Микола Гаврилов
Тернопільський національний технічний університет ім. Івана Пулюя (Україна)
Mykola Havrylov
Ternopil Ivan Puluj National Technical University (Ukraine)

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА ВІД КІБЕРЗАГРОЗ: ПІДХОДИ ТА ІНСТРУМЕНТИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ

PROTECTION OF ENTERPRISE INFORMATION SYSTEMS AGAINST CYBER THREATS: APPROACHES AND TOOLS IN THE CONTEXT OF BUSINESS DIGITAL TRANSFORMATION

Резюме. *Мета цього дослідження полягає у вивченні сучасних підходів до захисту інформаційних систем підприємств від кіберзагроз, що виникають в умовах цифрової трансформації бізнесу. Актуальність теми обумовлена зростанням кількості складних і динамічних кіберзагроз, які становлять значні ризики для економічної стабільності підприємств, особливо у зв'язку з інтеграцією хмарних технологій, Інтернету речей (IoT) та великих даних. Сучасні підприємства значною мірою залежать від цифрових технологій, що підвищує значення кібербезпеки як ключового фактора забезпечення безперервності бізнес-процесів. Основною метою цього дослідження є розробка комплексного підходу до захисту інформаційних систем, що включає інноваційні методи виявлення та запобігання кіберзагрозам, а також інтеграцію технологій штучного інтелекту (ШІ) для моніторингу безпеки в режимі реального часу. У дослідженні проаналізовано існуючі методи захисту інформаційних систем, зокрема системи виявлення та запобігання вторгненням (IDS/IPS), а також антивірусне та антималварне програмне забезпечення. Особливу увагу приділено застосуванню алгоритмів ШІ, які дозволяють оперативно виявляти аномалії та загрози, що виникають через нові типи атак, такі як фішинг, атаки програм-здирників і промисловий шпигунство.*

Дослідження містить огляд інноваційних інструментів для забезпечення кібербезпеки, включаючи хмарні рішення для управління ризиками та технології моніторингу на основі ШІ, які автоматизують процеси реагування на інциденти. Для дослідження обрано методику моніторингу з використанням алгоритмів машинного навчання, що забезпечує високу адаптивність системи до

нових загроз. Розроблена система також включає інструменти для підвищення обізнаності персоналу щодо кіберзагроз, що є важливою складовою стратегії інформаційної безпеки. Результати дослідження свідчать про те, що інтеграція сучасних підходів до захисту інформаційних систем значно знижує рівень вразливості підприємств до кіберзагроз. Особлива увага приділена запобіганню інцидентам шляхом постійного моніторингу та аналізу ризиків, що дозволяє виявляти потенційні загрози на ранніх етапах. Експериментальні дослідження підтвердили, що запропонований підхід підвищує точність і швидкість реагування на інциденти та знижує кількість помилкових спрацювань, що є важливим фактором для підтримки стабільності бізнес-процесів. Таким чином, впровадження розробленої системи кібербезпеки сприяє зниженню ризиків, пов'язаних із втратою даних та економічними збитками, а також забезпечує високий рівень захисту в умовах постійно зростаючої кількості кіберзагроз.

Summary. *The purpose of this research is to examine modern approaches to protecting enterprise information systems against cyber threats arising from the digital transformation of business. The relevance of this topic is due to the increase in complex and dynamic cyber threats that pose significant risks to the economic stability of enterprises, especially in connection with the integration of cloud technologies, the Internet of Things (IoT), and big data. Modern enterprises heavily rely on digital technologies, which raises the importance of cybersecurity as a key factor in ensuring business process continuity. The main goal of this study is to develop a comprehensive approach to protecting information systems, including innovative methods for detecting and preventing cyber threats and integrating artificial intelligence (AI) technologies for real-time security monitoring. The research analyzed existing methods of information systems protection, particularly intrusion detection and prevention systems (IDS/IPS), as well as antivirus and antimalware software technologies. Special attention is given to the application of AI algorithms, which allow for rapid detection of anomalies and threats arising from new types of attacks, such as phishing, ransomware, and industrial espionage.*

This study provides an overview of innovative cybersecurity tools, including cloud solutions for risk management and AI-based monitoring technologies that automate incident response processes. A monitoring methodology using machine learning algorithms was chosen for the study, which ensures high system adaptability to emerging threats. The developed system also includes tools to increase personnel awareness of cyber threats, which is an important component of an information security strategy. The

study results indicate that integrating modern approaches to protecting information systems significantly reduces enterprises' vulnerability to cyber threats. Special attention is paid to incident prevention through continuous monitoring and risk analysis, enabling early detection of potential threats. Experimental research has confirmed that the proposed approach improves the accuracy and speed of incident response and reduces false positives, which is crucial for maintaining business process stability. Thus, the implementation of the developed cybersecurity system helps mitigate risks associated with data loss and economic damage while ensuring a high level of protection in the face of an ever-increasing level of cyber threats.

Вступ. Зростаюча залежність підприємств від цифрових технологій створює нові можливості для розвитку бізнесу, але водночас підвищує рівень ризиків, пов'язаних із кібербезпекою [1]. Швидкий розвиток хмарних обчислень, Інтернету речей (IoT), великих даних та штучного інтелекту (ШІ) призводить до докорінних змін у структурі та функціонуванні інформаційних систем [2]. Підприємства, що активно впроваджують цифрові технології, стикаються з новими викликами, зокрема зі збільшенням обсягу та складності кіберзагроз. Ці загрози включають фішинг-атаки, програми-здирники, атаки на промислові системи та інші види шкідливого програмного забезпечення, що ставлять під загрозу конфіденційність, цілісність і доступність інформаційних ресурсів підприємств.

