https://doi.org/10.31891/2307-5732-2025-351-27
УДК 004.056

КОПИТІН ЮРІЙ
Академія електронного управління
https://orcid.org/0000-0003-1617-6556
e-mail: y.v.kopytin@gmail.com
КОПИТІНА МАРИНА
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0009-1665-6905
e-mail: myr19@i.ua
КОРЧИНСЬКИЙ ВОЛОДИМИР
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
ХАЛЕД АЛЬ-ФАЙЮМІ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-4624-2569
e-mail: khaled@alfaiomi.com
БЄЛОВА ЮЛІЯ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-0631-7282
e-mail: bilovaulia@gmail.com

МІНІМІЗАЦІЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У роботі проведено комплексний аналіз проблеми мінімізації інсайдерських загроз у системах захисту інформації компаній. Визначено ключові вектори загроз, що виникають у результаті діяльності інсайдерів, а також їхній вплив на інформаційну безпеку підприємства. Розглянуто основні канали витоку інформації та способи їх нейтралізації. Здійснено оцінку зовнішніх і внутрішніх ризиків підприємств з урахуванням ймовірності реалізації інсайдерських атак та потенційних фінансових і репутаційних збитків. Запропоновано підхід до класифікації інсайдерських загроз залежно від рівня доступу співробітників, мотивів та методів несанкціонованого використання інформації. На основі порівняльного аналізу ризиків запропоновано методику оцінки ефективності впровадження заходів кібербезпеки з урахуванням величини витрат на їх підтримку. Досліджено залежність між рівнем інвестицій у системи інформаційного захисту та ступенем зниження ризиків. Актуальність роботи обґрунтовується доцільністю для компаній проводити регулярний аналіз сучасних технологій і інструментів, які можуть бути використані для виявлення, попередження і запобігання інсайдерським загрозам, а також проводити безперервний моніторинг кіберзагроз, які постійно еволюціонують і удосконалюються методи атак. Основними завданнями дослідження є: огляд різних видів інсайдерських загроз та їх впливу на інформаційну безпеку підприємств; аналіз методів та стратегій мінімізації інсайдерських загроз; розробка рекомендацій для підприємств щодо впровадження комплексної стратегії захисту від інсайдерських загроз, адаптованої до змінних умов ведення бізнесу.

Отримані результати можуть бути використані для побудови ефективної системи управління ризиками інформаційної безпеки, що забезпечить стабільний розвиток підприємств в умовах зростаючих кіберзагроз.

Ключові слова: інсайдерські загрози, інформаційна безпека, кібербезпека, управління ризиками, мінімізація загроз, моніторинг, захист інформації, фінансові втрати, кіберзагрози, інвестиції в безпеку, адаптація.

KOPYTIN YURII
e-Governance Academy, Kyiv, Ukraine
KOPYTINA MARYNA, KORCHYNSKYI VOLODYMYR, KHALED ALFAIOMI, BIELOVA IULIIA
State University of Intellectual Technologies and Telecommunications

MINIMIZATION OF INSIDER THREATS IN INFORMATION PROTECTION SYSTEMS

The paper provides a comprehensive analysis of the issues of minimizing insider threats in enterprises' information protection systems. The key vectors of threats are identified, which appears as result of insider activities, as well as their impact on the information security of the enterprise. The main channels of information leakage and methods of their neutralization are considered. The external and internal risks of the enterprise are assessed, taking into account the probability of insider attacks and potential financial and reputational losses. The approach to classifying insider threats depending on the level of employee access, motives and methods of unauthorized use information is proposed. Based on comparative analysis of risks, methodology for assessing the effectiveness of implementing cybersecurity measures, taking into account the costs of their support, is proposed. The dependence between the level of investment in information protection systems and the degree of risk reduction is researched. The relevance of the paper is justified by the expediency for companies to conduct regular analysis of modern technologies and tools that can be used for detection, warning and prevention of the insider threats, as well as to conduct continuous monitoring of cyber threats, which are constantly evolving and improving the attack methods. The main objectives of the research are: an overview of various types of insider threats and their impact on the enterprises' information security; analysis of methods and strategies for minimizing insider threats; development of recommendations for enterprises on the implementation of comprehensive strategy for protecting against insider threats, adapted to changing business conditions.

