1,2 million people from their homeland that has been globally akcnowledged as ethnic cleansing, the Bishkek Protocol only imposed a cease fire. The political and economic crisis prevailing in Azerbaijan during the period of First Karabakh War, as well as the internal refugee displacement, did not distract the Azerbaijani people from the idea of liberating the occupied territories. Longing for Karabakh and the occupied surrounding regions began to be recorded in novels, epics and poems. Songs were composed expressing the desire for the return of the lost lands. Information about Armenian aggression and the martyrs of the First Karabakh War became part of lesson programs held in kindergardens, secondary schools, and institutions of higher education. The multiple occupation dates had been officialy remarked by the Azeribaijani government. Television and radio programs broadcasted these events highlighting the Azerbaijani psyche around Karabakh. Azerbaijani children are raised with the bitterness of the Karabakh loss. Thus, all of Azerbaijani people, from the child to the oldest, always kept the pain of the Karabakh

loss fresh in their minds. Simoultanously, calls by Azerbaijani officials in international forums encouraged the implementation of the UN resolutions 822, 853, 874 and 884 regarding the Nagorno-Karabakh conflict [2]. This increased the Azerbaijani people's self-confidence.

The factor of mental preparation for the Second Karabakh War ensured the unity of the people-Armed Forces-government. While the authorities purposefully used the available state resources to achieve the highest goal, the people did not spare their material and morale support from the members of the Armed Forces. In this context, the population that supported the military personnel with the material means they had, did not feel sorry for their relatives who were martyred for the sake of territorial integrity. On the contrary, the families of the martyrs were consoled by the fact that their children ascended to the highest level of heaven in order to take back Karabakh [3]. An example that confirms the unity of the people, Armed Forces and the government is that thousands of young and old Azerbaijanis protested in front of the military commissariats for not being involved in the war [4]. On the contrary, on the Armenian side, this mood was not observed. Surely, a part of the population living in Armenia understood that the occupied Azerbaijani territories do not belong to them and those territories are internationally recognized as Azerbaijani territories. Another advantage of the Azerbaijani side in the factor of mental preparation was that, although everyone understood that the victory won in the war cost the blood and lives of their natives. They did not interfere with the war objectives. On the contrary they encouraged and supported the government and the Azerbaijani Armed Forces.

References

1. Carl Von Clausewitz, On war. 1989. http://slantchev.ucsd.edu/courses/ps143a/readings/Clausewitz%20-%20On%20War,%20Books%201%20and%208.pdf
2. Ilham Aliyev delivered a speech at general debates of 75th session of United Nations General Assembly in a video format. September 24, 2020. https://president.az/en/articles/view/40937
3. Martyr's father: God bless the country! August 6, 2022. https://ikisahil.az/post/335776-shehid-atasi-veten-sag-olsun-foto
4. Ilham Aliyev met with members of Khojavand general public. October 10, 2021. https://president.az/az/articles/view/53402

SMART SETTLEMENTS OF AZERBAIJAN IN THE POST-WAR PERIOD

Nasibov Yashar
Military Scientific Research Institute of the National Defense University,
Baku, Azerbaijan

Occupied settlements of Karabakh and Eastern Zangezur economic regions were subjected to Armenian vandalism for 30 years. All historical, cultural and religious monuments in the area were destroyed and looted. Currently, those areas are being cleared of mines, local infrastructure is being rebuilt and new settlements are being built within the framework of the State Programs for the Great Return.

These works, carried out within the framework of State Programs, lead to the rapid development of those economic regions and the possibility of permanent residence for the population. During the creation of settlements in economic regions, "smart settlements" such as "smart cities" and "smart villages" are being applied. The project of creating smart settlements is expected to support the social and economic development of the existing region, as well as to organize fast and efficient infrastructure and create new opportunities that form employment for residents.

A smart city has its own components. These components are different in the concepts developed for the smart city. For example, the concept developed by the European Parliament includes 6 main components - smart economy, smart people, smart management, smart living, smart mobility and smart environment [1]. The components used should form a smart city that provides a complex infrastructure and service landscape where modern technologies and data analytics are effectively used. The development of the "Smart City" concept is ongoing in Azerbaijan. According to the relevant Decree of the President of the Republic of Azerbaijan, state organizations were instructed to prepare the concept of "Smart City and Smart Village" during 2020-2022 [2]. For this purpose, an inter-organizational "Working Group" was created. "Smart village" pilot project covers the 1st, 2nd, 3rd Agali villages of Zangilan district. The foundation of this village was laid by the President of the Republic of Azerbaijan in April 2021. Smart sensor networks, the Internet of Things (IoT) and connected technologies are the main solutions for the implementation of a smart city [3]. Geospatial information from GIS components is an important element for intelligent systems to work in high sensitivity [4, 5].

