МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ТЕХНОЛОГІЇ ЗАПОБІГАННЯ І ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дар'я ЛАБЯК

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувачка вищої освіти гр. УБДМ 61
Дар’я ЛАБЯК

Керівник:
к.держ.упр., доц Тетяна МУЖАНОВА

Рецензент:

_____

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Лабяк Дар`ї Сергіївні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "ТЕХНОЛОГІЇ ЗАПОБІГАННЯ І ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к. держ.упр., доц.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. № 145.

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: інформаційна безпека підприємства, внутрішня загроза інформаційній безпеці, технології запобігання і протидії внутрішнім загрозам.
4. Перелік питань, які потрібно розробити:
   1. Проаналізувати види і методи реалізації інсайдерських загроз.
   2. Дослідити технології виявлення і запобігання внутрішнім загрозам, зокрема IPC, IDS/ IPS, NIDS, управління доступом, SIEM.
   3. Порівняти сучасні SA&T та DLP рішень для підприємств.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Аналіз видів та методів реалізації інсайдерських загроз.	27.10.2023	
4.	Дослідження технологій виявлення і запобігання внутрішнім загрозам.	10.11.2023	
5.	Порівняльний аналіз кращих технологічних рішень SA&T і DLP як засобів подолання внутрішніх загроз.	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	.01.2024	

Здобувачка вищої освіти _____ Дар’я ЛАБЯК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувачка Лабяк Д.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "ТЕХНОЛОГІЇ ЗАПОБІГАННЯ І ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка **ЛАБЯК Дар'я** у кваліфікаційній роботі провела аналіз основних технологій виявлення та запобігання внутрішнім загрозам інформаційній безпеці підприємства, дослідила сутність і види внутрішніх загроз та методи їх реалізації, представила порівняльну характеристику сучасних SA&T та DLP рішень для підприємств.

ЛАБЯК Дар'я оформила кваліфікаційну роботу відповідно до встановлених вимог. Структура дослідження забезпечує досягнення поставленої мети і завдань.

Особливу увагу варто звернути на те, що дослідження поєднує вивчення як теоретичних, так і практичних аспектів внутрішніх загроз і технічних засобів їх протидії. За результатами дослідження запропоновано рекомендації щодо впровадження визначених технологічних рішень SA&T та DLP.

Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Актуальні проблеми кібербезпеки" 2023 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки **ЛАБЯК Дар'ї** на позитивну оцінку та присвоїти їй кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Лабяк Д. С. допускається дозахисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувачки вищої освіти Лабяк Дар'ї Сергіївни
На тему: УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ ПІДПРИЄМСТВА: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Актуальність: Сучасні технології та підходи до запобігання та протидії внутрішнім загрозам швидко розвиваються, що вимагає постійного оновлення та аналізу. Наявність широкого спектру інструментів та рішень, призначених для забезпечення інформаційної безпеки, створює необхідність у глибокому порівнянні цих технологій та визначенні їхньої ефективності в контексті конкретного підприємства. Зростаюча кількість інцидентів щодо витоку конфіденційної інформації, кібератак та інших загроз безпеці, пов'язаних із внутрішніми факторами, підкреслює важливість дослідження та впровадження найефективніших стратегій та технологій для захисту інформаційних ресурсів підприємства. Порівняльна характеристика технологій надає можливість вибрати оптимальні рішення для підприємств, враховуючи особливості та потреби.

Позитивні сторони. У кваліфікаційній роботі проаналізовано види і методи реалізації інсайдерських загроз; досліджено технології виявлення і запобігання внутрішнім загрозам, зокрема IPC, IDS/ IPS, NIDS, управління доступом, SIEM; проведено порівняння сучасних SA&T та DLP рішень для підприємств.

Кваліфікаційна робота засвідчила розуміння здобувачкою наукової проблеми та напрямів її вирішення, володіння методами дослідження. Здобувачка опрацювала достатню джерельну базу за темою, показала наявність практичних знань і навичок роботи за фахом. Робота оформлена відповідно до вимог. Виклад матеріалу здійснено згідно з планом, надано практичні рекомендації.

Недоліки

1. Доцільно було б детальніше описати в кваліфікаційній роботі використання засобів протидії та запобігання внутрішнім загрозам на підприємствах відповідно до вибраних рішень.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувачка Лабяк Дар'я Сергіївна заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____ _____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 83 стор., 25 рис., 4 табл., 61 джерело.

Метою роботи є вивчення й порівняння технологій запобігання і протидії внутрішнім загрозам інформаційної безпеки підприємства.