The obtained results can be used to construct an effective information security risk management system, which will ensure the stable development of the enterprise in the conditions of growing cyber threats.

Keywords: insider threats, information security, cybersecurity, risk management, threat minimization, monitoring, information protection, financial losses, cyber threats, security investments, adaptation.

Стаття надійшла до редакції / Received 11.04.2025
Прийнята до друку / Accepted 26.04.2025

Постановка проблеми

Інсайдерські загрози є одними з найбільш складних і небезпечних викликів для систем захисту інформації (СЗІ) підприємств у сучасному світі [1]. У той час, як зовнішні загрози, такі як хакерські атаки чи віруси, отримують більше уваги, інсайдери – співробітники, підрядники або інші особи, які мають доступ до внутрішньої інформації компанії – здатні викликати не менш, а часто й більш серйозні проблеми порушення безпеки СЗІ. Причини цього різноманітні [2]: від неуважності чи недостатньої кваліфікації працівників до навмисних спроб зловживання інформацією або саботажу. Інсайдерські загрози можна класифікувати за різними критеріями, такими як мотивація, рівень доступу, методи реалізації та наслідки для організації. При цьому, загрози бувають умисними або випадковими, однак в обох випадках вони завдають суттєвої шкоди репутації, фінансовій стабільності і правовому статусу підприємства.

Отже, важливим аспектом стає впровадження ефективних методів мінімізації ризиків, пов'язаних з інсайдерськими загрозами, що включає деяку сукупність технічних та організаційних заходів. Ризик-менеджмент в цій сфері має на меті виявлення та нейтралізацію потенційних загроз ще на ранніх етапах, що забезпечить належний захист від витоку чи зловживання конфіденційною інформацією. Тому, **метою роботи** є розгляд основних методів мінімізації інсайдерських загроз в СЗІ підприємств, що забезпечують для цього найефективніші стратегії і засоби. Доцільно визначити, що важливою частиною дослідження є також аналіз сучасних технологій і інструментів, які можуть бути використані для виявлення, попередження і запобігання інсайдерським загрозам. Основними завданнями роботи є: огляд різних видів інсайдерських загроз та їх вплив на інформаційну безпеку підприємств; розгляд методів та стратегій мінімізації інсайдерських загроз, включаючи технічні та організаційні засоби; аналіз сучасних інструментів та технологій, що допомагають виявляти та зменшувати ці загрози; рекомендації для підприємств щодо впровадження комплексної стратегії захисту від інсайдерських атак. Завдяки ефективним заходам і технологіям, підприємства можуть значно знизити рівень ризиків від інсайдерських загроз, забезпечивши високий рівень захисту інформації та стабільність своєї діяльності в умовах сучасного цифрового середовища.

Аналіз останніх джерел

Розвиток національного законодавства України у сфері інформаційної безпеки розпочався з прийняття в 1994 році Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3]. Згодом були прийняті такі нормативно-правові акти, як Закони України «Про захист персональних даних» [4], «Про електронний цифровий підпис» [5] та «Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації» [6]. Адаптація національного законодавства до стандартів Європейського Союзу є важливим завданням у контексті швидкого розвитку інформаційних технологій та необхідності вдосконалення систем захисту інформації (СЗІ) [2].

Інсайдерські загрози є однією з найсерйозніших проблем у сфері інформаційної безпеки підприємств. Вони можуть бути спричинені навмисними або ненавмисними діями співробітників, що вимагає розробки ефективних методів запобігання таким загрозам.