Рис. 1. Прогнозована динаміка зростання загроз

Актуальність даного дослідження обумовлена необхідністю вивчення сучасних кіберзагроз, які постають перед підприємствами у

цифрову епоху, та адаптації систем захисту до цих змін. З кожним роком кіберзагрози стають дедалі більш витонченими, а зловмисники – винахідливішими, що вимагає від підприємств не тільки оновлення методів захисту, а й застосування інноваційних підходів для моніторингу та протидії загрозам. Традиційні методи кіберзахисту, такі як антивірусне програмне забезпечення та міжмережеві екрани, вже не завжди достатньо ефективні в умовах постійно змінюваного ландшафту кіберзагроз. Це зумовлює потребу в інтеграції нових технологій, зокрема ШІ, які дозволяють виявляти аномалії та загрози в режимі реального часу, а також прогнозувати можливі атаки на основі аналізу великих обсягів даних.

Метою даного дослідження є розробка та обґрунтування комплексного підходу до захисту інформаційних систем підприємства від кіберзагроз, що враховує специфіку цифрової трансформації бізнесу. Основний акцент робиться на дослідженні ефективності інноваційних методів та інструментів кібербезпеки, які забезпечують надійний захист в умовах постійного зростання кількості та складності атак. Для досягнення цієї мети визначено такі завдання:

- провести аналіз сучасних кіберзагроз, з якими стикаються підприємства в умовах цифровізації, зокрема вивчити нові види атак та їхні особливості.
- оцінити існуючі методи кіберзахисту, визначити їхні переваги, недоліки та можливості для вдосконалення.
- обґрунтувати доцільність використання технологій ШІ для моніторингу та виявлення загроз у режимі реального часу, визначити найбільш ефективні алгоритми для аналізу аномалій та поведінкових змін у системах.
- розробити рекомендації щодо інтеграції системи кібербезпеки в інформаційну інфраструктуру підприємств з метою забезпечення стабільності бізнес-процесів та мінімізації ризиків.

Таким чином, дане дослідження має на меті сприяти вирішенню актуальних проблем кібербезпеки, що виникають у контексті цифрової трансформації підприємств. Застосування сучасних інструментів та технологій кіберзахисту дозволяє не лише зменшити ризики виникнення інцидентів, але й забезпечити безперервність бізнес-процесів, підвищуючи рівень довіри до підприємства серед партнерів та клієнтів.

Сучасні кіберзагрози. У сучасних умовах цифрової трансформації бізнесу та зростання ролі інформаційних технологій підприємства стикаються з різноманітними кіберзагрозами, які стають дедалі складнішими та агресивнішими. Це обумовлено, з одного боку,

розширенням спектра цифрових інструментів та сервісів, з іншого — активізацією кіберзлочинців, які використовують передові методи та технології для атак. Сучасні кіберзагрози охоплюють широкий спектр атак, включаючи фішинг, програми-здирники, шкідливе ПЗ, атаки на промислові контрольні системи (ІКС), а також атаки з використанням соціальної інженерії [3, 4, 5]. Розглянемо основні види загроз і їхні особливості. Основні види кіберзагроз:

- *Фішинг:* одна з найпоширеніших форм атак, що базується на методах соціальної інженерії. Мета фішинг-атак – змусити користувачів добровільно надати конфіденційну інформацію, таку як логіни, паролі, банківські дані тощо. Зазвичай зловмисники надсилають підроблені електронні листи або повідомлення, які виглядають як легітимні повідомлення від відомих компаній або установ. Основний ризик полягає в тому, що такі атаки можуть бути складними для виявлення та легко обходять базові засоби захисту.
- *Програми-здирники*: шкідливе програмне забезпечення, яке шифрує файли або блокує доступ до системи та вимагає викуп за відновлення доступу. Програми-здирники є серйозною загрозою для бізнесу, оскільки можуть призвести до втрати важливих даних, фінансових збитків та порушення роботи. Атаки програм-здирників часто націлені на організації з важливими даними, такі як медичні установи, фінансові організації та державні установи.
- *Шкідливе програмне забезпечення (ПЗ):* загальний термін для різних типів шкідливих програм, які використовуються для завдання шкоди комп’ютерним системам. До цього виду шкідливого ПЗ належать віруси, троянські програми, шпигунське ПЗ тощо. Шкідливе ПЗ може красти дані, видаляти файли, знижувати продуктивність системи або навіть контролювати комп’ютер без відома користувача.
- *Атаки на промислові системи (ІКС)*: загрози спрямовані на промислові підприємства та їхні контрольні системи, що використовуються для моніторингу та управління виробничими процесами. Атаки на ІКС можуть мати серйозні наслідки, оскільки здатні призвести до зупинки виробництва, порушення роботи обладнання та навіть спричинення ризиків для здоров'я і безпеки працівників. ІКС часто є більш вразливими до кібератак через застаріле обладнання та обмежені можливості для оновлення систем захисту.
- *Соціальна інженерія*: вид атак, в яких зловмисники маніпулюють людьми, щоб отримати доступ до конфіденційної інформації або систем. Соціальна інженерія може включати телефонні дзвінки, електронні листи або особисті зустрічі, під час яких

зловмисник видає себе за довірену особу або співробітника. Цей вид атак є небезпечним, оскільки залучає до атаки людський фактор і може обійти навіть найсучасніші технічні засоби захисту.

