МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Кваліфікаційна наукова
праця на правах рукопису

ВОРОХОБ МАКСИМ ВІТАЛІЙОВИЧ

УДК 004.056

ДИСЕРТАЦІЯ

МОДЕЛІ І МЕТОДИ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ МЕТОДОЛОГІЇ ZERO TRUST

Спеціальність 125 «Кібербезпека та захист інформації»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ М. В. Ворохоб

Науковий керівник:
Складанний П. М.
кандидат технічних наук, доцент

Київ – 2023

АНОТАЦІЯ

Ворохоб М.В. Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації». – Київський університет імені Бориса Грінченка, МОН України, Київ, 2023.

Дисертаційне дослідження присвячене вирішенню актуального наукового завдання, сутність якого полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в інформаційно-комунікаційних системах (ІКС), а також впровадженню заходів управління кіберкультурою на підприємстві.

Методологія zero-trust 'нульової довіри' являє собою зміну парадигми кібербезпеки, відхід від традиційних моделей безпеки на основі периметра до більш динамічного та адаптивного підходу, цьому сприяють декілька факторів, а саме:

1. Зміна ландшафту кіберзагроз. Зі збільшенням частоти та складності кібератак традиційні моделі безпеки, які покладаються на надійну внутрішню мережу, стають неадекватними. Zero-trust визнає необхідність перевірки та автентифікації кожного користувача та пристрою, незалежно від їх місцезнаходження чи мережі.

2. Мобільна робоча сила та віддалений доступ. У сучасному бізнес-середовищі працівники часто мають доступ до ресурсів підприємства з різних місць і пристроїв. Zero-trust визнає необхідність постійної перевірки, що робить її особливо актуальною в епоху віддаленої роботи.

3. Порушення даних і внутрішні загрози. Традиційні моделі безпеки часто не можуть захиститися від внутрішніх загроз і латерального руху в мережі. Zero-trust наголошує на принципі «ніколи не довіряй, завжди перевіряй», який має вирішальне значення для зменшення ризику внутрішніх загроз і неавторизованого доступу.

4. Запровадження хмарних служб. Оскільки підприємства все частіше використовують хмарні послуги та зберігають конфіденційні дані поза територією, потреба в моделі безпеки, яка виходить за межі традиційного периметра мережі, стає вкрай необхідною. Zero-trust дотримується принципів захисту даних незалежно від їх місцезнаходження.

5. Вимоги відповідності. Багато галузей підпорядковуються суворим нормам щодо захисту даних і конфіденційності. Впровадження моделі безпеки zero-trust може допомогти організаціям відповідати вимогам відповідності, забезпечуючи вищий рівень контролю та видимості доступу до даних і обробки.

6. Безперервний моніторинг і адаптивна безпека. Zero-trust побудовано на ідеї постійного моніторингу та адаптивної безпеки. Це має вирішальне значення в умовах кібербезпеки, що швидко розвивається, де загрози постійно розвиваються. Здатність динамічно налаштовувати заходи безпеки на основі даних у реальному часі є ключовою перевагою zero-trust.

7. Реагування на інциденти та виявлення загроз. Zero-trust включає надійні механізми реагування на інциденти та розширені можливості виявлення загроз. Це має вирішальне значення для швидкого виявлення та пом’якшення інцидентів безпеки, мінімізуючи потенційну шкоду.

Таким чином, дослідження щодо вдосконалення політики безпеки підприємств на основі методології нульової довіри є актуальним через його узгодження з поточним ландшафтом кібербезпеки, вирішення проблем, пов’язаних із віддаленою роботою, впровадженням хмарних технологій та еволюцією природи кіберзагроз. Він забезпечує проактивний та адаптивний підхід до безпеки, необхідний для захисту конфіденційної інформації в сучасному взаємопов’язаному та динамічному бізнес-середовищі.

Для досягнення мети в підвищенні ефективності застосування політики інформаційної безпеки підприємства було вирішено наступні задачі:

1. Вперше запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. На відміну від існуючих методів при вирішенні завдання автентифікації приховується зміст і обсяг інформаційного трафіку, клієнт і сервер отримують можливість обирати контейнери для доставки даних, замість складних фіксованих логінів клієнт отримує доступ до візуалізованого подання його особистої автентифікаційної інформації. Це дозволяє приховувати від зловмисника чутливу інформацію, яка може бути використана для реалізації атак, включаючи її руйнування, що в свою чергу знижає ймовірність помилкової автентифікації клієнта або сервера у випадку реалізації цільових атак.

2. Вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології радіочастотної ідентифікації ‘radio frequency identification’ (RFID). Це дозволяє в подальшому перевести в площину створення дослідного зразка відповідного багатофункціонального засобу автентифікації та підвищити за рахунок цього ефективність підсистеми ідентифікації і автентифікації.

3. Подальшого розвитку набула методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що сукупно з методикою оцінки трендів загроз кібербезпеки дає можливість оперативного реагування з боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

У вступі обґрунтовується важливість й актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні положення, наукову та практичну цінність отриманих результатів роботи та наведено особистий внесок автора.

У першому розділі здійснено аналіз стану розробки методів забезпечення політики безпеки сучасного підприємства . Визначено ролі політики безпеки у забезпечення інформаційної безпеки підприємства , проаналізований поточний стан застосування політик безпеки, визначено основні аспекти, підходи та принципі застосування концепції zero-trust. Сформульовано актуально наукове завдання, яке полягає в подальшому розвитку методів вдосконалення політики інформаційної безпеки підприємства на основі інтегрування концептуальних принципів zero-trust, зокрема технічних аспектів їх забезпечення. Зокрема для його вирішення визначено мету роботи, яка полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в ІКС.

У другому розділі визначено основні тренди загроз кібербезпеки та процеси управління кібербезпекою. Запропонована вдосконалена модель формування системи кібербезпеки та підходи щодо оцінки рівня культури кібербезпеки, що дало змогу створити формалізовану модель оцінки культури кібербезпеки.

З урахуванням отриманих в поточному розділі результатів щодо заходів політики безпеки організаційного характеру в наступному розділі уявляється приділити основну увагу організаційно-технічні положенням політики безпеки підприємства на основі концепції zero-trust.

У третьому розділі визначено ключові організаційно-технічні положення політики безпеки підприємства на основі концепції zero-trust. Запропонована вдосконалена модель загроз безпеки на основі концепції zero-trust. Визначено вимоги до безконтактного апаратного засобу автентифікації, розроблено стеганографічний протокол обміну даними, визначено загрози і ризики використання штучного інтелекту 'artificial intelligence' (ШІ), а також запропоновано структурно-логічну схему відповідної системи підтримки прийняття рішення (СППР) щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Зазначена технологія обробки

інформації в СППР по відновленню пошкодженого програмного забезпечення внаслідок впливу кібератак, у подальшому дає можливість здійснювати прийняття рішень відносно розв’язання складних структурованих або неструктурованих задач з метою оптимального вибору способу відновлення дефектів та технологічних операцій по їх усуненню

Дисертація виконувалась в Київському університеті імені Бориса Грінченка.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КУБГ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність Інституту програмних систем Національної академії наук України (акт від 18.09.2023 року) та Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (акт від 20.09.2023 року).

Ключові слова: zero-trust, кібербезпека, захист інформації, кіберзагрози, автентифікація, індентифікація, контроль доступу, критична інфраструктура, вразливість, машинне навчання, штучний інтелект, стеганографія, криптографія, політика безпеки, корпоративна мережа, управління інформаційної безпекою.

ANNOTATION

Vorokhob M. V. Models and Methods of Improving the Company's Information Security Policy based on the Zero Trust Methodology. – Qualification of scientific work on the rights of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 125 " Cybersecurity and information protection" – Borys Grinchenko Kyiv University, MES of Ukraine, Kyiv, 2023.

The dissertation is devoted to solving an urgent scientific problem, the essence of which is to increase the efficiency of the application of the information security policy of the enterprise, formed according to the principles of the zero-trust concept, through a combination of stenographic and cryptographic approaches to the construction of protocols for identification/authentication of subjects in information and communication systems, as well as the implementation of measures to manage cyberculture at the enterprise.

The zero-trust methodology represents a paradigm shift in cybersecurity, moving away from traditional perimeter-based security models towards a more dynamic and adaptive approach, facilitated by several factors, namely:

1. Changing the cyber threat landscape. With the increasing frequency and sophistication of cyberattacks, traditional security models that rely on a reliable internal network are becoming inadequate. Zero-trust recognizes the need to verify and authenticate every user and device, regardless of their location or network.

2. Mobile workforce and remote access. In today's business environment, employees often have access to enterprise resources from a variety of locations and devices. Zero-trust recognizes the need for constant verification, which makes it especially relevant in the era of remote work.

3. Data breaches and insider threats. Traditional security models often fail to protect against insider threats and lateral traffic on the network. Zero-trust emphasizes

the principle of “never trust, always verify,” which is critical to reducing the risk of insider threats and unauthorized access.

4. Implementation of cloud services. As businesses increasingly use cloud services and store sensitive data off-premise, the need for a security model that goes beyond the traditional network perimeter becomes imperative. Zero-trust adheres to the principles of data protection regardless of its location.

5. Eligibility requirements. Many industries are subject to strict regulations regarding data protection and privacy. Implementing a zero-trust security model can help organizations meet compliance requirements by providing a higher level of control and visibility into data access and processing.

6. Continuous monitoring and adaptive security. Zero-trust is built on the idea of continuous monitoring and adaptive security. This is crucial in a rapidly evolving cybersecurity environment where threats are constantly evolving. The ability to dynamically configure security measures based on real-time data is a zero-trust key advantage.

7. Incident response and threat detection. Zero-trust includes robust incident response mechanisms and advanced threat detection capabilities. This is crucial for quickly identifying and mitigating security incidents while minimizing potential damage.

Thus, the study on improving enterprise security policies based on the zero-trust methodology is relevant because of its alignment with the current cybersecurity landscape, addressing challenges related to remote work, cloud adoption, and the evolution of the nature of cyber threats. It provides the proactive and adaptive approach to security required to protect sensitive information in today’s interconnected and dynamic business environment.

To achieve the goal of improving the efficiency of the application of the company’s information security policy, the following tasks were solved:

1. For the first time, a method of authentication of users of the corporate network based on the steganographic protocol for the exchange of authentication data by the security policy, taking into account the concept of zero-trust, has been proposed and

mathematically substantiated. Unlike existing methods, when solving the authentication problem, the content and volume of information traffic are hidden, and the client and server get the opportunity to choose containers for data delivery, instead of complex fixed logins, the client gets access to a visualized representation of his personal authentication information. This makes it possible to hide from the attacker sensitive information that can be used to implement attacks, including its destruction, which in turn reduces the likelihood of false authentication of the client or server in the event of targeted attacks.

2. Improved methodology for the formation of initial requirements for the construction of a contactless hardware means of authentication of corporate network users based on RFID technology. This makes it possible to further transfer the creation of a prototype of the corresponding multifunctional authentication tool to the plane and thereby increase the efficiency of the identification and authentication subsystem.

3. The methodology of operational assessment of the current state of corporate cyberculture based on personnel questionnaires and the mathematical apparatus for processing questionnaire data has been further developed, which, together with the methodology for assessing trends in cybersecurity threats, makes it possible for security management to respond promptly in terms of adjusting security policy and implementing organizational and training measures.

The introduction substantiates the importance and relevance of the topic of the dissertation, formulates the purpose and objectives of the work, defines the main provisions, and scientific and practical value of the results of the work, and provides the author’s personal contribution.

In the first section, an analysis of the state of development of methods for ensuring the security policy of a modern enterprise is carried out. The role of security policy in ensuring the information security of enterprise is defined, the current state of application of security policies is analyzed, and the main aspects, approaches, and principles of application of the concept of zero-trust are determined. An urgent scientific task has been formulated, which consists of the further development of methods for improving the information security policy of enterprises based on the integration of the zero-trust

conceptual principles, in particular the technical aspects of their provision. In particular, to solve it, the purpose of the work is defined, which is to increase the efficiency of the application of the information security policy of the enterprise, formed according to the principles of the zero-trust concept through a combination of stenographic and cryptographic approaches to the construction of protocols for identification/authentication of subjects in information and communication systems.

The second section identifies the main trends in cybersecurity threats and cybersecurity management processes. An improved model for the formation of the cybersecurity system and approaches to assessing the level of cybersecurity culture have been proposed, which has made it possible to create a formalized model for assessing the cybersecurity culture.

Taking into account the results obtained in the current section regarding organizational security policy measures, the next section is supposed to focus on the organizational and technical provisions of the enterprise security policy based on the concept of zero-trust.

The third section defines the key organizational and technical provisions of the enterprise security policy based on the zero-trust concept. An improved model of security threats based on the zero-trust concept is proposed. The requirements for a contactless hardware authentication tool have been determined, a steganographic data exchange protocol has been developed, threats and risks of using artificial intelligence have been identified, and A structural and logical diagram of the relevant decision-making system for the recovery of damaged software as a result of cyberattacks has been proposed. This technology of information processing in decision support system for the recovery of damaged software due to the impact of cyberattacks, in the future, makes it possible to make decisions regarding the solution of complex structured or unstructured tasks to optimally choose the method of restoring defects and technological operations to eliminate them.

The dissertation was carried out at the Borys Grinchenko Kyiv University.

The results of scientific research were used at the Department of Information and Cyber Security named after Professor Volodymyr Buriachko of the Faculty of

Information Technologies and Mathematics of Borys Grinchenko Kyiv University within the framework of research work: “Methods and Models for Ensuring Cybersecurity of Information Systems, Information Processing and Functional Security of Software and Hardware Complexes for Critical Infrastructure Management” (No. 0122U200483, KUBG, Kyiv).

Also, the results of scientific research were accepted for implementation in the activities of the Institute of Software Systems of the National Academy of Sciences of Ukraine, Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine.

Keywords: zero-trust, cybersecurity, information protection, cyber threats, authentication, identification, access control, critical infrastructure, vulnerability, machine learning, artificial intelligence, steganography, cryptography, security policy, corporate network, information security management.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Літвінчук, І., Корчомний, Р., Коршун, Н., & Ворохоб, М. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112

2. Літвінчук, І., Коршун, Н., & Ворохоб, М. (2020). Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 135–143. https://doi.org/10.28925/2663-4023.2020.10.135143

3. Черненко, Р., Рябчун, О., Ворохоб, М., Аносов, А., & Козачок, В. (2021). Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 124–135. https://doi.org/10.28925/2663-4023.2021.11.124135

4. Скітер, І., & Ворохоб, М. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158–169. https://doi.org/10.28925/2663-4023.2021.13.158169

5. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

6. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

7. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

8. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Brzhevska, Z., Dovzhenko, N., Haidur, H., Anosov, A., & Vorokhob, M. (2021). Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model. Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2923, 272–276. (Scopus).

10. Brzhevska, Z., Kyrychok, R., Anosov, A., Skladannyi, P., & Vorokhob, M. (2021). Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3188(2), 257–264. (Scopus).

11. Skladannyi, P., Trofimov, O., Korniiets, V., Vorokhob, M., & Opryshko, T. (2023). Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3421, 97–106. (Scopus).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ....16

ВСТУП....17

РОЗДІЛ 1 АНАЛІЗ СТАНУ ТА ПОСТАНОВКА ЗАВДАННЯ РОЗРОБКИ МЕТОДУ ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА....24

1.1. Визначення ролі політики безпеки у забезпеченні інформаційної безпеки сучасного підприємства....24

1.2. Поточний стан застосування політики інформаційної безпеки, як одного з ключових елементів забезпечення інформаційної безпеки підприємства....30

1.3. Підходи, методи та сучасні практики побудови інформаційної безпеки підприємства....41

1.3.1. Основні аспекти застосування концепції zero-trust при формуванні політики інформаційної безпеки....56

1.3.2. Принципи концептуального підходу zero-trust....59

1.4. Постановка наукового завдання дослідження....67

Висновки до розділу 1....70

Список використаних джерел у розділі 1....71

РОЗДІЛ 2 Аналіз трендів розвитку кіберінцидентів та управління культурою кібербезпеки організації....80

2.1. Аналіз трендів загроз кібербезпеки в цивільному секторі....80

2.2. Процеси управління кібербезпекою в плані підвищення кіберкультури персоналу....88

2.3. Базові завдання різних рівнів управління безпекою через підвищення кіберкультури....98

2.4. Вдосконалення моделі формування системи кібербезпеки....100

2.5. Підходи щодо оцінки рівня культури кібербезпеки в інформаційній системі 102

2.6. Формалізована модель оцінки культури кібербезпеки.....104

Висновки до розділу 2.....106

Список використаних джерел у розділі 2.....107

РОЗДІЛ 3 Ключові організаційно-технічні положення політики безпеки підприємства на основі концепції zero-trust.....112

3.1. Вдосконалена модель загроз безпеки на основі концепції zero-trust.....112

3.2. Визначення вимог до безконтактного апаратного засобу автентифікації..118

3.3. Стеганографічний протокол обміну даними в процедурах управління ідентифікацією та доступом.....126

3.4. Загрози та ризики використання систем штучного інтелекту.....132

3.5. Підтримки прийняття рішення щодо відновлення попереднього стану після кіберінцидентів.....143

Висновки до розділу 3.....151

Список використаних джерел у розділі 3.....153

ВИСНОВКИ.....160

ДОДАТОК А.....162

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІКС – інформаційно-комунікаційна система

ПЕКК – пасивний електричний коливальний контур

ПВП – первинний вимірювальний перетворювач

СППР – система підтримки прийняття рішення

СУІБ – система управління інформаційною безпекою

СШІ – система штучного інтелекту

ШІ – штучний інтелект

DoS denial-of-service ‘відмова в обслуговуванні’

DDoS – distributed denial-of-service ‘розподілена відмова в обслуговуванні’

GDPR – General Data Protection Regulation ‘Загальний регламент про захист даних’

HAD – hardware authentication device ‘апаратний пристрій автентифікації’

IAM – identity & access management ‘авторизації та управління доступом’

IoT – internet of things ‘інтернет речей’

LSB – least significant bit ‘найменший значущий біт’

NIST – National Institute of Standards and Technology ‘Національний інститут стандартів і технологій’

PEP – Policy Enforcement Point ‘точка застосування політики’

PDP – Policy Decision Point ‘точка прийняття рішення’

RFID – radio frequency identification ‘радіочастотна ідентифікація’

VPN – virtual private network ‘віртуальна приватна мережа’

zero-trust – нульова довіра

ВСТУП

Актуальність теми. Сучасний світ характеризується зростаючим впливом інформаційних технологій та збільшеним обсягом цифрової інформації. Водночас, інформація є важливим активом будь-якого підприємства, і її захист стає стратегічною необхідністю для забезпечення стійкості та конкурентоспроможності. Однак, дане завдання останнім часом значно ускладнилося в зв'язку з низкою взаємопов'язаних факторів, зокрема пандемією COVID-19, сплеском впровадження технологій хмарних обчислень та тенденцією щодо використання власних цифрових пристроїв співробітниками замість корпоративних 'Bring Your Own Device' (BYOD). Така трансформація призвела до збільшення кількості пристроїв та сервісів підприємства, інформаційний обмін між якими відбувається через відкриті канали зв'язку – глобальну мережу Інтернет, що в свою чергу призводить до появи нових вразливостей та підвищення ризику реалізації кібернетичних атак на сучасні підприємства.

Згідно зі звітом Агентства Європейського Союзу з кібербезпеки (ENISA), за 2020–2021 роки зафіксовано зростання кількості кібернетичних атак на інформаційні системи, які використовуються для організації та забезпечення дистанційної роботи. Це зокрема призвело до серйозного зростання кількості загроз витоку корпоративної інформації, з 8,7% в 2020 році до 81% у другому кварталі 2021 року.

В результаті, виникає необхідність у впровадженні скоординованого комплексу заходів із захисту інформаційних активів підприємства, що зазвичай називають діяльністю з управління інформаційною безпекою. Щоб захистити інформацію, підприємства впроваджують низку заходів пов'язаних з контролем безпеки, контрзаходами або гарантіями, які можуть приймати різні форми, наприклад, політики, процедури, інструкції, практики та організаційні структури. Водночас, саме політика є основою для ефективного управління інформаційною безпекою і забезпечення безпеки інформаційних активів, а також бізнес-процесів на підприємстві. Однак в зв'язку з глибокою залежністю від впливу поведінкового фактору користувачів щодо забезпечення інформаційної безпеки, що зокрема

висвітлено цілою низкою наукових досліджень, політика інформаційної безпеки підприємства побудована на базових принципах забезпечення безпеки периметра, є малоефективною, особливо за умови віддаленої роботи працівників з «домашніх офісів».

У даному контексті, розгляд та розуміння різних підходів, методів та сучасних практик побудови політики інформаційної безпеки підприємства, є досить актуальним та має велике значення для формування ефективної стратегії протидії кіберзагрозам. Так, одним із найперспективніших підходів вважається концепція zero-trust.

Основний принцип zero-trust можна сформулювати так: «мінімум довіри до всіх, але максимум перевірок». Іншими словами, користувачі повинні підтверджувати свою достовірність при кожному запиті на доступ до інформаційних ресурсів, незалежно від того, чи знаходяться дані ресурси в мережевому периметрі підприємства, чи поза його межами. Завдяки використанню таких технологій, як автентифікація, керування доступом, шифрування, а також різноманітних технологій мережевої безпеки, концептуальний підхід zero-trust встановлює захищені мікроперіметри, при цьому регламентація доступу до ресурсів здійснюється політиками доступу. Водночас, слід відзначити, що дані політики ґрунтуються на принципі найменших привілеїв, згідно з яким кожному користувачеві надається мінімальний обсяг прав та повноважень доступу (з можливим обмеженням в часі), необхідний для виконання його завдань. Саме тому, останнім часом стрімко набирає вагомості питання застосування концептуальних принципів zero-trust при побудові та впровадженні політики інформаційної безпеки підприємства.

Дослідженням даного питання займається досить велика кількість вчених, серед яких: В.С. Харченка, В.Л. Бурячка, В.Б. Дудикевіча, Опірського І.Р, Толюпи С.В.,Гулака Г.М., Соколова В.Ю., Гнатюка С.О., Одарченка Р.С., Kindervag J., Cavalancia N., Ferretti L., Magnanini F., Teerakanok S., Uehara T., D'Silva D., Ambawade D., Alagappan A., Venkatachary S., Kerman A., Borchert O., Saini D., Lukaseder T., Halter M., Zaheer Z., Chang H., Decusatis C., Liengtiraphan A., Li S. та

інші. Переважна більшість робіт присвячена впровадженню, зокрема модернізації існуючих систем забезпечення інформаційної безпеки на підприємствах згідно різних сценаріїв концептуального підходу zero-trust, а також аналізу результуючого покращення рівня безпеки. Водночас, більшість уваги зосереджується саме на організаційних та технологічних аспектах, залишаючи відкритим питання щодо ефективності технічних заходів реалізації концепції zero-trust, зокрема її ключового механізму – ідентифікації/автентифікації суб'єктів доступу.

Таким чином, з приведеного аналізу можна зробити висновок, що в практиці застосування концептуальних принципів zero-trust при формуванні політики інформаційної безпеки підприємства загострилося протиріччя між необхідністю зменшення впливу поведінкових аспектів користувачів щодо забезпечення інформаційної безпеки та ефективністю існуючих теоретичних та технологічних рішень, які б дозволили реалізувати мінімізацію «людського фактору».

У зв'язку з цим, існує необхідність вирішення актуального наукового завдання, сутність якого полягає в подальшому розвитку методів вдосконалення політики інформаційної безпеки підприємства на основі інтегрування концептуальних принципів zero-trust, зокрема технічних аспектів їх забезпечення.

Зв'язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Київського університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КУБГ, м. Київ).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки

комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в ІКС, а також впровадженню заходів управління кіберкультурою на підприємстві.

У відповідності до поставленої мети, для вирішення наукового завдання, в роботі було визначено та розв'язано такі часткові завдання:

– проаналізовані поточний стан застосування політики інформаційної безпеки, як одного з ключових елементів забезпечення інформаційної безпеки підприємства, а також підходи, методи та сучасні практики побудови системи інформаційної безпеки підприємства;

– здійснено детальний аналіз концепції «нульової довіри» та виділено основні обмеження щодо центрального елемента системи забезпечення безпеки, а саме, використовуваних механізмів ідентифікації/автентифікації суб'єктів доступу;

– досліджені тренди виникнення кіберінцидентів та визначені елементи управління культурою кібербезпеки організації на основі обробки даних обстежень її поточного стану та впровадження корегуючих заходів;

– визначена формалізована модель оцінки рівня культури кібербезпеки;

– вдосконалена модель загроз безпеки інформаційних активів підприємства на основі концепції zero-trust;

– визначенні вимоги до безконтактного апаратного засобу автентифікації суб'єктів інформаційних відносин;

– запропоновано та обґрунтовано стеганографічний протокол обміну даними в процедурах управління ідентифікацією та доступом;

– визначені нові загрози та ризики що обумовлені поширенням використання систем штучного інтелекту (СШІ).

Об'єктом дослідження є технології забезпечення безпеки інформаційних активів підприємства в умовах постулату zero-trust щодо учасників інформаційної взаємодії.

Предметом дослідження є моделі і методи ідентифікації та автентифікації суб'єктів в ІКС, як ключових елементів формування дієвої політики

інформаційної безпеки підприємства на основі реалізації базових положень концепції zero-trust та управління культурою кібербезпеки підприємства.

Методи дослідження. Для проведення досліджень в дисертаційному дослідженні використовувалися методи системного аналізу, теорії ризиків, теорії ймовірностей та математичної статистики, методи моделювання систем управління інформаційною безпекою (СУІБ).

Наукова новизна одержаних результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей автоматизації активного аналізу захищеності корпоративних мереж:

1. Вперше запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. На відміну від існуючих методів при вирішенні завдання автентифікації приховується зміст і обсяг інформаційного трафіку, клієнт і сервер отримують можливість обирати контейнери для доставки даних, замість складних фіксованих логінів клієнт отримує доступ до візуалізованого подання його особистої автентифікаційної інформації. Це дозволяє приховувати від зловмисника чутливу інформацію, яка може бути використана для реалізації атак, включаючи її руйнування, що в свою чергу знижає ймовірність помилкової автентифікації клієнта або сервера у випадку реалізації цільових атак.

2. Вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID. Це дозволяє в подальшому перевести в площину створення дослідного зразка відповідного багатофункціонального засобу автентифікації та підвищити за рахунок цього ефективність підсистеми ідентифікації і автентифікації.

3. Подальшого розвитку набула методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що сукупно з методикою оцінки трендів загроз кібербезпеки дає можливість оперативного реагування з

боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

Практичне значення одержаних результатів полягає в наступному: зміни в ландшафті інформаційних технологій, поширене застосування засобів інтернету речей ‘internet of things’ (IoT), доступ до хмарних середовищ, включаючи використання для цього мобільних пристроїв, дозволяють зрозуміти важливість концепції zero-trust для сучасної підприємницької діяльності.

Саме ці тренди обумовлюють практичну значущість запропонованого в дослідженні принципового переходу від статистичної політики доступу до критичних даних, яка не корегується залежно від поточного контексту поведінки користувача та наступних його змін, до динамічної політики безпеки, що адаптується до поведінки користувача (його кіберкультури) для поточної та попередніх транзакцій. Запропоноване рішення щодо надання доступу до ресурсів з простим інтерфейсом на основі стеганографічного протоколу з одного боку візуалізує інформацію про наявні параметри безпеки, з іншого – не розкриває їх зміст та не потребує запам’ятовування не складних символьних (буквено-цифрових) конструкцій та структури таких даних. Перспективність запропонованих рішень для таких галузей як телемедицина, дистанційне управління засобами фізичної безпеки та охорони, систем дистанційної освіти тощо є очевидною.

Особистий внесок здобувача. Всі наукові результати, що виносяться на захист, одержано здобувачем самостійно. У роботах, написаних у співавторстві, здобувачеві належить: в [1] – оцінювання ризиків інформаційної безпеки, [2] – оцінювання систем безпеки на об'єкті інформаційної діяльності, [3] – визначення рівня захищеності систем, [4] – модель оцінки рівня культури кібербезпеки, [5] – СППР щодо відновлення пошкодженого програмного забезпечення, [6] – аналіз методів та моделей при побудові політки безпеки, [7] – визначення ризиків та загроз, [8] – блок-схема алгоритму роботи системи ідентифікації апаратного пристрою автентифікації ‘hardware authentication device’ (HAD), [9] – оцінка

інформації, [10] – визначення інформаційних впливів, [11] – удосконалення політики безпеки систем.

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені в ході ряду наукових конференцій:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2021.

2. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II), 2021.

3. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2023.

Публікації. За результатами проведеного дисертаційного дослідження було опубліковано 11 наукових праць. Зокрема основні наукові положення викладено в 8 наукових статтях, серед яких 8 опубліковані у спеціалізованих фахових виданнях, затверджених наказом Міністерство освіти і науки України, 3 опубліковано у закордонному науковому виданні, що входить до наукометричної бази Scopus.

Структура та обсяг дисертаційного дослідженя. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел із 176 найменувань на 160 сторінках. Загальний обсяг роботи становить 162 сторінки, 16 рисунків, 6 таблиці.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ТА ПОСТАНОВКА ЗАВДАННЯ РОЗРОБКИ МЕТОДУ ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА

1.1. Визначення ролі політики безпеки у забезпеченні інформаційної безпеки сучасного підприємства

Нині, коли інформаційні технології досягли високого рівня розвитку, задля підвищення ефективності своєї діяльності, багато підприємств перейшли до використання електронного документообігу. В результаті, передача, обробка та зберігання інформації, включаючи конфіденційну, здійснюється за допомогою електронних засобів.

Водночас, одним із найслабкіших місць успішного функціонування підприємств все ще залишається питання захисту своїх інформаційних систем та в цілому активів. Ба більше, дана ситуація ускладнилася та набула особливої гостроти на фоні появи пандемії COVID-19, коли більшість бізнес-процесів перейшли в онлайн-формат, що в свою чергу ще більше привернуло увагу кіберзлочинців. Це зокрема підтверджується чималою кількістю різноманітних досліджень щодо корпоративних кіберінцидентів.

Так Агентство Європейського Союзу з кібербезпеки своїм звітом ENISA [1] декларує зростання в 2020–2021 роках кількості кібернетичних атак на так звані «домашні офіси», тобто програмне забезпечення для створення єдиної корпоративної мережі та особистих кабінетів працівників задля організації дистанційної форми праці [2]. Як результат – збільшення загрози витоку корпоративних даних з 8,7% у 2020 році до 81% у другому кварталі 2021 року.

Схожа тенденція, також проглядається зі щорічних звітів щодо вартості витоку конфіденційних даних сформованих компанією IBM (Cost of a Data Breach Study) [3–12]. До прикладу, опубліковані дані за 2022 рік свідчать про збільшення

середньої вартості витоку даних для підприємств з усього світу з 3,62 млн до 4,35 млн доларів США у порівнянні з 2017 роком, тобто приблизно на 20%. Водночас, серед початкових векторів атак, які стали причиною витоку даних, IBM виділяють фішинг, викрадені або скомпрометовані дані, вразливості прикладного програмного забезпечення, а також витік за рахунок інсайдерів та компрометації ділової електронної пошти (рис. 1.1).

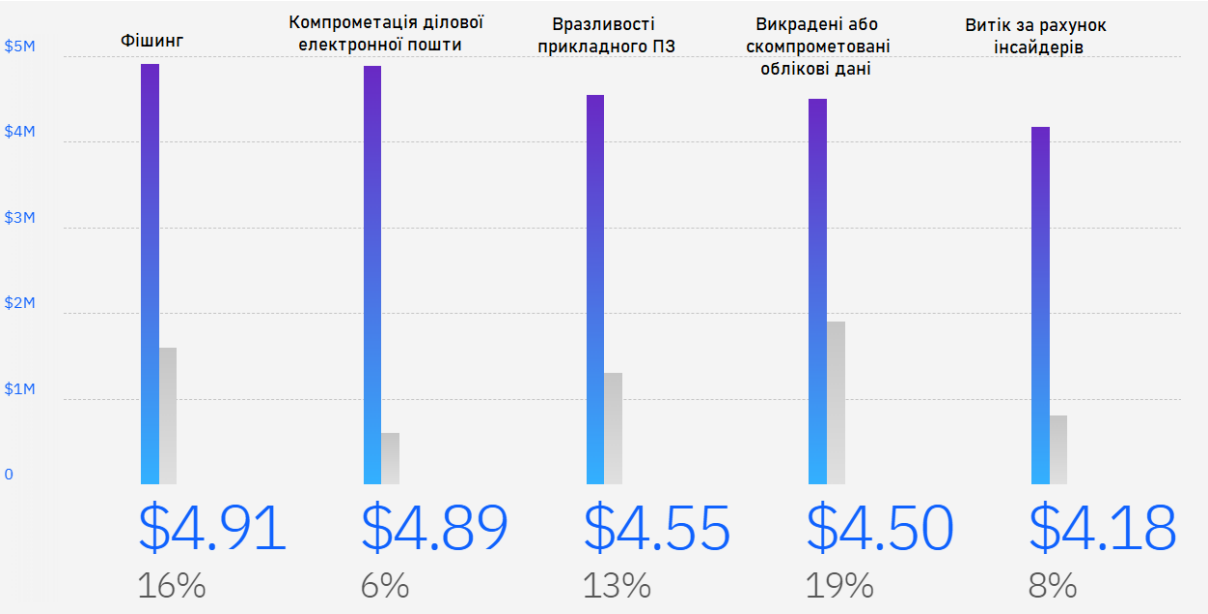

Рис. 1.1. Вартісна оцінка витоку даних за початковими векторами атак згідно звіту Cost of a Data Breach Study 2022 [13]

Дане дослідження проводиться в форматі інтерв'ю з IT-фахівцями та фахівцями з інформаційної безпеки в майже 500 міжнародних компаніях, які стикаються з витоком даних за поточний рік. В ході даного дослідження аналізуються численні фактори витрат, пов'язані з витоком, такі як технічне розслідування, відновлення системи, інформування спільноти, юридичні та нормативні дії, а також витрати, понесені в зв'язку з втратою репутації, або навіть частки бізнесу.

Біль того, переглядаючи звіт компанії Accenture [14] від листопада 2021 року, з'ясовується, що 55% підприємств з річним доходом більше 1 млрд. доларів США, в силу неспроможності швидкого виявлення та усунення вразливостей, взагалі недостатньо ефективно попереджують кібератаки.

В розрізі наведених досліджень, керівництво сучасних підприємств має чітко усвідомлювати, що головним завданням фахівця з інформаційної безпеки має бути не розслідування випадків витоку конфіденційних даних, а саме запобігання або, хоча б мінімізація ризиків втрати даних, що, у свою чергу, дозволяє зменшити збитки та підвищити стабільність роботи підприємства [15].

Так, з метою зменшення ймовірності порушення конфіденційності та забезпечення безпеки даних на підприємствах впроваджується ціла низка різноманітних засобів захисту інформації, серед яких засоби: міжмережевого екранування, побудови віртуальної приватної мережі ‘virtual private network’ (VPN), контролю доступу, управління оновленнями програмних компонентів, резервного копіювання та архівування, централізованого моніторингу та управління безпекою, виявлення вторгнень та аномалій, контролю та аналізу поведінки користувачів, запобігання витоку конфіденційних даних, захисту від спаму і атак класу «відмова в обслуговуванні» та чимало інших.

Однак, попри всю різноманітність технологій забезпечення інформаційної безпеки, їх впровадження не приносить фінансової вигоди тому, хто захищається, що в контексті функціонування сучасного підприємства є досить вагомим фактором, вони лише дозволяють зменшити збиток від можливих інцидентів. Адже будь-яка спроба несанкціонованого доступу, кібернетична атака або будь-яке інше порушення режиму інформаційної безпеки можуть призвести до критичних наслідків, зокрема прямих та непрямих збитків. В результаті, для підприємства є особливо важливим саме раціональне інвестування своїх ресурсів та часу у вирішення проблеми забезпечення інформаційної безпеки, що дозволить зменшити потенційні фактори ризику.

І хоча, попри відсутність прямих емпіричних досліджень, є переконливі докази того, що розробка та впровадження універсальної, функціональної та досить простої політики інформаційної безпеки є одним із найбільш ефективних та економічно доцільним рішенням захисту конфіденційних даних підприємства [16, 17]. Як видно з діаграми (див. рис. 1.2), сформованої за результатами проведеного дослідження витрат на корпоративну безпеку підприємства Стівеном

Россом директором Delloitte & Touche (група компаній у сфері аудиторських та консалтингових послуг), кожна політика безпеки може бути як найдешевшим, так і одночасно найефективнішим способом забезпечення інформаційної безпеки.