Об'єктом дослідження є запобігання і протидії внутрішнім загрозам інформаційної безпеки підприємства.

Предмет дослідження - технології запобігання і протидії внутрішнім загрозам інформаційної безпеки підприємства.

Методи дослідження. Для вирішення завдань дослідження щодо запобігання та протидії внутрішнім загрозам інформаційній безпеці використані методи аналізу й синтезу, порівняння й узагальнення, класифікації, спостереження.

Короткий зміст роботи. Як результат у роботі проведено аналіз основних технологій виявлення та запобігання внутрішнім загрозам інформаційній безпеці підприємства, досліджено сутність і види внутрішніх загроз та методи їх реалізації, представлено порівняльну характеристику сучасних SA&T та DLP рішень для підприємств.

Галузь застосування. Проаналізовані в ході дослідження рішення запобігання та протидії внутрішнім загрозам інформаційної безпеки підприємства можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ВНУТРІШНЯ ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ТЕХНОЛОГІЇ ЗАПОБІГАННЯ І ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 83 pages, 25 figures, 4 tables, 61 sources.

The purpose of the work is to study and compare technologies for preventing and countering internal threats to the information security of the enterprise.

The object of research is to ensure the information security of the enterprise.

The subjec*t *of research is the technologies for preventing and countering internal threats to the enterprise's information security.

Research methods Methods of analysis and synthesis, comparison and generalization, classification, and observation were used to solve research tasks related to prevention and countermeasures against internal threats to information security.

Brief content of research. As a result, the work analysed the main technologies for detecting and preventing internal threats to the company's information security, investigated the essence and types of internal threats and methods of their implementation, and presented a comparative characteristic of modern SA&T and DLP solutions for enterprises.

Field of research. The analyzed solutions for preventing and countering internal threats to the company's information security can be used in the planning and implementation of the company's information security management system.

KEYWORDS: INFORMATION SECURITY OF THE ENTERPRISE, INTERNAL THREAT TO INFORMATION SECURITY, TECHNOLOGIES FOR THE PREVENTION AND COMBATATION OF INTERNAL THREATS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CSIRT	Computer Security Incident Response Team
DCS	Distributed Control System
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DoS	Denial-of-Service
DSOC	Distributed SOC
GRC	Governance, Risk, and Compliance
GSOC	Grid SOC
IDS	Intrusion Detection System
IPFIX	The IP Flow Information eXport (IPFIX) protocol
IPS	Intrusion Prevention System
MDM	Mobile Device Management
MPLS	Multiprotocol Label Switching
NOC	Network Operations Center
NTP	Network Time Protocol
PPT	People, Processes, and Technologies
PPTGC	People, Processes, Technologies, Governance, Compliance
SCADA	Supervisory Control and Data Acquisition
SEM	Security Event Management
SIC	Security Intelligence Center
SIEM	Security Information & Event Management
SIM	Security Information Management
SLMS	Security Log Management Service
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
UEBA	User & Entity Behavior Analytics

ВСТУП

Актуальність теми. Інформація, яка сьогодні є фактично найважливішим активом організації, нерідко є об’єктом численних загроз, спрямованих на її видалення, викрадення та заподіяння шкоди.

Як свідчить статистика, однією з найголовніших причин компрометації інформації є люди, що працюють в організаціях. Протидія внутрішнім загрозам має вирішальне значення у забезпеченні інформаційної безпеки підприємства і охоплює комплекс різноманітних заходів для виявлення й ефективного вирішення проблем, пов’язаних з халатною чи деструктивною діяльністю персоналу.

Щоб запобігти і протидіяти загрозам, що виникають внаслідок неправомірних та випадкових дій співробітників, компанії мають обирати засоби захисту відповідно до свої мети і бізнес-цілей з урахуванням наявних потреб.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки підприємницької діяльності.

Мета роботи є вивчення й порівняння технологій запобігання і протидії внутрішнім загрозам інформаційної безпеки підприємства.

Об’єкт дослідження - є запобігання і протидія внутрішнім загрозам інформаційної безпеки підприємства.

Предмет дослідження – технології запобігання і протидії внутрішнім загрозам інформаційної безпеки підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Провести аналіз видів та методів реалізації інсайдерських загроз організації.
2. Дослідити особливості технологій запобігання та протидії внутрішнім загрозам організації, зокрема IPC, IDS/ IPS, NIDS, SIEM.
3. Порівняти сучасні SA&T та DLP рішень для підприємств.

Методи дослідження. Для вирішення завдань дослідження щодо запобігання та протидії внутрішнім загрозам інформаційній безпеці використані методи аналізу й синтезу, порівняння й узагальнення, класифікації, спостереження.