Основні напрямки досліджень інсайдерських загроз зосереджені на використанні методів аналізу поведінки користувачів для виявлення відхилень у роботі інформаційних систем [7, 8]. Зокрема, аналізуються ключові індикатори інсайдера та ознаки інсайдерської інформації [9]. Останнім часом дослідниками розглядаються підходи на основі машинного навчання для прогнозування ризиків, пов'язаних з діяльністю співробітників. Використання алгоритмів штучного інтелекту дозволяє ідентифікувати потенційних інсайдерів за їхньою поведінкою у системі [10]. В роботі [11] аналізуються витрати на заходи безпеки, оцінюючи їх ефективність у довгостроковій перспективі. Досліджуються співвідношення між інвестиціями в кібербезпеку та рівнем ризиків, що дозволяє підприємствам оптимізувати свої витрати. В роботі [2] пропонуються математичні моделі для оптимізації ресурсів, спрямованих на захист від інсайдерських загроз, включаючи стохастичне програмування та теорію ігор. Застосування таких моделей дозволяє підприємствам ефективно розподіляти ресурси для мінімізації загроз. Отже, аналіз літератури свідчить про те, що мінімізація інсайдерських загроз потребує комплексного підходу, який включає нормативно-правові, технічні та організаційні заходи. Поєднання поведінкового аналізу, машинного навчання, економічного оцінювання ризиків та математичного моделювання дозволяє значно підвищити рівень захисту інформації. Подальші дослідження мають бути зосереджені на розробці адаптивних систем кібербезпеки, здатних вчасно виявляти та нейтралізувати інсайдерські загрози.

Аналіз літератури свідчить про те, що мінімізація інсайдерських загроз потребує комплексного підходу, що включає нормативно-правові, технічні та організаційні заходи. Поєднання поведінкового аналізу, машинного навчання, економічного оцінювання ризиків та математичного моделювання дозволяє значно підвищити рівень захисту інформації. Подальші дослідження мають бути зосереджені на розробці адаптивних систем кібербезпеки, здатних вчасно виявляти та нейтралізувати інсайдерські загрози.

Оцінка рівня інсайдерських загроз

Інсайдерські загрози в СЗІ можуть мати різні форми, в залежності від мотивів, дій та наслідків. Для оцінки ефективності заходам і технологіям, за допомогою яких забезпечується зниження

інсайдерських загроз, потрібно визначення початкових ймовірнісних показників можливих ризиків. Це дасть уявлення про масштаби майбутніх збитків підприємства, а також дозволить визначити необхідні заходи для їх зменшення.

Загальну величину початкового ризику підприємства від можливих інсайдерських загроз пропонується розраховувати за формулою:

$$R_{\sum\text{заг}} = R_{\sum\text{зовн}} + R_{\sum\text{внут}}, \quad (1)$$

де $R_{\sum\text{зовн}}$ – сумарний зовнішній ризик; $R_{\sum\text{внут}}$ – сумарний внутрішній ризик.

Сумарний зовнішній ризик розраховується наступним чином [11]:

$$R_{\sum\text{зовн}} = \sum_i^{N_{\text{зовн}}} R_i, \quad (2)$$

де R_i - величина i-го зовнішнього ризику; $N_{\text{зовн}}$ – кількість обраних зовнішніх ризиків.

Сумарний внутрішній ризик розраховується аналогічним чином:

$$R_{\sum\text{внут}} = \sum_j^{N_{\text{внут}}} R_j, \quad (3)$$

де R_j - величина j-го внутрішнього ризику; $N_{\text{внут}}$ – кількість обраних внутрішніх ризиків.

Величини ризиків R_i та R_j розраховується за формулами [11]:

$$\begin{cases} R_i = p_i \times c_i \\ R_j = p_j \times c_j \end{cases}, \quad (4)$$

де p_i - ймовірність i-го зовнішнього ризику; c_i - величина збитку від реалізації i-ї зовнішньої загрози; p_j - ймовірність j-го внутрішнього ризику; c_j - величина збитку від реалізації j-ї внутрішньої загрози. Слід відзначити, що на значення ризиків R_i та R_j впливають ймовірності p_i, p_j та величини збитків c_i, c_j.

Для розрахунку загального значення ризику $R_{\sum\text{заг}}$ потрібно визначити величини окремих збитків c_i, c_j та ймовірностей p_i, p_j підприємства. Це можливо шляхом залучення фахівців відповідної кваліфікації для надання експертної оцінки.

Запровадження певних заходів і технологій зниження інсайдерських загроз можна оцінювати шляхом порівняння отриманих ризиків:

$$\begin{cases} R_{\sum\text{зовн-зт}} < R_{\sum\text{зовн}} \\ R_{\sum\text{внут-зт}} < R_{\sum\text{внут}} \end{cases}, \quad (5)$$

де $R_{\sum\text{зовн-зт}}$ – сумарний зовнішній ризик при впровадженні заходів і методів їх зменшення; $R_{\sum\text{внут-зт}}$ – сумарний внутрішній ризик при впровадженні заходів і методів їх зменшення.