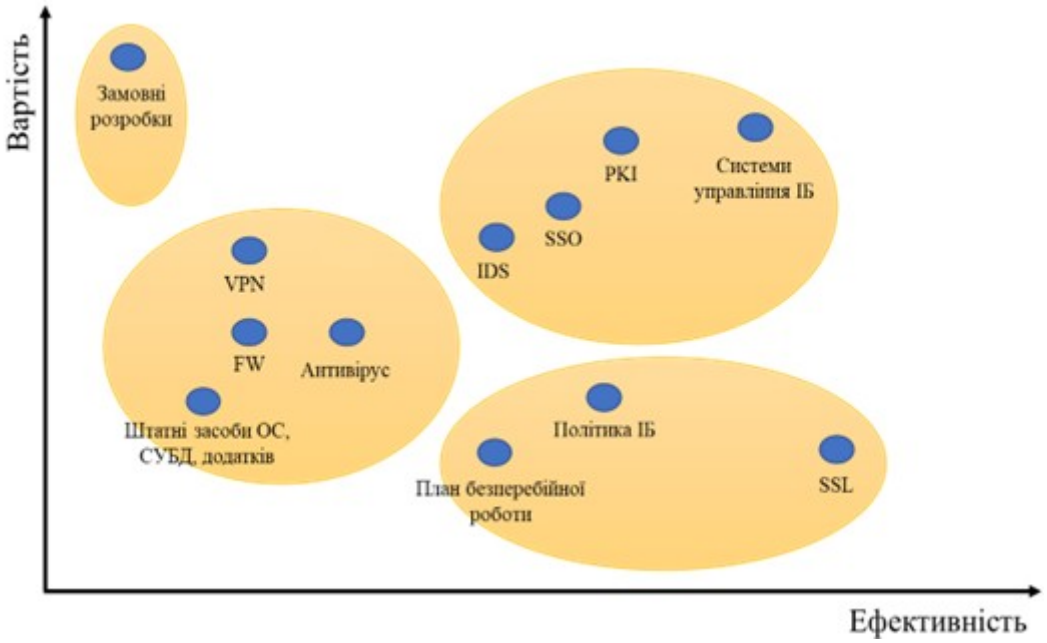

Рис. 1.2. Оцінка доцільності застосування окремих заходів і засобів забезпечення інформаційної безпеки

В контексті цього виникає необхідність у вірному трактуванні самого терміну «політики інформаційної безпеки». Слід відзначити, що на даний момент відсутнє загальноприйняте визначення для даного терміну. Так, ґрунтовний огляд літератури щодо політики інформаційної безпеки дозволив виявити три фундаментальні складові даного терміну.

Перша складова підкреслює суто технічний аспект щодо встановлення технічних вимог інформаційної безпеки, яким повинна відповідати система або окремий продукт. Зокрема, в контексті цієї складової, політика інформаційної безпеки може визначати та регламентувати набір правил, що використовуються системою керування доступом суб’єктів до об’єктів системи [18].

Друга складова підкреслює стратегічний аспект інформаційної безпеки всередині підприємства. В даному випадку, політика безпеки інтерпретується як високорівневе декларування організаційних переконань оформлене у вигляді документа, що інкапсулює рішення щодо управління інформаційною безпекою,

зокрема щодо цілей та завдань підприємства, а також загальних заходів, пов’язаних із захистом інформаційних активів підприємства [19].

А третя – підкреслює поведінковий аспект, де політика безпеки розглядається як керівний принцип або керівництво для дій організаційних суб’єктів у сфері інформаційної безпеки. Тобто, політика інформаційної безпеки підприємства декларує ролі та обов’язки працівників щодо захисту інформаційних і технологічних ресурсів даного підприємства. По суті, визначає, що дозволено, а що заборонено в інформаційних системах і мережах підприємства [3].

Водночас, основною метою політики безпеки вважається зниження інформаційних ризиків, захист важливих інформаційних активів, а також мінімізація витрат, пов’язаних із управлінням інформаційною безпекою на підприємстві [20]. Більш того, попри дотримання як внутрішніх, так і зовнішніх правил та процедур, політика безпеки також має сприяти розвитку та підвищенню ефективності самої інфраструктури інформаційної системи підприємства [21].

Тобто, політика безпеки здебільшого розглядається саме на організаційному рівні, формуючи підхід підприємства до управління інформаційною безпекою та створює основу для ефективного захисту його інформаційних активів. При цьому, серед основних аспектів, які може регламентувати політика, слід виділити: фізичний захист ресурсів, керування доступом, забезпечення цілісності та конфіденційності даних, а також аудит безпеки.

В результаті, можна сформувати узагальнююче визначення поняття «політики інформаційної безпеки», яким будемо надалі оперувати в даній дисертіції.

Політика інформаційної безпеки – це комплекс заходів, правил та принципів превентивного характеру, спрямованих на захист інформаційних процесів окремого підприємства та циркулюючих там конфіденційних даних. Політика безпеки включає вимоги та правила для персоналу, менеджерів і технічних служб, а також визначає цілі та завдання, які повинні досягатися під час її виконання. Водночас, слід відзначити, що політика інформаційної безпеки формалізується та

розробляється індивідуально для конкретного підприємства, а всі співробітники повинні бути своєчасно ознайомлені зі змістом даного документу.

Таким чином, політика безпеки відіграє важливу роль у забезпеченні інформаційної безпеки сучасного підприємства, зокрема щодо:

– встановлення загальних положень, норм та вимог щодо забезпечення інформаційної безпеки – політика безпеки визначає положення, норми та вимоги, які допомагають забезпечити належний рівень безпеки інформації;

– забезпечення конфіденційності та цілісності даних – політика безпеки визначає процедури та правила для захисту конфіденційної інформації від несанкціонованого доступу. Вона забезпечує, щоб лише авторизовані суб'єкти (користувачі, процеси) отримували доступ до цієї інформації. Крім того, політика безпеки також визначає заходи для забезпечення цілісності даних;

– зниження інформаційних ризиків – однією з цілей політики безпеки є мінімізація ризиків, пов'язаних із зберіганням, обробкою та передачею інформації. Вона допомагає зменшити шанси виникнення інцидентів безпеки, таких як втрата даних або злом системи;

– реагування на інциденти безпеки – політика безпеки визначає процедури реагування на інциденти безпеки, якщо такі інциденти все ж стались. Зокрема вказуються дії, які повинні бути вжиті для виявлення, нейтралізації та відновлення після інцидентів;

– відповідність вимогам законодавства – політика безпеки дозволяє визначити правила, відповідно до яких інформація може бути віднесена до категорії комерційної або службової таємниці, а також допомагає забезпечити відповідність законодавчим вимогам нормативної бази в галузі захисту інформації. Це зокрема дозволяє підприємствам юридично захистити оброблювану інформацію;

– створення корпоративної культури безпеки – політика безпеки сприяє формуванню культури безпеки на підприємстві підтримує свідоме ставлення співробітників до інформаційної безпеки та створює середовище, де безпека є важливою складовою кожного бізнес-процесу [22];

– забезпечення безперервності бізнесу – вірно розроблена та впроваджена політика безпеки дозволяє збільшити час доступності сервісів підприємства, в результаті чого збільшується загальна життєздатність компанії і забезпечується безперервність бізнесу;

– збільшення довіри клієнтів – політика інформаційної безпеки є свого роду доказом надання гарантій того, що конфіденційна інформація клієнтів та партнерів підприємства буде захищена належним чином (з можливістю юридичного підтвердження цього в контрактах), оскільки саме в політиці безпеки декларуються наміри підприємства щодо якості забезпечення інформаційної безпеки.

1.2. Поточний стан застосування політики інформаційної безпеки, як одного з ключових елементів забезпечення інформаційної безпеки підприємства

Як вже було висвітлено в попередньому підрозділі, останнім часом, зацікавленість підприємств в інформаційній безпеці значно зросла, вони почали визнавати необхідність впровадження та дотримання підвищених вимог до інформаційної безпеки. Одним із основних методів ефективного управління інформаційною безпекою є саме впровадження політики інформаційної безпеки, адаптованої під унікальні потреби кожного підприємства. Хоча, до недавнього часу велика частина індустрії інформаційної безпеки дотримувалася думки, що політика безпеки нічого не забезпечує, що для справжнього забезпечення інформаційної безпеки достатня лише наявність певних технології, тим самим, вважаючи політику інформаційної безпеки неефективним засобом. Тобто, до прикладу, у той час як міжмережевий екран може «активно» блокувати пакети, які не відповідають певним критеріям, «пасивне» положення політики інформаційної безпеки: «не використовувати однакові парольні фрази для декількох корпоративних сервісів», може бути просто проігнороване.

Безсумнівно, політика за своєю суттю є пасивною, однак і наведене вище судження, що «політика безпеки нічого не забезпечує» є не зовсім коректним. По перше, слід відзначити, що хоча самі положення політики є дійсно пасивними, однак регламентовані ними дії є активними. Загалом, серед основних аспектів інформаційної безпеки, які можуть регламентуватися політикою інформаційної безпеки, слід виділити:

– забезпечення конфіденційності даних, для чого визначаються конкретні принципи, процедури та технології, що забезпечують захист конфіденційної інформації від несанкціонованого доступу, витоку та використання. Зокрема даний аспект включає:

- класифікацію інформації, що дозволяє для різних видів інформації визначити їх рівень конфіденційності, визначаючи, яка інформація вимагає найвищого рівня захисту;
- керування доступом – встановлює правила та процедури для контролю доступу до систем, мереж та даних. Зазвичай реалізується шляхом застосування механізмів автентифікації та авторизації;
- шифрування – політика безпеки може вимагати застосування шифрування (зокрема встановлюючи вимоги до самих механізмів шифрування) для забезпечення захищеності даних під час їх передачі чи зберігання;
- фізичний захист – визначає процедуру контролю до приміщень та обладнання, що містить конфіденційну інформацію;
- заборону обміну конфіденційною інформацією – окремі положення політики інформаційної безпеки можуть забороняти обмін конфіденційною інформацією з особами або підприємствами, які не мають необхідних дозволів або укладених угод;
- видалення інформації – визначає процедуру безпечного видалення конфіденційної інформації з пристроїв та систем, що більше не використовується;

– забезпечення цілісності даних шляхом визначення спеціальних принципів, процедур та практик, що забезпечують захист від неправомірних змін,

редагування або порушення цілісності інформації. Зазвичай даний аспект включає:

- контроль цілісності та автентичності даних – визначає функціонування цифрового електронного підпису, або окремих механізми забезпечення цілісності, зокрема контрольної та хеш-суми, які дозволяють виявити несанкціоновані зміни;
- резервне копіювання та відновлення – визначає механізми створення резервних копій даних для відновлення інформації у випадку порушення її цілісності або повного знищення;

– забезпечення доступності даних шляхом встановлення конкретних принципів, процедур та практик, які мають на меті забезпечити доступ до інформації та ресурсів у вимогливий спосіб, мінімізуючи перебої та відмови в обслуговуванні. Зокрема даний аспект включає:

- відновлення систем – визначає процедуру відновлення систем, в тому числі з використанням резервних копій, після відмови для мінімізації перерв у роботі;
- формування технічних резервів – визначає використання дубльованого обладнання, серверів та мережевих засобів для забезпечення неперервності роботи в разі відмови основного;
- балансування навантаження – визначає механізми балансування навантаження для розподілу завантаженості між різними серверами, що допомагає запобігти перевантаженню та відмовам;
- запобігання атака на відмову в обслуговуванні ‘denial-of-service’ (DoS) / розподілена атака на відмову в обслуговуванні ‘distributed denial-of-service’ (DDoS) – регламентує застосування заходів для запобігання атакам, спрямованих на відмову в обслуговуванні та перекритті доступу до ресурсів;

– забезпечення безпеки мережі – визначає правила та механізми для захисту мережевих ресурсів і даних від несанкціонованого доступу та мережевих атак;

– моніторинг та аудит безпеки визначає процедури виявлення та фіксації будь-яких некоректних або несанкціонованих дій щодо змін в системі або даних, а також спроб несанкціонованого доступу;

– превентивні механізми – визначає заходи щодо виявлення та запобігання вразливостей, а також забезпечення відповідного реагування на загрози та атаки;

– навчання співробітників щодо основних положень політики інформаційної безпеки, загроз безпеці та правил поведінки в інтернеті;

– та інше.

Таким чином, політика інформаційної безпеки підприємства зазвичай може вимагати таких дій, як обов'язковий супровід відвідувачів підприємства, перевірку програмного забезпечення на наявність шкідливого коду перед встановленням, оцінку доцільності визначених прав і повноважень окремих облікових записів та інших проактивних заходів безпеки, які забезпечують ефективне управління інформаційної безпеки. Тобто, фактично, без сформованої політики безпеки ці заходи взагалі можуть не застосовуватися, або застосовуватися невчасно та неефективно.

По-друге, передбачається, що у випадку належного інформування та навчання щодо чітко визначених правил та процедур безпеки, переважна більшість працівників буде їх дотримуватися та виконувати. Звичайна наявність політики інформаційної безпеки на підприємстві не впливає на поведінку суб'єктів інформаційних відносин. Однак, якщо основні правила політики безпеки належним чином інтегруються в контрактні угоди, а також доводяться до співробітників під час тренінгів з інформаційної безпеки, це вже здійснює значний вплив на дії суб'єктів. Підтвердженням цього можуть слугувати статистичні дані щорічних досліджень стійкості до кібернетичного впливу [23, 24] від департаменту науки, інновацій і технологій Уряду Великої Британії (англ. United Kingdom Government's Department of Science, Innovation and Technology). Так, згідно [23], якщо ще в 2013 році частка підприємств у яких політика інформаційної безпеки була недостатньо зрозумілою та висвітленою, зокрема в них фіксувалися порушення інформаційної безпеки, становила 93% опитаних, то вже в 2015 році [24], дана кількість зменшилася до 72%.

Зрештою, без політики та регламентованих процедур інформаційної безпеки не існувало б запланованого, задокументованого та керованого набору засобів

управління інформаційною безпекою. Водночас, дослідження ISC2 Global Workforce [25] виявило, що три з чотирьох найважливіших аспектів безпеки інформаційної інфраструктури пов’язані саме з політикою безпеки. На перше місце до сформованого списку, опитані респонденти визначили «підтримку політики безпеки керівництвом підприємства» (89%), третє місце зайняло «дотримання політики безпеки працівниками» (86%), а за ним – «навчання персоналу з питань інформаційної безпеки в контексті основних положень політики інформаційної безпеки» (83%).

Таким чином, зараз досить гостро постає питання щодо необхідності розробки та впровадження офіційної політики безпеки як основного елементу забезпечення інформаційної безпеки. Політика інформаційної безпеки служить керівним документом, який визначає роль інформаційної безпеки в підтримці загального бачення розвитку підприємства, узгоджуючись з його бізнес-цілями та відображаючи зобов’язання керівництва управляти підприємством в контрольований і безпечний спосіб. Саме тому, досить важливим аспектом реалізації політики безпеки є саме підтримка з боку менеджменту підприємства. Однак, коли підтримку отримано, ще одна проблема полягає в тому, щоб гарантувати, що положення політики безпеки справді здатні покращити безпеку [26].

Тут слід відзначити, що проводячи порівняння між організаційними та технічними засобами захисту, стає очевидним, що визначити ефективність політики інформаційної безпеки значно складніше. Оцінка ефективності застосування технічних продуктів захисту інформації порівняно простіша, оскільки ґрунтується на статистичних даних. Щодо політики безпеки, без чіткого слідування викладеним в ній положенням, вона залишається лише на папері та не несе реального впливу на стан забезпечення інформаційної безпеки на підприємстві. Зокрема це підтверджується в одному з нещодавніх опитуваннях від компанії SANS Institute [27], яке встановило, що близько в 15% опитуваних підприємствах працівники взагалі не нічого знають про діючу політику

інформаційної безпеки на підприємстві і відповідно не дотримуються її основних положень.

Як вже було раніше встановлено, структура політики безпеки, в фундаментальному її представленні, має включати правила та процедури, які повинні виконуватися співробітниками задля захисту інформаційних активів підприємства та конфіденційної інформації його клієнтів. Водночас, з точки зору підприємства, згідно з [28], персонал є найслабшою ланкою безпеки, а його функціональна взаємодія з інформаційними системами є найбільшим ризиком інформаційної безпеки. Зокрема зловмисник може ввести в оману будь-якого працівника підприємства із залученням базової психології та отримати несанкціонований доступ до інформаційних ресурсів. Яскравим прикладом такої атаки є фішинг ‘phishing’, який використовує нездатність користувачів відрізнити довірені джерела (до прикладу, веб-сайти або доменні імена підприємств до яких належить електронна пошта) від підроблених. Крім того, працівники можуть також самостійно здійснювати ненавмисні порушення безпеки допускаючи помилки через власну некомпетентність, неуважність, або навмисні через особисте невдоволення, образи та інші причини.

Огляд літератури дійсно підтверджує, що працівники які мають зловмисні наміри або не дотримуються політики інформаційної безпеки за штатних умов, є основною загрозою для інформаційних активів підприємства. При цьому, слід відзначити, що є також велика кількість випадків, коли працівники порушують положення політики інформаційної безпеки, вважаючи, що їхні рішення є більш вигідним для реалізації бізнес-цілей підприємства, ніж дотримання політики [29, 30]. У сучасному технологічному середовищі, нерідко клієнти звертаються в останню хвилину з проханнями внести доповнення або зробити певні модифікації продуктів, сервісів, які вони отримують від підприємства. Враховуючи обмежений проміжок часу, доступний для реагування на ці зміни, співробітники можуть піддатися спокусі тимчасово знехтувати положеннями прийнятої політики інформаційної безпеки, щоб задовольнити прохання клієнта.

Так, під час проведення одного з досліджень компанією Cisco [31], понад 50% співробітників підприємств, які брали участь в дослідженні, визнали, що вони свідомо порушували положення політики інформаційної безпеки. Основна ж причина, яку вказували опитувані, ґрунтувалася на припущенні, що ризики, пов'язані з їхніми порушеннями, були несуттєвими. Хоча, самі підприємства повідомляли, що все ж таки порушення політики безпеки призводять, в кращому випадку, до негативних наслідків, які вимагають значних часових затрат та грошей на відновлення, в гіршому – до несанкціонованого ознайомлення, або навіть привласнення конфіденційних даних.

В контексті цього, багато фахівців з інформаційної безпеки вважають, що успіх політики безпеки залежить від розуміння багатогранної природи людини так само, як і від технічних знань [32]. Саме тому, більшість досліджень щодо ефективного застосування політики інформаційної безпеки зосереджені на визначенні чинників, які впливають на поведінку працівників та їхню мотивацію дотримуватися положень політики інформаційної безпеки.

Зокрема в дослідженні [4] стверджується, що погляд працівників на інформаційну безпеку формується на основі переплетіння організаційних, технологічних та індивідуальних факторів. Тим часом автори іншого дослідження [5], припускають, що працівники неохоче ставитимуться до політики безпеки, якщо бачитимуть, що дотримання її положень будуть дещо обмежувати звичні для них дії при виконанні робочих обов'язків. Такі працівники можуть сприймати дотримання політики інформаційної безпеки як обтяжливе, таке, що заважає їх повсякденній роботі, забирає час і зусилля, або навіть перешкоджає їхньому вільному діловому спілкуванню [3, 6].

Коли співробітники стикаються з суперечливими вимогами щодо ефективності роботи та дотримання процедур інформаційної безпеки, зазвичай бізнес стає в пріоритеті [4]. Подібне судження зокрема проглядається в роботі [7], в якій автори стверджують, що працівники швидше за все, позитивно сприйматимуть політику інформаційної безпеки, якщо її основні положення будуть узгоджуватися з їхніми робочими цілями та сприяти ефективному

виконанню завдань. Крім того, якщо працівники вважатимуть, що їхні дії та поведінка позитивно впливатимуть або приноситимуть користь підприємству, їхнє ставлення до політики безпеки також буде позитивним [5].

Загалом історично так склалося, що дослідження зосереджувалися на оцінці впливу явищ на поведінкові наміри, а не на реальну поведінку. Зокрема, автори наступної роботи [8] підкреслюють існування невідповідності між поведінковими намірами та реальною поведінкою. Дана розбіжність виникає через мотивацію поступливості, яку попередні дослідження визначили як значний фактор, що впливає на поведінкові наміри. Поряд з цим, в останніх дослідженнях виділяють й інші фактори серед яких найбільш використовуваними є суб'єктивні норми, самоефективність, ставлення, передбачувані переваги, вразливість до загроз, серйозність загроз, ефективність реагування, вартість реагування та досвід. Водночас основоположною теорією у вивченні людської поведінки вважається «теорія запланованої поведінки», яка передбачає поведінкові наміри засновані на особистому відношенні (стан внутрішніх міркувань), соціальному тиску з боку інших (суб'єктивні норми) і почутті контролю [9]. Проте, поведінкові наміри активуються лише тоді, коли поведінка знаходиться у сфері вольового контролю та відповідає соціальним нормам. Саме намір користувача змушує дотримуватися або не дотримуватися положень політики інформаційної безпеки [10].

Сьогодні, дослідники використовують й інші різноманітні теорії, щоб дослідити людський фактор у сфері захисту інформації. Однією з найпоширеніших є «загальна теорія стримування», яка стверджує, що оцінка превентивної поведінки може пом'якшити загрози інформаційній безпеці та зменшити ризики. «Теорія мотивації до захисту» є ще однією широко використовуваною теорією, що ґрунтується на оцінці поведінки під впливом страху [11]. Згодом, дана теорія була розширена до більш загальної «теорії переконливої комунікації» [12], яка стверджує, що два когнітивні процеси можуть визначати індивідуальні наміри реалізації захисної поведінки, тобто визначити мотивацію до захисту.

Попри вплив людського фактору на ефективність застосування політики інформаційної безпеки, також впливають різного роду проблеми з якими підприємства стикаються безпосередньо в процесі розробки політики. Згідно [33], деякі з цих проблем включають рівень прийнятного ризику, процедурні відмінності між відділами через унікальні загрози, юридичні обмеження в зв'язку з географічним розташуванням підприємства, особисті точки зору, а також філософію та політичні аспекти різних культур. В дослідженні [34] автори дійшли висновку, що у випадку коли підприємство зазнає інтенсивних внутрішніх змін у своїй структурі, існує тенденція до впровадження суворих заходів безпеки, які обмежують доступ працівників до конфіденційних даних, фактично діючи як бар'єр, який може перешкоджати успішній діяльності підприємства. Така ситуація є проблемою для розвитку підприємства та часто призводить до розробки суперечливої політики інформаційної безпеки.

Водночас, одна з найкритичніших проблем, з якими стикаються підприємства, полягає в тому, що погляди більшості людей на реальність суперечать деяким положенням, визначеним політикою інформаційної безпеки [35]. До прикладу, співробітник може надати доступ до конфіденційних документів колезі, який не має необхідних облікових даних (зокрема прав та повноважень доступу) просто через роботу над спільним проєктом, або може поділитися паролем виключно на основі довіри чи особистої спорідненості з колегою. Крім того, викладені положення політики інформаційної безпеки не завжди є достатньо чіткими та зрозумілими, що є наслідком відсутності організаційності, послідовності та ясності тексту. В такому випадку, навіть ті працівники, які дійсно прагнуть опанувати та дотримуватися даних положень, не можуть зрозуміти, які дії дозволені, а які заборонені або обмежені.

Таким чином, розробка політик інформаційної безпеки залишається досить складним завданням. Ця складність виникає через різні точки зору спеціалістів з інформаційної безпеки та співробітників, що призводить до потенційних непорозумінь і нереалістичних припущень щодо методів, які використовуються для управління інформаційною безпекою. На жаль, спеціалісти з інформаційної

безпеки часто ігнорують важливість прислухатися до співробітників роблячи самі лише припущення щодо того, як працівники підприємства будуть сприймати положення політики інформаційної безпеки. В результаті, прийнята політика безпеки залишається неефективною через недостатню зрозумілість, ясність її основних положень, неточність або ігнорування з боку працівників.

Ще одним аспектом ефективності застосування політики безпеки в якому виникають певні труднощі є її впровадження. Підприємства досить часто стикаються з проблемами, пов’язаними з інтеграцією політики інформаційної безпеки в практичну площину. Водночас, політика безпека, яка не регулює та не надає вказівок щодо реалізації засобів забезпечення та управління інформаційною безпекою, ймовірно, була сформована для задоволення вимогам аудиторів, дотримання нормативних вимог або запиту клієнтів, однак не була повноцінно впроваджена самим підприємством. Така політика безпеки, як правило, є похідною від стандартних галузевих шаблонів і майже не впливає на ефективне впровадження та керування засобами забезпечення інформаційної безпеки.

Шаблони та приклади політики інформаційної безпеки і справді є цінним інструментом для ілюстрації форматування даного нормативного документа, його основних розділів, а також рівня деталізації опису елементів управління безпекою. Тому, розробники політики інформаційної безпеки можуть використовувати шаблони як робочі приклади, однак вони в жодному разі не повинні бути заміною повноцінному ретельному аналізу робочого середовища, можливостей підприємства та конкретних вимог безпеки. Тобто, навіть за використання шаблонів, підприємства мають обов’язково їх адаптувати у відповідності до своєї сфери діяльності та відповідних потреб.

У процесі розробки політики інформаційної безпеки необхідно ретельно розглянути цілі підприємства щодо забезпечення безпеки, профіль ризику, галузеві норми та внутрішні обставини. Якщо покладатися лише на шаблони без розуміння того, як вони пов’язані з конкретними умовами функціонування підприємства, це може призвести до впровадження неефективної політики безпеки, яка не відповідатиме належним чином реальним проблемам

інформаційної безпеки підприємства. Тому, процес розробки політики інформаційної безпеки вимагає ретельного аналізу, співпраці на різних рівнях та адаптації під умови функціонування відповідного підприємства з метою набуття відповідності конкретним викликам безпеки (тобто, документальної фіксації готовності протистояти таким викликам), з якими теоретично може стикатися дане підприємство.

Зрештою, навіть коли підприємства все ж створюють та вдало впроваджують політику інформаційної безпеки, яка відповідає їхнім конкретним потребам і поточному контексту (на час її створення), вони не завжди усвідомлюють важливість регулярного оновлення або повноцінного перегляду даної політики з метою підтримання актуальності та забезпечення її ефективності.

Досить часто, окрім незначних правок, діюча політика безпеки залишається незмінною протягом 3–5 (і навіть більше) років. Політика безпеки, яка залишається незмінною протягом тривалого періоду часу, особливо в технологічній галузі, що швидко розвивається, може ставати застарілою та не відповідати бізнес-цілям і технологічним процесам підприємства, нормативним вимогам і змінюваному ландшафту загроз. В зв’язку з цим, виділяють декілька ознак застарілості політики безпеки, серед яких дата документа, згадування застарілих технологій, як от кишеньковий комп’ютер замість смартфонів, посилання на застарілі версії нормативних документів та актів, а також призначення обов’язків для структурних підрозділів підприємства, які були перейменовані, об’єднані або ліквідовані. Застаріла політика інформаційної безпеки не лише не відповідає поточним потребам та цілям безпеки, але також може створити неузгодженість всередині підприємства, що призводить до плутанини серед співробітників і неналежного узгодження зі стратегічними бізнес-цілями.

Таким чином, можна виділити наступні типові недоліки притаманні сформованим політикам інформаційної безпеки сучасних підприємств:

– відсутність чіткої структури: у політиках інформаційної безпеки, які не мають чіткої організаційної структури, може виникати плутанина, через що працівникам важко орієнтуватися та знаходити потрібні їм розділи;

– неузгодженість: у випадку, коли політика безпеки є не послідовною у своїх формулюваннях, термінології або визначеннях, працівникам важко інтерпретувати її положення. Це зокрема може призвести до певних непорозумінь і неправильного тлумачення передбачуваних правил;

– складність в сприйнятті: політика безпеки викладена в надмірно технічному стилі, може ускладнити сприйняття працівниками, які не володіють всіма технічними термінами;

– двозначність: використання досить широких або неоднозначних формулювань в політиці інформаційної безпеки може призвести до різноманітних тлумачень, залишаючи користувачів невпевненими щодо того, які дії є дозволеними, а які заборонені;

– об’єм та деталізація: занадто велика та деталізована політика безпеки, може перевантажувати працівників та ускладнювати визначення найважливіших моментів. Дієва політика безпеки має досягати балансу між достатньою інформативністю та стислістю для легкого розуміння;

– наявність застарілої інформації: політика безпеки, яка не відображає поточного ландшафту загроз, організаційної структури, а також технологічних процесів підприємства, можуть стати неактуальними та неефективними.

1.3. Підходи, методи та сучасні практики побудови інформаційної безпеки підприємства

На сьогодні, регуляторні вимоги до збереження та захисту інформації стають все більш жорсткішими, в зв’язку з чим, підприємствам життєво важливо вірно інвестувати свій час і ресурси в розробку політики інформаційної безпеки. Це

дозволить відповідати високим стандартам безпеки, а також уникнути не лише кібератак, але й серйозних правових та репутаційних наслідків.

Повноцінна, комплексна політика безпеки зазвичай охоплює широкий спектр суб'єктів політики інформаційної безпеки та елементів управління, особливо враховуючи тенденцію до розширення самого підприємства в контексті його розвитку. В зв'язку з цим, існує декілька архітектурних рішень, які обирають підприємства при формуванні структури своєї політики інформаційної безпеки. Більшість літературних джерел виділяють саме три базові архітектури, серед яких:

– частинна політика передбачає формування низки документів, кожен з яких відповідає окремій технології чи системі використовуваній на підприємстві, що в сукупності відповідає загальній політиці безпеки;

– повна політика передбачає формування єдиного документа, який централізовано визначає, контролює та керує правилами безпеки для всіх використовуваних підприємством технології та систем. Є найрозповсюдженішою на сьогоднішній день;

– модульна політика, як і у разі повної політики безпеки, передбачає архітектуру, що централізовано контролює та керує всіма аспектами організаційного забезпечення безпеки, складається із загальних розділів з описами використовуваних технологій, відповідних систем та належного їх використання. Водночас структура даної архітектури відрізняється від попередньої тим, що включає модульні додатки, в яких містяться конкретні відомості про кожну технологію, висуваються конкретні зауваження, відмінності, обмеження та функціональні можливості, пов'язані з використанням технологій, які належним чином не відображені у базовому документі. Таким чином, дана структура зазвичай подається у вигляді трьох ієрархічних рівнів:

- стратегічний рівень – найвищий рівень, який забезпечує формування «загальної концепції інформаційної безпеки» визначаючи мету та завдання забезпечення інформаційної безпеки у корпоративній інформаційній системі, корпоративні вимоги та практичні принципи управління інформаційною

безпекою. Водночас, даний рівень служать основою для всіх наступних, більш специфічних політик нижчого рівня, які його розширюють регулюючи окремі питання захисту інформації;

- тактичний рівень – передбачає розробку виконавчої документації орієнтованої на конкретну проблематику, яка реалізується у вигляді деталізованих (зокрема посадових) інструкцій та рекомендацій щодо використання процесів, технологій чи систем підприємства. До прикладу, інструкції щодо використання інтернету та електронної пошти, реагування на інциденти, планування безперервності бізнесу, використання особистого обладнання в мережі підприємства та інше. Окремо слід акцентувати на тому, що саме даний рівень регламентує порядок поводження з інформацією, що підлягає захисту, основні правила поведінки співробітників та їх відповідальність за забезпечення безпеки інформації у будь-яких ситуаціях та на всіх етапах життєвого циклу корпоративної інформаційної системи підприємства. Також, до тактичного рівня можна віднести «профіль захисту», який містить технічні вимоги до програмно-апаратних засобів захисту інформації, включаючи вбудовані в загальносистемне програмне забезпечення на основі відповідних державних і галузевих стандартів;
- операційний рівень – передбачає розробку технічних стандартів, налаштувань, конфігурацій, які використовуються під час налаштування або обслуговування систем, наприклад, для налаштування та конфігурації мережевого брандмауера або системи контролю доступу, що охоплює налаштування низького рівня для керування логічним доступом до інформаційних систем підприємства. Потреба та обсяг таких документів визначається на основі перших двох рівнів.

Слід зазначити, що велика кількість дослідників вважають саме модульну структуру політики інформаційної безпеки найбільш ефективною на сьогоднішній день [36].

Водночас, враховуючи індивідуальність кожного підприємства, сформована політика безпеки повинна бути досить унікальною [37]. Однак, натомість, більшість використовує певний узагальнюючий, так званий шаблонний підхід до побудови політики інформаційної безпеки [38].

Оскільки розробка, вдосконалення, отримання схвалення проєкту з подальшим затвердженням та впровадженням повноцінної політики інформаційної безпеки вимагають значних зусиль, виникає спокуса скористатися шаблонами або придбати набір заздалегідь написаних політик. Хоча вони дійсно можуть бути хорошими прикладами для розробки власної політики безпеки, однак в жодному разі їх не слід сприймати як готовий продукт «з коробки». Вся цінність та ефективність таких попередньо сформованих «універсальних» політик ґрунтується на загальноприйнятих розумінням інформаційної безпеки. Для більшої ясності, нижче наведено причини, які підкреслюють, чому політика інформаційної безпеки має бути унікально створена та адаптована для кожного підприємства:

– ділова ціль: найочевиднішою причиною не використовувати в чистому вигляді «універсальну політику безпеки» є те, що кожен бізнес, кожне підприємство є унікальним. Враховуючи, що для досягнення бізнес-цілей підприємства, безпека, яка регламентується політикою інформаційної безпеки, має бути узгодженою з даними цілями, а також забезпечувати економічну ефективність і надавати підприємству конкурентну перевагу, відповідно і політика безпеки має бути адаптованою під конкретне функціональне середовище підприємства;

– організаційна структура: політика інформаційної безпеки повинна визначати та встановлювати чіткі обов’язки, підзвітність та нагляд за інформаційною безпекою у відповідності до структури підприємства;

– культурний фактор: в залежності від корпоративної культури, існують певні відмінності при сприйнятті різноманітних ресурсів забезпечення інформаційної безпеки [39]. Нездатність визнати та вирішити культурні відмінності може призвести до неефективного функціонування політики безпеки [40]. Зокрема, якщо на підприємстві цінується безпека, їй надається пріоритет, вона забезпечується та підтримується на визначеному рівні. Інакше, нею можуть знехтувати заради економії ресурсів [41];

– особливості інформаційних загроз за галузями: загалом політика інформаційної безпеки будь-якого підприємства вирішує (або, принаймні, повинна) подібні проблеми, однак потужність та інтенсивність контролю, суворість покарань і рівень нагляду повинні узгоджуватися з ландшафтом загроз конкретного підприємства, галузі;

– законодавчі особливості регіону: досить часто формування політики інформаційної безпеки регулюється зовнішніми факторами, насамперед законодавством. Країни мають власні національні принципи та законодавчі норми щодо регулювання інформаційної безпеки, яких повинні дотримуватися підприємства при формуванні своєї політики безпеки. У країнах Європейського Союзу, наприклад, інформаційна безпека регулюється загальноєвропейською директивою «Загальний регламент про захист даних ‘General Data Protection Regulation’» (GDPR) [42], яка передбачає створення політики інформаційної безпеки та регламентує суворість її основних аспектів. В Україні, аналогом даної директиви можна вважати низку законів, зокрема Закон України «Про захист персональних даних» (№2297-VI від 27.10.2022 р.) [43], Закон України «Про основні засади забезпечення кібербезпеки України» (№2163-VIII від 17.08.2022 р.) [44] та Закон України «Про захист інформації в ІКС» (№80/94-ВР від 01.07.2022 р.) [45].

Окрім шаблонного підходу до побудови політики інформаційної безпеки підприємства, досить поширеними є ризик-орієнтований, ітеративний, низхідний та висхідний підходи.

Ризик-орієнтований підхід полягає у визначенні, аналізі та керуванні ризиками, пов’язаними з безпекою інформації. Основною метою цього підходу є забезпечення ефективного та пропорційного захисту інформації, зосереджуючись на найважливіших та найбільш небезпечних, вразливих ділянках. Цей метод дозволяє визначити пріоритети та конкретні заходи безпеки, які потрібно впровадити. Даний підхід передбачає:

– ідентифікацію всіх інформаційних активів підприємства (зокрема, інформація, додатки, обладнання тощо);

– виявлення потенційних загроз, що можуть призвести до порушення конфіденційності, цілісності та доступності інформації;

– оцінку інформаційних ризиків, в ході якої, для кожної ідентифікованої загрози визначаються ймовірність виникнення, можливі наслідки та рівень впливу на бізнес-процеси підприємства;

– визначення конкретних заходів забезпечення інформаційної безпеки на основі проведеної оцінки інформаційних ризиків з метою зменшення ймовірності виникнення загроз та мінімізації їх наслідків;

– оформлення офіційної політики безпеки підприємства.