The smart residential areas created and planned to be created in Karabakh and Eastern Zangezur economic regions have the title of residential areas of the future.

The creation of smart settlements in Karabakh and Eastern Zangezur economic regions will protect our land, which is a charming corner that contains natural beauty, from environmental pollution and will enable efficient use of our natural resources.

References

1. Manville, C. and etc., Mapping Smart Cities in the EU, European Parliament: [Elektronic resource] / – European Union, – January, 2014, – 200 p.
URL:https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

2. National Action Plan for the promotion of open government for 2020-2022, Decree No. 1859 of the President of the Republic of Azerbaijan dated February 27, 2020: [Electronic resource] / - Baku, - 2020. URL: http://www.e-qanun.az/framework/44619

3. Patel, M. Understanding the Role of Smart City & its Components in the IoT Era: [Elektronic resource] / – US/India, – 11.12.2019. URL: https://www.einfochips.com/blog/understanding-the-role-of-smart-city-and-its-components-in-the-iot-era

4. Bayramov, A.A., Hashimov, E.G. The numerical estimation method of a task success of UAV reconnaissance flight in mountainous battle condition // Advanced Information Sistems. Volume 1, №2, 2017, p.70-73 . DOI: 10.20998/2522-9052.2017.2.12

5. Nasibov, Y. Geographic Information System application areas and benefits // – Baku: Military Knowledge – 2014. №4, – p.18-27.

НАСЛІДКИ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ ДЛЯ ГЛОБАЛЬНОЇ БЕЗПЕКИ

Наджафов Зафар
Національний університет оборони, Баку, Азербайджан

Масштабний напад Російської Федерації на Україну став найважливішою подією у міжнародному світі у 2022 році. Ця війна є глобальним військовим конфліктом, оскільки вона торкнулася глобальної продовольчої та ядерної безпеки, загальних принципів міжнародного права і підкреслила важливість покарання за найсерйозніші злочини проти людства. Наслідки конфлікту проявилися у всьому світі, особливо на тлі порушення глобальних ланцюжків поставок, зростання цін на сировину, масштабної інфляції, продовольчої та енергетичної безпеки [1].

Глобальні військові витрати зростуть до $2,24 трлн у 2022 році, що стане найвищим показником за всю історію. Безперечно, війна в Україні стала основним чинником, який вплинув на збільшення глобальних та регіональних військових витрат минулого року. Військова допомога Києву призвела до збільшення військових витрат у Європі та Північній Америці, де більшість країн не лише надали фінансову допомогу ЗСУ у конфлікті з Росією, а й витратили великі суми грошей на збільшення військового потенціалу. постачання обладнання відправлено до України. Власні військові витрати України зросли більш ніж у сім разів і становили третину ВВП країни. Військові витрати Росії також збільшилися на 9,2 відсотка порівняно з попереднім роком, незважаючи на економічні санкції країн [2].

Війна, розпочата Росією в Україні, привертає увагу своїми унікальними особливостями, які раніше не зустрічалися у світовій практиці. Це перша війна історія людства, у якій об'єктом агресії стали ядерні об'єкти. Росія з першого дня направила свої війська у бік ядерних об'єктів України – зони відчуження у Чорнобилі, сховища ядерного палива у Прип'яті. Росія захопила Запорізьку АЕС, найбільшу в Європі, та намагається захопити Южно-Українську АЕС. Росія також приділяє увагу Рівненській АЕС, розташованій неподалік білоруського кордону, і регулярно робить заяви про можливість застосування ядерної зброї [3].

На тлі одностайного засудження Євросоюзом та країнами НАТО військової експансії Москви, спрямованої на окупацію України, Росія, яка перебуває під міжнародними економічними санкціями, намагається втягнути в цю війну Іран і Китай, шукає можливості для зміцнення своїх геополітичних позицій у ситуації. Слід зазначити, що навіть Росія закупила в Ірану велику кількість дронів та іншого озброєння.

Масштабний напад Росії на Україну явно носить агресивний характер, несе у собі всі ознаки геноциду та повністю порушує міжнародні норми безпеки та права людини.