Отже, виконання умови (5) забезпечить певну ефективність від впровадження обраних заходів і технологій. Це означає, що при фіксованих можливих збитках:

$$\begin{cases} c_i = \text{const} \\ c_j = \text{const} \end{cases} \quad (6)$$

зменшуються ймовірності p_i та p_j, тобто очкуємо, що:

$$\begin{cases} p_{i\text{-зт}} < p_i \\ p_{j\text{-зт}} < p_j \end{cases}, \quad (7)$$

де $p_{i\text{-зт}}$ – i-та ймовірність після впровадження заходів і технологій зменшення зовнішнього ризику; $p_{j\text{-зт}}$ – j-та ймовірність після впровадження заходів і технологій зменшення внутрішнього ризику. Кінцевим результатом є порівняння початкового загального ризику $R_{\sum\text{заг}}$ з ризиком $R_{\sum\text{заг-зт}}$, який був отриманий після впровадження заходів і методів зниження інсайдерських загроз. За умови, що:

$$R_{\sum\text{заг-зт}} < R_{\sum\text{заг}} \quad (8)$$

можна вважати, що мета захисту від інсайдерських загроз в певній мірі була досягнута.

Слід відзначити, що повністю зменшити ймовірності $p_{i\text{-зт}}$ і $p_{j\text{-зт}}$ до нульового значення не представляється можливим, тому що загрози постійно змінюються у часі і технології їх реалізацій постійно вдосконалюються. Отже, в цьому випадку можна стверджувати, що процес зниження рівня інсайдерських загроз в залежності від впровадження відповідних заходів і технологій відповідає наступній умові:

$$\begin{cases} p_{i\text{-зт}} \to 0 \\ p_{j\text{-зт}} \to 0 \end{cases}. \quad (9)$$

Аналіз та оптимізація інсайдерських загроз

Зниження інсайдерських загроз за допомогою впровадження відповідних заходів і технологій потребує певних фінансових витрат, які необхідно оптимізувати. Значна кількість підприємств, особливо середнього та малого бізнесу, не мають значних ресурсів для комплексного забезпечення інформаційної безпеки. Тому вкрай важливо знаходити баланс між ефективністю впроваджених заходів та їхньою вартістю.

Визначимо основні шляхи, за допомогою яких є можливість мінімізувати витрати підприємств на захист від інсайдерських загроз: ризик-орієнтований підхід; автоматизація процесів; використання хмарних рішень; підвищення обізнаності персоналу; контроль доступу та політика мінімальних привілеїв; використання відкритих та безкоштовних засобів захисту.

При використанні ризик-орієнтованого підходу проводиться аналіз та надається оцінка потенційним загрозам. При цьому, визначаються критичні активи і найбільш вразливі місця. Це дозволяє зосередити ресурси саме на тих ключових напрямах, які потребують пріоритетного захисту та контролю. Крім того, такий підхід дозволяє швидко реагувати на нові виклики та змінювати стратегію безпеки відповідно до актуальних ризиків. Покращене прийняття рішень цього підходу базується на аналізі реальних загроз і їхніх наслідків, що допомагає ухвалювати обґрунтовані рішення. Отже, це дозволяє підвищити рівень кіберстійкості, знижує ймовірність успішних інсайдерських загроз завдяки цілеспрямованому підходу до захисту.