Ітеративний підхід передбачає формування політики безпеки підприємства на основі послідовних ітерацій, з покроковим вдосконаленням. Розпочинаючи з базової політики, яка в подальшому вдосконалюється та доповнюється з часом.

При низхідному підході політика безпеки розробляється та впроваджується з подачі вищого рівня керівництва. Побудова політики безпеки може починатися з розробки стратегічних цілей та принципів безпеки, які потім деталізуються та втілюються у конкретні правила та процедури. Даний підхід забезпечує відповідність політики безпеки стратегії підприємства.

При висхідному підході, побудова політика безпеки розпочинається рядовими співробітниками та технічними експертами на основі свого розуміння конкретних ризиків та потреб підприємства. Перевагою такого підходу є більша конкретизація та адаптація, звісно за умови попереднього погодження та підтримки керівництва.

Однак, одним із найдоцільніших для використання підходів до побудови політики інформаційної безпеки підприємства вважається підхід, що ґрунтується на використанні національних та міжнародних стандартів.

Варто відмітити, що на сьогодні в різних країнах були розроблені різноманітні набори стандартів, які в певному сенсі можна вважати методологіями спрямованими на забезпечення інформаційної безпеки на підприємствах. Серед цих стандартів, в контексті формування політики інформаційної безпеки, важливе місце займають такі міжнародні стандарти, як

ISO/IEC 27001, ISO/IEC 27002 [46, 47], національні: НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 (Україна) [48, 49], BSI Standards (Німеччина) [50] та NIST Special Publication серії 800 (США) [51–53], а також додатково можна виділити декілька фреймворків, що мають подібні цілі та призначення: COBIT [54], ITIL, SAC або COSO.

Комбінування різних підходів може бути досить ефективним, забезпечуючи баланс між стратегічністю та конкретністю заходів безпеки. До прикладу, в НД ТЗІ 1.4-001 [49] вже передбачено, що термін «політика безпеки» можна використовувати в контексті автоматизованих систем[1], їх окремих компонентів, а також послуг (сервісів) забезпечення безпеки, що реалізуються системою та інших аспектів. Водночас вказується, що така політика безпека має бути частиною загальної політики інформаційної безпеки підприємства та успадковувати основні її принципи. Зокрема, щонайменше, повинні бути сформовані політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації як окремі складові загальної політики. Таким чином, даний нормативний документ заздалегідь визначає можливість формування політики безпеки у вигляді модульної архітектури із залученням різних підходів.

Водночас, на основі проведеного аналізу основних типів архітектури політики безпеки та підходів до її побудови, можна окреслити узагальнений процес формування політики інформаційної безпеки підприємства, який складається з наступних етапів:

1. Дослідження підприємства як об’єкта захисту для якого формується політика безпеки. Даний етап передбачає детальне вивчення об’єкта шляхом проведення обстеження середовищ функціонування ІКС підприємства, зокрема обчислювальної системи, фізичного середовища, середовища користувачів, оброблюваної інформації і технології її обробки. В ході такого обстеження визначаються ключові інформаційні активи, ресурси ІКС, що потребують захисту. Крім того, мають бути визначені основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового

[1] Згідно з ЗУ «Про захист інформації в ІКС» [45]: інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

режиму та режиму доступу, компонентів обчислювальної системи та персоналу, на основі чого формуються моделі загроз і потенційного порушника.

2. Аналіз ризиків інформаційної безпеки. Етап аналізу ризиків інформаційної безпеки передбачає вивчення сформованих на попередньому етапі моделей загроз і порушника, визначення можливих наслідків від реалізації потенційних загроз (тобто визначення рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації:

– визначаються компоненти та ресурси (загалом об’єкти захисту), які можуть бути об’єктами атаки або самі є потенційними джерелами порушення інформаційної безпеки;

– ідентифікуються загрози з об’єктами захисту шляхом встановлення відповідність моделі загроз і об’єктів захисту здебільшого у вигляді матриці, кожен елемент якої описує можливий вплив загрози на відповідний компонент або ресурс;

– оцінюється гранично припустимі та реальні ризики реалізації (ймовірність їх настання) кожної окремої загрози в продовж певного проміжку часу. Дану оцінку рекомендується проводити виходячи з припущення, що кожна подія має найгірший закон розподілу, з точки зору власника інформації, що потребує захисту, а також за умови відсутності заходів захисту інформації. Водночас, за результатами оцінки повинні бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків [49];

– кількісно або якісно оцінюються збитки, що можуть бути нанесені підприємству внаслідок реалізації загроз.

3. Визначення вимог до заходів, методів та засобів захисту.

4. Розробка концепції інформаційної безпеки.

Розробка концепції інформаційної безпеки здійснюється на основі отриманих результатів на попередніх етапах. Зокрема формуються загальні положення безпеки, які стосуються або впливають на технологію обробки інформації на підприємстві; мета і пріоритети, яких необхідно дотримуватись на підприємстві під час забезпечення інформаційної безпеки; загальні напрями діяльності,

необхідні для досягнення цієї мети, а також основні аспекти діяльності у галузі інформаційної безпеки, які повинні вирішуватися на рівні підприємства в цілому.

1. Вибір основних рішень із забезпечення інформаційної безпеки.

Передбачається, що забезпечення інформаційної безпеки на підприємстві повинне бути комплексним та розглядати три рівні засобів захисту:

– правовий рівень забезпечення інформаційної безпеки, який повинен включати розроблені підходи щодо:

- системи нормативно-правового регулювання заходів з захисту інформації на підприємстві;
- підтримки керівництвом підприємства заходів з забезпечення інформаційної безпеки, виконання правових та договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, розподілу обов'язків співробітників системи захисту інформації;
- процедур доведення до працівників основних положень політики інформаційної безпеки, їхнього навчання та підвищення кваліфікації з питань безпеки інформації;
- системи контролю за вчасністю, ефективністю та повнотою реалізації рішень з захисту інформації на підприємстві, дотриманням працівниками основних положень політики безпеки.

– організаційний рівень забезпечення інформаційної безпеки, який повинен включати розроблені підходи щодо:

- впровадження та застосування режимних заходів на окремих об'єктах підприємства;
- забезпечення фізичного захисту обладнання ІКС, носіїв інформації та інших ресурсів;
- виконання робіт з модернізації ІКС в цілому або її окремих компонентів;
- регламентації доступу сторонніх осіб до ресурсів ІКС підприємства;
- регламентації доступу співробітників різних категорій до ресурсів ІКС підприємства;

- здійснення заходів профілактичного характеру, до прикладу, попередження випадкових порушень політики безпеки, запобігання зараження комп'ютерними вірусами тощо;
- реалізації основних положень політики інформаційної безпеки;
- визначення відповідальності персоналу за виконання положень політики безпеки.

Окремо слід зазначити, що серед найсуттєвіших компонентів політики безпеки також виділяють правила розмежування доступу, які регламентують доступ користувачів та процесів до ресурсів ІКС підприємства. Правила розмежування доступу функціонують як абстрактний механізм, що виступає посередником у взаємодії об'єктів ІКС.

– технічний рівень забезпечення інформаційної безпеки, який повинен включати розроблені підходи щодо застосування технічних та програмно-технічних засобів захисту інформації, зокрема:

- планування, експлуатація та супровід інженерно-технічного обладнання, включаючи системи блокування технічних каналів витоку інформації, виокремлених приміщень, в яких розташовані компоненти ІКС підприємства;
- здійснення реєстрації та авторизації санкціонованих користувачів ІКС;
- керування доступом до інформаційних ресурсів та механізмів забезпечення безпеки, враховуючи розподіл ролей між користувачами і адміністраторами;
- виявлення та реєстрація подій, що можуть становити загрозу, з метою забезпечення щоденного контролю та можливості подальшого проведення службового розслідування;
- забезпечення та контроль цілісності критичних даних на всіх етапах їхньої обробки в ІКС;
- забезпечення конфіденційності інформації, включаючи використання криптографічних методів;
- резервне копіювання, архівування важливих даних та подальше їх супроводження;

- відновлення функціонування ІКС після відмов і збоїв, особливо для систем з підвищеними вимогами до забезпечення доступності інформації;
- забезпечення захисту програмного забезпечення, окремих компонентів та ІКС в цілому від несанкціонованих змін;
- забезпечення належного функціонування інструментів контролю, включаючи засоби виявлення технічних каналів витоку інформації.

2. Організація виконання відновлювальних робіт і забезпечення неперервного функціонування бізнес-процесів підприємства.

На даному етапі мають бути розроблені стратегії планування та порядку виконання відновлювальних робіт після виникнення надзвичайних ситуацій (збоїв, аварій або інших непередбачуваних обставин) з метою забезпечення неперервності функціонування бізнес-процесів підприємства. Водночас, процес планування даних заходів повинен включати розгляд наступних аспектів:

– виявлення критичних з точки зору безпеки компонентів ІКС підприємства, що забезпечують належне виконання бізнес-процесів;

– визначення можливого негативного впливу надзвичайних ситуацій на забезпечення належного виконання бізнес-процесів;

– визначення і узгодження обов’язків персоналу та користувачів, а також встановлення послідовності їх дій під час надзвичайних ситуацій;

– підготовка персоналу та користувачів до виконання дій в умовах надзвичайних ситуацій.

Безпосередньо вже сформований план проведення відновлювальних робіт і забезпечення неперервного функціонування бізнес-процесів підприємства повинен включати:

– опис типових сценаріїв надзвичайних ситуацій, які можуть виникати через вразливі місця окремих компонентів ІКС підприємства, що забезпечують належне виконання бізнес-процесів або, які вже траплялися раніше;

– опис процедур реагування на надзвичайні ситуації, які варто застосувати негайно після виникнення інциденту, який може порушити політику безпеки;

– опис процедур тимчасового переходу ІКС (або окремих її компонентів) підприємства у режим аварійного функціонування;

– опис процедур відновлення нормального режиму функціонування ІКС (або окремих її компонентів) підприємства, яка піддалася впливу надзвичайних ситуацій;

– процедуру тестування плану, включаючи навчання персоналу на симуляціях надзвичайних ситуацій.

3. Документальне оформлення політики інформаційної безпеки підприємства.

Зрештою, результати проведених робіт на окремих етапах розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена загальна політика інформаційної безпеки підприємства. Водночас, така політика має бути обов’язково затверджена керівником або заступником керівника підприємства.

При цьому спроба узагальнити список компонентів, які має включати політика інформаційної безпеки, ускладняється залежністю її складових від характеру підприємства, його розміру та цілей. Зокрема в [55] стверджувалося, що політика безпеки повинна включати загальні формулювання цілей, завдань, переконань і обов’язків, які часто супроводжуються загальними процедурами їх досягнення. В доповнення до цього, в роботі [56] йдеться про те, що політика безпеки повинна також окреслювати індивідуальну відповідальність, визначити легітимних користувачів системи, надати персоналу засоби для звітування про інциденти, визначити наслідки для порушень політики безпеки та створити механізм для подальшого її оновлення.

Попри вищезазначене, враховуючи декілька стандартів з управління інформаційною безпекою [46–49], все ж можливо виділити певний набір компонентів, які повинна включати загальна політика інформаційної безпеки, але в жодному разі не обмежуватися ними:

– загальну стратегію, цілі, завдання, обсяг, напрями розвитку та підходи до забезпечення інформаційної безпеки;

– декларацію намірів керівництва щодо підтримки цілей та принципів інформаційної безпеки узгоджених з цілями та бізнес-стратегією підприємства;

– визначення об’єктів захисту, виявлення загроз, аналіз та оцінка ймовірності їх реалізації;

– визначення ролей, відповідальних осіб, загальних та індивідуальних обов’язків щодо забезпечення інформаційної безпеки;

– встановлення відповідальності за забезпечення безпеки інформації;

– визначення процедур і вимог щодо доступу до інформації, управління інформацією та захисту інформації від несанкціонованого доступу;

– роз’яснення процедур виявлення та повідомлення про порушення інформаційної безпеки;

– визначення програми навчання працівників щодо ключових питань забезпечення інформаційної безпеки;

– перехресні посилання на інші документи, що доповнюють та деталізують сформовану політику інформаційної безпеки (процедури безпеки, керівництва, посадові інструкції, посилання на зовнішні нормативні документи, стандарти та ін.);

– загальні елементи (автори, дата затвердження та прийняття політики інформаційної безпеки, а також дати її перегляду).

Разом з тим, розробка ефективної політики і забезпечення інформаційної безпеки, як вже зазначалося раніше, є також важливою та невід’ємною частиною корпоративного управління. В контексті чого, слід зокрема відзначити, що захист інформації – це не завжди питання лише технічного характеру, але й бізнесу. Саме тому, щоб зробити інформаційну безпеку частиною корпоративного управління, рекомендується використовувати такий набір практик, як COBIT [55] від Асоціації аудиту і контролю інформаційних систем (Information Systems Audit and Control Association, ISACA).

COBIT (від Control Objectives for Information and Related Technologies) – це фреймворк, який надає вказівки та найкращі практики для ефективного управління інформаційними технологіями, включаючи в себе елементи

інформаційної безпеки. Він надає керівництво з забезпечення ефективного управління інформаційних технологій, визначення контрольованих об’єктивів та практичних заходів для забезпечення їхньої безпеки. Тобто, COBIT допомагає підприємствам досягати своїх бізнес-цілей покращити загальну продуктивність, адаптуючи стратегії інформаційних технологій до бізнес-цілей та забезпечуючи належне управління і контроль процесів інформаційних технологій. Він акцентує увагу на важливості управління ризиками, дотримання відповідності та постійному вдосконалення в інформаційних технологій та інформаційній безпеці.

Крім того, з метою сприяння універсалізації технологічних аспектів розробки, впровадження та забезпечення належного дотримання політики інформаційної безпеки, деякі технологічні лідери ринку інформаційних технологій, такі як IBM, Cisco Systems, Microsoft та інші, регулярно публікують так звані кращі практики. Вони по суті є сукупністю рекомендацій, методів та стратегій, які визнані галузевими експертами як оптимальні та ефективні для створення і реалізації політики інформаційної безпеки на підприємстві.

До прикладу, компанія Cisco, яка спеціалізується на розробці мережевих технологій та кібербезпеці, на основі багаторічного досвіду, сформувала власний концептуальний підхід до побудови політики інформаційної безпеки, який базується на кількох ключових принципах:

– стратегічне планування, в ході якого визначаються основні цілі та пріоритети в галузі інформаційної безпеки, охоплюючи аналіз потреб, ризиків та визначення напрямків розвитку;

– ризик-орієнтований підхід, який передбачає фокусування на оцінці ризиків та визначенні слабких, вразливих областей, які потребують найбільших зусиль для забезпечення безпеки;

– забезпечення відповідності вимогам законодавства та нормативних документів, які регулюють сферу кібербезпеки;

– інтеграція з передовими технологіями та інструментами для забезпечення та підтримки інформаційної безпеки на належному рівні;

– підвищення обізнаності та навчання працівників з питань кібербезпеки;

– постійне вдосконалення, яке наголошує на тому, що політика повинна бути гнучкою і постійно оновлюватись відповідно до змін в технологіях та ландшафті загроз;

– комунікація між всіма рівнями підприємства та співпраця з партнерами задля забезпечення цілісності та ефективності політики безпеки;

– впровадження принципу захисту «від периметра до кінцевого пристрою», який підкреслює важливість захисту всієї екосистеми, включаючи периметр, мережеві та кінцеві пристрої.

Таким чином, даний підхід, та аналогічні йому, зокрема від інституту SANS, спрямовані на побудову глибокої, комплексної, адаптивної з допущенням винятків з правил на основі унікальних обставин та врахуванням ризиків, політики інформаційної безпеки.

Звісно ж практичність будь-якої політики безпеки насамперед залежить від можливості її втілення та виконання. Погано або неналежним чином сформована політика безпеки призводить до обмеження практичності та зручності її використання, та загалом може негативно вплинути на готовність співробітників добровільно дотримуватись визначених в ній загальних принципів і правил. Крім того, співробітники з великою долею ймовірності можуть невірно зрозуміти зазначених положень або будуть намагатися обходити її вимоги, що в свою чергу призводить до порушення політики. Як результат, сама політика інформаційної безпеки може стати внутрішньою загрозою для підприємства [57].

Саме тому, спосіб написання політики є ще одним домінуючим фактором при побудові ефективної політики безпеки. Зокрема в роботі [58] стверджується, що формулювання політики має створювати документ(и), які є зрозумілими, простими та орієнтованими на цільову аудиторію, і що вони повинні включати визначення технічних термінів, які в них використовуються, щоб мінімізувати непослідовність у їх тлумаченні та запобігти недотриманню користувачами основних положень, вимог політики через нерозуміння сформованих документів. Водночас ключовий момент відводиться саме формулюванню ролей та обов’язків кінцевих користувачів, оскільки ця частина політики безпеки точно говорить про

те, що очікується від користувачів з точки зору інформаційної безпеки. Ролі та обов'язки повинні охоплювати всі аспекти інформаційної безпеки, а також індивідуальні обов'язки всіх сторін, які використовують інформаційні ресурси підприємства.

Водночас, беручи до уваги проведений в попередньому підрозділі аналіз досліджень в сфері визначення ефективності політики інформаційної безпеки на основі дотримання її основних положень, слід відзначити, що управління інформаційною безпекою повинне розглядати працівників з досить авторитарної точки зору, як внутрішнього ворога.

Зокрема, чимала кількість дослідників також виступають за побудову політики інформаційної безпеки, яка ґрунтується на принципі найменших привілеїв, згідно з яким кожному користувачеві надається мінімальний обсяг прав та повноважень доступу (з можливим обмеженням в часі), необхідний для виконання його завдань задля запобігання неналежне використання даних, обладнання та інформаційних процесів, тим самим зменшуючи ризики, які представляють працівники [59].

Саме ці два останніх судження були покладені в основу відносно нової концепції zero-trust для забезпечення інформаційної безпеки. Дана концепція зміщує акцент інформаційної безпеки від захисту статичних мережевих периметрів до зосередження уваги на користувачах, активах та ресурсах, стверджуючи, що нічого не може бути автоматично довіреним, навіть якщо вони находяться в межах периметру підприємства.

1.3.1. Основні аспекти застосування концепції zero-trust при формуванні політики інформаційної безпеки

Цифровий розвиток та інші фактори, як то пандемія COVID-19, змінили сучасний організаційний ландшафт і те, як підприємства ведуть сьогодні свій бізнес. Дана трансформація призвела до збільшення кількості співробітників, які

працюють поза традиційних офісних умов, віддалено. Крім того, зросла тенденція щодо використання BYOD замість або в поєднанні з роботою з корпоративними пристроями. Одночасно спостерігався сплеск впровадження технологій хмарних обчислень. Велика кількість підприємств або повністю переходять на хмарне середовище, або використовують гібридні середовища, які поєднують як хмарні, так локальні служби [60]. Як наслідок, більша кількість пристроїв співробітників і сервісів підприємства стають відкритими з'єднуючись між собою через відкриті мережі, що призводить до нових вразливостей та можливостей реалізації кібернетичних атак.

Стандартні політики інформаційної безпеки підприємства здебільшого орієнтовані на захисту від зовнішніх загроз будуючись на основі припущення, що дії, які відбуваються всередині периметра корпоративної мережі, є безпечними, всі решта – підозрілими. Такі політики втілюють підхід до організації інформаційної безпеки на основі периметра (або, такий підхід ще називають мережною безпекою) [61], тобто мережа умовно поділяється на «внутрішню довірену» та «зовнішню недовірену» мережу. Ресурси підприємства, сервіси, інформаційні системи, дані тощо знаходяться в межах саме «внутрішньої довіреної – надійної» мережі. Водночас, для захисту та ізоляції «внутрішньої мережі» від зовнішніх загроз, шляхом виявлення, аналізу та блокування несанкціонованого доступу ззовні, по периметру розміщуються такі системи захисту, як брандмауери, VPN, засоби контролю доступу до мережі, брандмауери веб-застосунків та інші. І у випадку, коли користувач отримує доступ до внутрішньої мережі, йому відповідно надається доступ до більшості ресурсів підприємства (звісно в залежності від визначених політикою безпеки його прав та повноважень). Тобто, даний підхід ґрунтується на певній довірі та донедавна був досить ефективним. Однак сьогодні впевненість у тому, що користувачі або пристрої насправді є тими, за кого себе видають, або що їхні наміри доброзичливі, стала вразливою для підприємства. Адже скомпрометувавши обліковий запис користувача або в інший спосіб отримавши доступ до системи в межах периметра, зловмисник з легкістю може рухатися далі та розвивати таку атаку.

Хоча, слід відзначити, що вперше, як відповідь на зловживання довірою, філософію «ніколи не довіряти» було запропоновано ще в 1994 році Полом Маршем, який в своєму дисертаційному дослідженні [62] розглядав вразливості засновані саме на довірі, враховуючи як внутрішні так і зовнішні фактори. Однак, як концептуальний підхід до забезпечення інформаційної безпеки, дану філософію було розвинено з метою усунення всіх форм внутрішньої довіри лише в 2010 році, колишнім аналітиком Forrester Research Джоном Кіндервагом [63].

Завдяки використанню таких технологій, як автентифікація, керування доступом, шифрування, а також різноманітних технологій мережевої безпеки, підхід zero-trust встановлює захищені мікропериметри, при цьому регламентація доступу до ресурсів здійснюється політиками доступу, що ґрунтуються на принципі «ніколи не довіряй, завжди перевіряй». Будь-який запит, в незалежності від суб'єкта (як працівника, так і пристрою), який його ініціює або місцезнаходження даного суб'єкта, на доступ до ресурсу та можливість взаємодії з ним в сформованому середовищі zero-trust підлягає повній автентифікації, авторизації та шифруванню.

Незважаючи на те, що zero-trust – це все ще концепція, однак основи її структури вже визначені Національним інститутом стандартів і технологій 'National Institute of Standards and Technology' (NIST) та аналітичними компаніями, такими як Gartner, Forrester, IDC та ESG. Зокрема в SP 800-207: Zero Trust Architecture [64], NIST визначає основні аспекти реалізації принципів zero-trust[2] та пропонує сценарії розгортання архітектури zero-trust[3] з відповідними прикладами. Дана спеціальна публікація зосереджена на проблематиці запобігання несанкціонованому доступу до всіх корпоративних ресурсів, включаючи не лише дані (тобто інформаційні ресурси), але й такі елементи, як

[2] У відповідності до NIST SP 800-207 [60]: нульова довіра (zero-trust) – це парадигма кібербезпеки, яка орієнтована на захист ресурсів і виходить із того, що довіра ніколи не надається беззастережно, вона має постійно оцінюватись (перевірятися).

[3] У відповідності до NIST SP 800-207 [60]: архітектура нульової довіри (zero-trust architecture) – це комплексний наскрізний підхід до забезпечення безпеки корпоративних ресурсів підприємства (при цьому, до ресурсів відносяться як дані, так і обчислювальні сервіси та їх апаратна складова), який охоплює ідентифікацію суб'єктів (осіб та неособових об'єктів, зокрема процесів, сервісів, служб та ін.), облікові дані, керування доступом (зокрема політики доступу), робочі процеси, операції, кінцеві точки, середовища їх розміщення та з'єднувальну інфраструктуру.

принтери, обчислювальні ресурси та IoT, у поєднанні з максимально деталізованим забезпеченням контролю доступу [65].

Так, абстрактна модель надання доступу (див. рис. 1.3) сформована згідно архітектури zero-trust демонструє, що доступ до корпоративного ресурсу надається через умовний «контрольно-пропускний пункт», який складається з точки прийняття рішення ‘Policy Decision Point’ (PDP)[4] щодо доступу на основі політики безпеки та точки застосування політики ‘Policy Enforcement Point’ (PEP)[5], що відповідає за звернення до PDP та правильну обробку відповіді [66].

Функціональність системи керування доступом повинна охоплювати як перевірку автентичності суб’єкта, так і підтвердження легітимності самого запиту. Тобто, це означає, що концепція zero-trust застосовується до двох основних областей забезпечення інформаційної безпеки: автентифікації та авторизації.

В контексті автентифікації, це стосується рівня впевненості в достовірності суб’єкта для конкретного запиту, що передбачає відповідну оцінку достовірності суб’єкта на основі різних факторів, таких як ім’я користувача/пароль, біометричні дані, дані багатофакторної автентифікації або інші автентифікаційні дані неособових об’єктів (до прикладу, електронні криптографічні ключі).

В контексті авторизації, це передбачає визначення того, чи суб’єкту дозволено доступ до запитуваного корпоративного ресурсу з огляду на визначений рівень впевненості в достовірності суб’єкта. Система оцінює, чи відповідає рівень доступу суб’єкта його «особистості» та вимогам безпеки ресурсу. Крім того, система повинна враховувати стан безпеки самого пристрою, який використовується для запиту, та інші контекстуальні фактори, які можуть змінювати рівень достовірності як-от час, місцезнаходження та загальний рівень безпеки суб’єкта.

[4] PDP – точка, яка аналізує та оцінює запити на доступ, враховуючи закладені авторизаційні політики, перед прийняттям рішення щодо надання доступу.

[5] PEP – точка, яка перехоплюючи запит доступу суб’єкта до корпоративного ресурсу ініціює звернення до PDP з метою отримання рішення (дозволу або відмови) щодо доступу та відповідним чином реагує на нього.

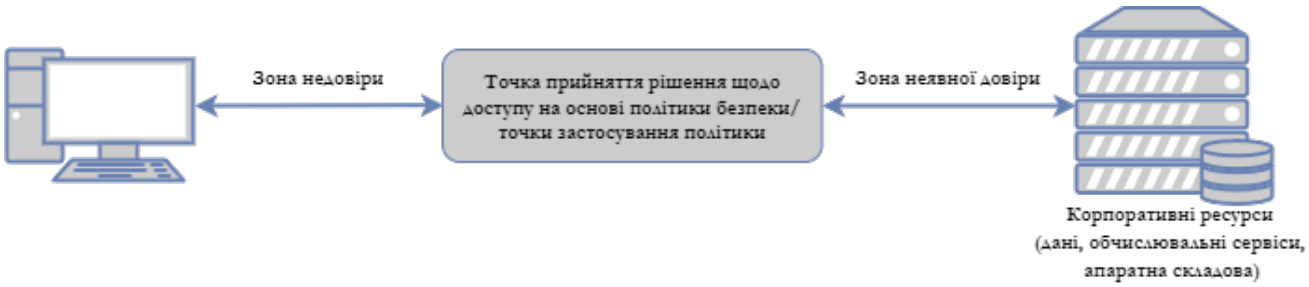

Рис. 1.3. Модель надання доступу згідно архітектури zero-trust

Водночас, ключовим моментом нульової довіри є те, що така система повинна забезпечувати послідовне й точне застосування сформованих авторизаційних політик для кожного окремого запиту на доступ до корпоративного ресурсу, а не покладатися на припущення, що попередня автентифікація гарантує постійну надійність. Крім того, «зона неявної довіри», яку NIST визначає як область, де всім об'єктам довіряють, принаймні, до рівня останнього шлюзу PDP/PEP [64], має бути якомога меншою задля того, щоб PDP/PEP був максимально конкретним. Такі зони і являють собою мікропериметри безпеки, які вже згадувалися раніше.

1.3.2. Принципи концептуального підходу zero-trust

Загалом концептуальний підхід zero-trust ґрунтується на наступних принципах:

1. Всі типи джерел даних, безпосередньо самі дані, а також обчислювальні сервіси вважаються корпоративними ресурсами. Тобто, будь-який пристрій або система, яка генерує, обробляє або зберігає дані (це можуть бути сервери, робочі станції, пристрої IoT, датчики та інших джерел, що генерують дані), сервіси, які забезпечують обчислення, зберігання або інші функції в мережі (зокрема хмарні обчислювальні сервіси, віртуальні машини, контейнери та ін.), вважаються ресурсами. Крім того, підприємства самостійно можуть визначити BYOD як ресурси за умови, що вони мають доступ до корпоративних ресурсів. Це означає,

що навіть пристрої, які не належать підприємству, але використовуються в мережі, можуть вважатися ресурсами в контексті концепції нульової довіри.

2. Довіра до суб'єкта, в жодному разі, не повинна ґрунтуватися на основі присутності пристрою, через який здійснюється взаємодія, в межах інфраструктури корпоративної мережі. Тобто вся взаємодія суб'єктів має бути захищеною в незалежності від їхнього розташування в мережі. Запити на доступ, що надходять від суб'єктів у межах корпоративної мережевої інфраструктури, навіть у межах застарілого мережевого периметра (який за стандартної моделі безпеки може вважатися цілком безпечним – довіреним), мають відповідати ідентичним стандартам безпеки, що й доступ і зв'язок із будь-якої зовнішньої мережі, що не належить підприємству. Зокрема передбачається обов'язкова автентифікація всіх з'єднань і шифрування всього трафіку.

3. Доступ до окремих корпоративних ресурсів надається після оцінки достовірності запитуючої сторони і лише в рамках одного сеансу. Водночас, доступ має бути надано з якомога найменшими привілеями, достатніми для виконання завдання.

4. Доступ до корпоративних ресурсів визначається динамічною політикою, яка враховує такі фактори, як спостережуваний стан ідентичності клієнта, програми/сервісу чи будь-якого іншого активу (апаратного забезпечення), що здійснює запит, а також інші поведінкові атрибути або атрибути середовища. Зокрема стан ідентичності клієнта може визначатися обліковими записами користувача (або ідентифікатором служби), будь-якими пов'язаними атрибутами, а також шаблонами поведінки, які дозволяють виявити підозрілу активність. Стан ідентичності активу може визначатися такими характеристиками пристроїв, як встановлені версії програмного забезпечення, розташування в мережі, час/дата запиту, поведінка, що спостерігалася раніше, і встановлені облікові дані. Водночас, поведінкові атрибути можуть охоплювати ряд автоматизованих аналізів предметів і пристроїв, а також відхилення від спостережуваних шаблонів їх використання. А атрибути середовища можуть враховувати такі елементи, як

мережеве розташування запитуючої сторони, час, повідомлення про активні атаки та ін.

5. Забезпечення максимально можливого безпечного стану, завжди враховуючи можливість витоку даних. Передбачається постійний аналіз наскрізного трафіку, забезпечуючи максимальну видимість активності суб'єктів, відстежування і визначення (тобто оцінювати) цілісності та стану безпеки всіх корпоративних активів або активів пов'язаних з підприємством, не довіряючи жодному з них. Що, зокрема, може бути реалізоване шляхом налаштування СУІБ та подіями, системи безперервної діагностики та пом'якшення або подібного механізму для постійного моніторингу стану пристроїв і програм, а також для застосування необхідних патчів або виправлень за потреби.

6. Всі ресурси автентифікації та авторизації є динамічними та суворо контрольованими. Дані процеси включають безперервні цикли запитів на доступ, сканування та оцінку потенційних загроз, коригування заходів безпеки та послідовну переоцінку рівня довіри до поточних взаємодій. Зокрема передбачається необхідність впровадження надійної системи керування ідентифікацією, обліковими даними та доступом, включаючи багатофакторну автентифікацію, а також системи управління активами.

7. Дослідження поточного стану активів, мережевої інфраструктури та взаємозв'язків задля підвищення загальної безпеки. Зокрема передбачається збір та обробка інформації про стан безпеки активів, мережевий трафік та запити на доступ, а результати повинні використовуються для покращення створення та застосування політики безпеки.

Виходячи з наведених принципів, слід зазначити, що сама архітектура zero-trust може формуватися з різних компонентів, які можуть бути як локальними, так і хмарними сервісами. При цьому більшість експертів наголошують, що універсальної архітектури zero-trust не існує. Кожне підприємство особливе, отже кожна реалізація принципів zero-trust теж має бути особливою. Більш того, слід відзначити, що унікально сформована для конкретного підприємства архітектура zero-trust, з часом, по мірі того, як будуть змінюватися IT- та бізнес-потреби, має

постійно проходити переоцінювання, модернізацію для того, щоб підтримувати та максимально посилювати ефект від застосування концептуального підходу zero-trust.

Однак, NIST пропонує базову абстрактну модель концептуального ядра архітектури zero-trust (див. рис. 1.4), яку можна брати за основу для подальшої адаптації під конкретні умови функціонування підприємства.

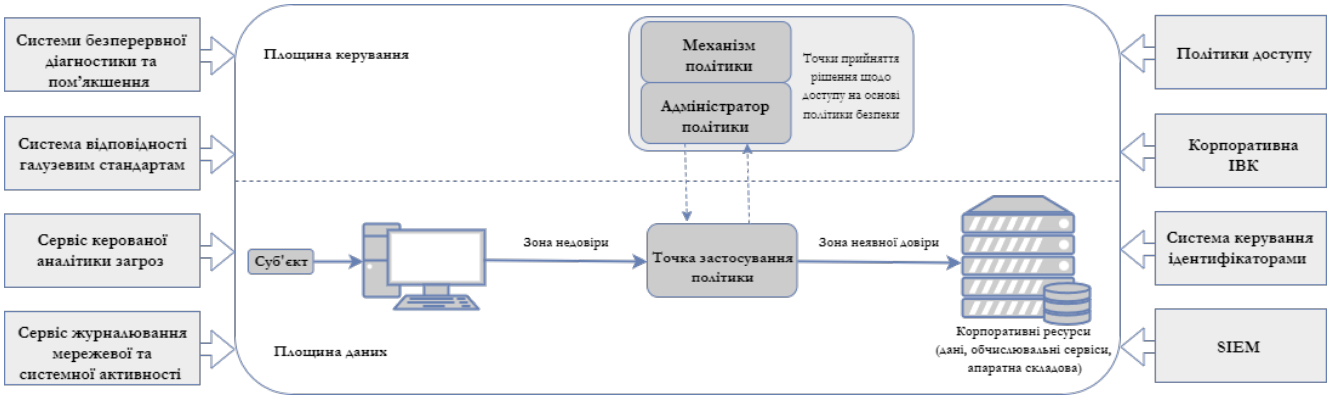

Рис. 1.4. Модель концептуального ядра архітектури zero-trust

Дана модель ілюструє фундаментальну взаємодію між основними логічними компонентами концептуального ядра архітектури zero-trust:

– механізм політики ‘policy engine’ – відповідає за прийняття остаточного рішення щодо надання доступу до ресурсу для конкретного суб’єкта. Даний компонент використовуючи політику безпеки підприємства, а також контекстуальні дані зовнішніх джерел (таких як системи безперервної діагностики та пом’якшення, сервісу керованої аналітики загроз тощо), як вхідні дані для алгоритму визначення достовірності суб’єкта, формує рішення щодо надання, відхилення або скасування доступу до ресурсу. Прийняте рішення передається на виконання адміністратору політики;

– адміністратор політики ‘policy administrator’ – відповідає за встановлення та/або закриття каналу зв’язку між суб’єктом та ресурсом, що досягається шляхом видачі відповідних команд до PEP. В залежності від конкретної реалізації ядра архітектури zero-trust, компоненти механізму політики та адміністратору політики можуть бути представлені як у вигляді двох окремих компонентів, так і у вигляді окремої повноцінної служба прийняття рішення щодо доступу на PDP;

– PEP – відповідає за встановлення, моніторинг та розрив з’єднань між суб’єктом та корпоративним ресурсом.