Таблиця 1

Основні види сучасних кіберзагроз та їх характеристика [6]

Вид кіберзагрози	Характеристика	Можливі наслідки
Фішинг	Використання соціальної інженерії для отримання конфіденційної інформації через підроблені повідомлення	Втрата доступу до облікових записів, фінансові збитки
Програми-здирники	Шифрування файлів з подальшою вимогою викупу для розблокування	Втрата даних, фінансові втрати, порушення роботи бізнесу
Шкідливе ПЗ	Програми, що крадуть інформацію, видаляють файли або знижують продуктивність	Порушення безпеки, зниження продуктивності, втрата даних
Атаки на ІКС	Кіберзагрози для промислових систем, що порушують роботу виробничих процесів	Зупинка виробництва, ризики для здоров'я та безпеки
Соціальна інженерія	Маніпуляція людьми з метою отримання конфіденційної інформації або доступу до систем	Втрата інформації, несанкціонований доступ до систем

Цифрова трансформація кардинально змінює спосіб функціонування підприємств і вимагає інтеграції нових цифрових рішень, таких як хмарні технології, Інтернет речей (IoT) та штучний інтелект (ШІ). Хоча ці технології приносять значні переваги, такі як підвищення ефективності, зниження витрат та вдосконалення аналітики, вони також розширюють поверхню атак, збільшуючи кількість точок вразливості, які зловмисники можуть використати:

- *Хмарні технології*: зберігання даних та обробки інформації надає підприємствам гнучкість та можливість швидкого масштабування, однак також відкриває ризики, пов'язані з витоком даних, несанкціонованим доступом та залежністю від зовнішніх провайдерів. Зростання числа віддалених користувачів у хмарних системах підвищує ймовірність атак на паролі, компрометації облікових записів та крадіжки даних.
- *Інтернет речей (IoT)*: для моніторингу та управління процесами, але часто мають обмежені можливості захисту, що робить їх легкою мішенню для зловмисників. Наприклад, несанкціонований доступ до IoT-пристроїв може спричинити значні збитки, такі як порушення роботи виробничого обладнання або отримання конфіденційних даних.
- *Штучний інтелект (ШІ)*: для виявлення загроз і автоматизації кіберзахисту, однак його також можуть використовувати зловмисники для створення складних атак, таких як створення

персоналізованих фішингових повідомлень або автоматизація процесів шкідливого ПЗ. Зловмисники можуть використовувати алгоритми ШІ для аналізу вразливостей та розробки адаптивного шкідливого ПЗ, що складно виявити за допомогою традиційних засобів захисту.

Таблиця 2

Порівняння основних кіберризиків залежно від ступеня цифровізації підприємства

Ступінь цифровізації	Основні ризики	Приклади галузей
Низький	Фізичні атаки, атаки на обмежений обсяг інформаційних активів	Традиційне виробництво, сільське господарство
Середній	Шкідливе ПЗ, фішинг, атаки на облікові записи	Логістика, роздрібна торгівля
Високий	Програми-здирники, атаки на хмарні сервіси, зловживання IoT, атаки на промислові системи	ІТ, охорона здоров'я, промисловість
Дуже високий	Цільові атаки на великі масиви даних, складні атаки з використанням ШІ	Фінансовий сектор, державні установи

Підходи до захисту інформаційних систем

Захист інформаційних систем є важливим елементом діяльності сучасних підприємств, що прагнуть зменшити ризики, пов'язані з витоками даних, несанкціонованим доступом та іншими кіберзагрозами. Ефективний підхід до кібербезпеки включає використання як традиційних, так і новітніх методів для виявлення та запобігання загрозам. Нижче розглянемо основні підходи до захисту інформаційних систем, зокрема традиційні методи та інноваційні підходи, що включають використання технологій штучного інтелекту та автоматизацію моніторингу загроз у реальному часі.

Традиційні методи захисту:

- *Антивірусне та антималварне програмне забезпечення*: такі програми є найпоширенішим методом захисту від шкідливого ПЗ. Вони функціонують на основі визначень вірусів, які регулярно оновлюються, та виявляють загрози шляхом порівняння файлів із відомими сигнатурами. Однак, такий підхід є обмеженим для виявлення нових, невідомих вірусів, які можуть не збігатися з базою даних сигнатур [7].
- *Міжмережеві екрани (брандмауери)*: дозволяють контролювати вхідний та вихідний трафік на основі заздалегідь визначених правил. Вони ефективні для блокування несанкціонованого доступу та обмеження підозрілих з'єднань, але мають обмежену здатність до виявлення складних атак, таких як багатоступеневі кіберзагрози.

- *Системи виявлення вторгнень (IDS)*: аналізують трафік та виявляють підозрілу активність у мережі. Вони можуть бути налаштовані для виявлення відомих шаблонів атак або аналізу аномальної поведінки. Проте, IDS мають високу ймовірність хибних спрацювань і вимагають додаткових ресурсів для моніторингу та обробки сигналів.
- *Контроль доступу та автентифікація*: передбачає використання політик, які обмежують доступ до систем залежно від ролей користувачів. Автентифікація може включати паролі, двофакторну автентифікацію або біометричні дані для підвищення рівня захищеності. Хоча контроль доступу ефективний для запобігання несанкціонованого доступу, він не завжди здатний запобігти атакам, здійсненим із внутрішніх облікових записів, або складним багатоступеневим атакам [9].