Наукова новизна одержаних результатів. Запропоновані за результатами дослідження рекомендації щодо застосування програмних засобів запобігання внутрішнім загрозам можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті протидії деструктивному впливу «людського чинника.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу підприємства відповідно до цілей бізнесу, корпоративних можливостей і завдань із протидії внутрішнім загрозам.

Апробація результатів кваліфікаційної роботи Результати дослідження апробовані на Всеукраїнській науково-практичній конференції “Актуальні проблеми кібербезпеки” 2023 року.

РОЗДІЛ 1.
ВИДИ І МЕТОДИ РЕАЛІЗАЦІЇ ІНСАЙДЕРСЬКИХ ЗАГРОЗ

1.1 Сутність і види внутрішніх загроз інформаційній безпеці

В еру інформаційних технологій кожна організація має комп’ютери для роботи з даними, а також майже кожна людина постійно працює з персональним комп’ютером, через що з кожним роком збільшується кількість інцидентів пов’язаних з інформаційною безпекою, що призводить як до внутрішніх загроз, так і зовнішніх в організації.

Інформаційна безпека - це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах організацій, правомірне визначення загроз безпеці інформації, джерел цих загроз, способів їх реалізації та мети, а також, інших умов і дій, що порушують безпеку. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.

Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень інформаційної безпеки.

Загрозу будемо розглядати як атаку й можливість порушення інформаційної безпеки і посягання на заволодіння інформацією. Відповідно, той, хто посягає на інформацію, вважається зловмисником. Загрози виникають через низький захист або знаходження вразливих місць у системі захисту інформаційних систем.

Спорідненим із загрозою поняттям є небезпека. Між загрозою і небезпекою нанесення шкоди існують відносини заподіяння, які визначаються як обумовлена сутністю взаємодіючих об'єктів, елементів системи, зв'язок між явищами, при якій одне явище, причина, за наявності певних умов неминуче породжує, викликає до життя інше явище, зване слідством. Небезпека завжди

виникає після виникнення загрози. Небезпека може бути визначена як стан, в якому знаходиться об'єкт безпеки внаслідок появи загрози.

Відмінність між ними полягає в тому, що небезпека є властивістю об'єкта безпеки, а загроза - властивістю об'єкта взаємодії або знаходяться у взаємодії елементів об'єкта безпеки, виступаючих як джерело загроз. Загроза знаходиться у відношенні заподіяння не тільки з небезпекою, але і з очікуваними збитками - наслідками негативної зміни умов існування, які необхідно подолати для відновлення необхідних умов - в тому сенсі, що очікувані збитки визначають величину небезпеки [1].

Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій.

Класичною класифікацією можна вважати поділ загроз інформаційній безпеці на основі тріади CIA:

– загрози конфіденційності: інформація стає відомою неавторизованому користувачу. Найчастіше в цьому контексті використовують термін «витік інформації». Такі загрози часто виникають внаслідок дії «людського чинника»;

– загрози цілісності : відбувається не санкціонована модифікація інформації, що зберігається в інформаційній системі. Такі загрози можуть бути спричинені різними чинниками - від навмисних дій персоналу до збоїв у роботі обладнання;

– загрози доступності: створення умов, за яких відсутній доступ авторизованого користувача до послуги або інформації у потрібний час та в потрібному обсязі.

Інші класифікації загроз інформаційній безпеці показані на рисунку 1.1.

