- Інтегровані платформи для управління охоронними процесами: Це комплексні системи, які включають всі аспекти охорони, управління персоналом, моніторинг ситуацій у реальному часі. Приклад: Genetec Security Center.

Виклики та обмеження впровадження інформаційних систем

- Висока вартість впровадження: Для великих підприємств або державних установ вартість встановлення таких систем може бути значною.
- Необхідність у кваліфікованих спеціалістах: Для налаштування, обслуговування та аналізу даних потрібні фахівці з високими технічними знаннями.
- Інтеграція з існуючими процесами: Впровадження нових технологій може потребувати значних змін в організаційних процесах, що може бути складним для великих компаній.

У майбутньому впровадження технологій штучного інтелекту дозволить ще більше автоматизувати процеси управління охороною. Інтелектуальні системи зможуть самостійно реагувати на загрози, прогнозувати потенційні інциденти та оптимізувати роботу охоронних підрозділів.

Зростає використання біометричних технологій, таких як розпізнавання обличчя та відбитків пальців, для підвищення безпеки доступу до критичних зон. Це дасть можливість забезпечити більш високий рівень точності та надійності в контролі за доступом, а також покращить взаємодію з користувачами.

Мобільні додатки для управління безпекою, що надають доступ до всіх функцій системи в режимі реального часу, стають все популярнішими. Це дозволяє оперативно реагувати на події, навіть перебуваючи поза межами основного офісу чи об'єкта.

Список використаних джерел

1. Predictive Analytics in Security Systems – Режим доступу: https://www.securityinfowatch.com/video-surveillance/article/12437403/industry-perspectives-understanding-the-impact-of-predictive-analytics-on-security-operations
2. Security Automation in Information Technology – Режим доступу: https://shorturl.at/GSXAp
3. The role of predictive analytics in cybersecurity – Режим доступу: https://shorturl.at/FGGX6
4. Home Automation and RFID-Based Internet of Things Security: Challenges and Issues – Режим доступу: https://onlinelibrary.wiley.com/doi/full/10.1155/2021/1723535

Науковий керівник: **Ріппа С. П.,** ., док. екон. наук, професор

Крошко І. А.
аспірант кафедри інформаційних систем в економіці,
Київський національний економічний
університет імені Вадима Гетьмана, Україна

ЗАХИСТ ДАНИХ У БІЗНЕС-СЕРЕДОВИЩІ, АКТУАЛЬНІ КІБЕРЗАГРОЗИ, ФІНАНСОВІ ВТРАТИ ТА НАПРЯМИ ІНВЕСТУВАННЯ

У сучасну епоху цифрової трансформації бізнесу та глобального об’єднання інформаційних систем проблема витоку даних стала надзвичайно важливою. Зростання обсягів цифрових ресурсів, активне впровадження хмарних рішень і розвиток електронної комерції підвищили вразливість

компаній до цілеспрямованих дій кіберзлочинців. Значні випадки компрометації баз даних не лише загрожують конфіденційності інформації, а й завдають компаніям серйозних фінансових втрат, підривають довіру клієнтів і можуть спричинити юридичні наслідки.

Відповідно до новітніх статистичних досліджень, більшість витоків даних спричиняються людськими помилками, неналежним рівнем безпеки корпоративних систем та експлуатацією вразливостей програмного забезпечення. До того ж спостерігається посилення загроз, пов'язаних з атаками на постачальників і партнерів, що акцентує увагу на необхідності впровадження цілісного підходу до менеджменту кіберризиків.

Проблематику витоку даних з корпоративних баз розглядають Лун Чен та колеги [1], визначаючи джерела таких інцидентів серед як зовнішніх, так і внутрішніх загроз. Дослідники наводять приклади масштабних порушень безпеки, здійснюють класифікацію загроз за їхнім походженням і причинами, аналізують сучасні методи та інструменти виявлення витоків і запобігання їм, а також вказують на наявні недоліки цих рішень. Особливу увагу у дослідженні приділено труднощам, пов'язаним із зростаючими обсягами даних.

Шанітамол Грейсі [2] досліджує динаміку та характер витоків даних за останні десять років (2004 – 2024), охоплюючи галузеву специфіку, способи здійснення атак, види скомпрометованої інформації та регіональні відмінності. Автори застосовують платформу Power BI для виявлення хронологічних тенденцій і встановлення кореляцій між наведеними чинниками.

Щороку фіксується зростання кількості інцидентів витоку даних, пов'язаних із недостатнім рівнем безпеки у контрагентів. Зокрема, сторонні постачальники та партнери, включаючи учасників ланцюгів постачання програмного забезпечення, хостинг-провайдерів та компанії, що забезпечують зберігання даних, були причиною 15% випадків компрометації інформації [3]. Ключовим фактором ризику залишається недостатній захист інформаційної інфраструктури таких організацій, що створює вразливі місця, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до корпоративних ресурсів. Подібні випадки загрожують не лише порушенням конфіденційності, а й призводять до суттєвих фінансових збитків для компаній.