Інноваційні підходи до захисту:

- *Технології штучного інтелекту (ШІ)*: дозволяє автоматизувати процес моніторингу та виявлення загроз. Алгоритми машинного навчання аналізують великий обсяг даних, виявляючи аномалії та потенційні загрози у реальному часі. Це дозволяє виявляти загрози на ранніх етапах та ефективно реагувати на нові та складні атаки. ШІ також здатен навчатися на основі нових даних, що підвищує ефективність системи захисту з часом [10].
- *Системи запобігання вторгнень (IPS)*: активниі системи, які не лише виявляють підозрілу активність, але й автоматично блокують підозрілі з'єднання або дії в мережі. Використання IPS дозволяє запобігати вторгненням у реальному часі, проте така система потребує налаштування та може блокувати легітимні дії, якщо не налаштована правильно [11].
- *Хмарні рішення для кібербезпеки*: використовуються для управління кіберризиками та дозволяють зберігати та обробляти дані в безпечному хмарному середовищі. Хмарні рішення можуть включати резервне копіювання, автоматизоване оновлення та управління даними, що підвищує рівень кібербезпеки підприємства.
- *Підхід "Нульова довіра" (Zero Trust)*: створення системи, яка не довіряє жодному користувачу або пристрою автоматично, навіть якщо вони знаходяться всередині мережі. Кожен доступ до системи перевіряється на основі низки факторів, включаючи геолокацію, роль користувача, історію дій тощо. Цей підхід ефективний для підприємств із високим рівнем цифровізації, але може бути ресурсомістким для впровадження.

Для забезпечення максимального рівня кібербезпеки підприємствам доцільно використовувати як традиційні, так і інноваційні підходи до захисту інформаційних систем. Нижче наведена порівняльна таблиця, яка ілюструє основні відмінності та переваги кожного з підходів.

Таблиця 3

Порівняльний аналіз традиційних та інноваційних підходів до захисту

Підхід	Традиційні методи	Інноваційні методи
Антивірусне ПЗ	Базується на сигнатурах відомих загроз	Використання ШІ для аналізу поведінкових аномалій
Міжмережеві екрани	Захист від зовнішніх атак, блокування портів	Zero Trust: контроль кожного доступу, незалежно від місцезнаходження
Виявлення вторгнень (IDS)	Аналіз трафіку, налаштування правил	IPS: автоматичне блокування підозрілих з'єднань у реальному часі
Контроль доступу	Класичний контроль доступу, автентифікація	Двофакторна автентифікація, біометрія, підхід Zero Trust
Управління даними	Місцеве зберігання даних, резервне копіювання	Хмарне зберігання з можливістю автоматизованого оновлення

Дослідження показують, що інноваційні методи кібербезпеки, такі як технології штучного інтелекту та підхід Zero Trust, мають вищу ефективність у запобіганні складним атакам порівняно з традиційними методами.

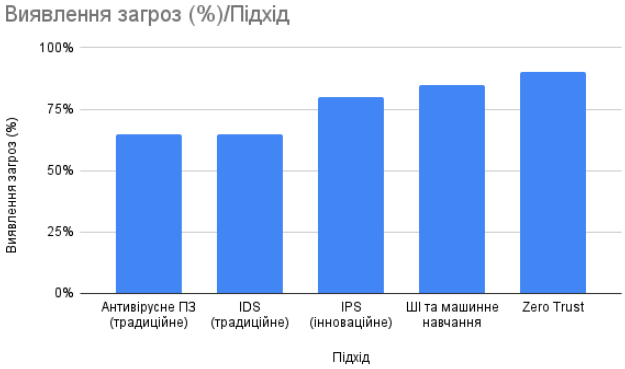

Рис. 2. Виявлення загроз використовуючи різні підходи

За результатами опитування кібербезпекових служб підприємств у різних галузях, рівень виявлення загроз за допомогою традиційних

методів становить близько 60-70%, тоді як із застосуванням ШІ цей показник підвищується до 85-90%.

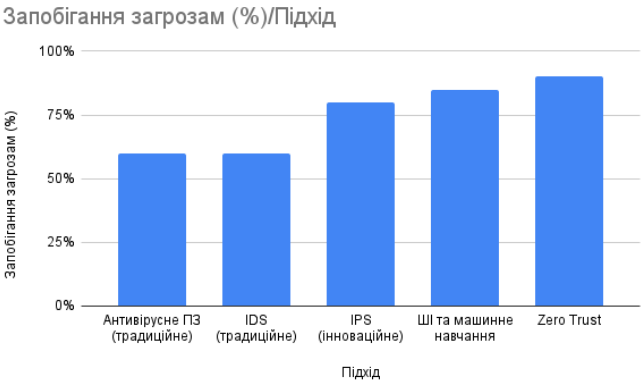

Рис. 3. Запобігання загрозам використовуючи різні підходи

Системи IPS виявляють та блокують атаки приблизно в 80% випадків, тоді як традиційні IDS виявляють загрози лише на 65%.