На додаток до основних компонентів, архітектура zero-trust містить додаткові компоненти, що надають всю необхідну інформацію (вхідні дані) для формування рішення щодо надання доступу:

– системи безперервної діагностики та пом’якшення ‘continuous diagnostics and mitigation’ – відповідає за збір даних про поточний стан активів підприємства, вносить зміни в конфігурацію та здійснює оновлення програмного забезпечення. Даний компонент надає механізму політики відомості про актив, який ініціює запит на доступ, зокрема щодо поточної версії операційної системи (визначаючи, чи вона є оновленою), цілісності дозволених підприємством програмних компонентів (прикладного програмного забезпечення), або наявності незатверджених компонентів, а також надає відомості щодо наявності у активу відомих вразливостей;

– система відповідності галузевим стандартам ‘industry compliance system’ – гарантує дотримання підприємством нормативних рамок, що застосовуються до його операцій;

– сервіс керованої аналітики загроз ‘threat intelligence feed’ – надає подробиці про нещодавно виявлені вразливості чи атаки на основі зібраних даних як із внутрішніх, так і з різноманітних зовнішніх джерел;

– сервіс журналювання мережевої та системної активності – поєднує відомості про активи, мережевий трафік, дії з доступу до ресурсів та інші події, які забезпечують зворотний зв’язок у режимі реального часу про стан безпеки інформаційних систем підприємства;

– політики доступу – охоплюють атрибути, правила та політики доступу до корпоративних ресурсів. Служать основою для авторизації доступу до ресурсів, оскільки дані політики визначають основні права та повноваження доступу, надані обліковим записам, програмам і службам у межах підприємства;

– корпоративна інфраструктура відкритих ключів ‘public key infrastructure’ – відповідає за створення та реєстрацію сертифікатів, виданих підприємством

ресурсам, суб’єктам, службам та додаткам, при чому, щоб сертифікати були виключно X.509. Водночас, корпоративна інфраструктура відкритих ключів може бути інтегрована з національною інфраструктурою відкритих ключів;

– система керування ідентифікаторами – відповідає за створення, зберігання та керування обліковими записами корпоративних користувачів та ідентифікаційними записами (наприклад, сервер полегшеного протоколу доступу до каталогів);

– СУІБ та подіями – збирає інформацію про події безпеки, яка згодом аналізується та застосовується для уточнення політики безпеки та попередження про можливі атаки на активи підприємства.

Водночас слід відзначити, що логічні компоненти взаємодіють через окрему площину керування, а взаємодія суб’єктів відбувається через площину даних.

Попри те, що дана концепція є досить дієвою та потужною в контексті протидії як внутрішнім так і зовнішнім загрозам інформаційної безпеки, її застосування, згідно проведеного опитування командою Cybersecurity Insiders, залишається відносно низьким, лише близько 15% опитаних команд з інформаційної безпеки успішно впровадили на своїх підприємствах концепцію zero-trust [67]. Водночас, 47% опитаних взагалі не впевнені у своїй здатності забезпечити концептуальні принципи «нульової довіри» за допомогою наявних в них технологій безпеки.

Існує кілька потенційних причин, чому впровадження концепції zero-trust є складним завданням, і загальним фактором цьому є природа трансформації [68]. Внесення будь-яких змін, модернізація наявної системи забезпечення інформаційної безпеки є досить тривалим та складним процесом, на який впливають технологічні, політичні та культурні фактори. Крім того, внесення значних змін до існуючої інфраструктури безпеки може супроводжуватися додатковими ризиками виникнення нових вразливостей [69].

В основні аспекти реалізації архітектури zero-trust зокрема заглиблюється автор наступного дослідження [70], підкреслюючи важливість суворих заходів автентифікації перед наданням користувачам доступу до ресурсів, а також

зосереджує увагу на аналізі процедури авторизації як для локальних, так і для хмарних ресурсів. Зокрема, у відповідь на швидке поширення повсюдного застосування хмарних технологій та IoT, в роботі [71] висвітлюється актуальність застосування принципів zero-trust для забезпечення безпеки даних в середовищах хмарних обчислень, а в дослідженні [72] автори представили основні кроки переходу та впровадження архітектури zero-trust для підприємств з існуючою системою інформаційної безпеки по типу захисту мережевого периметра. Також, детальні сценарії впровадження архітектури zero-trust висвітлюються фахівцями з NIST та MITRE в роботі [73].

На комплексності безпеки наголошується, в роботі практичного характеру [74], в якій висвітлюються основні аспекти впровадження архітектури zero-trust за допомогою системи контейнеризації Kubernetes для вирішення проблем безпеки на різних рівнях моделі взаємодії відкритих систем. Ще однією досить специфічною сферою, в якій проводяться дослідження щодо можливості застосування концепції zero-trust є енергетика, зокрема в дослідженні [75] представлено оцінку та спосіб впровадження систем безпеки з «нульовою довірою» на віртуальних електростанціях (хмарна інформаційна система до якої підключено розподілені джерела електроенергії), що спрямовано на захист ключових пристроїв та передбачає покращити загальну архітектуру безпеки віртуальних електростанцій.

В іншому практичному дослідженні [76] розглядаються переваг при впровадженні моделі zero-trust в банківському секторі. Дослідження показало, що дана модель виявилася високоефективною та дієвою у протидії поширеній проблематиці несанкціонованого проникнення в інформаційні інфраструктури в банківському секторі. Технічно, zero-trust допомагає вирішити проблему злому різних облікових записів клієнтів, чим зокрема покращує репутацію банківської галузі.

Крім того, подібні дослідження проводяться і в сфері науки та освіти. Так, задля забезпечення безпеки дослідницької роботи, через слабкість системи безпеки на основі периметра, в [77] запропоновано структуру оцінки

достовірності суб’єктів доступу в університетському середовищі. Модель zero-trust була доведена до практичного застосування у вигляді прототипу, який реалізує захищений доступ до загальновідомої системи електронного навчання під назвою Moodle.

В зв’язку з розвитком мікросервісної архітектури, що супроводжується збільшенням робочого навантаження на центри обробки даних, створюються нові додаткові ризики безпеки, оскільки атаки можуть порівняно легко поширюватися всередині центру обробки даних за рахунок використання міжсервісних залежностей. В контексті цього, автори дослідження [78] пропонують незалежний від мережі підхід щодо периметризації мікросервісів, в якому було перенесено цілі периметризації з кінцевих точок мережі на деталізовані, контекстно-насичені ідентифікатори мікросервісів. При цьому, їхня модель базується на принципах контролю доступу та механізмах забезпечення виконання політик скерованих на регламентацію забезпечення доступу та моніторинг пакетів у мережі.

Водночас, в іншому дослідженні [79], в контексті все ще зростаючої кількість загроз кібербезпеці центрів обробки даних, було запропоновано новий підхід до перебудови системи безпеки, заснований на принципах zero-trust. Сформована модель поєднує два ключових механізми безпеки: контроль транспортування та автентифікацію пакетів даних. Зокрема було запропоновано використання техніки стеганографічного накладання, щоб приховати маркери автентифікації в запитах TCP-пакетів із додатковим рівнем безпеки через автентифікацію першого пакету.

Ще в одному, з останніх інноваційних досліджень [80], розглядалися обмеження існуючих архітектур безпеки в боротьбі з останніми тенденціями та проблематиками безпеки. Автори в своїй роботі пропонують архітектура безпеки з «нульовою довірою» для IoT, в основу якої покладено автентифікацію пристроїв на основі блокчейну.

Таким чином, розглянуті дослідження в сукупності підкреслюють універсальність та ефективність застосування концептуального підходу zero-trust у вирішенні сучасних проблем безпеки в різних областях і технологічних сферах.

1.4. Постановка наукового завдання дослідження

Беручи до уваги розглянуті вище дослідження та дані з щорічних звітів щодо інцидентів інформаційної безпеки, слід визнати, що останнім часом, спостерігається зміщення вектору кіберзлочинів у напрямку саме внутрішніх загроз, що супроводжується збільшенням випадків їх реалізації та масштабів збитків від дій внутрішніх порушників безпеки [81]. Це певні навмисні дії, що призвели до нанесення збитків, вчинені як співробітниками підприємства, так і будь-якими іншими особами, які отримали доступ до внутрішніх ресурсів ІКС підприємства. Крім того, навіть звичайні користувачі можуть становити певну загрозу через можливість допущення ними помилок – ненавмисних дій, що можуть призвести до порушення інформаційної безпеки. Така ситуація нерідко складується в наслідок недостатніх знань, освіченості в питаннях забезпечення інформаційної безпеки. Зокрема користувачі можуть недооцінювати загрози для підприємства через власні судження або сприйняття того, що їхні ролі (посади) не є значимими або вирішальними в контексті забезпечення безпеки інформації та інформаційних систем. Водночас велика кількість користувачі не мають жодного технічного досвіду в управлінні конфіденційністю інформаційних активів [82].

В результаті, наразі, користувачі вважаються «найслабшою ланкою» у ланцюжку безпеки. Однак, постійні звинувачення або навіть притягнення до відповідальності користувачів за допущені помилки, не є ефективними заходами із забезпечення безпеки і навіть не призводять до їх формування. Для виправлення даної ситуації, підприємства повинні розширювати можливості кінцевих користувачів, перетворюючи їх із простих користувачів системи на осіб, які забезпечують безпеку, шляхом чіткого регламентування їхніх дій та обов’язків в політиці безпеки та належного роз’яснення основних положень політики.

Саме тому, розробка політики безпеки має ґрунтуватися на розумінні того, як поведінка людини, яка безпосередньо працює з інформаційними активами підприємства, може впливати на забезпечення дотримання основних її положень, і навпаки. Таким чином, переважна більшість досліджень зосереджується на

розгляді проблематики формування ефективної політики інформаційної безпеки підприємства в контексті організаційного рівня. Однак, в зв'язку з тим, що поведінкові аспекти користувачів щодо забезпечення інформаційної безпеки все ще залишаються важко контрольованими або навіть непередбачуваними, виникає необхідність у застосуванні концепцій, методів, які б нівелювали дані обмеження.

Одним зі шляхів вирішення вищезазначеної проблематики є мінімізація довіри до суб'єктів доступу, що і покладено в основу концепції zero-trust. В порівнянні з традиційними принципами захисту інформації на основі периметру, zero-trust пропонує ряд рішень, які значно знижують ризик виникнення внутрішніх загроз, а також мінімізують загрозу поширення навіть успішної поточної атаки ззовні на всю інформаційну інфраструктуру [69].

З проведеного аналізу в 1.3.1 слідує, що одним із ключових, навіть критичних компонентів концептуального підходу zero-trust до побудови та впровадження політики інформаційної безпеки підприємства є система розмежування та контролю доступу (система керування доступом), адже при ненадійному механізмі ідентифікації/автентифікації (перевірці ідентичності, справжності суб'єкта доступу), вся модель політики безпеки втрачає цінність через подолання основного принципу zero-trust. Водночас, окрім надійності, слід також відзначити складність механізмів автентифікації, зокрема багатофакторної, використання якої рекомендується при реалізації концепції zero-trust, що відповідно впливає на ефективність їхнього застосування. Чим більше факторів, тим складніша і сама реалізація такої системи керування доступом, і це може викликати труднощі у рядових працівників при користуванні такою системою, що також може призводити до потенційних порушень безпеки.

Однак, проведений в попередньому підрозділі аналіз літературних джерел щодо застосування основних концептуальних принципів zero-trust при побудові та впровадженні політики інформаційної безпеки підприємства, свідчить про зосередження уваги здебільшого саме на організаційних та технологічних аспектах, залишаючи відкритим питання щодо ефективності вище виділених технічних заходів.

Таким чином, можна зробити висновок, що в практиці застосування концептуальних принципів zero-trust при формуванні політики інформаційної безпеки підприємства загострилося протиріччя між необхідністю зменшення впливу поведінкових аспектів користувачів на забезпечення інформаційної безпеки та ефективністю існуючих теоретичних та технологічних рішень, які б дозволили реалізувати мінімізацію «людського фактору».

У зв’язку з цим, існує необхідність вирішення актуального наукового завдання, сутність якого полягає в подальшому розвитку методів вдосконалення політики інформаційної безпеки підприємства на основі інтегрування концептуальних принципів zero-trust, зокрема технічних аспектів їх забезпечення.

Метою дисертаційного дослідження є підвищення ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб’єктів в ІКС.

У відповідності до сформованої мети, для вирішення зазначеної науково-прикладної проблематики, в роботі сформульовані часткові завдання:

– проаналізовані поточний стан застосування політики інформаційної безпеки, як одного з ключових елементів забезпечення інформаційної безпеки підприємства, а також підходи, методи та сучасні практики побудови системи інформаційної безпеки підприємства;

– здійснено детальний аналіз концепції «нульової довіри» та виділено основні обмеження щодо центрального елемента системи забезпечення безпеки, а саме, використовуваних механізмів ідентифікації/автентифікації суб’єктів доступу;

– досліджені тренди виникнення кіберінцидентів та визначені елементи управління культурою кібербезпеки організації на основі обробки даних обстежень її поточного стану та впровадження корегуючих заходів;

– визначена формалізована модель оцінки рівня культури кібербезпеки;

– вдосконалена модель загроз безпеки інформаційних активів підприємства на основі концепції zero-trust;

– визначенні вимоги до безконтактного апаратного засобу автентифікації суб’єктів інформаційних відносин;

– запропоновано та обґрунтовано стеганографічний протокол обміну даними в процедурах управління ідентифікацією та доступом;

– визначені нові загрози та ризики що обумовлені поширенням використання СШІ [83].

Висновки до розділу 1

1. Визначено роль та проаналізовано сучасний стан застосування політики інформаційної безпеки, як одного з ключових елементів забезпечення інформаційної безпеки підприємства. Встановлено, що ефективна реалізація політики безпеки, створюючи корпоративну культуру безпеки, сприяє підвищенню загального рівня захищеності інформаційних ресурсів підприємства.

2. Проведено аналіз основних підходів, методів та сучасних практик побудови політики інформаційної безпеки підприємства, зокрема із застосуванням концептуальних принципів zero-trust. Це дозволило виявити основні обмеження, що пов’язані з впливом поведінкових аспектів користувачів на реалізацію основних положень сформованої політики безпеки підприємства та забезпечення інформаційної безпеки в цілому, в умовах присутності «людського фактору».

3. Сформульовано актуальне наукове завдання, яке полягає в подальшому розвитку методів вдосконалення політики інформаційної безпеки підприємства на основі інтегрування концептуальних принципів zero-trust, зокрема технічних аспектів їх забезпечення. Зокрема для його вирішення визначено мету роботи, яка полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб’єктів в ІКС.

Список використаних джерел у розділі 1

1. European Union Agency for Cybersecurity. (2021). ENISA Threat Landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2. ISO/IEC 27000:2018. Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary. https://www.iso.org/standard/73906.html

3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

4. Albrechtsen, E. (2007). A Qualitative Study of Users' View on Information Security. Computers & Security, 26(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004

5. Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

6. Puhakainen, P. (2006). A Design Theory for Information Security Awareness. University of Oulu, Oulu, Finland.

7. Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information Systems Security Policies: A Contextual Perspective. Computers and Security, 24(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.011

8. Merritt, C., & Dhillon, G. (2016). What Interrupts Intention to Comply with IS-Security Policy? Americas Conference on Information Systems, 1–10.

9. Ajzen, I. (1991). The Theory of Planned Behavior. In Organizational Behavior and Human Decision Processes, 50(2). 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

10. Abed, J., Dhillon, G., & Ozkan, S. (2016). Investigating Continuous Security Compliance Behavior: Insights from Information Systems Continuance Model. In 22nd Americas Conference on Information Systems, 1–10.

11. Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

12. Maddux, J.E. & Rogers, R.W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology, 19(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

13. IBM. (2022). Cost of a Data Breach 2022 Report. https://www.ibm.com/account/reg/us-en/signup?formid=urx-51643&adoper=192344_0_LS

14. State of Cybersecurity Resilience 2021 (4th Annual Report): How Aligning Security and the Business Creates Cyber Resilience. Accenture. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

15. Літвінчук, І., Корчомний, Р., Коршун, Н., & Ворохоб, М. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112

16. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

17. Skladannyi, P., Trofimov, O., Korniiets, V., Vorokhob, M., & Opryshko, T. (2023). Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3421, 97–106.

18. Bosch, C., Eloff, J., & Carroll, J. (1993). International Standards and Organizational Security Needs: Bridging the Gap. In 9th International Conference on Information Security, 171–183.

19. Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications, Boca Raton.

20. Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards. ProQuest Dissertations and Theses database, No. 3456209.

21. Nigam, A., & Siponen, M. (2011). Designing Information Systems Security Policy Methods: A Meta-Theoretical Approach. Proceedings of JAIS Theory Development Workshop. Sprouts: Working Papers on Information Systems, 11(150).

22. Скітер, І., & Ворохоб, М. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158–169. https://doi.org/10.28925/2663-4023.2021.13.158169

23. Department for Business, Innovation and Skills. (2013). Information Security Breaches Survey. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf

24. Department for Business, Innovation and Skills. (2015). Information Security Breaches Survey. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf

25. Frost & Sullivan. (2013). The 2013 (ISC)2 Global Information Security Workforce Study. https://icscsi.org/library/Documents/Threat_Intelligence/Frost-Sullivan%20-%20ICS2%20Global%20InfoSec%20Workforce%20Study%20-%202013.pdf

26. Nohlberg, M. (2009). Why Humans are the Weakest Link. Social and Human Elements of Information Security, 15–26. https://doi.org/10.4018/978-1-60566-036-3.ch002

27. SANS Institute. (2022). Security Awareness Report. https://go.sans.org/lp-wp-2022-sans-security-awareness-report

28. Schneier, B. (2015). Secrets and Lies. https://doi.org/10.1002/9781119183631

29. Siponen, M. (2006). Six Design Theories for IS Security Policies and Guidelines. Journal of the Association for Information Systems, 7(7), 445–472. https://doi.org/10.17705/1jais.00095

30. Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688

31. Cisco Systems. (2008). Data Leakage Worldwide: The Effectiveness of Security Policies. http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html

32. Hoo, K. J. S. (2002) How Much Is Enough? A Risk-Management Approach to Computer Security. Workshop on Economics and Information Security (WEIS), Berkeley.

33. Long, G. P. (2002). Security Policies in a Global Organization. SANS Institute InfoSec Reading Room. http://www.sans.org/reading_room/whitepapers/policyissues/security-policies-globalorganization_501

34. Baskerville, R., & Siponen, M. (2002). An Information Security Meta-Policy for Emergent Organizations. Journal of Logistics Information Management, 15(5/6), 2-8, 337-346. https://doi.org/10.1108/09576050210447019

35. Bosworth, S., & Kabay, M. E. (2002). Computer Security Handbook. 4th ed., New York, NY: John Wiley & Sons, Inc.

36. Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information Systems Security and the Need for Policy. Information Security Management, 9–18. https://doi.org/10.4018/978-1-878289-78-0.ch002

37. Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2016). Information Security Policy: A Management Practice Perspective. InfoSec Policy Management Practices. Presented at the Australasian Conference on Information Systems.

38. Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES. Communications of the ACM, 46(7), 101–106. https://doi.org/10.1145/792704.792706

39. Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are Nonprofit Organizations Influenced to Create and Adopt Information Security Policies? Issues in Information Systems, 14(2), 166–173. https://doi.org/10.48009/2_iis_2013_166-173

40. Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and Measuring Information Security Culture. School of Information Systems; Science & Engineering Faculty. http://aisel.aisnet.org/pacis2012/144

41. Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning. Computers & Security. https://doi.org/10.1016/j.cose.2018.02.001

42. European Union (2016). General Data Protection Regulation. Official Journal of the European Union.

43. Верховна Рада. (2022). Закон України «Про захист персональних даних». №2297-VI від 27.10.2022 р. https://zakon.rada.gov.ua/laws/show/2297-17

44. Верховна Рада. (2022). Закон «Про основні засади забезпечення кібербезпеки України». №2163-VIII від 17.08.2022 р. https://zakon.rada.gov.ua/laws/show/2163-19

45. Верховна Рада. (2022). Закон «Про захист інформації в інформаційно-комунікаційних системах». №80/94-ВР від 01.07.2022 р. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

46. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements. https://www.iso.org/standard/54534.html

47. ISO/IEC 27002:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Controls. https://www.iso.org/standard/75652.html

48. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Наказ ДСТСЗІ СБ України №22 від 28.04.1999 р. https://tzi.com.ua/downloads/1.1-002-99.pdf

49. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Наказ ДСТСЗІ СБ України №53 від 04.12.2000 р. https://tzi.com.ua/downloads/1.4-001-2000.pdf

50. BSI Standards. IT Baseline Protection Manual. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

51. NIST 800-12 Rev. 1. An Introduction to Computer Security: The NIST Handbook. https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

52. NIST 800-18 Rev. 1. Guide for Developing Security Plans for Federal Information Systems. https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

53. NIST 800-30 Rev. 1.Guide for Conducting Risk Assessments. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

54. Control Objectives for Information and Related Technology (CobiT) 4.1. http://www.isaca.org.ua/index.php/homepage/download/category/12-cobit

55. Wood, C. C. (1995). Writing InfoSec Policies. Computers & Security, 14(8), 667–674. https://doi.org/10.1016/0167-4048(95)97114-p

56. Whitman, M. E. (2004). In Defense of the Realm: Understanding Threats to Information Security. Informational Journal of Information Management, 24(1), 43–57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

57. Sipior, J., & Ward, B. (2008). A Framework for Information Security Management based on Guiding Standards: A United States Perspective. The Journal of Issues in Informing Science and Information Technology, 5, 51–60. https://doi.org/10.28945/3188

58. Simms, D. J. (2009). Information Security Optimization: From Theory to Practice. In International Conference on Availability, Reliability and Security, 675–680. https://doi.org/10.1109/ares.2009.106

59. Hadasch, F., Mueller, B., & Maedche, A. (2011). Leaking Confidential Information by Non-Malicious User Behavior in Enterprise Systems–Design of an Empirical Study. MCIS Proceedings. http://aisel.aisnet.org/mcis2011/126

60. Mandal, S., Khan, D.A. & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. In New Generation Computing, 39(3–4), 599–622. https://doi.org/10.1007/s00354-021-00130-6

61. Chen, Y., Hu, H-C. & Cheng, G-Z. (2019). Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. Frontiers of Information Technology & Electronic Engineering, 20(2), 238–252. https://doi.org/10.1631/fitee.1800516

62. Marsh, S. P. (1994), Formalising Trust as a Computational Concept. Computing.

63. Kindervag, J. (2010). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research.

64. NIST. (2020). SP 800-207: Zero Trust Architecture (ZTA). https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech:nist:zta

65. Черненко, Р., Рябчун, О., Ворохоб, М., Аносов, А., & Козачок, В. (2021). Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 124–135. https://doi.org/10.28925/2663-4023.2021.11.1241351.3

66. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

67. Cyberecurity Insiders. (2019). Zero Trust Adoption Rate. https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/

68. Garbis, J. & Chapman, J.W. (2021). Zero Trust Security. 1th Edition. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6702-8

69. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436

70. Cavalancia, N. (2020). Zero Trust Architecture Explained. AT&T CyberSecurity.

71. Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable Zero Trust for Cloud Computing Environments. Computers & Security, 110, 102419. https://doi.org/10.1016/j.cose.2021.102419

72. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. Security and Communication Networks, 1–10. https://doi.org/10.1155/2021/9947347

73. Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). Implementing a Zero Trust Architecture. National Institute of Standards and Technology.

74. D'Silva, D., & Ambawade, D. D. (2021). Building a Zero Trust Architecture using Kubernetes. In 6th International Conference for Convergence in Technology, 1–8. https://doi.org/10.1109/I2CT51068.2021.9418203

75. Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to Enhance Security in Virtual Power Plants. Energy Reports, 8, 1309–1320. https://doi.org/10.1016/j.egyr.2021.11.272

76. Saini, D. K., Saini, H., & Singh, S. (2021). Security and Trust Model Analysis for Banking System. In International Journal of Sensors, Wireless Communications and Control, 11(1), 135–145. https://doi.org/10.2174/2210327910666191218130129

77. Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based Access Control and Trust Scores in Zero Trust Campus Networks. Lecture Notes in Informatics, 53, 53–65, https://doi.org/10.18420/sicherheit2020_04

78. Zaheer, Z., Chang, H., Mukherjee, S., & Van der Merwe, J. (2019). eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices. In Proceedings of the ACM Symposium on SDN Research. https://doi.org/10.1145/3314148.3314349

79. DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. In IEEE International Conference on Smart Cloud (SmartCloud). https://doi.org/10.1109/smartcloud.2016.22

80. Li, S., Iqbal, M., & Saxena, N. (2022). Future Industry Internet of Things with Zero-trust Security. In Information Systems Frontiers. Springer Science and Business Media LLC. https://doi.org/10.1007/s10796-021-10199-5

81. Sokolov, V., & Skladannyi, P. (2023). Methodology for Assessing Comprehensive Damages from an Information Security Incident. Cybersecurity: Education, Science, Technique, 1(21), 99–120. https://doi.org/10.28925/2663-4023.2023.21.99120

82. Gross, J. B., & Rosson, M. B. (2007). Looking for Trouble: Understanding End-User Security Management. Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology. https://doi.org/10.1145/1234772.1234786

83. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

РОЗДІЛ 2
АНАЛІЗ ТРЕНДІВ РОЗВИТКУ КІБЕРІНЦИДЕНТІВ ТА УПРАВЛІННЯ КУЛЬТУРОЮ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1. Аналіз трендів загроз кібербезпеки в цивільному секторі

Принципове значення для побудови в хмарному середовище системи кіберзахисту згідно з концепцією zero-trust і подальшого управління нею має процедура попереднього вивчення стану безпеки навколишнього та внутрішнього, по відношенню до підприємства, середовищ та визначення тенденцій їх розвитку.

Стосовно аналізу зовнішнього середовища в багатьох випадках проєктанти систем безпеки можуть скористатись даними дослідників щодо впровадження інструментів кібербезпеки, які доцільно використовувати в сучасних інформаційних системах, а також аналітики проблем кібербезпеки [1–4].

На поточний час в наукових публікаціях, засобах масової інформації небагато актуальних статистичних даних за достатньо великий проміжок часу щодо кількості кіберінцидентів та їхнього секторального розподілу, але деяка інформація була зібрана та систематизована.

Для системного дослідження окремих аспектів кібербезпеки зібраних статистичних даних може бути недостатньо, залежно від джерел їх походження вони можуть бути суперечливими, звичайно для таких даних невідомі об’єм початкової вибірки та її реальна репрезентативність. Окремо постає проблемне питання щодо математичних методів обробки зібраних різноманітних даних. Саме тому, доцільно приділити особливу увагу визначеним проблемам аналізу стану кібербезпеки.

Наша аналітика трендів кіберзагроз базується на опублікованих даних провідних компаній світу [1–3] та фокусується переважно на кібератаках та інцидентах, які успішно реалізовані порушниками безпеки та мали згубний вплив на інформаційні активи (ресурси) компанії чи окремих осіб.

На підставі публікацій [1, 2] на діаграмі (рис. 2.1) наведені узагальнені дані щодо кількості спостережених реалізованих кібератак (кіберінцидентів) за квартами в 2019–2022 роках.

Слід зазначити, у більшості випадків результати спостережень багатьма компаніями, що досліджують кіберінциденти.

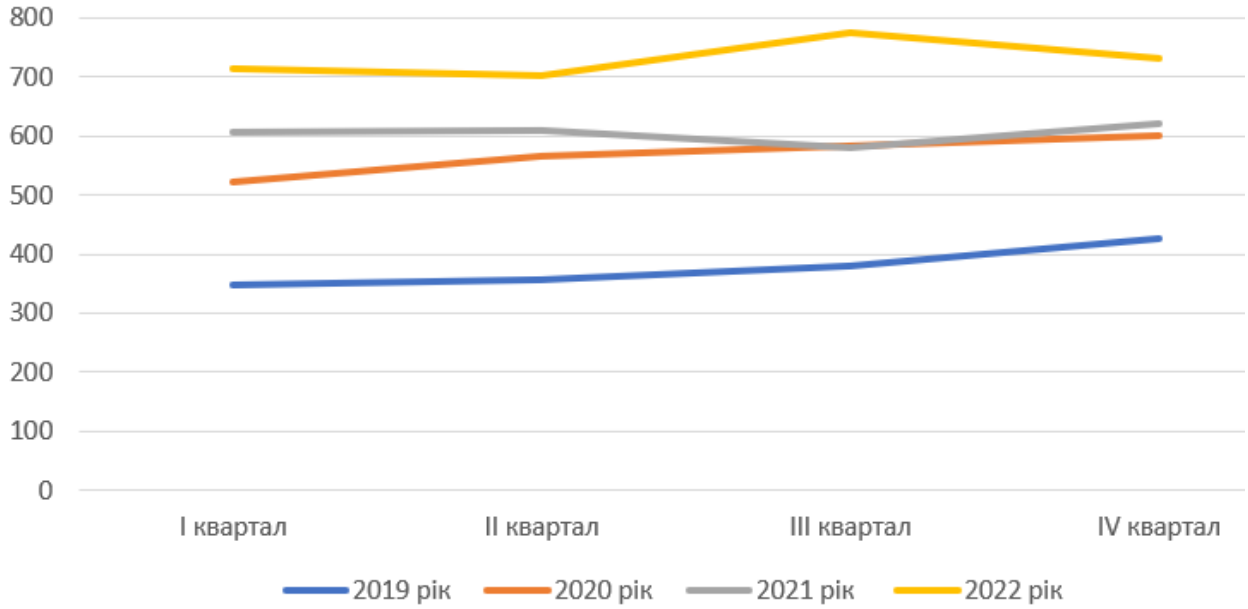

Рис. 2.1 Діаграма кількості випадків кіберінцидентів за кварталами

На підставі цієї діаграми вкрай складно зробити достатньо суттєві висновки щодо тенденцій змін у кількості реалізацій кібератак з тяжкими наслідками, крім доволі очевидного факту, щодо зростання їх кількості спостережених атак в середньому до 100 подій за рік.

Крім того, зважаючи на те, що одиницею виміру час обрано саме квартал, тому можливість деталізації подій у кіберпросторі доволі обмежена.

З метою покращення результатів аналізу згадані дані були перетворені у таблицю, щодо якої були застосовані методи математичної статистики для розрізняння певних гіпотез (табл. 2.1).

Зокрема, в межах кожного року були розраховані математичні сподівання a_i та стандартні відхилення σ, а також були обчислені відносні частоти для оцінки відхилення від рівномірного розподілу ймовірностей:

$$a_i = \frac{1}{n_i}\sum_{i=1}^{4} v_{ij},$$

$$\sigma_i = \frac{4}{3}\sqrt{\frac{1}{4}\sum_{j=1}^{4}\left(v_{ij}-a_i\right)^2} = \frac{2}{3}\sqrt{\sum_{j=1}^{4}\left(v_{ij}-a_i\right)^2}, \qquad (2.1)$$

$$\left\{\frac{v_{ij}}{n_i}, i=\overline{1,4}, j=\overline{1,4}\right\},$$

де n_i – кількість спостережених кіберінцидентів с важкими наслідками в i-му році (1 – «2019», 2 – «2020», 3 – «2021», 4 – «2022»),

v_{ij} – частота кіберінцидентів в j-тому кварталі (1–4), i-го року (1–4).

Слід зауважити, що обсяг наявних даних, з точки зору ефективного застосування методів математичної статистики, по роках відносно невеликий, але ж можливо відмітити певні тенденції, що мають значення в сенсі прогнозування загроз кібербезпеки.

Загалом, наведені в табл. 2.1 дані мають ознаки стохастичного процесу із середнім a (математичне сподівання) що зростає від 377 до 730 випадків на квартал та стандартним відхиленням σ (30.55..60.10) за відповідні роки (2019–2022 роках).

Таблиця 2.1

Узагальнені дані щодо кількості кіберінцидентів в світі в 2019–2022 роках

Квартал / **Рік**	**1**	**2**	**3**	**4**	**Загалом за рік**	**Середнє** a	**Стандартне відхил.** σ
2019	347	357	379	425	1508	377,00	60,1
	0,2301	0,2368	0,2513	0,2818	← Відносні частоти		
2020	521	567	583	600	2271	567,75	58,81
	0,2294	0,2497	0,2567	0,2642	← Відносні частоти		
2021	607	609	580	622	2418	604,50	30,55
	0,2510	0,2519	0,2399	0,2572	← Відносні частоти		
2022	714	702	774	731	2921	730,25	50,12
	0,2444	0,2403	0,2650	0,2503	← Відносні частоти		
Загалом за квартал	2189	2235	2316	2378	9118	**2279,50**	145,62
	0,2401	0,2451	0,2540	0,2608	← Відносні частоти		

Спочатку стосовно випадкового процесу змін кількості кіберінцидентів за квартал (табл. 2.1) зробимо деякі припущення, що несуттєво обмежують загальні підходи.

По-перше, будемо вважати що середнє значення ймовірності подолання систем захисту в інформаційних системах в світі протягом року змінюється не суттєво.

Тобто вважаємо, що в силу закону великих чисел, а саме, значної кількості ІС, що будуються в світі за певними стандартними правилами кібербезпеки, не виникає ситуацій з суттєвим покращенням або значним погіршенням середнього рівня безпеки систем, та, відповідно, значення вказаної середньої ймовірності. Безумовно, без інформації від власника первісних даних щодо методу і умов їх збирання це припущення є єдиним шляхом для їх оцінки.

Необхідність цього припущення обумовлена обмеженою придатністю для аналізу доступних статистичних даних про кіберінциденти, які звичайно під час їх збирання не враховують відомостей про стан захищеності інформаційних систем та рівень кіберкультури їхнього персоналу [3].

Спочатку розглянемо табл. 2.1 як 4×4 таблицю спряжених ознак, щодо якої висувається нульова гіпотеза про незалежність ознак (рік-квартал). Для перевірки гіпотези використовуємо статистику x_i – квадрат незалежності [5]:

$$\chi^2 = n \cdot \left(\sum_{i,j} \frac{v_{ij}^2}{v_{i\cdot} v_{\cdot j}} - 1 \right), \tag{2.2}$$

де $n = 9118$ – загальна кількість спостережень кіберінцидентів протягом 2019–22 роках,

v_{ij} – частота кіберінцидентів в j-тому кварталі i-го року, величини що розраховуються $v_{i\cdot} = \sum_j v_{ij}, v_{\cdot j} = \sum_i v_{ij}$.

В нашому випадку зазначена статистика матиме $(4 – 1)\times(4 – 1) = 9$ ступенів свободи, обираючи рівень значущості критерія $\alpha = 0{,}05$ визначимо границю критерія $\chi^2_C = 16{,}9$. Обчислене значення статистики для величин в таблиці 1 становить $\chi^2 = 11{,}9$ та не перевищує величини границі критерія, що узгоджується з нульовою гіпотезою про незалежність змінних.

В табл. 2.1 можливо побачити що відносні частоти кіберінцидентів по кварталам в рамках одного року доволі наближені до величини 0,25. Виникає гіпотеза про рівномірний розподіл частот інцидентів в межах одного року. Перевірку цієї гіпотези зробимо за допомогою критерія узгодженості Пірсона [5]:

$$\chi^2=\sum_{i=1}^{4}\frac{\left(v_i-4\cdot 0.25\right)^2}{4\cdot 0.25}=\sum_{i=1}^{4}\left(v_i-1\right)^2, \qquad (2.3)$$

де v_i – частота виникнення кіберінцидентів в i-том кварталі. Результати розрахункові дані наведені в табл. 2.2.

Таблиця 2.2

Статистика узгодження Пірсона для частот кіберінцидентів по роках

Рік	2019	2020	2021	2022	2019–22
Статистика Пірсона	9,15	6,13	1,58	3,99	9,28
Гіпотеза H_0	$p_i=0{,}25,\ \forall i=\overline{1,4}$				
Границя критерія	$\chi^2_C=7{,}81, \alpha=0{,}05$				

Виходячи з даних в табл. 2.2 гіпотеза щодо рівномірного розподілу кількості кіберінцидентів по кварталах в межах одного року відхиляється для 2019 року з рівнем значущості $\alpha=0{,}05$, оскільки значення статистики Пірсона в цьому випадку $9.15>\chi^2_C=7{,}81$. При цьому основне відхилення від рівномірного розподілу обумовлене зростанням кількості кіберінцидентів в 4 кварталі 2019 року порівняно з 3 кварталом цього року.

Далі, звернемо увагу на суттєву різницю кількості кіберінцидентів в суміжних кварталах різних років (табл. 2.1).

Перший особливий період в таблиці: 3 квартал 2019 року – 4 квартал 2019 року – 1 квартал 2020 року, де спостерігається зростання кількості кіберінцидентів з 379 до 425 і, навіть, до 521 випадка.

Виходячи з припущення, що цей випадок підпадає під умови центральної граничної теореми, вважаємо, що розподіл ймовірностей на цій ділянці відповідає гаусовському нормальному розподілу [5]. Тоді розрахункова границя відхилення C_α для рівня значущості $\alpha=0{,}05$ складає:

$$C_\alpha=a+t_{1-\alpha}\cdot\sigma=377+1{,}64\cdot 60{,}1=475{,}56, \qquad (2.4)$$

де $a=377, \sigma=60,1$ – відповідно математичне сподівання та стандартне відхилення кіберінцидентів по кварталах 2019 року,

$t_{1-\alpha}=1,64$ – квантіль стандартного нормального розподілу $N(0,1)$.