У цій війні військове насильство здійснюється у гібридній формі. Кібератаки, проксі-війни за участю приватної військової та охоронної компанії (наприклад, Вагнера), дрони, радіоелектронна боротьба, супутниковий зв'язок та інші технології характерні для сучасних іррегулярних воєн, що зустрічаються у російсько-українській війні [4].

Перетворення Росії на глобальну загрозу змусило навіть країни, які проводять «пацифістську політику», озброїтися. Такі країни, як Німеччина та Японія, які частково прийняли «пацифістський» зовнішньополітичний напрям і досягли значного економічного прогресу після Другої світової війни, фактично відмовилися від своїх колишніх позицій і перейшли до «реальної політики». Німеччина виділила майже 109 мільярдів доларів на військову модернізацію після серйозних конституційних змін у Бундестазі для створення військового фонду і планує витратити понад 2 відсотки ВВП на військові потреби відповідно до узгоджених цілей НАТО на 2014 рік [5].

Тенденція збільшення військових витрат торкнулася й інших країн світу. Нейтральні країни – Швеція та Фінляндія – відкинули колишній підхід і подали заявку на членство в НАТО [5]. Ретельне вивчення нещодавно опублікованих політичних документів, зокрема Стратегічної концепції НАТО на 2022 рік, Стратегії національної безпеки США та Стратегії національної безпеки Японії, дає достатньо свідчень відходу від ізоляційної та оборонно-орієнтованої політики у традиційному сенсі.

Все це говорить про те, що значення війни вийшло далеко за межі європейського континенту та її наслідки мали глобальний характер.

Список літератури

1. Война в Украине является глобальным конфликтом – Подоляк: [Электронный ресурс] / Гордон. – Киев, 20 февраля, 2023. – URL: https://gordonua.com/news/war/voyna-v-ukraine-yavlyaetsya-globalnym-konfliktom-podolyak-1651347.html

2. SIPRI: Война в Украине сделала мир менее безопасным 12 июня 2023 г.: [Электронный ресурс] / МЕДИАКОМПАНИЯ DW. – Россия, 12 июня 2023 г. – URL: https://www.delfi.lt/ru/abroad/global/sipri-voyna-v-ukraine-sdelala-mir-menee-bezopasnym-93628583

3. Характер российско-украинской войны и ее влияние на региональную и глобальную безопасность. Результаты отчета «Индекс войны 2022»: [Электронный ресурс] / Polskie radio. – 15.02.2023. URL: https://www.polskieradio.pl/397/9770/Artykul/3120215,%D1%85%D0%B0%D1%80%D0%B0%D0%BAeuters

4. Министр цифровой трансформации: Украина превзойдет Россию в «войне технологий»: [Электронный ресурс] / Голос Америки – Москва, 22 Апрель, 2023. – URL: https://www.golosameriki.com/a/minister-ukraine-will-beat-russia-in-war-of-technologies/7061326.html

5. Ниведита Д. К, Таймур Х. Российско-украинский конфликт: будущее глобальной безопасности: [Электронный ресурс] / Валдай международный дискуссионный клуб. – Россия, 23.02.2023. – URL: https://ru.valdaiclub.com/a/highlights/budushchee-globalnoy-bezopasnosti/

ІНФОГРАФІКА ЯК НОВА ТЕХНОЛОГІЯ РОЗРОБКИ ТА СТВОРЕННЯ КОМПЛЕКТУ ПЛАКАТІВ БУДОВИ СУЧАСНИХ ЗРАЗКІВ БРОНЕТАНКОВОГО ОЗБРОЄННЯ ТА ТЕХНІКИ

Ісаков О.В., Пономаренко М.С, Кулага О.М.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна
Богуцький С.М., Живчук В.Л.
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна

Освітній процес будується передачі інформації, тому роль наочного подання у навчанні велика. Використання таблиць, схем, малюнків сприяє швидкому запам'ятовування та осмислення матеріалу, що вивчається. З урахуванням сучасних технічних можливостей ідея візуалізації інформації в процесі навчання набуває нових рис [1].

Комплект навчальних плакатів − один із найважливіших елементів освітнього процесу будови сучасних зразків бронетанкового озброєння та техніки **(**БТОТ), який дає змогу подати інформацію у доступній формі та забезпечує керування відображенням даних через взаємодію користувача з елементами плакату. За результатами дослідження навчальні плакати допомагають прискорити процес навчання спеціалістів на 20% та покращити засвоєння матеріалу на 40% [2].