Проте, слід відзначити деякі недоліки ризик-орієнтованого підходу, для реалізації якого необхідно мати на підприємствах достатньо кваліфікованого фахівця з оцінки ризиків. Такий фахівець повинен володіти знаннями та навичками: автоматизації процесів; використання технології хмарних рішень; організації заходів підвищення обізнаності персоналу; запровадження контролю доступу та політики мінімальних привілеїв; використання відкритих та безкоштовних засобів захисту. Наприклад, використання автоматизації процесів шляхом впровадження сучасних систем моніторингу поведінки користувачів (User Behavior Analytics – UBA) та рішень на основі штучного інтелекту дозволяє зменшити витрати на ручний контроль та аудит дій співробітників. Використання хмарних рішень дає змогу замість дорогих локальних систем безпеки підприємства використовувати послуги провайдерів, які пропонують комплексний захист за передплатною моделлю, що знижує початкові інвестиції. Підвищення обізнаності персоналу на основі регулярних тренінгів та навчання з питань інформаційної безпеки дозволяють запобігати випадковим витокам інформації, що може бути дешевшим і ефективнішим заходом, ніж дорогі технічні рішення. Контроль доступу та політика мінімальних привілеїв шляхом обмеження доступу до критичних даних лише для тих співробітників, які дійсно його потребують, значно знижує ймовірність загроз без додаткових витрат. Використання відкритих та безкоштовних засобів захисту, за допомогою яких можна здійснювати ефективні рішення для аудиту безпеки, виявляти аномалії та виконувати управління доступом, можуть бути використані без значних фінансових витрат. Отже, застосування цих підходів дозволяє підприємствам ефективно знижувати рівень інсайдерських загроз, не витрачаючи на це надмірних фінансових ресурсів.

Проте, невеликі підприємства часто не мають у штаті досвідченого фахівця з оцінки ризиків, що пояснюється обмеженням ресурсів, тому що зарплата кваліфікованого експерта може бути занадто високою для малого бізнесу. Крім того, відсутність необхідності на постійній основі тримати в штаті такого фахівця, тому що оцінка ризиків не завжди вимагає щоденної роботи. Також потрібно відзначити, що власники та керівники малого бізнесу не завжди мають глибоких знань у сфері кібербезпеки та управління ризиками і ця проблема поширюється на персонал підприємства.

Вирішення проблеми можливо за рахунок періодичного залучення сторонніх експертів, а також використання автоматизованих систем оцінки ризиків. Немаловажним є навчання внутрішніх співробітників, наприклад, можна інвестувати у підготовку IT-адміністратора чи іншого співробітника, який відповідатиме за безпеку. Доцільним є впровадження базових стандартів безпеки, що передбачає навіть без глибокого аналізу ризиків і дотримання рекомендацій ISO 27001 чи NIST CSF зменшити ризики інсайдерських загроз.

Отже, навіть без високооплачуваного фахівця невелике підприємство може ефективно управляти ризиками, якщо використовуються ефективні інструменти та підходи.

Аналіз та порівняння отриманих значень ризиків $R_{\sum\text{заг-нт}}$ та $R_{\sum\text{заг-нт}}$ потрібно виконувати з урахуванням загальних витрат на СЗІ та фінансових можливостей підприємства:

$$S_{\sum\text{заг-зт}} = S_{\sum\text{зовн-зт}} + S_{\sum\text{внут-зт}}, \quad (10)$$

де $S_{\sum\text{зовн-зт}}$ – витрати на заходи безпеки зовнішніх загроз; $S_{\sum\text{внут-зт}}$ – витрати на заходи безпеки внутрішніх загроз. Вочевидь, що загальна сума витрат на безпеку $S_{\sum\text{заг-зт}}$ не може перевішувати втрати $C_{\sum\text{заг}}$ від успішних реалізацій зовнішніх і внутрішніх загроз, тобто:

$$S_{\sum\text{заг-зт}} < C_{\sum\text{заг}}, \quad (11)$$

де

$$C_{\sum\text{заг}} = \mathrm{C}_{\sum\text{зовн}} + \mathrm{C}_{\sum\text{внут}}, \quad (12)$$

де $\mathrm{C}_{\sum\text{зовн}}$ та $\mathrm{C}_{\sum\text{внут}}$ – втрати підприємства від реалізації зовнішніх і внутрішніх затрат.

Слід відзначити, що витрати компаній на кібербезпеку, включаючи захист від інсайдерських загроз, можуть значно варіюватися залежно від розміру компанії, галузі та специфічних потреб. Згідно з даними [1], компанії можуть витрачати від 10% до 50% свого річного IT-бюджету на кібербезпеку. Наприклад, компанія з 200 працівниками витратила $98,000 у 2023 році, що становить приблизно $500 на одного працівника.