Інструменти кібербезпеки охоплюють різноманітні технології та методи, що забезпечують всебічний захист інформаційних систем від кібератак. Вибір інструментів залежить від специфіки бізнесу, потенційних загроз, а також від рівня цифровізації підприємства. Сучасні інструменти кібербезпеки можна умовно поділити на інструменти для моніторингу, виявлення та реагування, управління доступом, а також засоби резервного копіювання та відновлення даних. Кожен з них відіграє важливу роль у побудові комплексної стратегії безпеки, створюючи багатошаровий захист систем:

- SIEM-платформи (Security Information and Event Management) є ключовим інструментом для централізованого збору, моніторингу та аналізу даних про безпеку з різних систем у мережі. SIEM систематизує і зберігає журнали подій, забезпечуючи можливість швидкого виявлення аномалій, кореляції інцидентів та створення звітів. Завдяки SIEM компанії можуть швидко отримувати повну картину кіберзагроз і оптимізувати процес реагування [12].
- DLP-системи (Data Loss Prevention) спрямовані на захист конфіденційних даних підприємства від несанкціонованого доступу та витоку. Вони контролюють доступ до даних, фільтрують інформаційні потоки і блокують спроби несанкціонованого поширення або передачі важливої інформації за межі компанії. DLP-системи особливо важливі

для підприємств, що працюють з великою кількістю чутливої інформації (персональні дані, фінансова інформація тощо).

- SOAR (Security Orchestration, Automation, and Response) – це платформи, що автоматизують процеси управління інцидентами та реагування на них. SOAR об'єднує дані з різних джерел, таких як SIEM, антивірусні рішення та IPS/IDS, і надає автоматизовані сценарії реагування. Це дозволяє значно знизити час реагування на кіберзагрози та покращити ефективність роботи команд безпеки, оптимізуючи процеси аналізу та реагування [13].
- Резервне копіювання є критичним елементом кібербезпеки, який дозволяє відновити дані після інциденту, наприклад, після атак програм-здирників. Автоматизовані системи резервного копіювання зберігають копії даних на віддалених серверах або в хмарному середовищі. Це забезпечує можливість швидкого відновлення роботи системи в разі інциденту і знижує ризик втрати важливих даних [14].
- Управління привілеями користувачів є важливим інструментом для обмеження доступу до критичних систем і ресурсів. PAM (Privileged Access Management) системи забезпечують моніторинг і контроль привілейованих облікових записів, які мають розширені права доступу. Вони обмежують права користувачів відповідно до їхніх ролей і дозволяють здійснювати контроль за використанням привілеїв, що знижує ризик несанкціонованого доступу та можливих витоків даних.

Таблиця 5

Порівняльна ефективність інструментів кібербезпеки

Інструмент	Основні функції	Виявлення загроз (%)	Запобігання загрозам (%)	Реагування на інциденти (%)
SIEM	Моніторинг, кореляція інцидентів, звіти	80%	65-75%	85-90%
DLP	Захист даних, контроль доступу до конфіденційної інформації	70%	80-85%	70-75%
SOAR	Автоматизація реагування на інциденти, оркестрація процесів	75-85%	85%	90%
Резервне копіювання	Захист даних, відновлення після інцидентів	60%	80%	90%
PAM	Контроль привілейованого доступу	65-70%	85-90%	75%

Ефективність кожного інструменту кібербезпеки вимірюється за різними критеріями, зокрема: здатністю виявляти та запобігати інцидентам, швидкістю реагування та рівнем захисту даних. Вибір

відповідного набору інструментів для підприємства залежить від конкретних потреб, але найвищий рівень безпеки досягається завдяки поєднанню декількох інструментів.

Розглянемо можливий сценарій застосування кількох інструментів кібербезпеки на підприємстві, яке стикнулося з атакою програм-здирників. Нижче наведено діаграму розробленого алгоритму роботи.

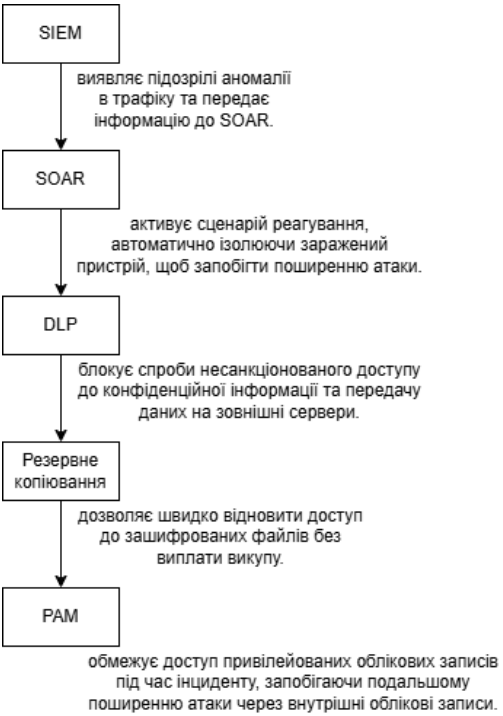

Рис. 4. Алгоритм роботи системи активного виявлення атак

Стратегії реагування на кіберінциденти та ефективний моніторинг є ключовими елементами для забезпечення безперервного захисту інформаційних систем. Сучасні кіберзагрози, зокрема атаки програм-здирників, фішинг, та атаки на промислові системи, вимагають від компаній застосування комплексного підходу до моніторингу, швидкого реагування та адаптації до змін у загрозах. Висока швидкість реагування дозволяє знизити можливі збитки від

кіберінцидентів, а моніторинг, заснований на використанні автоматизованих систем, дозволяє своєчасно виявляти підозрілі дії [15].