У доповіді розглядаються методичні особливості розробки та створення комплекту плакатів будови сучасних зразків БТОТ. Так, варто взяти до уваги, що у графіці дуже легко відображати існуюче в реальності, значно важче перенести у візуальну площину абстрактні поняття і майже неможливо − думки та коментарі.

Авторами розглядаються перспективи створення плакатів з динамічними зображеннями на основі відео та анімації (їх ще називають мультимедійними плакатами); тривимірних інтерактивних плакатів, у яких спосіб відображення інформації визначається діями користувача [3].

Список літератури

1. Eells, W.C. The relative merits of circles and bars for representing component parts [Text] / W.C. Eells // J. of the American Statistical Association. – 1926. – Vol. 21. – P. 119–132.

2. Cairo, A. The Functional Art: An introduction to information graphics and visualization / A. Cairo. - San Francisco : New Riders, 2012. - 384 p.

3. The Difference between Infographics and Visualization [Electronic resource] / R. Kosara // EagerEyes. – 2010. – Access mode: http://eagereyes. org/blog/2010/the-difference-between-infographicsand-visualization (reference date: 08.07.2013). 4. Lewi, P.J. Speaking of Graphics. An Essay on Graphicacy in Science, Technology and Business [Electronic resource] / P.J. Lewi // DataScope. – 2006. – Access mode: http://www.datascope.be/sog/ SOG-Preface.pdf (reference date: 08.07.2013).

USING THE SIMULATION MODELING FOR THE FORMATION OF THE CONCEPT OF CONSTRUCTIVE AND COMPONENT SOLUTIONS FOR INCREASING THE COMBAT CAPABILITIES OF BMP-1

Makogon H., Matias A., Serhieiev A., Klimov O.
Military Institute of Tank Troops of National Technical University
"Kharkiv Polytechnic Institute", Kharkiv, Ukraine
Zabolotnyuk V.
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine

The war in Ukraine once again vividly proved the relevance of the effective use of the armored vehicles, including infantry fighting vehicles. According to the authors, the implementation of promising constructive and design solutions should be aimed at creating an infantry fighting vehicle that will be able to fight against an enemy that is superior in force or that attacks "in the back"; mainly on own territory; in conditions of limited human, economic and other resources [1]. Analytical substantiation of the modernization results aimed at expanding the capabilities of the existing BMP-1 is illustrated in the report with the BMP-1TS vehicle. One of its modernization features is the installation of a new single turret, which was named "Spear". It is similar in size to the original BMP-1, but it allows you to install a variety of weapons. Combat module "Spear" has a 30-mm automatic cannon 3TM-1 (2A72), a 7.62-mm machine gun, and a 30-mm automatic grenade launcher (AGS-17). The module can also use the anti-tank complex "Barrier". The authors propose the use of simulation modeling to determine promising directions for improving the machine by constructing a regression equation links its combat effectiveness and tactical and technical characteristics. Thus, the need to take weapons and ammunition out of the populated compartment, as well as to provide protection against "anti-roof" ammunition while desired (to 1.4 m) of the landing compartment determine internal height the shape and design of the tower [2, 3]. So, the creation of a modern BMP allows us to consider new opportunities and qualities of the promising BMP-1TS as the main element of the modern armed struggle system

References

1. І.Г. Бондарєв, М.В. Коломієць. Перспективна БМП. Деякі аспекти формування концепції конструктивних і компонувальних рішень [on-line]. URL: https://www.ukrmilitary.com/2017/10/perspective-ifv.html

2. Українські модернізації БМП-1: приватна ініціатива [on-line]. − URL: https://armyinform.com.ua/2023/10/09/ukrayinski-modernizacziyi-bmp-1-pryvatna-inicziatyva/

3. S. Tyshko, O. Lavrut, V. Vysotska, O. Markiv, O. Zabula, Y. Chernichenko and T. Lavrut. Compensatory Method for Measuring Phase Shift Using Signals Bisemiperiodic Conversion in Diagnostic Intelligence Systems. Proceedings of the 4nd International Workshop on Modern Machine Learning Technologies and Data Science. Volume I: Main Conference Lviv-Shatsk, Ukraine, November 25, 2022.- P. 144-154. − [Електронний ресурс].- URL: https://ceur-ws.org/Vol-3312/paper12.pdf.