Щодо захисту від інсайдерських загроз, конкретні дані про відсоток доходу або прибутку, який виділяється на ці заходи, є обмеженими. Однак, відомо, що організації можуть витрачати значні суми на усунення наслідків інсайдерських інцидентів. Наприклад, у 2022 році кількість таких подій перевищила 6800, а середні витрати на їх усунення становили близько $15.4 мільйона на рік [1].

Загалом, інвестиції в кібербезпеку та захист від інсайдерських загроз є важливими для

забезпечення безпеки даних та безперервності бізнесу. Розмір цих інвестицій залежить від конкретних ризиків та потреб кожної організації.

Для розуміння цього, як приклад, на рис. 1 наведено наступні залежності у відсотках: витрати компанії на кібербезпеку $S_{\sum заг\text{-}зт}$; збитки компанії при відсутності витрат на кібербезпеку $C_{\sum заг}$; сумарні витрати компанії з доходу D урахуванням інвестиції на кібербезпеку та потенційних збитків від несанкціонованого втручання:

$$S_{\sum заг} = S_{\sum заг\text{-}зт} + C_{\sum заг}. \quad (13)$$

Оптимальна точка залежності $S_{\sum заг}$ свідчить, при якому рівні витрат на кібербезпеку мінімізуються загальні втрати $S_{\sum заг\text{-}опт}$. Бачимо, що чим більше компанія інвестує в кібербезпеку, тим менші потенційні втрати від кібератак. Залежність $C_{\sum заг}$ показує, що при нульових витратах на кібербезпеку компанія зазнає максимальних збитків. Зі збільшенням інвестицій у безпеку втрати зменшуються. Залежність $S_{\sum заг\text{-}зт}$ відображає зростання витрат компанії на кібербезпеку. Залежність $S_{\sum заг}$ характеризує суму витрат на кібербезпеку та втрат від атак. Вона має U-подібну форму, оскільки на початку витрати низькі, але збитки високі, а при надлишкових витратах захист стає занадто дорогим без значного зниження ризику. Оптимальна точка $S_{\sum заг\text{-}опт}$ характеризує мінімум залежності $S_{\sum заг}$, яка показує, який відсоток від доходу компанії варто виділяти на кібербезпеку, щоб зменшити загальні втрати до мінімуму.

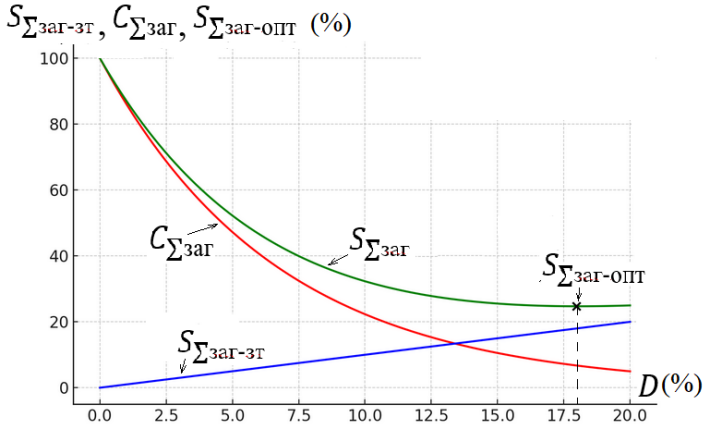

Рис. 1. Залежність між витратами на кібербезпеку та втратами, якщо відсутній захист

Наданий аналіз допомагає визначити баланс між витратами на безпеку та можливими втратами, щоб забезпечити оптимальний рівень захисту без зайвих фінансових навантажень.