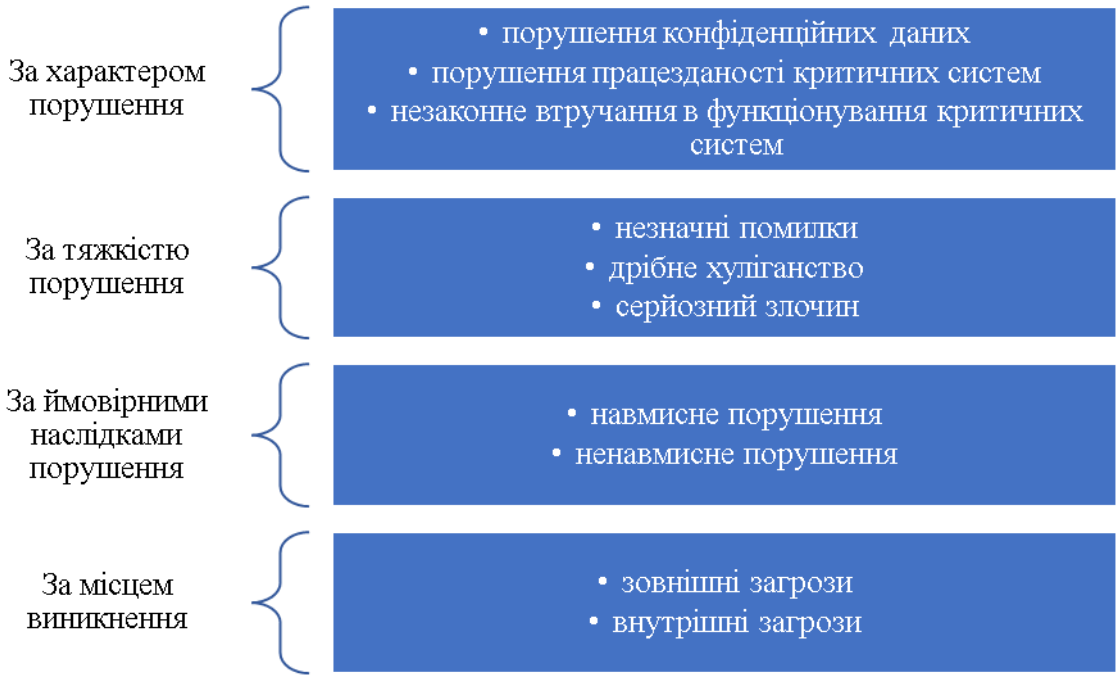

Рис. 1.1. Види загроз інформаційній безпеці

Джерела загроз інформаційній безпеці поділяють на внутрішні та зовнішні.

Внутрішня загроза – це загроза безпеці, яка походить зсередини цільової організації. Зазвичай це пов’язано з поточним або колишнім співробітником або діловим партнером, який має доступ до конфіденційної інформації або привілейованих облікових записів у мережі організації та зловживає цим доступом [2].

Також розглянемо визначення «внутрішня загроза» зі стандарту NIST (National Institute of Standards and Technology) NIST 800-53. Security and Privacy Controls for Information Systems and Organizations [3]. **Внутрішня загроза** – суб'єкт із авторизованим доступом (в межах домену безпеки), який потенційно може завдати шкоди інформаційній системі чи підприємству через розкриття, знищення, зміну даних або відмову в наданні послуг.

Традиційні заходи безпеки, як правило, зосереджені на зовнішніх загрозах і не завжди здатні визначити внутрішню загрозу, що походить зсередини організації.

Ключові ролі у реалізації внутрішніх загрозах відіграють (Рис. 1.2):

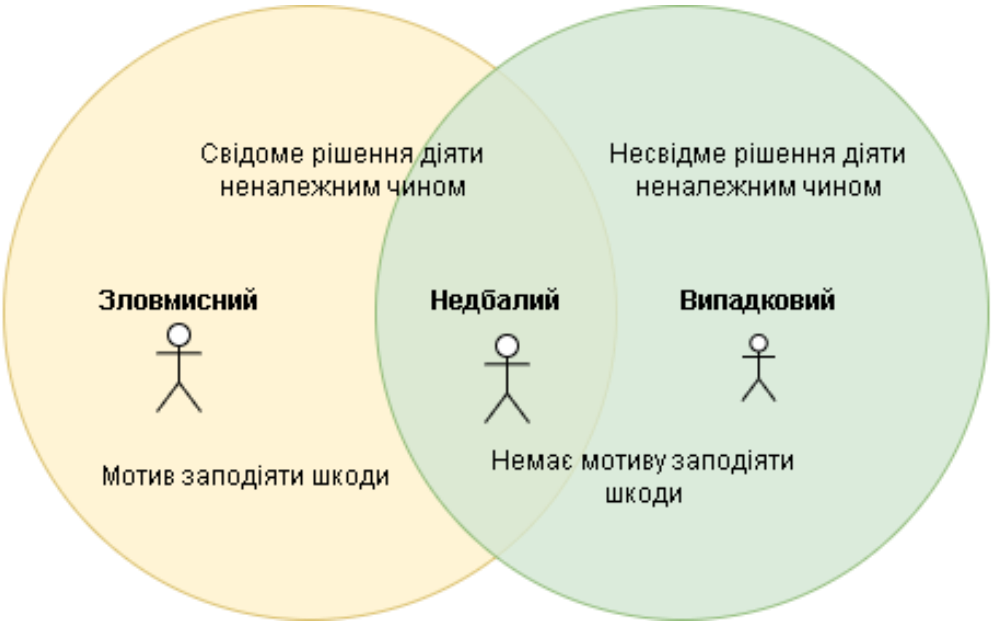

Рис. 1.2. Типи ризикованої поведінки

Зловмисний інсайдер - також відомий як Turncloak, особа, яка зловмисно та навмисно зловживає законними обліковими даними, як правило, для викрадення інформації з фінансових або особистих мотивів. Наприклад, особа, яка ображається на колишнього роботодавця, або співробітник, який продає секретну інформацію конкуренту. Turncloaks мають перевагу перед іншими зловмисниками, оскільки вони знайомі з політикою безпеки та процедурами організації, а також з її вразливими місцями.