BATTLE PLANNING AND ORGANIZATION LOGISTICS SUPPORT IN THE FORMS AND METHODS OF NATO STANDARDS MILITARY MANAGEMENT TOOLS BASED ON THE USE OF THE GAME THEORY MATHEMATICAL APPARATUS

Makogon H., Serpukhov O., Rybak T.
Military Institute of Tank Troops of National Technical University
"Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Effective implementation of unit management procedures and coordination of available forces and means is impossible without taking into account risks, situational conditions, own capabilities and possible options for the enemy's actions. The analysis of possible options for actions, including with the help of a military raffle, is a promising toolkit of military management according to NATO standards.

Modeling a military operation in the sense of considering the most likely and dangerous options for the enemy's actions and one's own involves drawing up a table of analysis of options for making a decision. Based on the selected evaluation criteria, the headquarters determines the relative effectiveness and objectivity of one course of action relative to others. The analysis of action options for decision-making is carried out on the basis of a matrix, the values of the elements of which are determined by an expert method, and during the briefing of the relevant officials. Expert evaluations are usually subjective, and the set of decision-making options with the help of "brainstorming" may not be complete enough [1].

Therefore, the development of a methodology for the analysis of an action option for making a decision on combat operations based on scientific approaches is a relevant task.

The method of analyzing options for making a decision on combat operations using the mathematical apparatus of game theory is one that is devoid of subjectivity. The authors propose a solution of the matrix game compiled on the basis of data on combat operations in the sphere of operation of the S-4 section of the headquarters of the military unit is the basis of the methodology of logistical support for the planning and organization of the battle in the forms and methods of the military management toolkit according to NATO standards [2].

References

1. Рекомендації з планування та організації бою за стандартами НАТО [on-line]. – URL: https://sprotyvg7.com.ua/lesson/rekomendacii-z-planuvannya-ta-organizacii-boyu-za-standartami-nato-chastina-2

2. Математичні основи теорії вогневих дуелей : монографія / І. О. Кириченко, Л. Г. Раскін. – Харків : Військ. ін-т ВВ МВС України, 2005. – 292 с.

USING INNOVATIVE DIAGNOSTIC METHODS FOR OPTIMIZING MAINTENANCE OF ACCUMULATORY BATTERIES IN THE ARMED FORCES OF UKRAINE

Makogon H., Zhivchenko O., Moskalenko V.
Military Institute of Tank Troops of National Technical University
"Kharkiv Polytechnic Institute", Kharkiv, Ukraine
Stashkov V., Lavrut O.
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine

The main means of maintaining starter batteries (SB) in a technically sound condition during the operation of combat vehicles is timely and high-quality maintenance. In this regard, the authors consider the possibility of using innovative diagnostic methods for monitoring the technical condition of the vehicle, using the experience of the modern automotive industry, to be a relevant study [1].

The so-called battery analyzer or battery tester allows you to carry out a complete analysis of the state of the batteries in a matter of seconds. The standard device has the function of checking the SB under load, and also checks the operation of the starter and generator. Testing can be done both after charging the battery and without charging [1, 2].

Since modern control and measuring devices work in accordance with international standards, as a primary task, the authors propose the creation of a single terminological basis for the maintenance of GB using the latest technologies. In particular, it will be interesting to note that the electromotive force is called the open circuit voltage, and the starting current is called the cold scroll current.

According to the world experience of battery operation, the determination of their technical state is similar to the procedures of Battery Management and Battery Status control; therefore the authors propose to introduce the following generalized technical state of batteries operated in the military: SOH (State of Health) and SOC (State of Charge).

Monitoring the technical state of the battery according to the Battery Care and Battery Management procedure provides an opportunity to optimize the schedule of maintenance of the battery and to switch from a planned and warning system of maintenance to maintenance on demand with parameter control.

References

1. Тестер АКБ AUTOOL BT760 12V 24V. Аналізатор автомобільних акумуляторів з принтером [Електронний ресурс]: URL: https://greenmilya.com.ua/ua/p1924467541-tester-akb-autool.html (Дата звернення 09.10.2023).

2. Battery University, How to Measure State-of-Charge [On-line]: http://batteryuniversity.com/learn/article/how_to_measure_state_of_charge/ (Accessed 01.10.2023).