6. Адаптація кібербезпеки до динамічного середовища

Отже, можна відзначити, що кібербезпека компанії не є статичним процесом і вона потребує постійної адаптації до змінних зовнішніх та внутрішніх загроз. Зовнішні загрози включають нові види атак, появу вразливостей у програмному забезпеченні, зміну регуляторних вимог. Внутрішні загрози можуть бути пов'язані з розширенням інфраструктури, появою нових співробітників або зміною бізнес-процесів. Для забезпечення ефективної адаптації необхідний циклічний процес управління кібербезпекою, який включає такі ключові етапи: моніторинг загроз, який полягає в безперервному збору та аналізі даних про потенційні кібератаки та вразливості; оцінка ризиків полягає в аналізі виявлення загроз та їхнього впливу на бізнес; коригування політики безпеки полягає в оновленні правил доступу, налаштувань мережі та протоколів безпеки; впровадження змін з метою оновлення систем захисту, посилення контролю, впровадження нових технологій; навчання персоналу для підвищення обізнаності співробітників про актуальні загрози та методи їх запобігання; аудит та тестування для перевірки ефективності заходів безпеки, проведення пентестів і внутрішніх аудитів. Цикл адаптації кібербезпеки до зовнішніх та внутрішніх загроз компанії надано на рис. 2.

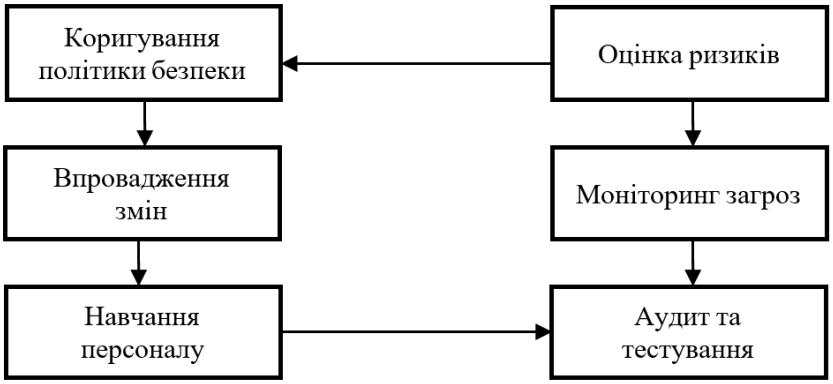

Рис. 2. Цикл адаптації кібербезпеки компанії до зовнішніх та внутрішніх загроз

Висновки

У статті доведено, що мінімізація інсайдерських загроз потребує комплексного підходу з використанням адаптивних систем кібербезпеки, здатних вчасно виявляти та нейтралізувати інсайдерські загрози. Це передбачає регулярний аналіз загроз, коригування витрат і вдосконалення захисних механізмів, що дозволяють зменшити ризики та забезпечити стабільну роботу компанії в умовах постійно зростаючих кібервикликів. В результаті дослідження було встановлено наступне: важливість безперервного моніторингу кіберзагроз, які постійно еволюціонують, а методи атак удосконалюються; доцільність використання адаптивного коригування бюджету на кібербезпеку з урахуванням сучасного стану кіберзагроз, масштабних змін в компанії, появи нових технологій і вимог; необхідність дотримання оптимального балансу між витратами та потенційними втратами від кібератак.

Література

1. В Україні ринок кібербезпеки зросте на 50% до 2029 року. (2025). *[Електронний ресурс]*. – Режим доступу : https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/?utm_source=chatgpt.com.

2. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(15), 175–185. *[Електронний ресурс]*. – Режим доступу : https://doi.org/10.28925/2663-4023.2022.15.175185.

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286. *[Електронний ресурс]*. – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

4. Закон України «Про захист персональних даних». Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481. *[Електронний ресурс]*. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2297-17#Text.

5. Закон України «Про електронний цифровий підпис». Відомості Верховної Ради України (ВВР), 2003, № 36, ст. 276. *[Електронний ресурс]*. – Режим доступу : https://zakon.rada.gov.ua/laws/show/852-15#Text.

6. Закон України «Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації». Відомості Верховної Ради України (ВВР), 2013, № 26, ст. 252. *[Електронний ресурс]*. – Режим доступу : https://zakon.rada.gov.ua/laws/show/3306-17#Text.

7. Дудоров, О.О., Каменський, Д.В. (2019). Інсайдерська інформація та кримінальний закон: від американських реалій до європейських перспектив, *Юридичний науковий електронний журнал*, 3, 185–201. – Режим доступу : http://dspace.lduvs.edu.ua/jspui/handle/123456789/306.