Таким чином, спостерігаємо, що кількість кіберінцидентів в 1 квартале 2020 року перевищує припустиму границю відхилення $C_\alpha=475,56<521$, що дає підстави відхилити гіпотезу про стаціонарність процесу.

Що стосується цього періоду часу можливо відмітити реально глобальні конфліктні або небезпечні ситуації, зокрема, згідно [6] на початок 2020 року припадає:

– загострення відношень США з Іраном на тлі убивства іранського високопосадовця і виходу Ірану з ядерної угоди;

– активна фаза збройного конфлікту між Азербайджаном і Вірменією;

– вихід Великої Британії з Європейським Союзом (Brexit).

В табл. 2.1 в іншому періоді часу: 4 квартал 2021 року – 1 квартал 2022 року знову ж спостерігаємо значне зростання кількості кіберінцидентів з 622 до 714 випадків.

Розрахункова границя відхилення C_α для рівня значущості $\alpha=0.05$ в цьому випадку складає:

$$C_\alpha=a+t_{1-\alpha}\cdot\sigma=604,5+1,64\cdot30,55=655,5185. \quad (2.5)$$

При цьому спостерігаємо, що кількість кіберінцидентів в першому кварталі 2022 року перевищує припустиму границю відхилення:

$$C_\alpha=655,52<714, \quad (2.6)$$

що знову дає підстави відхилити гіпотезу про стаціонарність процесу.

Саме в першому кварталі 2022 року центром уваги майже всього світу став початок повномасштабної російської агресії проти України та поступе введення протягом року економічних санкцій проти агресора. Про це опосередковано свідчить факт [2], що в 2022 році державні установи постраждали найбільше, кількість успішних атак на їхні веб-сайти зросла порівняно з 2021 роком більш ніж удвічі.

Таким чином, можливо стверджувати, що зростання глобальної напруженості в кіберпросторі протягом 2019–2022 років відбувалось під впливом надзвичайних подій в світі, а стохастичний процес загальної кількості реалізованих кіберінцидентів в світі, корельований з стохастичним процесом виникнення глобальних загроз світовому порядку.

Водночас, звернемо увагу, що дані дослідження свідчать про відносно стабільний характер подій в кіберпросторі (див. табл. 2.2) в 2020–2021 роках, що узгоджується з неускладненням глобальної військово-політичної обстановки та соціально-економічних проблем у світі, які могли виконати функції спускових тригерів для реалізації кіберзагроз.

Підсумовуючи викладений аналіз кількості кіберінцидентів в 2019–2022 роках можливо зробити висновок про існування відносно стабільних періодів розвитку подій в кіберпросторі, періодів ускладнення ситуації і періодів підвищення рівня протистояння та суттєвого зростання кібератак.

А це, відповідно, вимагає від менеджменту безпеки впровадження додаткових організаційних та технічних заходів щодо підвищення рівня кібербезпеки інформаційної системи підприємства. Виходячи з результатів аналізу зовнішніх загроз раціональним кроком в цьому випадку буде впровадження навчальних заходів, включаючи проведення з персоналом тренінгів та інструктажів.

Також наведена методика дає певні підстави стверджувати, що відстеження та аналіз в режимі реального часу ситуації в кіберпросторі в глобальному вимірі, а також оперативне інформування зацікавлених об’єктів інформаційної діяльності про існуючий стан і тенденції розвитку подій вже є не тільки нагальною потребою сьогодення з погляду на необхідність динамічного управління безпекою критичних інформаційних інфраструктур, а й реальна можливість.

Викладене стосується узагальненої статистики реалізації кібератак, які успішно реалізовані порушниками безпеки та мали згубний вплив на інформаційні активи. Водночас, для прогнозування можливих подій для вжиття комплексу попереджувальних заходів, зокрема, щодо підвищення кіберкультури

персоналу, має значення розуміння менеджментом підприємства трендів цільових кібератак, атак які реалізуються з певною зловмисною метою.

В [3] на основі аналізу фактів понад 10^3 випадків кіберінцидентів із застосуванням програм-вимагачів запропоновані напрями для покращення управління ризиками шкідливих кодів (програм – вимагачів):

– бізнес тільки із партнерами, які добре дотримуються правил кібербезпеки;

– увага рейтингам внутрішнього ризику бізнес партнерів, злочинці націлені на кожного;

– впевненість, що ваші бізнес партнери, важливі для роботи, мають цілодобову безпеку;

– сумнів, що останні жертви програм – вимагачів суттєво покращили свої програми кібербезпеки;

– готовність на довгострокову перспективу, загроза програм-вимагачів залишається.

За суттю, перші чотири напрями є переклад на бізнес мову, концепції «повної недовіри», включаючи положення щодо контролю дотримання правил кібербезпеки, уваги до його політики інформаційної безпеки в частині керування ризиками, впевненості що ця політика реалізується безперервно, а також сумнів щодо адекватності дій партнера стосовно реагування на кіберінциденти.

П’ятий напрям пропозицій щодо покращення політики інформаційної безпеки свідчить, що ці заходи з кібербезпеки підприємства матимуть тривалий термін дії.

Використовуючи наведені в [3] дані щодо кількості успішно реалізованих кібератак з 2017 по 2022 рік за допомогою вірусів – вимагачів, а також інформацію з табл. 1 щодо кількості загалом успішних атак за рік, з урахуванням [2], що на застосування програм – вимагачів припадає біля 50% успішних кібератак, можливо провести порівняльний аналіз (табл. 2.3) даних з двох джерел.

Таблиця 2.3

Порівняльний аналіз кількості атак вірусів вимагачів

Роки	2016	2017	2018	2019	2020	2021	2022

Дані з [3]	23	26	15	64	284	333	255
Дані з [2] всього	–	–	–	1508	2271	2418	2921
Дані з [2] × 0,5	–	–	–	754	1136	1209	1461
%	–	–	–	6,3	25,0	27,5	17,4

Нажаль, загальна кількість даних не дозволяє підтвердити кореляцію даних між двома джерелами, але ж може свідчити, обсяг даних щодо кіберінцидентів, що збираються джерелом [2], суттєво більший ніж [3], що підвищує рівень довіри до висновків першого джерела.

В секторальному плані реалізації кіберінцидентів можливо відмітити наступне.

Загалом, з урахуванням викладеного аналіз даних щодо кількості та типів кіберінцидентів [2, 3] може спряти актуалізації програм тренінгів і навчань персоналу, зокрема щодо вразливості і захисту корпоративних веб-ресурсів, убезпечення конфіденційної інформації, протидії програмам – вимагачам, посиленню заходів нейтралізації соціальної інженерії та фішингу, убезпеченню клієнтської інфраструктури, підвищення обізнаності в напряму дій в умовах збоїв та відмов апаратного або програмного забезпечення тощо.

2.2. Процеси управління кібербезпекою в плані підвищення кіберкультури персоналу

Згідно положень міжнародних стандартів в галузі інформаційної безпеки та кібербезпеки [7, 8] забезпечення необхідного рівня захисту інформаційних активів потребує від акторів (зацікавлених сторін) впровадження системи узгоджених заходів, що спрямовані на:

– визначення пріоритетних завдань у сфері інформаційної безпеки, які включають захист інформаційних активів підприємства, та методів їх вирішення, призначення та навчання посадових осіб, що виконуватимуть відповідні функції згідно встановлених вимог;

– детального планування робіт та відповідних заходів;

– здійснення дієвого поточного та позапланового контролю за виконанням запланованих заходів;

– впровадження коригувальних дій щодо системи захисту залежно від цінності інформації, загроз її безпеці та виявлених вразливостей у СУІБ.

СУІБ досліджена в багатьох науково-практичних публікаціях з різних точок зору та аспектів.

Наприклад, в [9] детально розглядається вплив культурних особливостей на різні етапи розробки ISO 27001 на державному, корпоративному та індивідуальному рівнях, тобто поведено аналіз досвіду, що може бути корисним в випадку середніх і малих підприємств.

В цій роботі, зроблено висновок, що культурні фактори здатні значною мірою впливати на організацію управління підприємством та цілі діяльності, включаючи аспекти прийняття рішень, впровадження інновацій та нові практики, забезпечення комунікацій, мотивування персоналу та його мобілізація на досягнення позитивних результатів [10].

У той же час, питання управління кіберкультурою на підприємстві в корпоративному та індивідуальному сенсі розглянуто доволі обмежено, тому ми зробимо далі акцент на підвищенні її рівня виходячи з концепції zero-trust.

В рамках наших припущень, в загальному випадку ми аналізуємо наступні навмисні загрозливі дії [11], що можуть нанести шкоди власнику інформаційної системи (табл. 2.4):

При цьому вважаємо, що для реалізації таких дій можуть бути необхідні певні умови доступу до ресурсів системи. Наприклад, хакер атакує інформаційні системи виключно за рахунок доступу до глобальної мережі, персонал системи може здійснювати такі дії як в обхід встановлених правил розмежування доступу, так і на основі легально отриманих прав і повноважень.

В останньому випадку реалізації небезпечних дій може сприяти помилки процедури розподілу повноважень.

Таблиця 2.4

Види вірогідних небезпечних дій в рамках концепції «повної недовіри»

№	Опис небезпечної дії	Особливості реалізації
1	Відмова від факту відправлення деякого повідомлення.	Без доступу до ІС
2	Маскування (імітація прав) – доступ в систему з використанням прав і привілеїв іншого користувача з метою нелегального отримання доступу до конфіденційної інформації або до деяких (можливо платних) сервісів, або ініціалізації та запуску процесів і програм.	Несанкціонований доступ Доступ з боку глобальної мережі
3	Модифікація переданого або прийнятого повідомлення і спроба стверджувати, що воно прийнято саме у такому вигляді від будь-кого.	Легальний доступ Доступ з боку глобальної мережі
4	Підробка – створення фіктивного повідомлення, зокрема, від імені конкретного користувача системи.	Несанкціонований доступ Доступ з боку глобальної мережі
5	Повтор повідомлення, яке передавалось раніше.	Легальний доступ Доступ з боку глобальної мережі
6	Перехоплення активне (перехоплення типу А) – втручання в роботу інформаційної системи з метою вилучення або блокування повідомлень, що передаються.	Несанкціонований доступ Доступ з боку глобальної мережі
7	Перехоплення пасивне (перехоплення типу П) – втручання в роботу інформаційної системи з метою ознайомлення із змістом повідомлень, що передаються	Несанкціонований доступ Доступ з боку глобальної мережі

Для протидії перерахованим навмисним діям (табл. 4) використовуються різні механізми технічного та криптографічного захисту інформації [4, 8], включаючи розмежування доступу, ведення захищених журналів обліку дій в системі, застосування ґеш-функції та кодів автентифікації повідомлень, формування та перевіряння цифрового підпису та цифрових сертифікатів, а також реалізацію організаційних заходів, які включають, зокрема, навчання, виховання та моніторинг дій персоналу.

Згідно з постулатами СУІБ вказані заходи відображаються в керівному документі вищого рівня – політиці інформаційної безпеки підприємства, на підставі якої формуються конкретні правила безпеки, що визначають припустимі та обов’язкові процедури в системі захисту.

На підставі публікацій щодо кіберінцидентів за нашою моделлю основними суб'єктами концепції «повної недовіри» (акторами сценарію небезпечних подій) є наступні (рис. 2.2).

1. Користувач 1, …, Користувач N, які на підставі затверджених функціональних обов'язків та визначених повноважень отримують доступ до інформаційних активів підприємства.

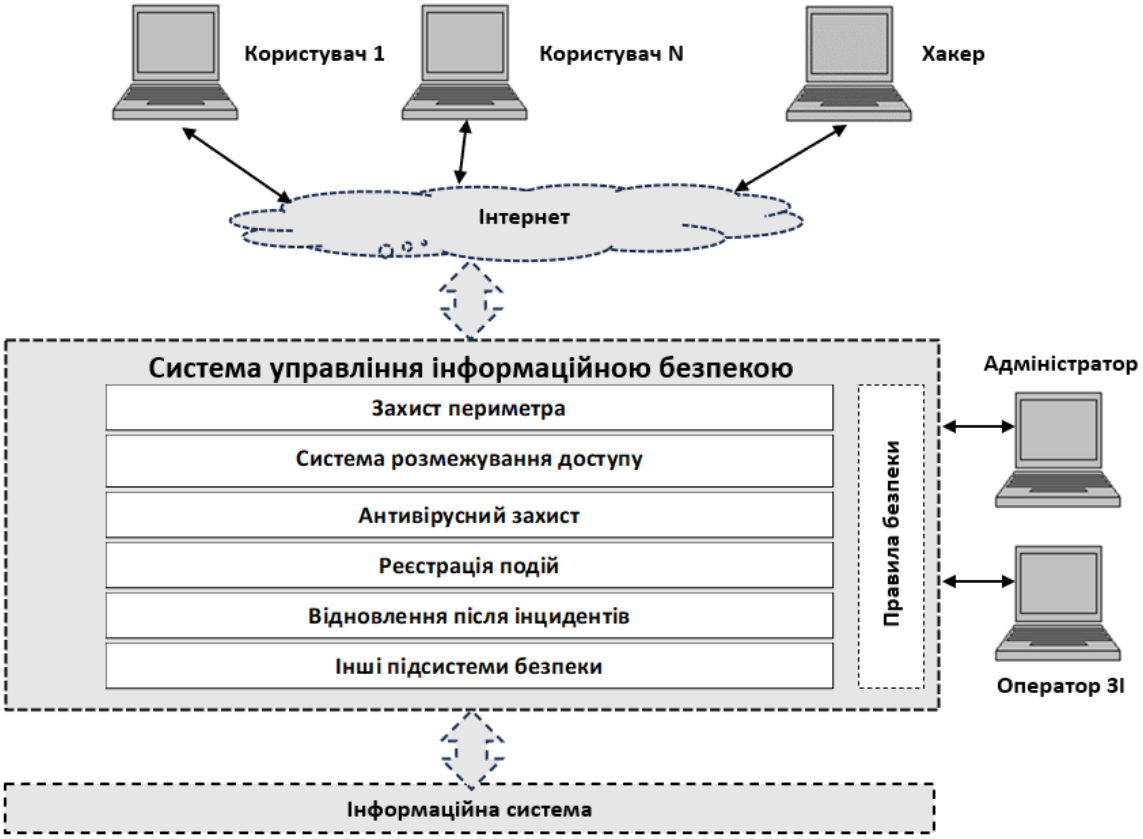

Рис. 2.2. Основні суб'єкти концепції «повної недовіри»

Згідно з концепцією користувачі можуть свідомо здійснювати навмисні небезпечні для активів підприємства дії або сприяти таким діям у випадку змови з іншими акторами. Потенційно вони можуть зробити спробу реалізації будь яких небезпечних дій в системі використовуючи легальні помилкові повноваження або методи несанкціонованого доступу в комп'ютерних системах.

2. Адміністратор безпеки, налаштовує систему захисту, включаючи підсистему розмежування доступу, потенційно може сприяти спробам небезпечних дій.

3. Оператор системи захисту інформації, маючи доступ до засобів та обладнання інформаційної системи та системи захисту інформації може сприяти спробам небезпечних дій.

4. Хакер може намагатись виконати будь-які дії з перерахованих в табл. 2.4 шляхом втручання в роботу комп'ютерної системи.

На підставі визначеної характеристики суб'єктів концепції «повної недовіри» уявляється доцільними з'ясувати, якім чином це впливатиме на СУІБ в цілому та , зокрема, її політику безпеки [10].

За суттю СУІБ є складовою системи управління бізнесом, яка заснована на аналізі і оцінці ризиків, що є підставою для розробки, реалізації, адміністрування, моніторингу, підтримки та підвищення ефективності бізнес процесів і реалізації, визначених на підставі цілей організації, її структури та розмірів, процедур планування заходів, їх впровадження, перевірки достатності та виконання корегувальних дій.

При цьому в СУІБ (рис. 2.3) реалізується наступна схема виконання процесів: Планування (*Plan*) → Заходи (*Do*) → Контроль (*Check*) → Дії (*Act*).

Зазначимо, що в основу методології побудови СУІБ покладені науково обґрунтовані та практично апробовані ідеї та рішення з побудови системи управління якістю на підприємствах [12], яку визначено сімейством міжнародних стандартів серії ISO 9001.

Одним з базових принципів стандарту ISO 9001 є максимальне залучення персоналу для реалізації поставлених цілей [13]. Це означає, що для досягнення бажаної результативності та ефективності управління підприємством необхідно залучення кожного співробітника всіх ланок діяльності та поважне ставлення до кожного як особистості. Досягненню цілей підприємства у визначеній у сфері діяльності сприяють розширення прав співробітників, визнання особистого їх особистого внеску у спільну справу [14] та їх розвиток навичок і можливостей, підвищення компетентності.

Фактично, слід констатувати, що заходів кіберзахисту суто технічного характеру часто недостатньо для захисту системи, оскільки більшість інцидентів у

сфері кібербезпеки пов’язані з людиною, яка вживає помилкових дій або приймає сумнівне рішення [15].

Це дозволяє дійти до висновку, що для покращення ситуації навколо проблеми людського фактору потрібно оперативне реагування ситуація, що утворюється навколо та в середині інформаційної інфраструктури, та вдосконалення технічних і організаційних навичок з кібербезпеки, які дозволять персоналу ефективно діяти для убезпечення інформаційних активів, зокрема, шляхом проведення планових та позапланових тренінгів і навчань забезпечувати.

Проводячи відповідні паралелі з одного боку між процесами управління згідно з стандартом ISO 9001 якістю послуг що надаються та продуктів що створюються, та, з іншого боку, між процесами, що визначені сімейством ISO/IEC 27000 та націлені на реалізацію раціональної стратегії захисту інформаційних активів, можливо дійти до *базових засад управління культурою кібербезпеки* в рамках СУІБ.

Зрозуміло, що етапи реалізації процесів управління культурою кібербезпеки підприємства збігаються із загальними етапами СУІБ (рис. 2.3).

На етапі *Планування*, який є першим кроком на шляху побудови СУІБ, головні завдання полягають у визначенні області дії СУІБ, у формуванні вихідних вимог до проєктування, збиранні даних про об’єкт захисту, з’ясуванні вимог державних та відомчих нормативних актів, визначенні правил та обмежень, які діють стосовно конкретного виду підприємств.

В рамках виконання цього етапу доцільно опрацювати питання щодо визначення початкового стану індивідуальної та групової культури інформаційної безпеки в середовищі персоналу підприємства.

Дієвим інструментом отримання первинної інформації є опитування персоналу [14, 16], яке здійснюється у зручний спосіб, наприклад, шляхом анкетування в електронному вигляді. Ключовими моментами методики опитування є формування змістовної частини анкет та методика їх подальшої обробки.

Досвід проведення практичних опитувань [17] свідчить, що для зручності аналітичної обробки анкет попередньо всі питання в них доцільно згрупувати за напрямами, наприклад:

1. Загальна особисте уявлення про правила кібербезпеки.

2. Особисте ставлення щодо правил і норм інформаційної безпеки.

3. Індивідуальна оцінка стану інформаційної безпеки в підрозділі.

4. Уявлення про цілі, задачі і стан безпеки на підприємстві.

Формулювання запитань в анкеті повинні виходи з наступних принципів:

– неупереджене ставлення до всіх і кожного;

– розуміння важливості особистого внеску в загальну справу кожного співробітника;

– поважне звернення ставлення до особистих думок, забезпечення відкритих відповідей для внесення пропозицій;

– створення умов для ініціатив співробітників в рамках опитування;

– залишення можливості для самооцінки співробітника.

Формування змістовної частини анкет доцільно корелювати з рекомендаціями відповіді на загальні питання запитання, що стосуються створення СУІБ, зокрема:

– чому інформаційна безпека важлива для підприємства?

– які загрози електронним сервісам, інформаційним ресурсам і активам більше всього викликають занепокоєння (витік комерційної таємниці, втрата даних через їх руйнування, шахрайство через інформаційні системи тощо)?

– які вимоги бізнес процесів підприємства потрібно враховуватися при побудові СУІБ?

– які цілі у термінах цілісності, конфіденційності й доступності необхідно досягти?

– який рівень ризику фінансових і матеріальних втрат в разі реалізації загроз інформаційної безпеки (кібербезпеки) є прийнятним для підприємства?

Зауважимо, що всі учасники опитування повинні читко розуміти і однаково тлумачити зміст використаних в анкетах термінів, тому застосування термінів

типу конфіденційність, цілісність, ризик тощо може бути припустимім для колективів, які переважно мають хоча б початковий рівень знань щодо змісту і завдань кібербезпеки.

З урахуванням зробленого зауваження, для успішного виконання етапу *Планування* в частині передбачає заходи щодо оцінки ризику, включаючи вибір методу оцінки ризиків і визначення прийнятного для підприємства, обов'язково мають бути проведені просвітницькі заходи (тренінги, семінари) для учасників цього етапу.

В ході цих заходів необхідно надати відповіді на такі базові питання щодо [7, 8]: сутності процедури ідентифікації ризиків; визначення ресурсів і активів що захищаються та їх власників; виявлення загроз для цінних ресурсів і вразливостей, завдяки яким можлива реалізація загроз; встановлення вірогідного впливу на конфіденційність, цілісність та доступність інформаційних ресурсів тощо.

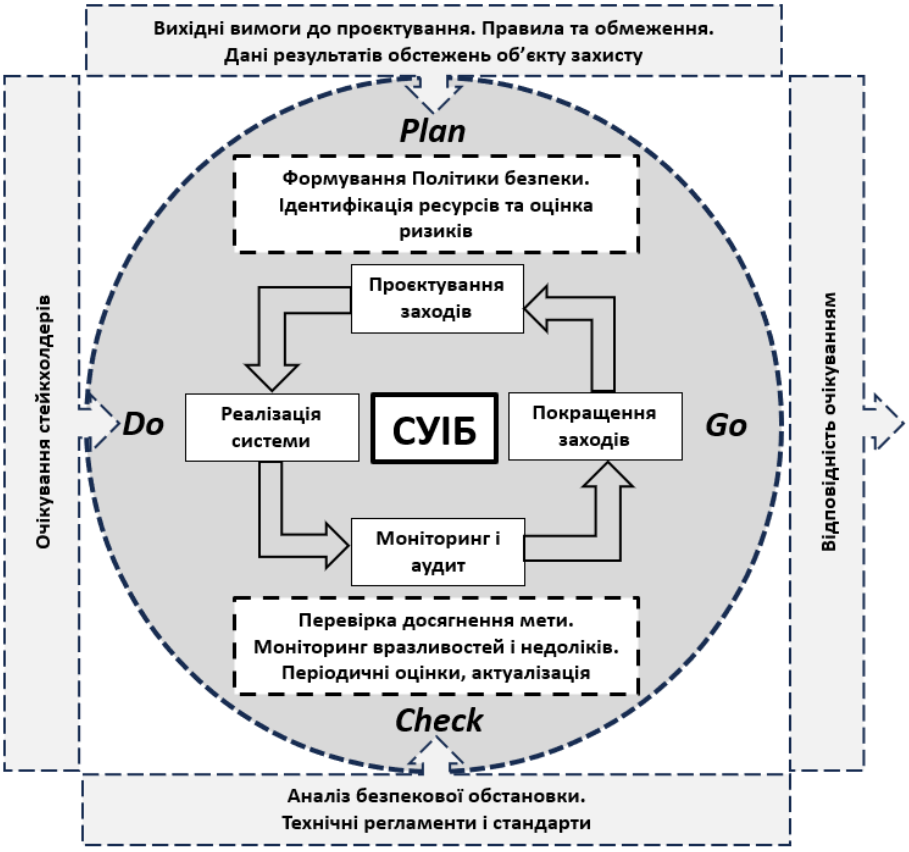

Рис. 2.3. Організаційна модель СУІБ

Етап побудови СУІБ – *Реалізація* – передбачає впровадження запланованих організаційно-технічних заходів та керування механізмами контролю. Для успішної реалізації цього необхідна наявність з одного боку – документованих процедур впровадження, планування й управління необхідними ресурсами, керування інцидентами безпеки, а також процедур навчання і інформування персоналу, який реалізовуватиме необхідні заходи, та користувачів інформаційної системи, що забезпечують автоматизовану підтримку виконання бізнес процесів підприємства.

На етапі побудови СУІБ – *Контроль* – здійснюються аналіз безпекової обстановки, перевірка досягнення мети, моніторинг вразливостей і недоліків, періодичні оцінки, актуалізація. Ця процедура вимагає від учасників найвищого рівня професійної підготовки, тому, за можливості, вона реалізується зовнішніми незалежними експертами.

На етапі – *Дії* – мають бути усунені виявлені на попередньої частині циклу вразливості, помилки та недоліки СУІБ, забезпечується та підвищується ефективність

Перелічені етапи деталізуються, за суттю, фундаментальною частиною побудови СУІБ – політикою інформаційної безпеки підприємства, під якою розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

Політика інформаційної безпеки визначає стратегію організації в області інформаційної безпеки, а також пріоритетність вирішення завдань і ресурси, що виділяються для цього. Політика інформаційної безпеки є джерелом вихідних даних для розробки часткових політик безпеки, що регулюють процедури таких основних складових системи інформаційної безпеки та кібербезпеки розмежування доступу, обліку подій в комп’ютерних системах, антивірусного захисту, шифрування і цифрового підпису, резервування і відновлення, реагування на інциденти в інформаційних системах.

Таким чином, незалежно від множини потенційних загроз безпеки та виду інформації, яка підлягає захисту, формування політики інформаційної безпеки завдяки:

– визначенню використовуваних нормативних документів і стандартів в області інформаційної безпеки та кібербезпеки, а також основних її положень щодо окремих безпекових процедур;

– визначенню правил управління ризиками: чи є достатнім базовий рівень захищеності або потрібно проводити повний варіант аналізу ризиків;

– оцінки відповідності стандартам в області інформаційної безпеки визначається потенційна ефективність цієї системи щодо протидії викликам і загрозам порушення конфіденційності, цілісності та доступності інформаційних активів підприємства.

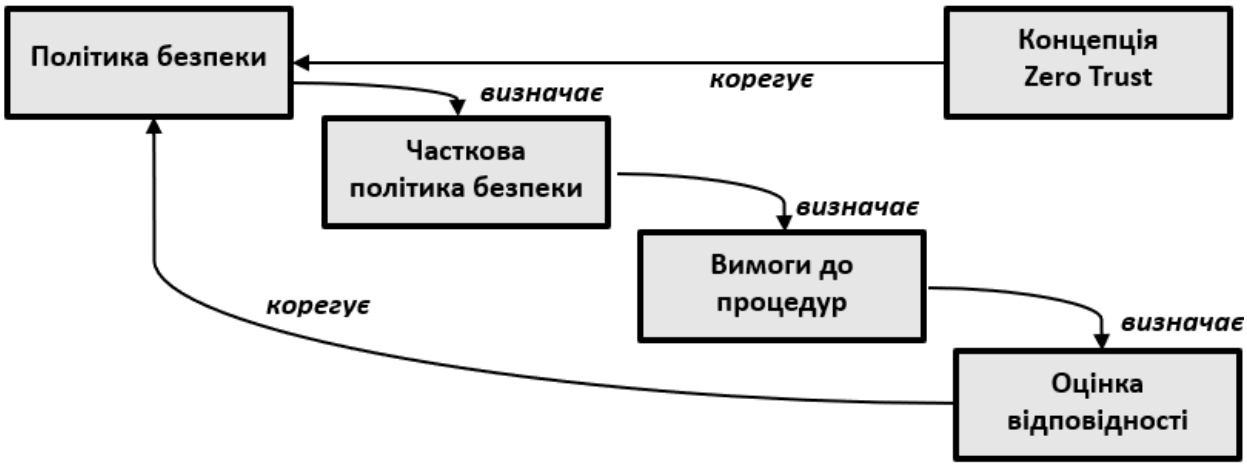

Рис. 2.4. Онтологічна модель формування вимог до системи управління інформаційної безпеки

Таким чином, відстежено ланцюги визначення вимог до процедур безпеки, що дало можливість сформувати онтологічну модель визначення та корегування вимог в СУІБ.

Процедури оцінки відповідності в онтологічній моделі виконують функцію арбітра в питанні чи вдалося досягти поставленої мети стосовно забезпечення інформаційної безпеки (кібербезпеки) або потрібне коригування політики інформаційної безпеки.

Концепція «повної недовіри» визначає додаткові умови щодо політики інформаційної безпеки, яка в свою чергу має визначити вимоги до часткових політик безпеки, які встановлюють правила та обмеження для створення системи захисту, включаючи підсистему управління культурою кібербезпеки підприємства.

Для побудови системи захисту інформації необхідно визначити границі системи, для якої повинен бути забезпечений режим інформаційної безпеки (границі СУІБ). Опис границь системи, виконується за наступним планом.

1. Структура організації. Опис існуючої структури й змін, які передбачається ввести у зв’язку з розробкою або модернізацією автоматизованої системи обробки даних.

2. Розміщення комп’ютерів і підтримуючої інфраструктури. Модель ієрархії засобів комп’ютерної техніки.

3. Ресурси інформаційних систем, що підлягають захисту. Рекомендується розглянути ресурси автоматизованої системи наступних класів: комп’ютери, дані, системне й прикладне програмне забезпечення. Усі ресурси мають бути оцінені, для оцінки обирається система критеріїв і методологія оцінок.

4. Технологія обробки інформації й розв'язувані завдання. Для цих завдань повинні бути побудовані моделі обробки інформації в термінах ресурсів.

Далі доцільно уточнити архітектуру системи управління кібербезпекою шляхом підвищення кіберкультури.

2.3. Базові завдання різних рівнів управління безпекою через підвищення кіберкультури

Звичайно на підприємстві розрізняють наступні категорії або рівні управління (менеджменту):

– стратегічне планування ‘strategic planning’ – це процес ухвалення рішень щодо цілей підприємства (організації), змін у цих цілях, ресурсів, які

використовуються для досягнення цих цілей, і політики, яка має керувати придбанням, використанням і розпорядженням цими ресурсами. Даної категорії відповідає стратегічний рівень управління;

– управлінський контроль ‘management control’ – це процес, завдяки якому керівники переконуються, що ресурси використовуються ефективно та результативне для досягнення цілей організації. Даної категорії відповідає так званий тактичний рівень управління;

– операційний контроль ‘operational control’ – це процес забезпечення ефективного та результативного виконання конкретних завдань. Цей процес реалізується на операційному рівні управління.

Виходячи з аналізу типових завдань, які потребують опрацювання на етапах створення та підтримки функціонування системи кібербезпеки організації [7, 8] в табл. 2.5 наведені базові завдання, що виконуються на різних рівнях управління та умови їх реалізації.

Таблиця 2.5

Базові завдання управління та умови їх виконання

Рівень управління Учасники	Базові завдання	Витрати	Термін реалізації

Стратегічне планування Власники ІС, топ менеджмент	1. Схвалення політики безпеки, визначення її цілей і завдань, виділення для їх вирішення фінансових, матеріальних і людських ресурсів. 2. Нормативне регулювання аспектів кібербезпеки. 3. Забезпечення фізичної безпеки. 4. Прийняття рішень щодо порядку роботи у умовах надзвичайного стану. 5. Виділення ресурсів для ліквідації наслідків кіберінцидентів. **6. Визначення секторів відповідальності та затвердження функціональних обов'язків, зокрема, в плані забезпечення кібербезпеки.** **7. Організація вивчення рівня кіберкультури установи та проведення незалежних аудитів стану кібербезпеки.** **8. Оцінка поточного стану кіберкультури та прийняття рішень щодо вжиття додаткових заходів.** **9. Організація заходів щодо навчання і виховання персоналу, його мотивації.** **10. Організація та керівництво проведенням кібернавчань.**	Великі (придбання основних засобів + навчання і утримання персоналу + роботи зовнішніх виконавців)	Трив.
Управлінський контроль Адміністратори безпеки	1. Оцінка ефективності та результативності використання ресурсів для досягнення цілей організації. 2. Формування концепції захисту, управління системою розмежування доступу, визначення повноважень операторів безпеки та прав доступу користувачів. 3. Реалізація оцінки і аудиту безпеки інформаційних систем. 4. Моніторинг і оцінка поточного стану загроз для інформаційних системи. 5. Планування роботи в умовах надзвичайного стану. 6. Управління відновлювальними заходами. 7. Аналіз трендів загроз та розробка сценаріїв протидії вірогідним атакам. **8. Моніторинг рівня підготовки та навчання операторів безпеки і користувачів системи.** **9. Тренінги чергових змін, команд швидкого реагування.**	Середні (утримання)	Серед.
Операційний контроль Оператори безпеки	1. Керування апаратними и програмними засобами захисту, включаючи їх інсталяцію, ініціалізацію, налаштування і обслуговування. 2. Проведення відновлювальних робіт після інцидентів.	Середні (утримання+ витратні матеріали)	Корот.

Можливо звернути увагу, що на стратегічному рівні левову частину базових завдань становлять питання що безпосередньо або опосередковано стосуються підвищення та контролю стану кіберкультури організації.

2.4. Вдосконалення моделі формування системи кібербезпеки

Результати вивчення та порівняння сучасних підходів до побудови систем кібербезпеки [18] дозволяють узагальнити існуючи засади створення моделі формування системи та дещо їх вдосконалити. Внаслідок визначеного запропоновано

Модель формування системи кібербезпеки (рис. 2.5), яка з одного боку визначає умовні межі різних рівнів управління, з іншого враховує особливості формування та функціонування підсистеми кадрового забезпечення кіберкультури.

Рис. 2.5. Модель формування системи кібербезпеки

Зокрема, модель враховує три регуляторних впливи на підсистему кадрового забезпечення кіберкультури, а саме:

– R1 – висновки за результатами обстежень та аудитів об’єктів інформаційної діяльності та середовищ інформаційних систем;

– R2 – вимоги щодо побудови підсистем кіберзахисту;

– R3 – вказівки, доручення та інші дії організаційно-просвітнього характеру з боку керівного складу організації.

Підсумовуючи викладене, можливо зазначити, що визначити деталі побудови як системи кіберзахисту в цілому, так її окремих підсистем (на рис. 2.4 їх налічує чотирнадцять) можливо тільки за умов проведення системного аналізу реального проєкту інформаційної мережі об’єкту критичної інфраструктури та обстеження всіх ключових об’єктів інформаційної діяльності щодо як впроваджуються заходу з кіберзахісту.

Зауважимо, що в випадку побудови інформаційної мережі на основі технології корпоративної хмари, доступ до хмари повинен здійснюватися за допомогою захищених каналів (наприклад, за допомогою VPN) [19]. Тому концентрація основних сервісів безпеки в хмарі поділяється між клієнтами та провайдером сервісних послуг, що знижує матеріальні, фінансовий та організаційні втрати на забезпечення кіберзахисту.

У випадку підприємства, яке має статус державного або обробляє державні інформаційні ресурси, пріоритетними процедурами системи захисту інформації згідно [8] вважаються технології, що реалізуються підсистемами: *автентифікації* і *ідентифікації*, *розмежування доступу*, *антивірусного захисту*, *обліку подій*, *копіювання* і *резервування, шифрування трафіка* і *цифрового підпису,* а також захисту периметра.

Побудова захищеної розподіленої корпоративної мережі що має логічне або фізичне з’єднання з глобальною мережею повинна враховувати тенденції розвитку стану безпеки у кіберпросторі та виходити з системного аналізу трендів розвитку кіберінцидентів в світі.

Наступний аналіз трендів розвитку кіберінцидентів побудований на матеріалах провідних компаній в сфері кібербезпеки, які публікують власні статистичні дані.

2.5. Підходи щодо оцінки рівня культури кібербезпеки в інформаційній системі

У попередніх розділах визначено, що в багатьох випадках недостатньо враховуються проблеми аналізу сукупності факторів, пов’язаних з людино-машинною взаємодією – культури кібербезпеки та інформаційної системи.

Одним з актуальних завдань, які вирішуються адміністраторами систем управління кібербезпекою, є оцінка ефективності впроваджених заходів щодо забезпечення основних функцій інформаційної системи. При цьому інформація про результати проведених дій може мати не тільки кількісний, але і якісний характер. Оцінка культури кібербезпеки інформаційних систем підприємств, організацій тощо в даний час мало формалізована і проводиться, в основному, за допомогою оцінки ризиків [20]. Слід також зазначити, що основна увага кібербезпеці організацій та їх інформаційних систем приділяється окремо технічним та організаційним аспектам. Крім того, аналіз досліджень у сфері кібербезпеки інформаційних систем показав, що існує проблема формалізації оцінки рівня культури кібербезпеки, оцінки його складових, оцінки динаміки загального рівня культури кібербезпеки окремих його складових тощо.