Розглянемо різні стратегії реагування:

- Проактивний підхід передбачає постійне відстеження мережевої активності, аналіз подій, а також збір даних для прогнозування потенційних загроз. Для цього використовуються платформи SIEM, які централізовано збирають журнали подій, виконують кореляційний аналіз та сигналізують про виявлені аномалії. Проактивний моніторинг дозволяє виявити загрози на ранніх етапах, що дає можливість підприємствам уникнути масштабного впливу інциденту [16].
- Автоматизовані сценарії реагування, реалізовані за допомогою SOAR платформ, дозволяють швидко та ефективно реагувати на інциденти. SOAR може виконувати завдання автоматичної ізоляції заражених пристроїв, блокування підозрілих IP-адрес, повідомлення команди безпеки та ініціювання резервного копіювання. Автоматизація прискорює процеси реагування, зменшуючи залежність від людського фактора та знижуючи час реагування до секунд.
- План безперервності бізнесу (BCP) та план відновлення (DRP) допомагають організаціям швидко відновити свої операції після інциденту. BCP визначає, як компанія може продовжувати роботу під час кіберінциденту, тоді як DRP деталізує процеси відновлення IT-інфраструктури. Наприклад, DRP може містити інструкції для резервного копіювання, відновлення даних, заміни критичних систем та забезпечення віддаленого доступу [17].
- Використання даних кіберрозвідки, таких як індикатори компрометації (IoC) та індикатори атаки (IoA), допомагає розпізнавати нові типи загроз, прогнозувати тенденції атак та адаптувати стратегії реагування.

Розглянемо існуючі підходи до моніторингу загроз:

- Реальний час моніторинг використовує SIEM та SOAR рішення, які виявляють аномальні дії у мережі та аналізують дані у момент їх надходження. Це дозволяє швидко реагувати на будь-які зміни, що можуть свідчити про потенційну загрозу.
- Моніторинг поведінкових моделей передбачає аналіз дій користувачів, пристроїв та систем. Інструменти, що використовують алгоритми машинного навчання, визначають поведінкові аномалії, які можуть свідчити про проникнення або компрометацію. Наприклад, якщо користувач здійснює дії, що відхиляються від звичної поведінки,

система може заблокувати його доступ або направити сигнал до служби безпеки.

- Моніторинг трафіку та аналіз мережевих пакетів дозволяють виявляти аномалії, такі як DDoS-атаки, спроби проникнення, несанкціонований обмін даними. Мережевий моніторинг відстежує підозрілий трафік, визначаючи IP-адреси, які можуть бути джерелом загроз.

Ефективність різних стратегій реагування залежить від їхньої здатності швидко ізолювати загрози, відновити нормальну роботу та мінімізувати збитки. У таблиці нижче наведено порівняння основних стратегій за часом реагування, рівнем запобігання та ефективністю відновлення.

Таблиця 6

Порівняльна ефективність стратегій реагування та моніторингу

Стратегія реагування	Час реагування	Рівень запобігання	Ефективність відновлення
Проактивний моніторинг (SIEM)	Швидкий	Високий	Середній
Автоматизовані сценарії (SOAR)	Дуже швидкий	Високий	Середній
BCP та DRP	Повільний	Низький	Високий
Інтеграція з кіберрозвідкою	Середній	Високий	Середній
Резервне копіювання та відновлення	Середній	Низький	Високий

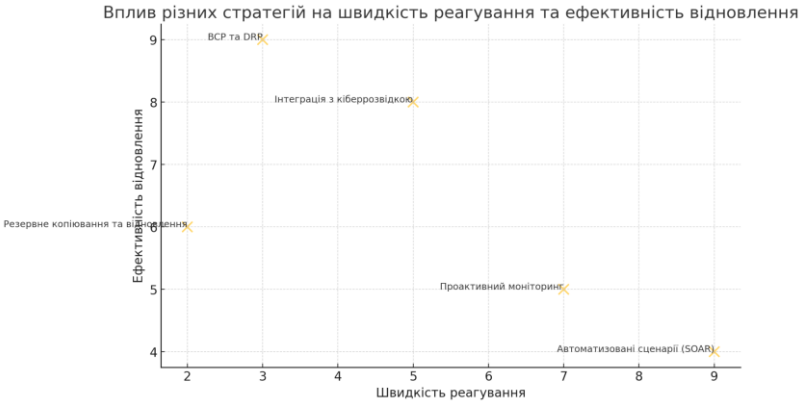

Рис. 5. Порівняння стратегій на швидкість та ефективність

Для забезпечення надійного захисту інформаційних систем підприємства та ефективного реагування на кіберзагрози важливо реалізувати комплекс заходів, які враховують особливості бізнес-процесів, рівень цифровізації та існуючі загрози. Наведені нижче рекомендації спрямовані на підвищення кібербезпеки, мінімізацію ризиків інцидентів та оптимізацію роботи служби безпеки підприємства.