8. Копитін Ю.В. Розслідування інцидентів інформаційної безпеки [текст] / Копитін Ю.В. // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. – 2010. – № 2(21). – С. 58 - 66. – Режим доступу : https://ela.kpi.ua/server/api/core/bitstreams/34223b6b-fcfa-409f-a473-b6bcb024eae0/content.

9. Лавренчук, А. (2024). Майбутнє кібербезпеки: виклики штучного інтелекту та машинного навчання. *Молодий вчений*, 6.1 (130.1), 38-41. https://doi.org/10.32839/2304-5809/2024-6.1-131.1-9.

10. Антоненко, А. В., Бенедіко, І. В., Вічкарук, А. І., Лисенко, К. В., & Сижко, О. Ю. (2023). Класифікації моделей застосування машинного навчання у кібербезпеці. *Таврійський науковий вісник. Серія: Технічні науки*, (4), 11-22. – Режим доступу : https://doi.org/10.32782/tnv-tech.2023.4.2.

11. Корчинський В.В. (2019). Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// *Наукові праці ОНАЗ ім. О. С. Попова* – Одеса: ОНАЗ, № 2. – С. 112-116. – Режим доступу: https://ojs.suitt.edu.ua/index.php/sbornik_onat/article/view/1149.

Referenses

1. V Ukraini rynok kiberbezpeky zroste na 50% do 2029 roku. (2025). [Elektronnyi resurs]. – Rezhym dostupu : https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/?utm_source=chatgpt.com.

2. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Insaidery ta insaiderska informatsiia: sut, zahrozy, diialnist ta pravova vidpovidalnist. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika», 3(15), 175–185. [Elektronnyi resurs]. – Rezhym dostupu : https://doi.org/10.28925/2663-4023.2022.15.175185.

3. Zakon Ukrainy «Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh». Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31, st. 286. [Elektronnyi resurs]. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

4. Zakon Ukrainy «Pro zakhyst personalnykh danykh». Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2010, № 34, st. 481. [Elektronnyi resurs]. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/2297-17#Text.

5. Zakon Ukrainy «Pro elektronnyi tsyfrovyi pidpys». Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2003, № 36, st. 276. [Elektronnyi resurs]. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/852-15#Text.

6. Zakon Ukrainy «Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo insaiderskoi informatsii». Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2013, № 26, st. 252. [Elektronnyi resurs]. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/3306-17#Text.

7. Dudorov, O.O., Kamenskyi, D.V. (2019). Insaiderska informatsiia ta kryminalnyi zakon: vid amerykanskykh realii do yevropeiskykh perspektyv, Yurydychnyi naukovyi elektronnyi zhurnal, 3, 185–201. – Rezhym dostupu : http://dspace.lduvs.edu.ua/jspui/handle/123456789/306.

8. Kopytin Yu.V. Rozsliduvannia intsydentiv informatsiinoi bezpeky [tekst] / Kopytin Yu.V. // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. – 2010. – № 2(21). – S. 58 - 66. – Rezhym dostupu : https://ela.kpi.ua/server/api/core/bitstreams/34223b6b-fcfa-409f-a473-b6bcb024eae0/content.

9. Lavrenchuk, A. (2024). Maibutnie kiberbezpeky: vyklyky shtuchnoho intelektu ta mashynnoho navchannia. Molodyi vchenyi, 6.1 (130.1), 38-41. https://doi.org/10.32839/2304-5809/2024-6.1-131.1-9.

10. Antonenko, A. V., Benediko, I. V., Vichkaruk, A. I., Lysenko, K. V., & Syzhko, O. Yu. (2023). Klasyfikatsii modelei zastosuvannia mashynnoho navchannia u kiberbezpetsi. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, (4), 11-22. – Rezhym dostupu : https://doi.org/10.32782/tnv-tech.2023.4.2.

11. Korchynskyi V.V. (2019). Ryzyky insaiderskykh zahroz u systemakh zakhystu informatsii pidpryiemstv /V.V. Korchynskyi, Al-Faiiumi Kh., Kopytin Yu.V., Kopytina M.V.// Naukovi pratsi ONAZ im. O. S. Popova – Odesa: ONAZ, № 2. – S. 112-116. – Rezhym dostupu: https://ojs.suitt.edu.ua/index.php/sbornik_onat/article/view/1149.