Тому важливо формалізувати процеси оцінки культури кібербезпеки на основі розробки комплексної моделі з урахуванням технічних і організаційних параметрів інформаційної системи та пов'язаних з ними ризиків [21].

В роботі [3] дано визначення поняття кібербезпеки стосовно об’єктів критичної інфраструктури в атомній енергетиці. Охоплено апаратно-технологічні складові кібербезпеки системи, а також комплекс параметрів, що характеризують вплив людського фактора на культуру кібербезпеки в процесі внутрішньої та

зовнішньої діяльності. В основу аналізу культури кібербезпеки покладено виявлення окремих компонентів ризиків безпеки системи і загального ризику [22]. При цьому ваги окремих складових не виділяються, оцінка дії управлінських рішень по ним, динаміки загального показника і його складових не проводиться.

Моделі культури інформаційної безпеки, представлені в [23], виділили 16 інструментів вимірювання культури кібербезпеки. Автори відзначають, що не існує перевіреного і загальноприйнятого інструменту, який можна було б використовувати в різних галузях і організаціях. Більшість розглянутих інструментів використовують тільки кількісний метод; Однак культура безпеки включає дуже різні сфери, і тому слід використовувати змішаний підхід.

Спроба узагальнити підходи до визначення рівня культури кібербезпеки запропонована в роботі [24]. Запропоновано розробку стандартів визначення факторів культури кібербезпеки, оцінки їх ризиків тощо. Але немає єдиної моделі оцінки культури кібербезпеки на їх основі.

В роботі [25] розроблена нечітка модель комплексної оцінки рівня культури інформаційної безпеки організації з урахуванням особливостей людино-машинної взаємодії. Модель дозволяє оцінити культуру кібербезпеки тільки поточний стан системи, ґрунтуючись на моделях нечіткої логіки, в яких набори правил формуються суб’єктивно, в залежності від запитів і потреб експертів або осіб, які приймають рішення.

Таким чином, виникає завдання створення узагальненої математичної моделі визначення комплексного показника культури кібербезпеки з урахуванням масивів факторів/загроз, оцінки їх внеску в загальний показник і оцінки динаміки після реалізації відповідних управлінських рішень.

2.6. Формалізована модель оцінки культури кібербезпеки

Однією з актуальних завдань, що стоять перед адміністраторами систем управління, є оцінка стану безпеки, її динаміки і динаміки її складових, а також ефективності впроваджених заходів.

При цьому інформація про результати оцінки та зміни стану кібербезпеки системи може бути не тільки кількісною, але й якісною [26–29].

Розглянемо інформаційну систему в якийсь момент часу $t \in [0,T]$. Припустимо, що в даний момент часу ми спостерігаємо N кластерів характеристик станів системи безпеки $Q_1(t), Q_2(t), \ldots, Q_N(t)$, де $N > 2$.

Аналізуємо ідеалізований випадок стану системи. А саме, будемо вважати, що ці кластери не перетинаються парами, є некорельованими і вносять однаковий внесок в загальну оцінку кібербезпеки інформаційної системи.

Будемо також вважати, що *i*-й кластер містить m_i елементів, які можна спостерігати за поліноміальною схемою розподілу ймовірностей де $(p¿¿i1(\tau), p_{i2}(\tau), \ldots, p_{iM_i}(\tau))¿$. $\tau \in [0,T]$ і $p_{i1}(\tau)+p_{i2}(\tau)+\ldots+p_{iM_i}(\tau)=1$.

Також слід зазначити, що розподіл ймовірностей може змінюватися в дискретні моменти τ.

Зміна розподілу ймовірностей може відбуватися внаслідок організаційної (в тому числі навчальної) діяльності підприємства з персоналом інформаційної системи, який має доступ до критичних ресурсів (користувачами, операторами, обслуговуючим персоналом тощо).

Існує проблема кількісної оцінки зміни (оцінки параметрів тренду) антропогенного фактору системи безпеки після заходів, вжитих на основі кластерів

Припустимо, що кластер характеристик безпеки описується одиницею:

$$Q_i(t) = \left\langle k_{ij}, p_{ij}(t) \right\rangle, j \in [1, M_i], i \in [1, N], \tag{2.7}$$

де M_i – кількість елементів в наборі;

$p_{ij}(t)$ – ймовірність прояву фактору #j, (наприклад, фактор *#j* може означати, що випадково обраний співробітник завжди відкриває заявку в електронному листі від невідомого відправника);

k_{ij} – деякий коефіцієнт, пропорційний тяжкості наслідків для кібербезпеки системи в разі прояву фактору *#j*. У цьому випадку, якщо фактор #j має більш серйозні наслідки для безпеки, ніж фактор #l, то ми припускаємо, що існує сувора нерівність $k_{ij} > k_{il}$.

Для всіх кластерів існує вираз:

$$k_{i1} + k_{i2} + \ldots + k_{\Im_i} = S, \forall i \in [1, N], \tag{2.8}$$

де S – ціле число, діапазон рейтингової шкали.

Функцію W середньої ваги кластера в загальному показнику рівня загроз інформаційній системі можна визначити як лінійну адитивну функцію виду:

$$W_i(t) = W(Q_i(t)) = \sum_{j=1}^{M_i} k_{ij}\, p_{ij}(t) \cdot M_i \tag{2.9}$$

або

$$W_i(t) = W(Q_i(t)) = \sqrt{\sum_{j=1}^{M_i} k_{ij}\, p_{ij}^2(t)} \cdot M_i \tag{2.10}$$

Для випадку рівномірного розподілу у випадку визначення (2.3) маємо:

$$p_{i1} = p_{i2} = \ldots = p_{iM_i} = \frac{1}{M_i}, \tag{2.11}$$

а потім

$$W_i(t) = M_i \cdot \sum_{j=1}^{M_i} k_{ij} \frac{1}{M} = \sum_{j=1}^{M_i} k_{ij} = S, \tag{2.12}$$

У випадку визначення (4) маємо:

$$W_i(t) = M_i \cdot \left(\sum_{j=1}^{M_i} k_{ij}\, p_{ij}^2(t) \right)^{\frac{1}{2}} = M_i \cdot \frac{1}{M_i} \cdot \left(\sum_{j=1}^{M_i} k_{ij} \right)^{\frac{1}{2}} = \sqrt{S}. \tag{2.13}$$

Таким чином, в обох визначеннях в точках максимальної ентропії [5] значення вагової функції не залежать від різних елементів в кластері.

Висновки до розділу 2

1. Сучасні практичні публікації щодо стану кібербезпеки у світі містять великі обсяги статистичних даних з відносно тривіальною аналітикою кількісного характеру типу «зросло на кілька процентів», «збільшилась загальна кількість

випадків» тощо. Подібні огляди дають недостатньо інформації щодо системного аналізу перспектив розвитку подій в кіберпросторі як в стратегічному аспекті так і на короткострокову перспективу. В цьому сенсі запропоновані в розділі математичні підходи та проведений аналіз трендів загроз кібербезпеки в цивільному секторі надають можливість сформулювати пріоритети політики безпеки на основі концепції zero-trust в частині забезпечення конфіденційності та цілісності інформаційних активів підприємства.

Запропоновані математичні методи несуттєво залежать від методів формування вихідних статистичних інформаційних масивів та можуть бути використані для оперативного відстежування трендів розвитку подій в кіберпросторі.

2. Адекватність рівня професіоналізму персоналу та його навичок та умінь набувають особливого значення в плані управління кібербезпекою шляхом підвищення кіберкультури персоналу. Це потребує формування у менеджменту безпеки підприємства реального розуміння щодо необхідності внесення коригуючих змін у політику безпеки та вжиття заходів щодо відповідного навчально-тренувального процесу на підприємства. У цьому розумінні питання оперативної оцінки поточного стану кіберкультури є ключовим в плані відповідності політики безпеки концепції zero-trust.

Тому в дослідженні подальшого розвитку набула методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що сукупно з методикою оцінки трендів загроз кібербезпеки дає можливість оперативного реагування з боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

3. Логічним кроком у дослідженні стало визначення базових завдань різних рівнів управління кібербезпекою через підвищення кіберкультури та уточнення моделі формування системи кібербезпеки виходячи з визначених завдань.

4. Формалізована модель оцінки рівня культури кібербезпеки в інформаційній системі дає можливість коректної обробки даних анкетування персоналу та формування висновків щодо її покращення.

5. З урахуванням отриманих в поточному розділі результатів щодо заходів політики безпеки організаційного характеру в наступному розділі уявляється приділити основну увагу організаційно-технічні положенням політики безпеки підприємства на основі концепції zero-trust.

Список використаних джерел у розділі 2

1. Positive Technologies. (2023). Cybersecurity Threatscape: 2022 Rundown. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2022/?sphrase_id=264584

2. Positive Technologies. (2021). Cybersecurity threatscape: Q4 2020. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q4/?sphrase_id=264606

3. Riskrecon. (2023). White Paper: Five Lessons Learned from Over 1000 Ransomware Attacks. https://www.riskrecon.com/report-five-lessons-learned-from-ransomware-attacks

4. Efimova, Y., Gavrilov, A., & Svirina, A. (2019). Data Driven Cyber-Security Corporate Systems: Development and Implementation. In 34th International-Business-Information-Management-Association (IBIMA), 6768–6775.

5. Korn, G. A., &Korn, T. M. (2013). Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review. Courier Corporation.

6. Euronews. (2020). Не тільки коронавірус: головні події 2020. https://ru.euronews.com/2020/12/30/year-2020-events

7. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги

8. ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.

9. Shojaie, B., Federrath, H., & Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. In 10th International Conference on Availability, Reliability and Security, 159–167. https://doi.org/10.1109/ares.2015.25

10. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

11. Aviad, A., & Węcel, K. (2019). Cyber Treat Intelligence Modeling. In Business Information Systems, 361–370. https://doi.org/10.1007/978-3-030-20485-3_28

12. ДСТУ EN ISO 9001:2018. Системи управління якістю. Вимоги.

13. Basir, S. A., Davies, J., & Rudder, A. (2011). The Elements of Organizational Culture which Influence the Maintenance of ISO 9001: A Theoretical Framework. African Journal Business Management, 5(15), 6028–6035.

14. Britvic, J., Grebenar, V., & Jakupec, G. (2017). Influence of the new Standards ISO 9001:2015 and ISO 9001:2015 on Human Resource Management in Organization. In International Conference on Interdisciplinary Management Research, 13, 1268–1278.

15. Hall, J. L., & Rao, A. (2020). Non-Technical Skills Needed by Cyber Security Graduates. In IEEE Global Engineering Education Conference (EDUCON), 354–358. https://doi.org/10.1109/educon45650.2020.9125105

16. Sanchez-Lizarraga, M. A., Limon-Romero, J., Tlapa, D., Baez-Lopez, Y., Puente, C., Puerta-Sierra, L., & Ontiveros, S. (2020). ISO 9001 Standard: Developing and Validating a Survey Instrument. IEEE Access, 8, 190677–190688. https://doi.org/10.1109/access.2020.3029744

17. Baylon, C., Brunt, R., & Livingstone, D. (2015). Cyber Security at Civil Nuclear Facilities Understanding the Risks (Charity Registration No. 208223). The Royal Institute of International Affairs.

18. Кононович, І., Маєвський, Д., & Подобний, Р. (2015). Моделі системи забезпечення кібербезпеки із запізнюванням реагування на інциденти. Інформатика та математичні методи в моделюванні, 5(4), 339–346.

19. Соколов, В., & Карацюба, К. (2012). Використання дерев атак для аналізу захищеності безпроводових технологій стандарту IEEE 802.11. Вісник ДУІКТ, 10(1), 42–49.

20. Літвінчук, І., Корчомний, Р., Коршун, Н., & Ворохоб, М. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112

21. Соколов, В. (2010). Кількісні показники оцінювання захищеності і ризиків від порушення безпеки у розподілених системах рухомого зв’язку. Захист інформації, 3(48), 19–34. https://doi.org/10.18372/2410-7840.12.1957

22. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. Encyclopedia, 1(3), 602–617. https://doi.org/10.3390/encyclopedia1030050

23. Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the Security Culture in Organizations: A Systematic Overview of Existing Tools. Security Journal, (34), 340–357. https://doi.org/10.1057/s41284-020-00228-4

24. Seeba, M., Matuleviˇcius, R., & Toom, I. (2021). Development of the Information Security Management System Standard for Public Sector Organisationsin Estonia. In 24th International Conference on Business Information Systems, 355–366.

25. Войцеховська, М. (2020). Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації. Національний університет «Чернігівська політехніка».

26. Solic, K., Ocevcic, H., & Golub, M. (2015). The Information Systems’ Security Level Assessment Model based on an Ontology and Evidential Reasoning

Approach. Computers & Security, 55, 100–112. https://doi.org/10.1016/j.cose.2015.08.004

27. Скітер, І., & Ворохоб, М. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158–169. https://doi.org/10.28925/2663-4023.2021.13.158169

28. Shkarlet, S., Dorosh, M., Druzhynin, O., Voitsekhovska, M., & Bohdan, I. (2021). Modeling of Information Security Management System in the Project. Advances in Intelligent Systems and Computing, 1265, 364–376. https://doi.org/10.1007/978-3-030-58124-4_35

29. Han, Q., & Yang, D. (2018). Hierarchical Information Entropy System Model for TWfMS. Entropy, 20(10), 1–20. https://doi.org/10.3390/e20100732

РОЗДІЛ 3
КЛЮЧОВІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ПОЛОЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ КОНЦЕПЦІЇ ZERO-TRUST

3.1. Вдосконалена модель загроз безпеки на основі концепції zero-trust

Створення складних систем інформаційної взаємодії та управління структурними підрозділами організації, яка є об’єктом критичної інфраструктури або забезпечує прийняття критично важливих рішень в інтересах суспільства або держави [1] потребує розв’язку низки складних завдань, зокрема, визначення архітектури СУІБ та застосовних в ней механізмів захисту інформаційних ресурсів [2].

Відповідно до вимог нормативних документів [3] вихідними даними для розробки Політики інформаційної безпеки є результати обстеження об’єктів інформатизації та розроблення моделі загроз та моделі порушника. У зв’язку з поширенням технологій хмарних сервісів та аналізом потенційних можливостей порушників безпеки [4, 5] набувають актуальності дослідження та розробки методів побудови систем захисту інформації з урахуванням положень концепції zero-trust, інакше – моделі «повної недовіри».

В якості моделі безпеки zero-trust [6] запропонована відомим аналітиком Дж. Кіндервагом в 2010 році. З того часу ця модель набула значної популярності серед експертів як ефективна концепція забезпечення кібербезпеки [7].

Аксіомою концепції zero-trust є відсутність довіри до будь-якого суб’єкта і об’єкта (пристрою) інформаційної системи, навіть якщо вони перебувають у середині контуру безпеки. За суттю, модель передбачає, що для кожного випадку звернення до ресурсу системи всередині або зовні контуру безпеки, кожен користувач або пристрій повинні підтверджувати власні ідентифікаційні дані.

Викладене актуалізує завдання дослідження та побудови ефективних рішень, що підвищують рівень кібербезпеки інформаційних систем державного рівня в умовах збройної агресії та потужних кібератак на критичну інфраструктуру.

Базовими механізмами захисту інформаційних ресурсів в комп'ютерних системах традиційно є процедури ідентифікації суб'єктів, процесів і об'єктів цих систем, авторизація суб'єктів та управління доступом суб'єктів та процесів до об'єктів згідно з визначеною Політикою безпеки. Належним чином ідентифікована та автентифіковані суб'єкти та процеси отримують на основі правил розмежування доступу право на читання інформації (отримання даних) з певного її носія та/або запис (передачу) деякої інформації на носій, або запуск в системі обчислювального процесу (програми).

В умовах початкового уявлення про порушника інформаційної безпеки переважно (іноді, навіть, виключно) як сторонньої по відношенню до системи особи підсистема авторизації та управління доступом 'identity & access management' (IAM) замислювалася як централізований механізм для обмеження доступу до ресурсів системи та контролю за ним на основі надання дозволів користувачам або групам користувачів. Метою функціонування IAM спочатку було надання прав, а не контроль, а доступ повністю ґрунтувався на реєстрації в IAM умовного імені користувача (логіна) та пароля у поєднанні з членством у групі чи дозволами, що визначають право скористатись тим чи іншим ресурсом [8].

Пізніше ця модель зазнала різних модифікацій з метою:

– посилення надійності і ефективності процедур ідентифікації і автентифікації, зокрема, шляхом впровадження їх багатофакторної побудови;

– конкретизації повноважень користувачів і менеджменту безпеки, при цьому деталізація рішення щодо умов надання доступу в системі відбувалась централізовано в таких органах управління як служба або інфраструктура ідентифікації.

З часом, як було зазначено раніше, ландшафт вірогідних загроз суттєво змінився, і сьогодні поняття потенційного порушника включає не тільки

конкретну особу, а й деякий альянс осіб, які можуть ситуативно або системно діяти для досягнення певної зловмисної мети, що може бути визначена в термінах порушення конфіденційності, цілісності та доступності інформації. Нині нерідко спостерігаються випадки, коли спочатку лояльні до роботодавця співробітники згодом з різних мотив починали діяти на користь його конкурентів або зловмисників, коли виходячи корисливих спонукань відповідальні особи починають діяти всупереч норм корпоративної етики і моралі для власного збагачення.. Застосування для доступу до інформаційних систем мобільних пристроїв, включаючи ноутбуки, планшети, смартфони підвищує ризики їх втрат та крадіжок, що утворює підґрунтя для реалізації несанкціонованого доступу до цих систем завдяки доступу зловмисників до апаратної ї програмної платформи, а також критичної інформацій, яка може зберігатись на цьому пристрої [9].

Зважаючи на те, що IAM є ключовим механізмом будь-якої моделі розмежування доступу до ресурсів системи, та виходячи з необхідності його постійного вдосконалення і розвитку для забезпечення спостережності подій в комп'ютерних мережах уявляється доцільним з'ясувати вразливості існуючих рішень щодо побудови цієї системи.

Для цього, на підставі аналізу публікацій та повідомлень у засобах масової інформації про інциденти та негативні явища в комп'ютерних системах розроблена описове доповнення моделі загроз безпеки з урахуванням концепції zero-trust (табл. 3.1, рис. 3.1).

Таблиця 3.1

Часткова модель загроз згідно концепції zero-trust

Роль	Точка доступу	Небезпечні дії	Співвідношення рівень *SC* – ймовірність загрози *P*
Відправник (*sender*)	Своє АРМ або АРМ колеги	S1. Помилкове порушення політики безпеки	$\uparrow SC \Rightarrow \downarrow P_з$ *
		S2. ВІДМОВА щодо відправлення даних	Залежить від мотивації
		S3. МАСКАРАД / видача себе за іншу особу	Залежить від мотивації

		S4. ЗМОВА із зловмисником	$\uparrow SC \underset{\rightarrow}{Prob} \downarrow P_з$ **
Отримувач (*recipient*)	Своє АРМ або АРМ колеги	R1. Помилкове порушення політики безпеки	$\uparrow SC \Rightarrow \downarrow P_з$
		R2. ВІДМОВА щодо отримання даних	Залежить від мотивації
		R3. МАСКАРАД / видача себе за іншу особу	Залежить від мотивації
		R4. ЗМОВА із зловмисником	$\uparrow SC \underset{\rightarrow}{Prob} \downarrow P_з$
		R5. МОДИФІКАЦІЯ отриманих даних	–
		R6. ПІДРОБКА / створення фіктивних даних	–
Провайдер (*provider*)	АРМ безпеки (адміністратор)	P1. Ненавмисні (помилкові)дії	$\uparrow SC \Rightarrow \downarrow P_з$
		P2. ЗМОВА із зловмисником	$\uparrow SC \underset{\rightarrow}{Prob} \downarrow P_з$
Зловмисник (*intruder*)	Легальне АРМ або власний засіб	I1. ПЕРЕХОПЛЕННЯ змісту даних I2. МОДИФІКАЦІЯ перехоплених даних I3. ПІДРОБКА / створення фіктивних даних I4. МАСКАРАД / видача себе за іншу особу I5. ПОВТОР перехопленого повідомлення I6. ПІДБУРЕННЯ до незаконних дій	–

* $\uparrow SC \Rightarrow \downarrow P_з$ – означає що в загальному випадку підвищення рівня індивідуальної кіберкультури сприяє зниженню ймовірності реалізації загрози;

** $\uparrow SC \Rightarrow \downarrow P_з$ – означає що внаслідок реалізації заходів з підвищення рівня корпоративної кіберкультури можуть бути виявлені ознаки ризику реалізації кіберзагрози.

Запропонована модель робить більш очевидними потенційні вразливості існуючих рішень щодо побудови підсистем ІАМ:

– одноразова процедура автентифікації може бути використана іншими користувачами або зловмисником. Зокрема, у випадку, якщо процедури ІАМ виконані, а легальний користувач з певних причин залишив робоче місце, подальші дії зловмисника обмежуються лише можливістю входу, контрольовану територію і визначеними для конкретного користувача правами доступу;

– відкрито застосовані логіни користувачів можуть бути використані зловмисником для аналізу трафіка в інформаційній мережі, який в певних застосуваннях, навіть без розкриття його змісту, може становити значний інтерес для отримання розвідувальної інформації;

– процедури ідентифікації і автентифікації сприймаються як логічні предикати, що можуть мати значення лише значення «істина» (true) або «хиба» (false). Насправді, переважна більшість процедур при цьому носить ймовірнісний характер Реальне виконання або не виконання умов авторизації завжди має ймовірнісний характер. Наприклад, користувачі достатньо часто помиляються під час набору реально стійкого паролю, його зчитування з носія може супроводжуватись збоєм або помилкою, біометричні процедури взагалі виконується з певною ймовірністю помилки;

– користувачі, що мають доступ до декількох систем (включаючи власні комп'ютери), зазнають проблеми з надійним збереженням складних стійких паролів, які мають значну кількість букв, цифр та інших символів.

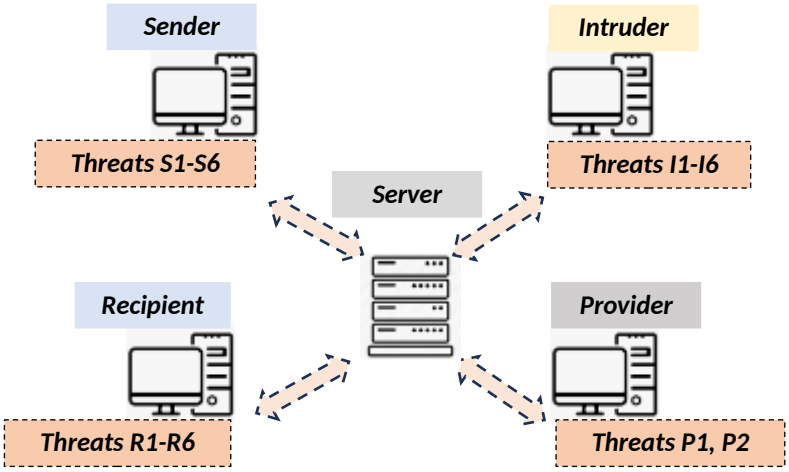

Рис. 3.1. Візуалізація моделі загроз згідно концепції zero-trust

Застосування звичайних компактних флеш носіїв для збереження критичної інформації звичайно не покращує безпекову ситуацію, оскільки незахищені носії паролів та інших чутливих даних дуже часто залишаються користувачами системи без дієвого контролю та, іноді, взагалі губляться.

Вартість же захищених носіїв доволі велика, що може суттєво обтяжувати бюджет власника великої інформаційної системи.

З метою покращення безпекової ситуації та нейтралізації існуючої вразливостей доцільно розглянути низку рішень, що можуть бути реалізовані без значних капітальних вкладень.

1. Політикою безпеки повинен бути визначений гранично припустимий час дійсності процедури автентифікації, звернення до більш чутливих даних потребує нової автентифікації. Частота автентифікація суб'єктів інформаційного обміну та використовуваних пристроїв на основі їх облікових даних має бути інструментом реагування на інциденти в системі: у випадку зростання кількості інцидентів в системі припустимий час дії з попередньою автентифікацією повинен скорочуватись.

2. Політика безпеки повинна максимально обмежувати надання доступу до ресурсів, дозволяючи доступ лише до необхідної інформації та пристроям.

3. Джерелом прийняття рішень менеджментом безпеки має бути об'єктивна інформація про стан роботи ІАМ. З метою аналізу та прийняття рішень щодо проведення тестування або модернізації ІАМ, додаткових тренінгів з персоналом або обмеження прав доступу до критичних ресурсів певним особам загальна статистика помилок автентифікації кожного учасника інформаційного обміну повинна накопичуватися протягом визначеного проміжку часу (місяць, квартал, рік).

4. Логіни доступу суб'єктів інформаційних відносин повинні зберігатись як службова інформація, а для їх приховування доцільно застосування криптографічних або стеганографічних протоколів.

5. Для підвищення рівня безпеки процедур автентифікації доцільно застосовувати фактори особистості співробітника, які не потребують застосування складних біометричних технологій.

Зокрема, така автентифікація може забезпечуватись шляхом впізнання голосу «диктора», що зачитує визначену на екрані монітора послідовність чисел. При цьому програмний засіб на основі еталонних даних про голос кожного користувача та відомих математичних алгоритмів їх обробки [10] може розраховувати меру належності тестового повідомлення всім потенційним

учасникам процедури автентифікації. А це суттєво скоротить кількість бажаючих випробувати свої акторські здібності.

6. Для переключення IAM в режим автентифікації доцільно використовувати картки користувачів, що реалізують технології безконтактного підключення, Зокрема, це може бути достатньо проста і ефективна технологія RFID.

3.2. Визначення вимог до безконтактного апаратного засобу автентифікації

Виходячи з побудованої моделі загроз визначимо основні функціональні та ергономічні вимоги до HAD, з урахуванням системних вимог до побудови центру кібербезпеки критичної інфраструктури [2], а саме:

– безконтактне підключення до засобів контролю доступу;

– невеликі малогабаритні характеристики;

– малий рівень електроспоживання;

– зручність застосування для автентифікації різних видів доступу, включаючи прохід в приміщення підвищеної безпеки, двофакторна автентифікація користувачів в інформаційній системі тощо;

– можливість багаторазового застосування та перепрограмування параметрів;

– фізичний захист від несанкціонованого доступу до даних, які зберігаються в HAD;

– накопичення даних поточної активності в системі, включаючи спроби доступу до ресурсів с порушенням визначених правил, облік фактичного часу доступу до ресурсів системи тощо;

– створення сеансового ключу шифрування для віддаленого доступу до ресурсів. Кожен блок даних, що надсилається одним з учасників освітнього іншому має бути захищений за допомогою коду автентифікації повідомлень;

– шифрування конфіденційних даних за допомогою ключа симетричного алгоритму, який генерується та зберігається в HAD без можливості його

вилучення. Для розшифрування даних має бути передбачена процедура відновлення ключа (recovery) на основі 2-х ключів з 3-х певної множини ключів, власниками яких є персонал системи;

– формування/перевірка електронного підпису власника HAD та перевірка підпису посадових осіб за наявності сертифікату відкритого ключа. Кожен документ, що зберігається в HAD, має бути підписаним його власником та адміністратором безпеки).

Раціональним рішенням реалізації в HAD безконтактного методу передачі автентифікаційних даних може бути використання стандартизованих на поточний час радіо інтерфейсів типів Bluetooth, WiFi та RFID.

При цьому задача створення HAD з усіма переліченими вище елементами полягатиме у виборі серед сукупності можливих такого варіанту системи ідентифікації, який забезпечив би надійну її роботу із заданою якістю при мінімальних капітальних та експлуатаційних витратах.

Найважливішою складовою частиною зазначеної системи ідентифікації є її первинний вимірювальний перетворювач (ПВП). ПВП повинен мати високу швидкодію, бути чутливим до первинного інформативному параметру та забезпечувати стабільність характеристик в умовах впливу дестабілізуючих факторів [11, 12]. Зазначені характеристики тісно взаємопов’язані.

При цьому поліпшення однієї призводить, як правило, до погіршення інших. Так, підвищення точності вимірювання інформативного параметра сприятиме зниженню швидкодії, і навпаки, при підвищенні швидкодії ПВП знижується точність вимірювання. Оскільки точність – це категорія економічна (тобто, чим точніше вимірюється інформативний параметр, тим ефективніше отримана інформація може бути використана, однак вартість її отримання зростає), при створенні системи ідентифікації HAD необхідно вирішувати компромісну задачу вибору оптимальних співвідношень усіх, перелічених вище параметрів.

Можливими методами її вирішення є [13]:

– математичне моделювання системи ідентифікації HAD. Його перевага полягає в можливості проведення оцінювання статичних та динамічних

характеристик таких систем [14]. Обмеженість обумовлена тим, що ступінь достовірності моделей залежить від практичного та теоретичного досвіду їх розробників;

– формування та дослідження узагальнених показників системи ідентифікації HAD з використанням графоаналітичного методу, методу «прогресуючого еталону» тощо. Перевага цих методів полягає в можливості урахування великої кількості часткових показників єдиною числовою характеристикою – узагальненим показником, що дає можливість достатньо просто проводити порівняльне оцінювання таких систем. Обмеженість пов'язана з тим, що ці методи не враховують деякі економічні та виробничі фактори;

– застосування експертних методів оцінювання, що базуються на використанні узагальненого людського досвіду – «колективної мудрості».

При цьому саме методи експертних оцінок вважаються визначальними при вирішенні складних завдань оцінювання та вибору будь-яких об’єктів, при аналізі та прогнозуванні ситуацій з великою кількістю значимих факторів. Їх застосовують, як правило за умови, що «…вибір, обґрунтування та оцінювання результатів рішень не можуть бути виконані на основі точних розрахунків.

Це забезпечує активну й цілеспрямовану участь фахівців на всіх етапах прийняття рішень, що уможливлює суттєве підвищення їхньої якості й ефективності» [13]. Експертні методи дають можливість більш глибоко вивчити явища, які слабко піддаються вивченню іншими методами, а також виявити найбільш важливе та істотне, не опускаючи тих деталей і взаємозв’язків, без яких не може бути побудована модель досліджуваної проблеми.

Основними недоліками методів є суб'єктивізм думок експертів у відшукуваних оцінках та обмеженість їхніх суджень. Головна перевага зазначених методів, враховуючи незначні вимоги щодо наявності апріорної інформації про об'єкт дослідження, полягає у відносній простоті та зручності застосування для прогнозування практично будь-яких ситуацій.

Головним показником для оцінки якості системи ідентифікації HAD експерти вважають, як правило, достовірність результатів ідентифікації. Вона виражається

ймовірністю правильної ідентифікації HAD. Правомірність імовірнісного підходу при оцінці якості системи ідентифікації пояснюється випадковим характером процесів, що відбуваються при ідентифікації, коли внаслідок впливу дестабілізуючих факторів і випадкових зовнішніх збурень змінюються параметри як вимірювальних засобів, так і самих ідентифікаційних ознак HAD. Результати ідентифікації при цьому розглядаються як випадкові події, з певною ймовірністю відповідні реальним ідентифікаційним ознакам HAD.

Зважаючи на викладене найбільш прийнятною для ідентифікації HAD є технологія RFID з індуктивним зв’язком, яка в якості ідентифікаційних ознак використовує пасивні електричні коливальні контури (ПЕКК). Власне сама система ідентифікації HAD має складатися з (рис. 3.2):

– комплекту HAD з носіями ідентифікаційних ознак;

– зчитувачів з приймально-передавальним інтерфейсом для зв’язку з носіями коду HAD, розташованих в зоні ідентифікації;

– додатку, встановленого на комп’ютері (планшеті).

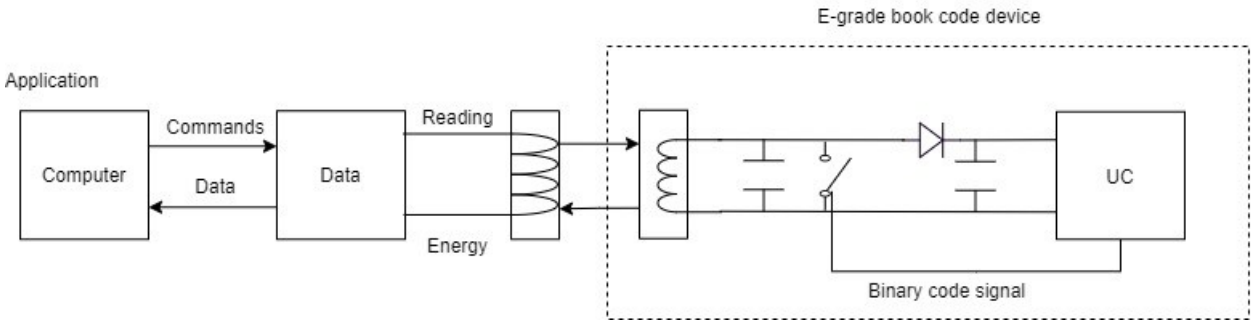

Рис. 3.2. Функціональна схема взаємодії компонентів RFID з ПЕКК

Завдання зчитувача: активізувати носій коду, внесений в зону ідентифікації; приймати ідентифікаційний номер носія з подальшою передачею за допомогою програмних драйверів до ІАМ.

Первинний вимірювальний перетворювач в технології RFID з індуктивним зв'язком являє собою електричний коливальний контур, налаштований в резонанс на частоту живлючого генератора. Чутливим елементом ПВП є індуктивність, виконана у вигляді рамки. Як інформативний параметр ПВП використовується амплітуда вихідної напруги ПВП.

При попаданні в зону ідентифікації, ПЕКК, частота налаштування якого збігається з частотою електромагнітного поля зчитувача, відбирає енергію цього поля. Таким чином, пасивні RFID мітки з чіпом отримують енергію для функціонування.

Ідентифікаційний код HAD формується шляхом комутації (закорочування) ПЕКК відповідно з присвоєним кодом (так звана навантажувальна модуляція ‘load modulation’). Обробку вхідної інформації та вироблення відповідного сигналу забезпечує кремнієвий чіп комплементарної структури «метал-оксид-напівпровідник». Вибір такого чипу – напівпровідникової технології побудови інтегральних мікросхем пояснюється близьким до нуля енергоспоживанням в статичному стані. Схема взаємодії ПВП і ПЕКК представлена на рис. 3.3.

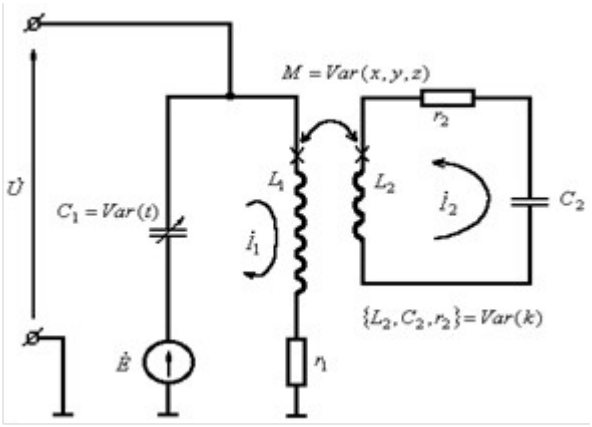

Рис. 3.3. Схема взаємодії ПВП и ПЕКК:

$L1$ – джерело поля; $L1C1$ – контур джерела поля; $\dot{E}$ – генератор напруги, що живить контур джерела поля; $L2C2$ – ПЕКК; $\dot{U}$ – інформативний параметр; M – коефіцієнт взаємної індукції між котушками $L1$ і $L2$; x, y, z – координати внесення ПЕКК; k – поле значень частот налаштування ПЕКК

Процес взаємодії ПВП з ПЕКК об’єкта може бути поданий [13] у вигляді наступної математичної моделі:

$$\dot{U} = \dot{E}\frac{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_{L_1} - \frac{w^2M^2}{|z_2|^2}x_{2})}{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_1 - \frac{w^2M^2}{|z_2|^2}x_{2})} \qquad (3.1)$$

де r_1 та r_2 – власні втрати в контурі джерела поля і ПЕКК;

$$Z_1 = r_1 + j(\omega L_1 - \frac{1}{\omega C_1}) \tag{3.2}$$

та

$$Z_2 = r_2 + j(\omega L_2 - \frac{1}{\omega C_2}) \tag{3.3}$$

де Z_1 та Z_2 – комплексний опір кожного з контурів; ω – кругова частота джерела е.р.с. E.

Максимальний радіус зчитування R обмежується величиною ближньої зони електромагнітного поля: $R < \lambda / 2\pi$, де λ – довжина хвилі електромагнітного поля, створюваного джерелом поля. Аналіз рівняння (3.1) показує, що зміна напруги на джерелі поля визначається зміною знаменника.