Впровадження багаторівневої системи захисту:

- *Захист периметру та мережевий моніторинг*: використання міжмережевих екранів, систем IDS/IPS для моніторингу та блокування несанкціонованого доступу.
- *Захист робочих станцій та серверів*: встановлення антивірусного ПЗ та систем контролю доступу, що запобігає несанкціонованому доступу та поширенню шкідливого ПЗ.
- *Двофакторна автентифікація (2FA)*: додавання додаткового рівня захисту, який забезпечує контроль доступу до критичних облікових записів.
- *Резервне копіювання даних*: регулярне створення резервних копій даних для швидкого відновлення у разі інциденту.
- Використання сучасних технологій для виявлення загроз:
- *Платформи SIEM для моніторингу подій*: центральна платформа для збору, аналізу та кореляції даних з різних систем безпеки.
- *Інструменти штучного інтелекту (ШІ) для аналізу аномалій*: використання алгоритмів ШІ дозволяє виявляти аномалії в поведінці користувачів та систем, що може свідчити про загрози.
- *Інтеграція з кіберрозвідкою*: отримання та обробка даних кіберрозвідки для своєчасного виявлення нових загроз та прогнозування потенційних атак.
- Оптимізація процесу реагування на інциденти:
- *Впровадити SOAR для автоматизації реагування на інциденти*: автоматизовані платформи дозволяють прискорити час реагування завдяки готовим сценаріям дій.
- *Регулярне оновлення плану безперервності бізнесу*: розробка та тестування плану безперервності бізнесу, який включає сценарії для критичних інцидентів.
- *Навчання та підвищення кваліфікації персоналу*: регулярні тренінги для співробітників служби безпеки та всього персоналу, щоб підготувати їх до потенційних інцидентів та забезпечити обізнаність щодо останніх загроз.
- Підвищення обізнаності персоналу:

- *Проведення регулярних тренінгів із кібербезпеки*: співробітники повинні знати основні типи загроз, зокрема фішинг, соціальну інженерію та методи захисту.
- *Інструктаж щодо використання особистих пристроїв*: зокрема, у випадках віддаленої роботи, співробітники мають дотримуватись правил безпечного підключення до корпоративної мережі.
- *Ознайомлення з політиками кібербезпеки компанії*: усі співробітники повинні бути поінформовані про корпоративні політики щодо кібербезпеки, зокрема про наслідки порушень.
- Регулярний аудит та оновлення політик кібербезпеки:
- *Проведення регулярних аудитів кібербезпеки*: перевірка захищеності систем, оцінка ефективності інструментів безпеки та виявлення вразливостей.
- *Оновлення політик безпеки*: політики безпеки повинні регулярно переглядатися, з урахуванням нових загроз та технологій.
- *Тестування системи безпеки (Penetration Testing)*: регулярне проведення тестувань на проникнення для оцінки готовності системи до атак.
- Використання резервного копіювання та планів відновлення:
- *Розробка політики резервного копіювання*: регулярне створення копій критичних даних на віддалених серверах або у хмарному середовищі.
- *Автоматизоване резервне копіювання*: впровадження автоматизованих систем резервного копіювання, що знижує людський фактор.
- *Періодичне тестування процесів відновлення*: перевірка працездатності резервних копій та відпрацювання процесів відновлення у разі інциденту.

Висновки. Аналіз сучасних кіберзагроз показав, що в умовах цифрової трансформації підприємства повинні дотримуватись комплексного підходу до забезпечення інформаційної безпеки. Основні кіберзагрози, такі як фішинг, програми-здирники, атаки на промислові системи та інші форми шкідливого ПЗ, стають дедалі складнішими та руйнівнішими. Підприємства мають використовувати багаторівневу систему захисту, яка охоплює моніторинг, контроль доступу, антивірусний захист, двофакторну автентифікацію, резервне копіювання та інші методи для забезпечення надійного захисту інформаційних систем.

Ключові висновки та рекомендації:

- Запровадження багаторівневого захисту дозволяє створити надійну систему протидії кіберзагрозам на різних етапах атак. Комбінація таких інструментів, як міжмережеві екрани, IDS/IPS для захисту периметру, контроль доступу до облікових записів, а також регулярне резервне копіювання, забезпечує всебічний захист від зовнішніх та внутрішніх загроз. Застосування двофакторної автентифікації значно знижує ризик несанкціонованого доступу до критичних даних, що є важливим елементом у запобіганні компрометації облікових записів.
- Сучасні загрози стають дедалі витонченішими, що вимагає використання інноваційних технологій для їх ідентифікації та запобігання. Використання SIEM платформ дозволяє централізовано збирати, аналізувати та корелювати дані з різних систем у реальному часі, що дозволяє швидко виявляти аномалії та запобігати інцидентам. Інтеграція інструментів штучного інтелекту для аналізу поведінкових даних підвищує точність виявлення нових видів атак, які не збігаються з відомими шаблонами. Завдяки цим технологіям компанія може своєчасно реагувати на потенційні загрози.
- Своєчасне та ефективне реагування на інциденти є критичним аспектом кібербезпеки. Автоматизовані платформи SOAR дозволяють налаштувати сценарії реагування на загрози, автоматизуючи такі дії, як ізоляція заражених пристроїв, блокування підозрілих IP-адрес та активація резервного копіювання. Це значно скорочує час реагування, знижує ризики людських помилок та мінімізує вплив інцидентів на роботу компанії. Крім того, впровадження плану безперервності бізнесу та плану відновлення після інциденту гарантує, що підприємство зможе швидко відновити роботу навіть у разі серйозного інциденту.
- Людський фактор є однією з основних причин кіберінцидентів, оскільки співробітники часто не обізнані з основами кібербезпеки та можуть стати жертвами фішингу або інших форм соціальної інженерії. Для мінімізації цього ризику важливо регулярно проводити навчальні тренінги для співробітників, розповсюджувати інформацію про методи розпізнавання загроз та дотримання політик безпеки. Такі заходи допомагають знизити ризик витоку даних та підвищують обізнаність персоналу щодо відповідальності за захист корпоративних даних.
- Кіберзагрози постійно еволюціонують, тому важливо регулярно проводити аудит систем безпеки для виявлення вразливостей, оновлення політик безпеки та вдосконалення інструментів захисту. Рекомендовано періодично виконувати