Посилений тиск з боку регуляторних органів також змушує компанії зосереджувати більше уваги на питаннях захисту даних. Останніми роками чимало корпорацій були оштрафовані на мільйони доларів за порушення норм конфіденційності, що свідчить про зростання контролю у сфері кібербезпеки. Подібні фінансові санкції не лише покривають збитки від інцидентів, але й є чітким сигналом для бізнесу щодо необхідності впровадження ефективних рішень з інформаційного захисту. Жорсткі нормативні заходи покликані знизити ймовірність витоків даних і сприяти формуванню відповідального підходу до інформаційної безпеки.

Кібербезпека все частіше сприймається бізнесом як один із ключових стратегічних пріоритетів, що відображається у зміні структури фінансування на користь посилення систем захисту даних та забезпечення швидкого реагування на загрози. Зростання вкладень у тестування безпеки та розробку планів дій у разі інцидентів свідчить про усвідомлення критичної важливості підготовленості до можливих кібератак.

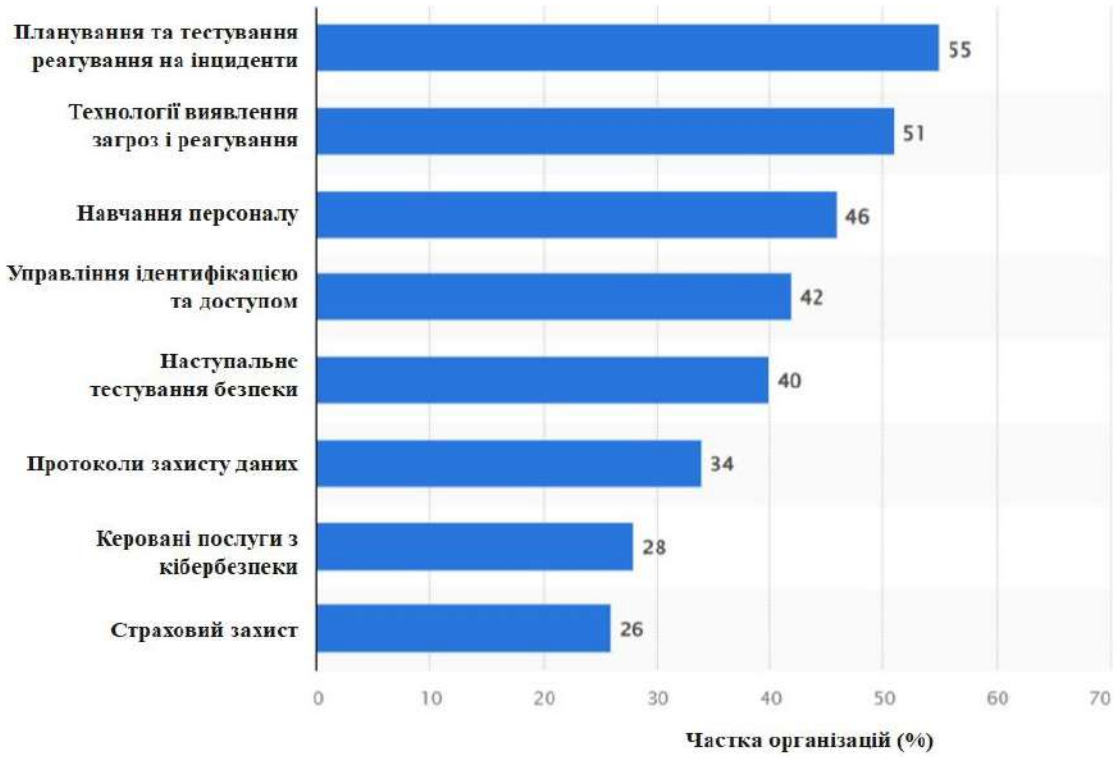

Рисунок 1. Основні напрями інвестицій у кібербезпеку після витоку даних у компаніях світу у 2024 році. Джерело: Statista, Inc [4]

Один із провідних напрямів у сфері кібербезпеки — це впровадження хмарних технологій, що дає змогу компаніям підвищити масштабованість, оптимізувати управління інформаційними потоками та скоротити витрати на фізичну інфраструктуру. Водночас відкритий характер доступу та складна архітектура хмарних рішень роблять їх привабливою ціллю для кібератак, що обумовлює потребу у суттєвих інвестиціях для забезпечення їх надійного захисту.

Отже, вивчення динаміки кіберзагроз, потенційних фінансових втрат та обсягів інвестицій у захисні заходи підкреслює важливість впровадження комплексного підходу до кібербезпеки в бізнес-середовищі. Ефективне поєднання технологічних інструментів, нормативного нагляду та стратегічного управління ризиками є ключовим елементом у зменшенні шкоди від кіберінцидентів і підвищенні стійкості компаній до зовнішніх і внутрішніх загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cheng, L., Liu, F., & Yao, D.D. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7. 2017. URL : https://doi.org/10.1002/widm.1211

2. Gracy, Shanitamol. A global analysis of data breaches from 2004 to 2024. 2025. URL : 10.48550/arXiv.2502.05205.

3. 2024 Data Breach Investigations Report. 2024. URL : https://www.verizon.com/business/resources/reports/dbir/

4. Statista. Main security investment types following a data breach in companies worldwide in 2024. 2024. URL : https://www.statista.com/statistics/1484625/top-cybersecurity-investment-types-after-a-breach-worldwide/