Збільшення активного опору контуру джерела поля призводить до зменшення напруги на джерелі поля L_1. Отже, по зменшенню напруги на джерелі поля, викликаного збільшенням необоротних втрат енергії, можна судити про наявність на об’єкті ПЕКК, частота налаштування якого збігається з частотою поля (рис. 3.3).

ПЕКК «спрацьовує», коли залишкове значення інформативного параметра досягає контрольованого рівня. Зона вибору контрольованого рівня інформативного параметра, задається опорним (пороговим) значенням напруги компаратора U_n, обмежується зоною нестабільності початкового значення інформативного параметра ПВП. Системи RFID з індуктивним зв'язком між носієм ідентифікаційного коду і зчитувачем, працюють на частоті нижче 135 кГц або в діапазонах частот 6,78; 13,56 і 27,125 МГц [15, 16].

Блок-схема узагальненого алгоритму ідентифікації HAD представлена на рис. 3.4.

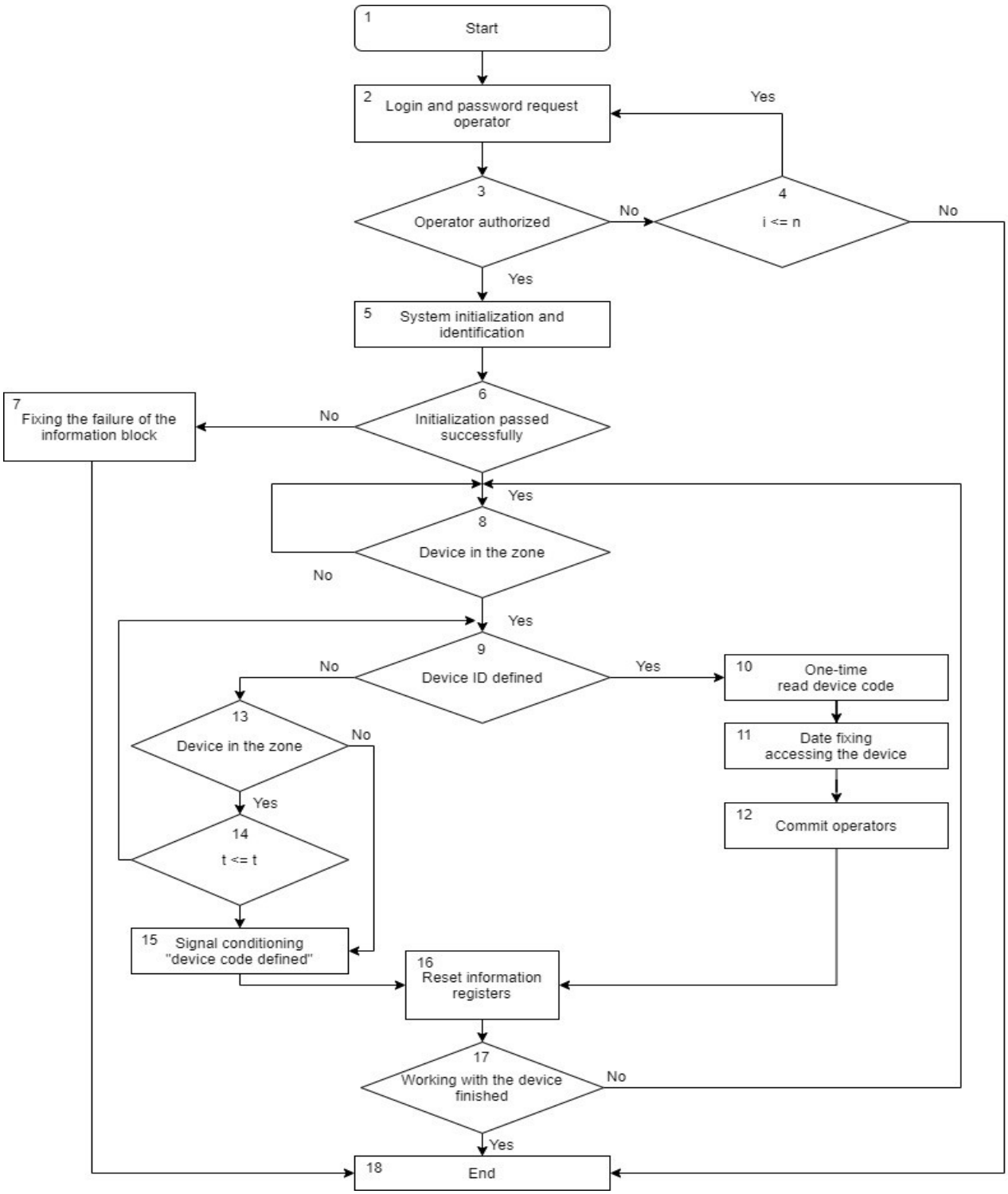

Рис. 3.4. Блок-схема алгоритму роботи системи ідентифікації HAD

Для підвищення достовірності ідентифікації в зчитувачі застосовується процедура «хитання» частоти генерованого електромагнітного поля між двома граничними значеннями. Коли частота електромагнітного поля точно збігається з частотою настройки ПЕКК носія, виникає виразний перепад інформативного параметра, який достовірно фіксується зчитувачем.

Необхідні для достовірної ідентифікації параметри зчитувача і носія ідентифікаційного коду регламентуються стандартами ISO/IEC 18000 [17–19]. При цьому ISO/IEC 18000-2:2004, наприклад, визначає:

– фізичний рівень, який використовується для зв'язку між зчитувачем і носієм ідентифікаційного коду;

– протокол і команди;

– метод виявлення і зв’язку з одним носієм серед кількох носіїв («антіколлізія»).

Стандарт ISO/IEC 18000-2:2004 визначає два типи носіїв: Тип A (FDX) і Тип B (HDX). Ці два типи відрізняються тільки своїм фізичним рівнем. Обидва типи підтримують один і той самий протокол захисту від взаємних впливів.

Носії FDX працюють на частоті 125 кГц і постійно отримують живлення від зчитувача, в тому числі під час передачі ідентифікаційного коду від носія до зчитувача. Носії HDX працюють на частоті 134,2 кГц і отримують живлення від зчитувача, за винятком часу передачі ідентифікаційного коду від носія до зчитувача.

Авторизація оператора проводиться з метою виконання вимог політики розмежування доступу.

Ініціалізація системи ідентифікації HAD забезпечує приведення програмних і апаратних засобів системи в стан готовності до використання. При внесенні HAD в зону ідентифікації системи і успішного визначення коду проводиться фіксація цього коду в СУІБ. При цьому фіксуються дата звернення до носія та ім’я оператора.

Після винесення HAD із зони зчитування проводиться скидання інформаційних регістрів і система ідентифікації вважається готовою до роботи з наступним HAD. У разі невизначення коду HAD після певного періоду, $t_{ож}$ системою формується сигнал «код носія не визначений».

3.3. Стеганографічний протокол обміну даними в процедурах управління ідентифікацією та доступом

Побудова системи IAM потребує опрацювання питань захисту чутливої інформації під час її передавання через деяке потенційно небезпечне середовище. Основним методом, що забезпечує захист даних при обміні в комп'ютерних системах, є застосування криптографічних протоколів типів SSL, TLS, SET, SSH тощо. Вони поєднують достатню швидкодію з надійним захистом даних. При цьому забезпечується їх конфіденційність і цілісність [20].

Водночас необхідно зазначити що стандартні криптографічні протоколи іноді можуть використовувати за замовчуванням застаріли криптографічні механізми які вразливі до деяких видів атак [21–23]. Також слід звернути увагу на те, що у випадку використання стандартного протоколу основний контроль за ключовою та іншою критичною інформацією забезпечує операційна система комп'ютера, яка може зберігати у власному ядрі дані про застосовані ключі, що не підвищує рівня довіри до системи захисту.

На відміну від криптографічних перетворень стеганографія приховує факт передавання критичної інформації, що фактично є доволі ефективним способом убезпечення конфіденційної інформації [24, 25].

Цифрової або комп'ютерна стеганографії оперує з поняттям стеганографічної системи (далі – стегосистеми) яка задається наступним рівнянням:

$$\widetilde{Q}=F(Q,k,D), \tag{3.4}$$

де $D=(d_1,\ldots,d_L)\in V_2^L$ – інформаційний вектор – двійковий рядок довжини L;

$Q\in\{Q_i, i=1,2,\ldots\}$ – двійковий файл з деякої кінцевої їх множини форматів аудіо, зображення тощо. Цей файл зазнає перетворень згідно з правилом - функцією F на основі інформаційного вектору та з використанням таємного параметру $\overline{k}\in\{k_j, j=1,2,\ldots\}$ – ключа стегосистеми.

Файл Q отримав назву пустого контейнера, файл $\widetilde{Q}$ – контейнер що містить замаскований інформаційний вектор I та використовується для прихованого

передавання цього вектору через незахищене середовище [24]. При цьому сукупність $\langle F, Q \rangle$ є стеганографічною системою, або коротко – стегосистемою.

Як і загально відомі широкосмугові системи радіозв'язку стеганографічні системи забезпечують ефективне маскування факту передачі деякого повідомлення. Отже властивість стегосистем може бути використана захисту інформаційного обміну в рамках реалізації процедур автентифікації. Таким чином, виходячи з потреби практики можливо відмітити актуальність розробки безпечної стегосистеми.

Загально визнаними критеріями щодо визначення безпеки застосування стегосистеми є надання відповіді на наступні базові питання.

П.1. Чи існує деяка процедура, яка дозволяє стосовно перехопленого контейнера стверджувати, що він пустий?

П.2. Чи можна без знання ключу стегосистеми за оперативне прийнятний час з заданим рівнем надійності з контейнеру вилучити саме то повідомлення, яке в нього було вбудоване?

Очевидно відповіді на ці питання залежать від характеристик функції перетворення та обраних контейнерів.

Для побудови захищеного стеганографічного протоколу перш за все почнемо з визначення функції перетворення F, за допомогою якої встановлюється правило вбудовування інформаційного вектора в стеганографічний контейнер Q.

Логічно вимагати, щоб відповідне правило F для забезпечення високої швидкості перетворення мало відносно невелику обчислювальну складність та його реалізація програмним засобом була узгоджена з системою команд використаного процесора.

Серед значної кількості таких функцій [24–26] вказаній вимогі відповідає метод заміни найменшого значущого біту 'least significant bit' (LSB) двійкового подання зображення.

Тобто LSB-стеганографія – це метод стеганографії, за якої повідомлення приховується всередині зображення, замінюючи молодший значущий біт зображення на елементи повідомлення, яке потрібно приховати.

Вважаємо, що контейнер є зображення, що може бути подане у вигляді двійкової матриці розміром $n_1 \cdot n_2 = N$:

$$Q = \begin{Vmatrix} q_{11} & \dots & q_{1n2} \\ \dots & \dots & \dots \\ q_{n11} & \dots & q_{n1n2} \end{Vmatrix} = \begin{Vmatrix} \overline{q_1} \\ \dots \\ \overline{q_{n1}} \end{Vmatrix}, \tag{3.5}$$

де q_{ij} – біти контейнера $\overline{q_j}, j = 1,2,\dots,n_1$ – вектори рядки матриці Q.

Для простоти подальшого запису рівняння перетворення контейнера трансформуємо послідовність векторів – рядків в єдиний вектор:

$$(\overline{q_1},\dots,\overline{q_{n1}}) = (q_{11},\dots,q_{1n2},\dots,q_{n11},\dots,q_{n1n2}) = (\theta_1,\dots,\theta_N) = \overline{\theta}, \tag{3.6}$$

де $(\theta_1,\dots,\theta_N)$ – вектор бітів контейнера після наскрізної перенумерації його бітів.

Задаємо функцію стегосистеми за допомогою наступних рівнянь:

$$\begin{cases} \tilde{\theta}_j = \theta_j \cdot (k_j \oplus 1) \oplus d_l \cdot k_j, \text{де } j = \overline{1,N}, l = \overline{1,L} \\ l = \begin{cases} 1, \text{для } j = 1 \\ \sum_{i=1}^{j-1} k_i + 1, \ j \geq 2 \end{cases} \end{cases} \tag{3.7}$$

де $\tilde{\theta}_j$ – послідовність бітів контейнера стегосистеми що модифіковані згідно з інформаційним вектором D,

$\overline{k} = (k_1, k_2, \dots, k_N) : |\overline{k}| = L$ – двійковий вектор ключа, що має вагу Гемінга яка дорівнює L (вектор містить рівно L одиниць). Вочевидь, у визначених умовах кількість різних ключів дорівнює значенню біноміального коефіцієнта C_N^L

Зауважимо, вектор $\tilde{\overline{\theta}} = (\tilde{\theta}_1, \tilde{\theta}_2, \dots, \tilde{\theta}_N)$ згідно з рівняннями (3.6) і (3.7) може буть трансформований в вигляд контейнера:

$$\tilde{\overline{\theta}} = (\tilde{\theta}_1, \tilde{\theta}_2, \dots, \tilde{\theta}_N) \to \tilde{Q} = \begin{Vmatrix} \tilde{q}_{11} & \dots & \tilde{q}_{1n2} \\ \dots & \dots & \dots \\ \tilde{q}_{n11} & \dots & \tilde{q}_{n1n2} \end{Vmatrix}. \tag{3.8}$$

Рівняння (3.7) визначає, якщо черговий біт ключа дорівнює одиниці, то відповідний біт контейнера набуває значення чергового біту інформаційного вектору. Це означає наступне:

Твердження 1. Елементи $q_{ij} ma \tilde{q}_{ij}$ контейнерів $Q ma \widetilde{Q}$ збігаються в одному з двох випадків:

1. Якщо в (3.7) біт вектора ключа дорівнює нулю, то зміна контейнера на цьому місці не відбувалася.

2. Якщо в (3.7) цей біт ключа дорівнює 1, а біт контейнера збігається з бітом чергового інформаційного вектора, то знову зміна контейнера не спостерігається.

Зважаючи на викладене, можливо зробити висновок, що для певних інформаційних векторів шляхом формування відповідного ключу в (3.7) потенційно можна забезпечити, що б вихідний та модифікований контейнери збігались: $Q=\widetilde{Q}$.

Більше того, за умов певного співвідношення розміру контейнера та довжини інформаційного вектора, можливо припустити, що в контейнері можуть бути розміщені декілька повідомлень, які вибираються за допомогою відповідного ключу.

Для оцінки можливості відповіді на питання П.1 і П.2 що визначені на початку цього розділу проаналізуємо ймовірнісні характеристики модифікованого контейнера $\widetilde{Q}$

Вважаємо, що біти векторів $\bar{\theta}=(\theta_1,\ldots,\theta_N)$ та $D=(d_1,\ldots,d_L)$ мають біноміальний розподіл з ймовірностями відповідно:

$$P\{\theta_i=0\}=\pi_0, P\{\theta_i=1\}=\pi_1, \pi_0+\pi_1=1, i=\overline{1,N}. \tag{3.9}$$

$$P\{d_i=0\}=p_0, P\{d_i=1\}=p_1, p_0+p_1=1, i=\overline{1,L}. \tag{3.10}$$

Надалі, виходячи з твердження 1 оцінімо ймовірність збігу бітів пустого та модифікованого контейнерів:

$$P\{\theta_i=\widetilde{\theta}_i\}=P\{k_i=0\}+P\{k_i=1\}\cdot P\{\theta_i=d_l\}, \tag{3.11}$$

де індекс l розраховується на підставі (3.7).

Виходячи з (3.9) і (3.10) та враховуючи, що

$$P\{k_i=0\}=\frac{N-L}{N}, P\{k_i=1\}=\frac{L}{N}, \tag{3.12}$$

за умов незалежності бітів пустого контейнера та інформаційного вектору для ймовірності співпадіння бітів цих контейнерів отримуємо вираз:

$$P\left(\theta_i=\widetilde{\theta}_i\right)=\frac{N-L}{N}+\frac{L}{N}\cdot\left(\pi_0\cdot p_0+\pi_1 p_1\right)=1-\frac{L}{N}\left(1-\pi_0\cdot p_0+\pi_1 p_1\right). \quad (3.13)$$

Таким чином за умов виконання зроблених припущень з останнього рівняння слідує наступне справедливість наступного твердження.

Твердження 2. В разі наближення до рівномірного розподілу бітів контейнера, або їх частини, що обрана для модифікації, має місце наступна оцінка ймовірності збігу ϑ на однакових місцях бітів пустого та модифікованого контейнерів:

$$\vartheta=P\left(\theta_i=\widetilde{\theta}_i\right)\approx 1-\frac{L}{2N}, якщо\ \pi_0\to\frac{1}{2}. \quad (3.14)$$

Зауважимо, що оцінка (3.14) не залежить від розподілу бітів інформаційного вектору.

Зазначимо, що саме в випадку застосування методу LSB, внаслідок впливу процедури округлення результату під час оцифрування початкового зображення найменший значущий біт наближується до рівномірного розподілу. Це фактично обумовлює кращу застосовність цього методу для цілей стеганографії.

Для побудови статистичного критерія розрізняння контейнерів введемо функцію – індикатор події $\left(\theta_i=\widetilde{\theta}_i\right)$:

$$I\left(\theta_i=\widetilde{\theta}_i\right)=\begin{cases}1, якщо\left(\theta_i=\widetilde{\theta}_i\right)\\0, в\ разі\left(\theta_i\neq\widetilde{\theta}_i\right)\end{cases} \quad (3.15)$$

Введемо випадкову величину δ – міру наближення двох контейнерів:

$$\delta=\sum_{i=1}^{N} I\left(\theta_i=\widetilde{\theta}_i\right). \quad (3.16)$$

Залежно від обраного в стегосистемі ключу $\overline{k}$ величина δ може приймати цілі значення з інтервалу $[0,N]$. Тоді ймовірність того, величина $\delta=m$ дорівнює:

$$P\left(\delta=m\right)=C_N^m P\left(\theta_i=\widetilde{\theta}_i\right)^m\cdot\left(1-P\left(\theta_i=\widetilde{\theta}_i\right)\right)^{N-m}. \quad (3.17)$$

Нехай, $P\left(\theta_i=\widetilde{\theta}_i\right)=\vartheta$, тоді згідно центральної граничної теореми [27] випадкова величина δ має нормальний розподіл з математичним сподіванням $a=N\vartheta$ та дисперсією $\sigma^2=N\vartheta(1-\vartheta)$.

Зрозуміло, що в разі $\delta > C_\alpha$ для певної заздалегідь визначеної границі критерія C_α з заданим рівнем значущості α не має підстав вважати що два контейнера за суттю є парою «пустий – модифікований» контейнери.

В випадку застосування нормального наближення для випадкової величини δ для визначення границі критерія скористуємся виразом:

$$C_\alpha = a + t_{1-\alpha} \cdot \sigma = N\vartheta + t_{1-\alpha} \cdot \sqrt{N\vartheta(1-\vartheta)}, \qquad (3.18)$$

де $t_{1-\alpha}$ – квантіль стандартного нормального розподілу, що відповідає рівню надійності критерія $1-\alpha$.

Таким чином, доведено наступне твердження.

Твердження 3. Сторонній спостерігач, який отримав два контейнера, може з рівнем значущості α визнати їх парою «пустий – модифікований» контейнери або відхилити цю гіпотезу залежно від виконання або невиконання нерівності:

$$\delta > N\vartheta + t_{1-\alpha} \cdot \sqrt{N\vartheta(1-\vartheta)}. \qquad (3.19)$$

Якщо спостерігач має лише один контейнер, стосовно якого він намагається визначити його статус «пустий – модифікований», то для побудови критерія розрізняння відповідних гіпотез йому потрібна інформація, що визначена в (3.9).

Проведене статистичне моделювання в цілому підтвердило отримані теоретичні результати, при цьому з'ясовано, що в разі достатньо великого контейнера статистичний критерій дозволяє з високим рівнем надійності виявляти модифіковані контейнери, якщо обсяг вбудованої інформації сягає величини $L \approx 0{,}37N$ або більше.

Таким чином, за умов невеликого обсягу інформаційного вектору відносно розміру контейнера можливо приховувати факт передавання певної конфіденційної інформації, яка стосується процедури автентифікаці в деякій корпоративній мережі.

Для цього клієнт, що має намір авторизуватись надсилає серверу модифікований за допомогою інформаційного вектору D_I контейнер $\widetilde{Q}_i$ використовуючи визначену для цього напряму інформаційного обміну множину пустих контейнерів $Q_i \in \{Q_1, Q_2, \ldots, Q_I\}$ ключ $\bar{k}_I$, а також сеансовий вектор ініціалізації, що використовується для зміни поточного ключа стегосистеми.

Інформаційний вектор клієнта D_I може містити дані щодо ідентифікатору пристрою з якого надсилається запит, власного ідентифікатора клієнта, часу початку сеансу взаємодії а також іншу інформацію, яка може бути ефективно використана сервером для ідентифікації клієнта.

У відповідь сервер навмання вибирає з визначеної для цього напряму інформаційного обміну множини пустий контейнер $Q_j \in \{Q_1, Q_2, \ldots, Q_I\}$. Вибраний контейнер зазнає модифікації з ключе $\overline{k}_I$ та сеансовим вектором ініціалізації з використанням власного інформаційного вектору, що містить інформацію, яка необхідна клієнту для підтвердження ідентифікації сервера.

Наступним кроком клієнт в новому модифікованому контейнері надсилає серверу ґеш-образ власного паролю на підставі якого сервер завершує процедуру первинної авторизації, про що інформує клієнта наступним модифікованим контейнером. Таким чином в процедурі використовуються чотири контейнера.

Використання контейнерів – зображень додає ще одного кроку перевірки повноважень, зважаючи на те, що клієнт візуально оцінює достовірність отриманого контейнеру.

За попередніми підрахунками загальний обсяг даних, що пересилаються в процедурі не перевищує 100 Кбайт, що несуттєво впливатиме швидкість її реалізації.

3.4. Загрози та ризики використання систем штучного інтелекту

Національна безпека і оборона, стан та розвиток об’єктів критичної інфраструктури, фінансово-економічний розвиток суспільства залежать від впровадження високих технологій. Специфічною галуззю, що грає важливу роль в цьому процесі, стає ШІ.

Принципи та алгоритми функціонування СШІ переважної більшості суспільства практично невідомі. За суттю СШІ сприймаються як деякі «чарівні чорні скриньки», які здатні розуміти природню мову людини, музичні опуси або

графічні зображення та адекватно реагувати на запитання користувачів шляхом надання статистично вірної відповіді [28].

При цьому, звичайно, користувачі системи, що отримують результат відповідно до завдання, поставленого такій системі, не розуміють джерел формування відповіді і методів розв’язання завдання [29].

З одного боку, на відміну від звичайних обчислювальних систем, в випадку СШІ спостерігається ефект непередбачуваності (частково – не тривіальності) результатів її «роздумів», що в загальному випадку є однією з ознак творчості та інноваційної діяльності, яка притаманна людині.

З іншого боку, відсутність прозорих методів перевірки запропонованих СШІ висновків та рекомендацій утворює джерело невизначеності щодо їх вірності і практичної цінності. Це фактично означає, що СШІ можуть бути частиною сукупності заходів інформаційної війни, які спрямовані на поширення сумнівних неперевірених відомостей та звичайних фейків. СШІ може стати потужним інструментом в інформаційних війнах, створюючи більш переконливі та цільові фейкові новини, а також автоматизуючи їх поширення. Звернемо увагу, що платформа розповсюдження контенту, яка використовує алгоритми рекомендацій із підтримкою ШІ, була використана для визначення пріоритетності вмісту з метою маніпулювання емоціями, переконаннями та поведінкою [30].

В [31] відмічене, що потужні СШІ слід розробляти лише в тому випадку, якщо ми впевнені, що їхній ефект буде позитивним, а ризики керованими.

Таким чином, поширення сфери застосування СШІ на об’єкти критичної інфраструктури, складність верифікації створених цими системами інформаційних ресурсів та рішень, загрози небезпечного впливу результатів їхнього функціонування на безпеку людини, суспільства та держави призводить до виникнення ризиків, пов’язаних з використанням СШІ, а це висуває вимогу формування процедур виявлення та обробки таких ризиків, що може мати визначальне значення для майбутнього суспільства та забезпечення національної безпеки.

На поточний час серед поширених систем, що доступні широкому загалу суспільства та сприяють формуванню суспільної думки щодо можливостей ШІ, бачимо наступні СШІ генеративного типу:

ChatGPT – чат-бот, що створений компанією OpenAI, підтримує діалог з користувачем з використанням природних мов та генерує тексти на задану тему;

Midjourney (проміжний шлях) – сервіс від однойменної компанії, які виходячи з текстових описів – запитів щодо бажаного зображення генерує його.

На основі вивчення цих засобів вкрай складно зробити висновок щодо перспектив застосування в інтересах державних структур технологій ШІ, але за умов належного проєктування систем можливо прогнозувати можливість розвитку деяких напрямів, що вимагають від інформаційно-управляючих систем забезпечення певних якостей, притаманних ШІ.

На основі окремих повідомлень можливо зробити висновок, що СШІ включають різні компоненти, такі як алгоритми машинного навчання, глибокого навчання, нейронні мережі, обробка природної мови, комп'ютерний зір, робототехніка та інші технології. Вони також можуть включати комплекси автоматизації, аналітики даних, системи управління знаннями та інші інструменти для обробки інформації та прийняття рішень [32].

Які головні переваги від застосування СШІ можливо виділити у порівнянні зі звичайними програмними системами?

В багатьох СШІ застосовуються інтерпретатори природних мов, що суттєво підвищує їх ефективність порівняно із звичайними програмними системами у випадку обробки неструктурованих даних [33, 34].

Застосування в перспективі [35] в СШІ потужних комп’ютерних архітектур з швидкісними процесорами, що здатні підтримувати значну кількість глибоких нейронних мереж, дозволить вирішувати за оперативне придатний час розв’язання складних завдань, які потребують великої кількості обчислень.

ШІ забезпечує ефективну обробку великих обсягів даних ‘big data’ завдяки застосуванню алгоритмів машинного навчання та аналізу даних, що забезпечує автоматизацію процесів їх обробки та аналізу, дає можливість виявляти приховані

закономірності та прогнозувати тренди (тенденції) та патерни (зразки), оптимізувати процеси прийняття рішень та створювати інтелектуальні системи управління даними [36]. Таким чином, СШІ сприяє отриманню знань з великих обсягів даних та приймати обґрунтовані рішення на основі їх аналізу.

Застосування технології ШІ здатне покращити рівень комп’ютерної безпеки, зокрема, в [37] запропоноване використання ШІ та нейронних мереж для проєктування системи захисту комп'ютерної мережі. При цьому, на основі експериментальних досліджень продемонстрований гарний ефект від цього в плані забезпечення безпеки комп'ютерної мережі.

Перелічені властивості технології ШІ дають підстави прогнозувати її ефективне застосування також для вирішення інших завдань забезпечення кібербезпеки. Зокрема, зважаючи на великі обсяги даних що обробляються ситуаційними центрами [38] та підвищені вимоги щодо їх гарантоздатності, кібербезпеки та оперативності прийняття рішень в кризових ситуаціях вказані центри є першочерговими об’єктами для впровадження технологій ШІ.

Аналогічна ситуація має у випадку протидії шифрувальним вірусам – вимагачам [39] при цьому успіху заходів протидії зазначеним загрозам сприяє головна особливість ШІ – здатність розв’язання складних завдань, які потребують великої кількості обчислень, без прямого втручання людини.

Водночас, вибуховий характер розвитку технології ШІ та її застосування, не дивлячись на позитивні властивості технології, несе великі потенційні ризики [30]. Важливо зазначити, що здатність керувати цими ризиками на думку авторів відкритого листа [40] потребує спільної розробки та впровадження набору загальних протоколів безпеки для передового проєктування та розробки ШІ, які ретельно перевіряються та контролюються незалежними зовнішніми експертами.

Необхідність визначати та регулювати ризики, пов’язані з використанням систем ШІ шляхом прийняття законодавчих актів та стандартів визнали Європейський Союз, Сполучені Штати Америки та інші країни світу.

Зокрема, Європейський Парламент схвалив основні положення [41], що утворять основу майбутнього закону, якій визначатиме правила в сфері ШІ.

Документом встановлюється високий рівень ризику застосування ШІ в галузі критичної інфраструктури, громадського порядку, освіті та управління міграцією. При цьому особливі вимогі висуваються до СШІ, що забезпечують генерацію аудіо, відео та іншого контенту.

В США NIST визначив рамковим документом AI RMF 1.0 [42] орієнтири для покращення здатності враховувати важливі аспекти щодо надійності під час проєктування, розробки, використання та оцінки продуктів, послуг і систем, що засновані на технології ШІ.

Загалом, аналіз законодавчих записів 127 країн за індексом ШІ показує, що кількість законопроєктів, які згадують ШІ та були прийняті як закон, зросла з одної у 2016 році до 37 у 2022 році. Аналіз парламентських записів щодо ШІ у 81 країні також показує, що згадки про ШІ у глобальних законодавчих процедурах зросли майже в 6,5 рази з 2016 року [43].

Для визначення можливого впливу загроз що пов’язані з СШІ та мінімізації ймовірності їх реалізації необхідно об’єднання зусиль науковців, дослідників та розробників наукових і освітніх установ, виробничих і промислових структур, державних і громадських організацій, законодавчих та виконавчих органів влади та міжнародної спільноти.

Реалізація таких заходів допоможе створити систему зниження ризиків, що дозволить швидше виявляти, готуватися і реагувати на виклики та загрози, які походитимуть від створення та використання СШІ.

Ризики, що породжені СШІ, багато в чому унікальні. СШІ, наприклад, можуть бути навчені на даних, які можуть змінюватися з часом, іноді суттєво й несподівано, впливаючи на функціональність і надійність системи у спосіб, який важко зрозуміти. СШІ та контексти, в яких вони розгортаються, часто складні, що ускладнює виявлення збоїв і реагування на них**.**

СШІ за своєю природою мають соціально-технічний характер, тобто на них впливає суспільна динаміка та поведінка людей. Ризики та переваги ШІ можуть виникати через взаємодію технічних аспектів у поєднанні з суспільними факторами, пов’язаними з тим, як використовується система [42].

Розвиток СШІ створює передумови для посилення існуючих загроз національній безпеці в інформаційній сфері. Ці загрози включають:

1. Посилення кібератак. ШІ може підвищити ефективність процедур виявлення вразливостей в системах безпеки, виконання атак, маскування їх наслідків, імітацію поведінки людини в окремих фазах кібератаки [38, 44].

2. Утворення каналів витоку інформації з обмеженим доступом. СШІ можуть бути використані для посилення комп'ютерної розвідки завдяки аналізу шляхом аналізу великих обсягів даних, визначення трендів і патернів, щоб виявити конфіденційні дані про об'єкти, які стосуються національної безпеки, критичну інфраструктуру тощо. Зокрема, завдяки інтерактивній карті, що опублікована в інтернеті та показує місцезнаходження людей, які використовують такі фітнес-пристрої, як Fitbit, була продемонстрована можливість ідентифікації військових об'єктів США [45].

3. Атаки отруєння даних 'data poisoning' – це цільові атаки з метою модифікації або спотворення даних, що використовуються для машинного або глибокого навчання СШІ, внаслідок чого СШІ отримує небажані навички, які можуть завдати шкоди особі, суспільству та державі. Зазначимо, що процедури навчання СШІ зазвичай передбачають використання великої кількості даних для тренування моделі. Ці дані можуть бути зібрані з різних джерел і можуть містити помилки або неточності. Атака отруєння даних використовує ці неточності з метою введення помилкових чи зловмисних даних у навчальний набір [46–48].

Зважаючи на те, що СШІ можуть використовуватися для створення роботизованих збройних систем, які можуть самостійно визначати та атакувати цілі без участі оператора [49], атака отруєння даних може мати без перебільшення жахливі наслідки.

4. Містифікація даних. Спеціалістами компанії «Vulcan» [50] виявлена схильність генеративної СШІ ChatGPT до створення недостовірних фактів і даних 'hallucinated facts and figures'. А саме, ChatGPT в разі запиту рішень для кодування може пропонувати неіснуючі пакети (рис. 3.5, кроки 1 і 2). Ці уявні пакети можуть бути використані зловмисниками для перетворення їх в

замаскований шкідливий код, який завантажується в репозиторії кодів (крок 3). Якщо користувач, запитує у ChatGPT рекомендації щодо розробки (кроки 4 і 5), в пропозиціях (кроки 6 і 7) можуть з'явитися ці шкідливі пакети. Таким чином, ці недостовірні пакети СШІ потенційно перетворяться на канал витоку інформації користувач (крок 8).

Наведений вище перелік загроз не є вичерпним, але дає можливість оцінити складність, глибину та впливовість проблеми. Кожна з цих загроз вимагає глибокого розуміння технологій ШІ та формування ефективних стратегій для протидії їм.

Для блокування або нейтралізації визначених загроз необхідна реалізація низки заходів, спрямованих на мінімізацію (обробку) ризиків використання СШІ, і в першу чергу – на ідентифікацію ризиків використання СШІ. Як і ризики для інших типів технологій, ризики ШІ можуть виникати різними способами та можуть бути охарактеризовані як довготермінові чи короткострокові, з високою чи низькою ймовірністю, системні чи локалізовані, а також із сильним чи низьким впливом [42].

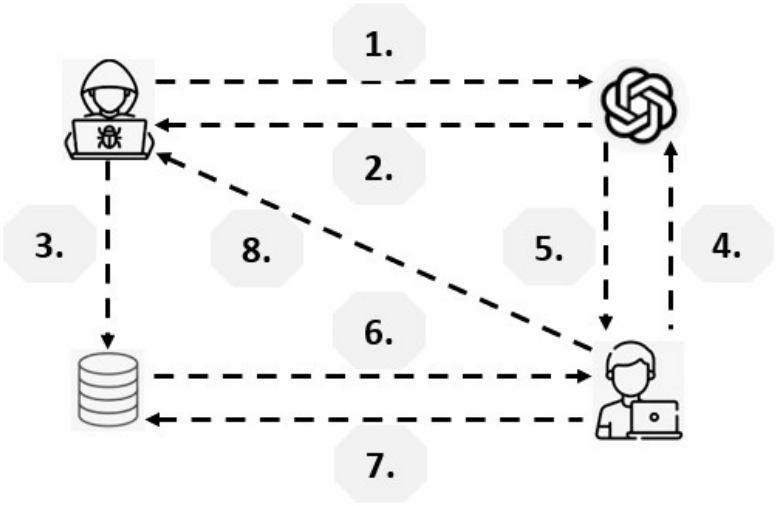

Рис. 3.5. Реалізація загрози витоку інформації через недійсні пакети СШІ

Загальні принципи та орієнтири для управління ризиками будь-якого типу, розміру чи природи визначені стандартом ISO 31000:2018 Risk management – Guidelines [51, 52]. Основна ідея полягає в тому, щоб створити систематичний і структурований підхід до ідентифікації, оцінки, керування та моніторингу

ризиків. Ось деякі ключові етапи та аспекти управління ризиками за стандартом ISO 31000:

1. Встановлення контексту: необхідно розуміти свій контекст і визначити фактори, що впливають на здатність до досягнення цілей.

2. Ідентифікація ризиків: ризики ідентифікуються шляхом виявлення подій або ситуацій, які можуть впливати на досягнення цілей.

3. Оцінка ризиків: визначення ймовірності та впливу ризиків для визначення їхньої значущості. Це допомагає визначити пріоритети для подальшого керування ризиками.

4. Обробка ризиків: в цьому етапі визначаються можливі стратегії обробки ризиків. Це може включати уникнення ризику, зменшення його впливу, передачу ризику та прийняття ризику.

5. Заходи управління ризиками: розробляються та впроваджуються конкретні заходи для керування ризиками згідно з визначеними стратегіями.

6. Моніторинг та перегляд: ризики та їхні заходи управління мають бути систематично переглянуті та оцінені для впевненості, що вони залишаються ефективними та актуальними.

7. Звітність та комунікація: інформація про ризики та їхній стан повинна бути передана відповідним зацікавленим сторонам, включаючи керівництво та інші зацікавлені групи.

Загалом, управління ризиками за стандартом ISO 31000 вимагає системного підходу на всіх етапах життєвого циклу з області оцінювання [53].

Звернемо увагу, що в [40] для нашого випадку фактично визначена мета управління ризиками: сучасні СШІ зробити більш точними, безпечними, інтерпретованими, прозорими, надійними, узгодженими, заслуговуючими на довіру і лояльними.