тестування на проникнення для оцінки готовності системи до атак, а також оновлювати політики безпеки відповідно до сучасних стандартів та рекомендацій. Це дозволяє забезпечити високу ефективність системи кібербезпеки та адаптуватися до нових викликів.

- Резервне копіювання є важливою складовою системи кібербезпеки, яка дозволяє зберегти критичні дані у разі інциденту. Автоматизовані системи резервного копіювання зберігають копії даних на віддалених серверах або у хмарному середовищі, що дозволяє швидко відновити роботу підприємства у разі кібератаки або збоїв. Регулярне тестування процесів відновлення даних забезпечує впевненість у працездатності резервних копій і мінімізує ризики, пов'язані з втратою даних.

Реалізація представлених рекомендацій дозволить підприємствам побудувати надійну систему кібербезпеки, здатну ефективно протидіяти сучасним загрозам та забезпечувати захист інформаційних активів. Багаторівневий підхід, інтеграція інноваційних технологій, автоматизація реагування на інциденти та підвищення обізнаності персоналу формують комплексну систему захисту, яка є основою для стабільного розвитку компанії в умовах зростаючого рівня кіберризиків. Регулярний аудит, оновлення політик безпеки та резервне копіювання забезпечують постійну готовність підприємства до можливих інцидентів та мінімізують їхній вплив на бізнес. Таким чином, дотримання запропонованих рекомендацій допоможе компанії захистити свої інформаційні ресурси, зберегти репутацію та уникнути фінансових втрат.

Список використаних джерел:

1. Андрієнко, В. І., & Шевченко, М. О. (2018). Основи кібербезпеки: навчальний посібник. Київ: КНТ.
2. Гладкий, В. В., & Ковальчук, П. І. (2017). Моніторинг та реагування на кіберзагрози в інформаційних системах. Харків: ХНЕУ ім. С. Кузнеця.
3. Іванова, Л. В., Кравченко, О. Ю., & Дмитренко, О. М. (2020). Вплив цифрової трансформації на кібербезпеку підприємств. *Економічний простір*. № 7. С. 59-67.
4. Карпов, І. В., & Тимошенко, Р. С. (2019). Використання штучного інтелекту у забезпеченні кібербезпеки: сучасні тенденції. Київ: КНТ.
5. Коваленко, Д. О. (2018). Адаптивні системи кіберзахисту на базі штучного інтелекту. *Вісник Харківського національного університету імені В. Н. Каразіна*. Вип. 35(3). С. 145-153.

6. Козлов, П. П., & Савченко, Л. А. (2019). Інструменти кібербезпеки для моніторингу інформаційних систем. *Інформаційна безпека*. № 1. С. 83-89.
7. Кузнєцов, С. М., & Мартинюк, В. Г. (2021). Підходи до захисту інформаційних систем в умовах цифрової трансформації. *Наукові праці ЧНУ ім. Петра Могили*. Вип. 325(1). С. 33-42.
8. Ляшенко, С. О., & Гриценко, О. І. (2020). Сучасні методи кіберзахисту підприємств: монографія. Дніпро: Ліра.
9. Матвієнко, Н. І. (2018). Стратегії забезпечення інформаційної безпеки в умовах сучасних загроз. *Бізнес Інформ*. № 6. С. 58-64.
10. Національна стратегія кібербезпеки України до 2025 року. (2021). Київ: Кабінет Міністрів України.
11. Петренко, Т. С. (2019). Резервне копіювання даних як засіб кіберзахисту: методологічний підхід. *Вісник Одеського національного університету*. Вип. 24 (2). С. 96-102.
12. Полякова, О. В., & Воробей, І. М. (2021). Використання кіберрозвідки у системах захисту інформаційних систем. *Журнал інформатики та кібернетики*. Вип. 5 (2). С. 102-109.
13. Соловйов, Ю. А., & Борисенко, М. В. (2018). Інноваційні підходи до моніторингу кіберзагроз. *Інформаційні технології та кібербезпеки*. Вип. 10 (3). С. 125-132.
14. Тимошенко, І. П., & Коваленко, Н. І. (2019). Підвищення рівня кібербезпеки підприємства: методи та технології. Київ: КНУ.
15. Ткаченко, О. В., & Литовченко, П. І. (2020). Управління інцидентами кібербезпеки на основі SOAR. *Захист інформації*. № 4 (3). С. 15-24.
16. Федоренко, Л. В., & Дмитрієв, А. П. (2020). Роль кібербезпеки в забезпеченні стабільності підприємства. *Науковий журнал СНАУ*. № 6 (1). С. 120-127.
17. Черненко, П. І., & Ситник, І. П. (2021). Моніторинг кібербезпеки на основі SIEM-платформ. *Комп'ютерні системи і мережі*. № 8 (2). С. 45-52.