ДО ПИТАННЯ ПРАВОВОГО ТА ІНФОРМАЦІЙНОГО СУПРОВОДЖЕННЯ ГУМАНІТАРНОГО РОЗМІНУВАННЯ В УКРАЇНІ

Макогон О.А., Янішен А.С.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут" , Харків, Україна
Новік С.А.
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Крамчанінова І.О.
Громадська організація "Чисті серця Калуш", Калуш, Україна

Розмінування України − один з найбільших викликів, який залишиться з нами на роки після війни. Передусім − через високу вартість, великі затрати часу на виявлення та знешкодження мін на величезних площах, тотальну нестачу людей і техніки та через забюрократизованість сфери розмінування і в Україні, й на міжнародному рівні [1, 2]. Автори присвятили доповідь правовим аспектам гуманітарного розмінування та розглянули питання щодо змісту законодавства у відношенні діяльності, пов'язаної із розмінуванням, а також акредитації і моніторингу операторів з проведення заходів по розмінуванню. В цьому контексті були визначені особливості перекладу міжнародних документів з питань розмінування в гуманітарних цілях та раціональні шляхи формування термінологічного базису сфери гуманітарного розмінування відповідно до норм міжнародного права [3].

Окремо розглядаються можливості діджиталізації процесу інформаційного супроводження гуманітарного розмінування. А саме: використання інтерактивних карт та баз даних для координації, розстановки пріоритетів та розподілу ділянок для розмінування. Перспективним, на думку авторів, слід вважати розвиток роботизованих комплексів для розмінування, оснащених відповідними детекторами (сенсорами, датчиками), засобами прийняття рішень, які б могли застосовуватись на етапах розвідки, пошуку, локації, маркування, ідентифікації, знешкодження та знищення вибухово-небезпечних предметів [4].

Список літератури

1. ДСТУ-П 8820:2018 // Протимінна діяльність. Процеси управління. Основні положення. − Київ: ДП "УкрНДНЦ", 2019. – 84 с.

2. Штучний інтелект пришвидшить розмінування України [on-line]. – URL: https://www.ukrinform.ua/rubric-technology/3740325-stucnij-intelekt-prisvidsit-rozminuvanna-ukraini-ekspert.html

3. A Guide to Developing National Mine Action Standards // Женевский международный центр по гуманитарному разминированию GICHD. − Geneva, 2016. – 56 с.

4. В. Б. Струтинський, О. Я. Юрчишин, О. М. Кравець. Розвиток основних положень проектування маніпуляторів мобільних роботів спеціального призначення адаптованих для роботи з небезпечними об'єктами // Мат. XXII МНТК "Прогресивна техніка, технологія та інженерна освіта". – Київ: КПІ, 2021.– С. 129–131.

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 6)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський технічний університет, Баку, Азербайджан
Академія Державної прикордонної служби, Баку, Азербайджан
Академія міністерства надзвичайних ситуацій, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Громадська організація "Чисті серця Калуш", Калуш, Україна
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Державний університет інфраструктури та технологій, Київ, Україна
Інститут геології і геофізики Азербайджанської НАН, Баку, Азербайджан
Інститут проблем математичних машин та систем НАН України, Київ
Інститут систем управління Азербайджанської НАН, Баку, Азербайджан
Кіровоградська льотна академія, Кропивницький, Україна
Національна академія Національної гвардії України, Харків, Україна
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "ХПІ", Харків, Україна
Національний університет оборони, Баку, Азербайджан
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет цивільного захисту України, Харків, Україна
Національний університет "Чернігівська політехніка", Чернігів, Україна
Представництво «Оракл Іст Сентрал Юроп Сервісис Б.В.», Київ, Україна
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Управління метрології та стандартизації, Київ, Україна
Харківський військовий інститут танкових військ, Харків, Україна
Харківський національний автомобільно-дорожній університет, Україна
Харківський національний економічний університет ім. С. Кузнеця, Україна
Харківський національний університет внутрішніх справ, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О. М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна
Черкаський державний технологічний університет, Черкаси, Україна
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Україна
Черкаський національний університет імені Б. Хмельницького, Україна

ДЛЯ НОТАТОК

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
одинадцятої міжнародної науково-технічної конференції
(16 – 17 листопада 2023 року)
Том 2: секції 3, 6

Відповідальна за випуск *Н. Г. Кучук*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук, І. Ю. Петровська*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 06.11.2023 Формат 60 × 84/16
Ум.-вид. арк. 7,5. Тираж 100 пр. Зам. 1106-23/2

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**