Використання СШІ для управління ризиками, які виникають внаслідок використання інших СШІ може бути ефективним засобом забезпечення безпеки та стабільності. Такий підхід може включати в себе ряд етапів (рис. 3.6) та функціональних можливостей:

1. Ідентифікація ризиків: аналіз архітектури системи та алгоритмів, що використовуються, типи даних та інші параметри. Система може визначати слабкі місця, потенційні точки виникнення помилок або зони, де система може взаємодіяти з оточенням.

2. Моніторинг поведінки СШІ: система управління ризиками на базі СШІ може безперервно стежити за поведінкою інших систем управління, аналізуючи їх виходи, метрики та поведінку в реальному часі.

3. Автоматичне виявлення аномалій: використовуючи методи машинного навчання, система може виявляти аномалії або відхилення від норми в поведінці СШІ, що може свідчити про потенційні ризики.

4. Прогнозування ризиків: на основі історичних даних та актуального стану системи управління ризиками прогнозуються потенційні проблеми або непередбачувана поведінка СШІ у майбутньому.

5. Автоматична корекція: у випадках, коли виявлено ризик, система може автоматично вносити корективи в роботу іншої СШІ, наприклад, змінюючи її параметри або обмежуючи її дії.

6. Сценарії «чорної скриньки»: для вивчення і розуміння поведінки СШІ можна використовувати сценарії, де СШІ піддається ряду тестів у контрольованому оточенні.

7. Аналіз причинно-наслідкових зв’язків: система може допомогти аналізувати причини певної поведінки СШІ, визначаючи, чи була ця поведінка результатом вхідних даних, алгоритмів, або інших факторів.

8. Зворотний зв'язок і навчання: на основі аналізу ризиків та інцидентів система може навчатися, вдосконалюючи свої методи виявлення та реагування на ризики.

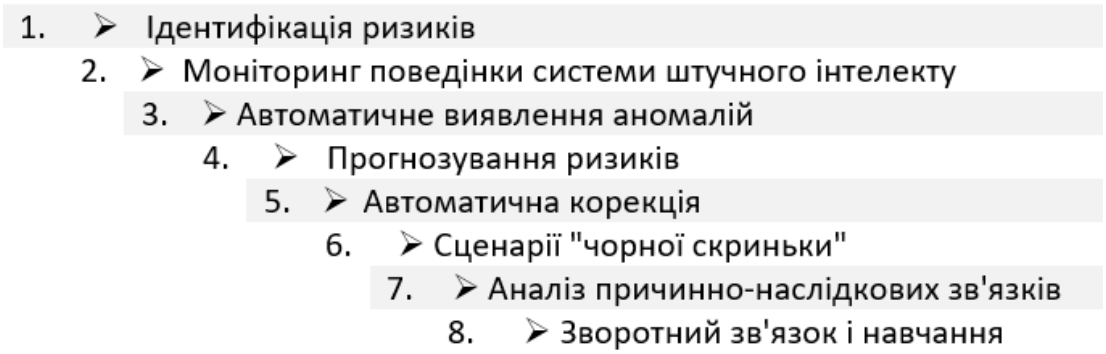

Рис. 3.6. Етапи використання систем штучного інтелекту для управління ризиками

Одним з найважливіших заходів є створення системи управління ризиками ШІ, на якому має базуватися регуляторна політика держави у цій галузі.

Система управління ризиками базується на використанні класичного підходу до оцінки ризиків, який наведено нижче:

1. Ідентифікація ризиків: це початковий етап, де ідентифікуються потенційні ризики, пов’язані з ШІ. Це може включати розробку політик та алгоритмів, використання даних, вплив на користувачів і багато іншого.

2. Оцінка ризиків: після ідентифікації ризиків вони повинні бути оцінені за їх потенційним впливом та ймовірністю виникнення. Це може включати аналіз чутливості, упередженості, моделювання ризиків або інші методики оцінки.

3. Прийняття рішень щодо ризиків: після оцінки ризиків слід вирішити, як краще ними управляти. Це може включати прийняття рішень про вдосконалення процесів, модифікацію баз даних та баз знань ШІ або внесення змін в спосіб використання ШІ.

4. Управління ризиками: це включає в себе виконання дій по управлінню ризиками, які було визначено на попередньому етапі. Це може включати виконання контрольних заходів, навчання персоналу, зміни в дизайні систем та інші заходи.

5. Моніторинг та перегляд ризиків: Ризики слід постійно моніторити та переглядати, щоб впевнитись, що вони залишаються під контролем та що вжиті заходи ефективні. Це може включати регулярний аудит, моніторинг впливу, збір зворотного зв’язку від користувачів та інші механізми моніторингу [54].

Всі ці етапи мають повторюватись циклічно, оскільки ризики можуть змінюватися з часом. Також, оцінку ризиків необхідно проводити на всіх етапах життєвого циклу системи ШІ.

Реалізація заходів з управління ризиками ШІ пропонується за трьома напрямками: нормативно-правовим, технічним та організаційним.

Нормативно-правові заходи:

1. Визначення та прийняття державної політики в галузі ШІ.

2. Законодавче регулювання: створення чітких законодавчих норм, які регулюють розробку та використання ШІ, може бути ефективним способом відповіді на ці загрози. Держава може прийняти закони, які обмежують використання ШІ в автономних збройних системах або встановлюють стандарти безпеки для ШІ в кібернетичних системах.

3. Міжнародне співробітництво: участь в міжнародних угодах та ініціативах, спрямованих на регулювання ШІ, створенні міжнародних норм і стандартів безпеки для ШІ та забезпечення їх використання в Україні.

Технічні заходи:

1. Розробка безпечних систем ШІ: сприяння на рівні держави розробці та впровадженню безпечних систем ШІ, що включають вбудовані заходи безпеки.

2. Обмеження доступу до даних: Встановлення технічних обмежень на доступ ШІ до даних, таких як персональні дані громадян, що запобігає несанкціонованому використанню цих даних.

3. Створення систем ШІ для проведення аудиту знань прикладних систем ШІ.

4. Розробка механізмів виявлення ознак роботи небезпечних ШІ.

5. Розробка заходів з активної протидії небезпечним ШІ.

Організаційні заходи:

1. Управління ризиками: створення моделі управління ризиками ШІ, яка містить механізми визначення рівнів загроз та імовірності їх реалізації в різних областях діяльності людини, суспільства, держави.

2. Освіта: проведення освітніх кампаній для збільшення обізнаності про потенційні ризики, пов'язані з ШІ.

3. Співпраця з приватним сектором: держава співпрацює з приватним сектором для створення безпечних систем ШІ і розробки ефективних стратегій протидії потенційним загрозам.

4. Створення спеціалізованих державних органів: створення спеціалізованих органів, які будуть відповідальні за моніторинг та реагування на загрози, пов'язані з ШІ.

5. Організаційне обмеження доступу до масивів даних та спеціалізованих баз знань створених державними установами для використання їх в моделях навчання ШІ.

3.5. Підтримки прийняття рішення щодо відновлення попереднього стану після кіберінцидентів

Суттєвою проблемою щодо визначення причин пошкодження компонентів програмного забезпечення та виявлення дефектів у його роботі внаслідок виникнення кіберінцидентів, включаючи вплив кібератак, є неповнота і суперечливість інформації стосовно властивостей дефектів, способів їх відновлення, а також переліку технологічних операцій та послідовності їх призначення з метою забезпечення захисту інформаційних ресурсів, що обробляються в ІКС та комплексах.

Технологію відновлення пошкодженого програмного забезпечення складно формалізувати за відсутності теорії і математичних моделей, що описують функціональні залежності між об’єктами, які приймають участь у процесі діагностування та відновлення пошкодженого програмного забезпечення.

Розв’язання вище описаної задачі потребує застосування спеціального математичного апарату, а також розробки методичних та технологічних засад щодо створення та впровадження спеціалізованих автоматизованих СППР з метою відновлення пошкодженого програмного забезпечення, внаслідок впливу кібератак.

Це дозволить класифікувати та виявляти якісні зв’язки між технологічними операціями, а також формалізувати технологію їх призначення за допомогою прийняття рішень відносно розв’язання складних структурованих або неструктурованих завдань стосовно оптимального вибору способу відновлення дефектів та технологічних операцій щодо усунення дефектів.

На теперішній час дослідженням та розробкою систем підтримки прийняття рішення активно займаються вітчизняні та закордонні науковці.

Проблеми формування методології проєктування, класифікації, архітектури, розробки та застосування СППР, а також методів та моделей прийняття раціональних рішень на підставі системного аналізу висвітлюються у роботах багатьох вчених.

Так у наукових працях [55–58] представлені методологія проєктування інформаційних систем підтримки прийняття рішень та альтернативні підходи до застосування і супроводження СППР. Особливий інтерес у зазначених наукових роботах представляє запропонований метод розробки систем підтримки прийняття рішень на основі мережі Байєса, а також систем, обробка інформації в яких здійснюється шляхом використання експертних оцінок.

У роботах [59, 60] розглядаються теоретичні та практичні питання щодо технології прийняття рішень, яка передбачає застосування певної послідовності управлінських операцій і процедур, які необхідні під час використання СППР. Значна увага приділяється операціям присвяченим питанням діагностування виявлених проблем, визначення можливих способів їх розв’язання та оцінювання варіантів їх усунення.

Окремі дослідники [61, 62], спираючись на важливість забезпечення рівня інформаційної безпеки автоматизованих систем та комплексів під час накопичування та обробки даних, пропонують застосування СППР для практичної реалізації процесів обробки інформації евристичного походження, а також щодо підвищення рівня інформаційної безпеки підприємств, на підставі індивідуального підбору методів та засобів, що належать до політики безпеки суб’єкта господарювання, з використанням експертних даних.

Інтерес представляє робота науковців [63], яка може бути взята за основу для розробки концептуальних підходів з проєктування систем підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. У дослідженні, на підставі досвіду та наукових джерел надаються методичні матеріали щодо розробки систем управління екологічною безпекою. На думку фахівців у галузі екологічної безпеки, такі системи необхідні для виявлення негативних тенденцій в екологічних процесах, знаходження взаємозв'язків між параметрами і факторами, що впливають на екологічну безпеку, а також розробку пропозицій щодо покращення стану управління екологічною безпекою.

Питання безпеки систем підтримки прийняття рішень розглядається у роботі [64]. Автори стверджують , що внаслідок загроз інформаційній та кібербезпеці, питання захисту інформації в СППР набувають усе більшої актуальності та пропонують методичні, технологічні заходи, а також програмні засоби щодо побудови захищених СППР.

Метою цього розділу є формування методичних рекомендацій та пропозицій з питань розробки структурно-логічної схеми автоматизованої системи підтримки прийняття рішення, яка дозволяє визначати властивості дефектів програмного забезпечення, способи та послідовність їх відновлення після впливу кібератак.

Система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, являє собою складну ієрархічну структуру з високим рівнем організації. У відповідності до призначення зазначена система повинна забезпечити виконання наступних завдань:

$$Z=\{zi\},i=1....n(1), \qquad (3.20)$$

де *z1* – введення завдання;

*z*2 – прийняття рішення;

*z*3 – програмна реалізація щодо прийняття рішення;

z4 – зберігання постійної інформації;

z5 – надання результатів рішення завдання у текстовій та графічній інформації;

*z*6 – визначення спеціальних завдань;

*z*7 – оцінювання результатів.

СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак включає ряд підсистем, а саме, з методичних, технічних, інформаційних, введення бази даних тощо (див. рис. 3.7).

Рис. 3.7. Структурна схема системи підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак

Компонентами методичного забезпечення в СППР є документи, що регламентують технологію процесу прийняття рішення під час роботи з системою.

Метою документів є організація функціонування СППР з мінімальними витратами та високою якістю прийняття рішень. Така задача передбачає проведення робіт з формалізації процесу прийняття та підтримки рішень, яка визначає послідовність виконання кожної проєктної задачі, з максимально структурованим описом прийняття рішення.

Робота СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу передбачає наступне:

– надання відомостей, що стосується інформації о можливих комп'ютерних атаках, дефектів програмного забезпечення, прогнозованих ситуаціях та наслідків від прийняття рішення;

– визначення способів відновлення дефектів пошкодженого програмного забезпечення, їх аналіз та можливість корегування;

– оцінку прийнятих рішень, формування послідовності операцій та кращого маршруту відновлення програмного забезпечення.

Завдання СППР – автоматизація усіх процедур прийняття рішень, пошук інформації та її аналіз, попередню обробку інформації та прийняття самого рішення. Окремі процедури в СППР не підлягають формалізації, тому частина з них буде виконуватися у інтерактивному режимі.

Програмні компоненти СППР реалізують типові запити. Зазначені запити повинні включати опис структури даних, типові команди, складні лексеми. Під час застосування запитів, передбачається вивід результатів запиту у форматі мови XML.

Особливе значення у СППР приділяється інформаційно-довідкової підсистемі. Засоби зазначеної підсистеми, повинні реалізувати введення інформації, формування словників щодо опису ситуацій, виводу довідкової інформації, можливість підключення зовнішніх програмних компонентів.

У системі активно використовується реляційна база даних, програмні засоби якої повинні забезпечувати зберігання інформації та надання її користувачам системи у зручному форматі.

У якості програмного продукту, який підтримує структурні компоненти бази даних, може бути використовуватися програмне забезпечення сучасних систем керування базою даних. Екземпляр системи керування базою даних повинен підтримувати роботу декілька баз та забезпечувати їх управління та адміністрування, використовуючи для цього простий та зручний інтерфейс. Основу структури бази даних складають таблиці, між якими забезпечується взаємозв'язок. Для забезпечення цілісності даних в таблицях застосовуються ключові поля.

Для зберігання інформації в СППР виконується створення резервної копії, а також передбачена можливість відновлення роботи системи в разі пошкодження файлів даних або інформаційних масивів бази.

Засоби програмного забезпечення СППР повинні забезпечувати:

– супроводження бази даних інформаційного забезпечення системи (введення, отримання нормативно-довідкової інформації, класифікаторів, довідників, картотек);

– кодування інформації;

– працездатність СППР у локальної мережі підприємства;

– застосування клієнт-серверної архітектури;

– застосування сучасних телекомунікаційних технологій та введення електронної пошти;

– багатокористувальний режим роботи користувачів;

– цілодобовому режимі.

Програмне забезпечення СППР відноситься до спеціального програмного забезпечення, яке може працювати під управлінням різних версій операційної системи Windows. Зазначене спеціальне програмне забезпечення СППР забезпечує рішення інформаційно-аналітичних, розрахункових та завдань щодо виконання технологічних операцій з визначення стану дефекту програмного забезпечення, призначення способу його відновлення та послідовності усунення дефектів програмного забезпечення. Крім того програмне забезпечення є

уніфікованим засобом щодо організації інформаційної взаємодії між користувачами і окремими програмними компонентами (модулями).

Компонентами технічного забезпечення СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, є комплекс технічних засобів у складі серверного та мережного обладнання, клієнтські машини.

Інформаційне забезпечення СППР містить інформацію про існуючі кібератаки, які можуть виникати під час експлуатації автоматизованих систем та комплексів, дефекти програмного забезпечення, способи їх відновлення, технологічні операції що застосовуються з метою забезпечення відновлення роботи програмних компонентів систем тощо.

Інформацію, яка обробляється в СППР, можливо позначити як *{І}*. Зазначена інформація включає множину інформації *{Ік},* що необхідна для керування системою, множину вхідній інформації *{Ів},* множину термінальної інформації*{ІТ}*.

Множина інформації для керування СППР може бути описана, як:

$$Ік = \{Ік1, Ік2, Ік3\}, \quad (3.21)$$

де *Ік1* – інформація що належить до програм;

Ік2 – інформація, що належить до проєктних рішень;

Ік3 – відомості щодо оцінки прийняття рішень;

Вхідна інформація *{Ів}* включає:

$$Ів = \{Ів1, Ів2, Ів3\}, \quad (3.22)$$

де *Ів1* – інформацію, що містить вхідні данні щодо наявні дефекти програмного забезпечення;

Ів2 – інформацію, що є загальної для системи;

Ів3 – інформацію**,** що містить нормативно-довідникові данні, необхідні для введення аналізу та прогнозування. Зазначена інформація представляє собою форми документів, які можуть бути первинними, вторинними та нормативними. Вторинні документи розподілені на групи: текстові, звіти, класифікатори,

картотеки. Для організації інформаційного забезпечення у підсистемі СППР використовуються принципи удосконалення інформації.

Під час організації інформаційного забезпечення підтримуються власні принципи:

– виключення масових первинних документів;
– застосування єдиних потоків інформації;
– одноразове введення повідомлень в систему;
– використання інформації, яка має оптимальну цінність.

Форми усіх документів системи уніфіковані. Це дозволяє значно покращити трудомісткість налаштування програм, а також експлуатації підсистеми.

Під час роботи уся інформація, що використовується на ручних операціях, значна зменшена за рахунок того, що користувач здійснює роботу з системою у інтерактивному режимі, шляхом введення в систему запитань та отримання від машини відповіді.

Система класифікації та кодування побудована на локальних цифрових кодах, які використовуються в основному самою системою.

Нормативна база підсистеми зберігається у масивах бази. Додатково у системі використовуються групи документи, які класифікуються на первинні, вторинні та нормативні документи.

Висновки до розділу 3

1. В рамках дослідження запропонована часткова модель загроз безпеки корпоративної мережі на основі концепції zero-trust, що може бути основою покращеної політики безпеки підприємства та надає можливість аналізувати стан кібербезпеки мережі виходячи з реалізації заходів з підвищення кіберкультури.

2. Під час дослідження вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID в напрямку покращення його

функціональних та інженерних характеристик в плані автентифікації суб'єктів інформаційної взаємодії під час доступу до інформаційних та технічних ресурсів систем. Це дозволяє в подальшому перевести в площину створення дослідного зразка відповідного багатофункціонального засобу автентифікації та підвищити за рахунок цього ефективність підсистеми ідентифікації і автентифікації.

3. В розділі вперше запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. На відміну від існуючих методів при вирішенні завдання автентифікації приховується зміст і обсяг інформаційного трафіку, клієнт і сервер отримують можливість обирати контейнери для доставки даних, замість складних фіксованих логінів клієнт отримує доступ до візуалізованого подання його особистої автентифікаційної інформації. Це дозволяє приховувати від зловмисника чутливу інформацію, яка може бути використана для реалізації атак, включаючи її руйнування, що в свою чергу знижає ймовірність помилкової автентифікації клієнта або сервера у випадку реалізації цільових атак.

В якості пріоритетних напрямів подальших досліджень уявляється проведення розрахунків параметрів процедури обміну та їх імітаційного моделювання, а також визначення практично застосовних значень параметрів стеганографічного протоколу з метою забезпечення його необхідної швидкодії.

4. Найважливішим етапом в системі управління ризиками, які виникають в наслідок використання СШІ є оцінка ландшафту можливих ризиків та їх ідентифікація. Це ітеративний процес пошуку нових типів ризиків та профілювання їх основних характеристик для подальшої інтерпретації, аналізу та обробки. Проведений аналіз загроз та ризиків для корпоративних мереж у зв'язку із широким застосуванням СШІ дозволів визначити пов'язані з цією технологією чотири нових категорії загроз, включаючи: посилення кібератак, посилення комп'ютерної розвідки, атаки отруєння даних що використовуються для навчання ШІ, містифікація даних.

5. Завдання обробки ризиків за допомогою ШІ, включаючи їхню ідентифікацію, можливо вирішувати як задачу пошуку аномалій в масивах даних про діяльність, що стосується галузі застосування ризик-менеджменту. Аномальні спостереження в таких даних можуть пояснюватися наявністю взаємозв'язків та взаємодій між об’єктами та суб’єктами діяльності, що призводять до появи ще не ідентифікованих ризикових ситуацій та відповідних наслідків, або є потенційними джерелами виникнення таких ситуацій у майбутньому.

6. В умовах концепції zero-trust актуальним постає питання автоматизації процесів і процедур прийняття рішень щодо відновлення попереднього стану корпоративних мереж після кіберінцидентів. Аналіз впровадження та експлуатації у різних галузях виробництва СППР дозволів запропонувати структурно-логічну схему відповідної СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Запропонована схема являє собою складну ієрархічну структуру з високим рівнем організації та складається з окремих підсистем, які забезпечують виконання задач з аналізу дефектів програмного забезпечення, вибору способів їх відновлення, оцінку та обрання найкращих альтернатив відновлення.

7. Зазначена технологія обробки інформації в СППР по відновленню пошкодженого програмного забезпечення внаслідок впливу кібератак, у подальшому дає можливість здійснювати прийняття рішень відносно розв’язання складних структурованих або неструктурованих задач з метою оптимального вибору способу відновлення дефектів та технологічних операцій по їх усуненню.

Список використаних джерел у розділі 3

1. Гречанінов, В., Кузьменко, Г., Морозов, А., & Лопушанський, А. (2018). Мережа ситуаційних центрів органів державної влади – базис для підвищення ефективності їх діяльності (взаємодії). Математичні машини і системи, 3, 32–39.

2. Skiter, I, Hulak, H., Grechaninov, V., Klymenko, V., & Ievlev, N. (2021) System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure. Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II-2021), 3187, 244–250.

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910

4. Гречанінов, В., Оксанич, І., & Лопушанський, А. (2022). Використання хмарних технологій для вирішення питань інтеграції інформації у багаторівневих системах управління. Системи керування та комп'ютери, 4(300), 24–34. https://doi.org/10.15407/csc.2022.04.024

5. Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable Zero Trust for Cloud Computing Environments. Computers & Security, 110, 102419. https://doi.org/10.1016/j.cose.2021.102419

6. Buckbee, M. (2023). What Is Zero Trust? Architecture and Security Guide. https://www.varonis.com/blog/what-is-zero-trust

7. Hulak, H., Skladannyi, P., Sokolov, V., Hulak, Y., & Korniiets, V. (2023). Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System. Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN), 3530, 102–111.

8. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

9. Літвінчук, І., Корчомний, Р., Коршун, Н., & Ворохоб, М. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112

10. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові

політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

11. The Manufacture of Transponders and Contactless Smart Cards. (2003). RFID Handbook, 329–339. Portico. https://doi.org/10.1002/0470868023.ch12

12. Anakhov, P., Zhebka, V., Koretska, V., Sokolov, V., & Skladannyi, P. (2022). Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir. Proceedings of the Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things (TTSIIT), 3149, 169–176.

13. Астапеня, В., Соколов, Ю., & Таждіні, М. (2019). Результати та засоби оцінки ефективності систем фокусування для підвищення доступності в безпроводових мережах. Кібербезпека: освіта, наука, техніка, 4, 90–103. https://doi.org/10.28925/2663-4023.2019.4.90103

14. Літвінчук, І., Коршун, Н., & Ворохоб, М. (2020). Спосіб оцінювання інтегрованих систем безпеки на об’єкті інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 135–143. https://doi.org/10.28925/2663-4023.2020.10.135143

15. Microchip Technology. (2004). MicroID 125 kHz RFID. System Design Guide. http://ww1.microchip.com/downloads/en/devicedoc/51115f.pdf

16. Microchip Technology. (2004). MicroID 13.56 MHz RFID. System Design Guide. http://ww1.microchip.com/downloads/en/devicedoc/21299e.pdf

17. ISO/IEC 18000-1:2004 (en). Information Technology. Radio Frequency Identification for Item Management. Part 1: Reference Architecture and Definition of Parameters to be Standardized. https://www.iso.org/standard/34112.html

18. ISO/IEC 18000-2:2009 (en). Information Technology. Radio Frequency Identification for Item Management. Part 2: Parameters for Air Interface Communications below 135 kHz. https://www.iso.org/standard/46146.html

19. ISO/IEC 18000-3:2010 (en). Information Technology. Radio Frequency Identification for Item Management. Part 3: Parameters for Air interface Communications at 13.56 MHz. https://www.iso.org/standard/53424.html

20. Brzhevska, Z., Kyrychok, R., Anosov, A., Skladannyi, P., & Vorokhob, M. (2021). Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3188(2), 257–264.

21. Гулак, Г., Жданова, Ю., Складанний, П., Гулак, Є., & Корнієць, В. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 1(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158

22. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of Applied Cryptography. https://doi.org/10.1201/9780429466335

23. Шелест, М. (1999). Цифрова стеганографія та її можливості. Захист інформації, 1, 11–19.

24. Стасюк, О., Гнатюк, С., Довгич, Н., & Літош, М. (2011). Сучасні стеганографічні методи захисту інформації. Захист інформації, 13(1). https://doi.org/10.18372/2410-7840.13.1994

25. Setiadi, D. R. I. M., Rustad, S., Andono, P. N., & Shidik, G. F. (2023). Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset). Signal Processing, 206, 108908. https://doi.org/10.1016/j.sigpro.2022.108908

26. Korn, G. A., &Korn, T. M. (2013). Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review. Courier Corporation.

27. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

28. Bagchi, S. (2023). Why We Need to See Inside AI's Black Box. Scientific American. https://www.scientificamerican.com/article/why-we-need-to-see-inside-ais-black-box/

29. Auchard, E., & Ingram, D. (2018). Cambridge Analytica CEO Claims Influence on U.S. Election, Facebook questioned. https://www.reuters.com/article/us-facebook-cambridge-analytica-idUSKBN1GW1SG

30. Future of Life Institute. (2023). Pause Giant AI Experiments: An Open Letter. https://futureoflife.org/wp-content/uploads/2023/05/FLI_Pause-Giant-AI-Experiments_An-Open-Letter.pdf

31. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

32. Abdullah, M. F., & Ahmad, K. (2013). The Mapping Process of Unstructured Data to Structured Data. In International Conference on Research and Innovation in Information Systems (ICRIIS), 151–155. https://doi.org/10.1109/icriis.2013.6716700

33. Abdullah, M. F., & Ahmad, K. (2015). Business Intelligence Model for Unstructured Data Management. In International Conference on Electrical Engineering and Informatics (ICEEI), 473–477. https://doi.org/10.1109/iceei.2015.7352547

34. Venieris, S. I., Bouganis, C.-S., & Lane, N. D. (2023). Multiple-Deep Neural Network Accelerators for Next-Generation Artificial Intelligence Systems. Computer, 56(3), 70–79. https://doi.org/10.1109/mc.2022.3176845

35. Jiang, D. (2021). Application of Artificial Intelligence in Computer Network Technology in Big Data Era. In International Conference on Big Data Analysis and Computer Science (BDACS), 211–215. https://doi.org/10.1109/bdacs53596.2021.00063

36. Bian, L. (2023). Design of Computer Network Security Defense System Based on Artificial Intelligence and Neural Network. Wireless Personal Communications. https://doi.org/10.1007/s11277-023-10721-9

37. Grechaninov, V., Hulak, H., Sokolov, V., Skladannyi, P., & Korshun, N. (2021). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149, 107–117.

38. Hulak, H., Buriachok, V., Skladannyi, P., & Kuzmenko, L. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. Cybersecurity: Education, Science, Technique, 2(10), 6–28. https://doi.org/10.28925/2663-4023.2020.10.628

39. Moskalenko, V., Kharchenko, V., Moskalenko, A., & Kuzikov, B. (2023). Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods. In Algorithms, 16(3), 165. https://doi.org/10.3390/a16030165

40. Madiega, T. (2023). Artificial Intelligence Act. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

41. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/nist.ai.100-1

42. Human-Centered Artificial Intalligence. (2023). The Artificial Intelligence Index 2023. https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf

43. Satter, R. (2023). Exclusive: AI Being Used for Hacking and Misinformation, top Canadian Cyber Official Says. https://www.reuters.com/technology/ai-being-used-hacking-misinfo-top-canadian-cyber-official-says-2023-07-20

44. Sly, L. (2018). U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging. https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

45. Rahman, M., Siddika Arshi, A., Hasan, M., Farzana Mishu, S., Shahriar, H., & Wu, F. (2023). Security Risk and Attacks in AI: A Survey of Security and Privacy. In IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 1834–1839. https://doi.org/10.1109/compsac57700.2023.00284

46. MathCo. (2023). Data Poisoning and Its Impact on the AI Ecosystem. https://themathcompany.com/blog/data-poisoning-and-its-impact-on-the-ai-ecosystem

47. Zhu, Y., Wen, H., Wu, J., & Zhao, R. (2023). Online Data Poisoning Attack Against Edge AI Paradigm for IoT-Enabled Smart City. Mathematical Biosciences and Engineering, 20(10), 17726–17746. https://doi.org/10.3934/mbe.2023788

48. Knight, W. (2023). The AI-Powered, Totally Autonomous Future of War Is Here. https://www.wired.com/story/ai-powered-totally-autonomous-future-of-war-is-here

49. Keizman, O., & Divinsky, Y. (2023). New Attack Technique Alert. AI Package Hallucinations. https://vulcan.io/blog/ai-hallucinations-package-risk

50. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови.

51. Barafort, B., Mesquida, A., & Mas, A. (2018). ISO 31000-based Integrated Risk Management Process Assessment Model for IT Organizations. Journal of Software: Evolution and Process, 31(1). https://doi.org/10.1002/smr.1984

52. Brzhevska, Z., Dovzhenko, N., Haidur, H., Anosov, A., & Vorokhob, M. (2021). Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model. Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2923, 272–276.

53. Бідюк, П., Кожухівський, А., & Кожухівська, О. (2013). Система підтримки прийняття рішень для аналізу і прогнозування стану підприємства. Радіоелектроніка, інформатика, управління, 1, 128–136.

54. Kipchuk, F., Sokolov, V., Skladannyi, P., & Ageyev, D. (2021). Assessing Approaches of IT Infrastructure Audit. In IEEE 8th International Conference on Problems of Infocommunications, Science and Technology. https://doi.org/10.1109/picst54195.2021.9772181

55. Бурячок, В., & Соколов, В. (2018). Технологія забезпечення об’єктивного контролю захищеності корпоративних інформаційно-телекомунікаційних систем і мереж. Матеріали Всеукраїнської науково-практичної конференції «Актуальні питання протидії кіберзлочиннос-ті та торгівлі людьми», 242–247.

56. Бідюк, П., Терентьєв, О., & Коновалюк, М. (2010). Байєсівські мережі в технологіях інтелектуального аналізу даних. Штучний інтелект, 2, 104–113.

57. Нестеренко, О., Савенков, О., & Фаловський, О. (2016). Інтелектуальна система підтримки прийняття рішень: навчальний посібник. Національна академія управління.

58. Ситник, В., & Дубровіна, А. (2002). Проблеми моделювання рішень у групових СППР. Моделювання та інформаційні системи в економіці, 68, 9–14.

59. Цюцюра, С., Криворучко, О., & Цюцюра, М. (2012). Теоретичні основи та сутність управлінських рішень. Моделі прийняття управлінських рішень. Управління розвитком складних систем, 9, 50–58.

60. Волошин, О., & Мащенко, С. (2010). Моделі та методи прийняття рішень: навчальний посібик. Видавничо-поліграфічний центр «Київський університет».

61. Бурячок, В., Толюпа, С., Аносов, А., Козачок, В., & Лукова-Чуйко, Н. (2015). Системний аналіз та прийняття рішень в інформаційній безпеці: підручник, ДУТ.

62. Азарова, А., Дьогтєва, І., & Шиян, А. (2022). Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. Інформаційні технології та комп'ютерна інженерія, 1, 12–18.

63. Яцишин, А., Попов, О., Артемчук, В., Ковач, В., & Зінов'єва, І. (2019). Автоматизовані інформаційні системи підтримки прийняття управлінських рішень у галузі екологічної безпеки. Інформаційні технології і засоби навчання, 4, 286–300.

64. Ковтунець, В., Нестеренко, О., & Савенков, О. (2016). Безпека систем підтримки прийняття рішень: навчальний посібник. Національна академія управління.

ВИСНОВКИ

У дисертації вирішено актуальне наукове завдання, яке полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в ІКС, а також впровадженню заходів управління кіберкультурою на підприємстві.

У процесі виконання дисертаційного дослідження отримано такі основні результати:

1. Вперше запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. На відміну від існуючих методів при вирішенні завдання автентифікації приховується зміст і обсяг інформаційного трафіку, клієнт і сервер отримують можливість обирати контейнери для доставки даних, замість складних фіксованих логінів клієнт отримує доступ до візуалізованого подання його особистої автентифікаційної інформації. Це дозволяє приховувати від зловмисника чутливу інформацію, яка може бути використана для реалізації атак, включаючи її руйнування, що в свою чергу знижає ймовірність помилкової автентифікації клієнта або сервера у випадку реалізації цільових атак.

2. Вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID. Це дозволяє в подальшому перевести в площину створення дослідного зразка відповідного багатофункціонального засобу автентифікації та підвищити за рахунок цього ефективність підсистеми ідентифікації і автентифікації.

3. Подальшого розвитку набула методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що сукупно з методикою оцінки трендів загроз кібербезпеки дає можливість оперативного реагування з

боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

В дослідженні принципового переходу від статистичної політики доступу до критичних даних, яка не корегується залежно від поточного контексту поведінки користувача та наступних його змін, до динамічної політики безпеки, що адаптується до поведінки користувача (його кіберкультури) для поточної та попередніх транзакцій. Запропоноване рішення щодо надання доступу до ресурсів з простим інтерфейсом на основі стеганографічного протоколу з одного боку візуалізує інформацію про наявні параметри безпеки, з іншого – не розкриває їх зміст та не потребує запам’ятовування не складних символьних (буквено-цифрових) конструкцій та структури таких даних. Перспективність запропонованих рішень для таких галузей як телемедицина, дистанційне управління засобами фізичної безпеки та охорони, систем дистанційної освіти тощо є очевидною

Таким чином, поставлене актуальне наукове завдання розв’язане у повному обсязі. Усі визначені часткові завдання вирішено, мету досліджень досягнуто.

ДОДАТОК А

ЗАТВЕРДЖУЮ
Директор Інституту програмних систем
Національної академії наук України
д.т.н., с.н.с., лауреат державної премії
України в галузі науки і техніки

І.П. СІНІЦИН

__ вересня 2023 року

АКТ
впровадження матеріалів дисертаційних досліджень
Ворохоба Максима Віталійовича
на тему:
«Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust»

Комісія у складі:

голова комісії – заступник директора з наукової роботи Шевченко В.Л., д.т.н., проф., лауреат державної премії України в галузі науки і техніки;

члени комісії:

учений секретар Дергильова О.В., к.т.н., с.н.с.
завідувача відділу Федоренко В.М., к.е.н.

Встановила та цим актом засвідчує, що нижчеперелічені матеріали дисертаційних досліджень Ворохоба Максима Віталійовича, а саме:

- вперше запропонований та математично обґрунтований метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції Zero Trust.
- вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID.

Впроваджені в Інституті програмних систем Національної академії наук України. Надані матеріали були використані при формуванні плану перспективних досліджень. Даний акт не є підставою для фінансових зобов'язань.

Голова комісії Віктор ШЕВЧЕНКО

Члени комісії Олена ДЕРГИЛЬОВА

Руслан ФЕДОРЕНКО

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

бульвар.Чоколівський, 13, м.Київ, 03186, тел/факс (044) 245-88-38, тел. 245-87-97
E-mail: itgis@nas.gov.ua, м. Києва, ЗКПО: 26022051, МФО: 820172

_____ № _____ На № _____ від _____

АКТ
про впровадження результатів дисертаційного дослідження
Ворохоба Максима Віталійовича
на тему «Моделі і методи вдосконалення політики безпеки підприємства на основі методології zero-trust»,
поданої на здобуття наукового ступеня доктора філософії
зі спеціальності 125 «Кібербезпека»

Цим Актом, ґрунтуючись на рішенні відділу інформаційної безпеки Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (ІТГІП НАНУ), засвідчуємо, що *нижчеперелічені наукові положення, а саме:*

- вперше запропонований та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust;
- вдосконалена методики формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології радіочастотної ідентифікації 'radio frequency identification' (RFID);
- методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що сукупно з методикою оцінки трендів загроз кібербезпеки дає можливість оперативного реагування з боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

Розроблені особисто Ворохобом Максимом Віталійовичем у ході проведення ним дисертаційних досліджень та *отримали високу оцінку* при обговоренні на засіданнях відділу інформаційної безпеки ІТГІП НАНУ.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес ІТГІП НАНУ у робочих програмах навчальних дисциплін спеціальностей 113 Прикладна математики та 122 Комп'ютерні науки третього (освітньо-наукового) рівня вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення лабораторій ІТГІП НАНУ.

Дослідження Ворохоба Максима Віталійовича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Директор, д.т.н., професор
Член-кореспондент НАН України Олександр ТРОФИМЧУК

Україна * Національна академія наук України * Інститут телекомунікацій і глобального інформаційного простору * Ідентифікаційний код 26022051