Необережний інсайдер - невинний пішак, який неусвідомлено наражає систему на зовнішні загрози. Це найпоширеніший тип інсайдерської загрози, яка виникає внаслідок помилок, таких як залишення пристрою незахищеним, або використання методів соціальної інженерії. Наприклад, працівник, який не має наміру завдати шкоди, може натиснути небезпечне посилання, заразивши систему шкідливим програмним забезпеченням.

Кріт - самозванець, який технічно є аутсайдером, але зміг отримати внутрішній доступ до привілейованої мережі. Ця особа працює з-поза меж організації та представляє себе співробітником або третьою особою [4].

Існують індикатори внутрішньої загрози в мережевому середовищі. Аномальна активність на рівні мережі може вказувати на внутрішню загрозу. Таким чином, якщо працівник виглядає незадоволеним, тримає образу або

починає виконувати додаткові завдання з надмірним ентузіазмом, це може бути ознакою нечесної роботи. Індикатори внутрішньої загрози, які можна відстежити, включають:

– Активність у незвичайний час.
– Обсяг трафіку - передача занадто великої кількості даних через мережу.
– Вид діяльності - доступ до незвичних ресурсів.

У той час, як зовнішні загрози є більш поширеними та спричиняють ширший резонанс, внутрішні загрози як зловмисні, так і внаслідок недбалості, можуть бути дорожчими та більш небезпечними.

Відповідно до звіту IBM Cost of a Data Breach Report 2023, у 2023 середня вартість витоку даних досягла свого максиму в 4,45 мільйони доларів США. Порівняно з 2022 роком, це на 2,3% більше. Розглядаючи більший період часу, з 2020 року, зростання – на 15,3% [5].

13-й рік поспіль Сполучені Штати утримують лідерство з найвищими витратами внаслідок витоку даних. Щодо інших країн, то в п’ятірці країн або регіонів із найвищою середньою вартістю витоку даних відбулися значні зміни порівняно з 2022 роком (Таблиця 1.1).

Можемо на таблиці побачити, що з п’ятірки лідерів цього року Японія – єдина країна, яка не потрапила до п’ятірки лідерів 2022 року, піднявшись із 6-го місця. Також, до п’ятірки найкращих минулого року також увійшла Велика Британія із середнім збитком від витоку даних у 5,05 мільйона доларів США. Цього року у Великій Британії спостерігалося значне зниження середньої вартості на 4,21 мільйона доларів США, що на 16,6% менше, ніж у минулому році та призвело до розміщення за межами першої п’ятірки.

Таблиця 1.1.

Рейтинг країн з найвищими витратами внаслідок витоку даних у 2022-2023 рр

		2023	2022
		США 9,48 мільйонів	**США** 9,44 мільйонів
		Середній Схід 8,07 мільйонів	**Середній Схід** 7,46 мільйонів
		Канада	**Канада**
		Німеччина 4, 67 мільйонів	**Велика Британія** 5,05 мільйонів
		Японія 4, 52 мільйони	**Німеччина** 4,85 мільйонів

Внутрішні загрози, в більшості випадків, виникають у результаті витоку конфіденційних даних внаслідок неправомірних дій працівників і підрядників або через зловживання їхнім доступом до систем для отримання особистої вигоди, завдання шкоди й порушення роботи організації.

Внутрішні атаки можуть спричинити широкий спектр негативних наслідків для організацій. В опитуванні [5] спеціалісти з інформаційної безпеки надали інформацію про найпоширеніші наслідки внутрішніх атак, з якими вони зіткнулися:

– втрата важливих даних – 45% спеціалістів проголовували, що це найбільша внутрішня загроза;

– збиток бренду – 43%;

– збої та перебої в роботі – 41%.

Компанії виділяють три типи людей, які можуть стати основними чинниками створення внутрішніх загроз: постійні працівники, привілейовані користувачі й адміністратори систем, підрядники.

Враховуючи, що значна частина внутрішніх загроз реалізується за участі або сприяння персоналу, основним джерелом таких загроз є працівники організації. Виходячи з цього внутрішні загрози можуть виникати внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних і комунікативних особливостей працівників [2].

Очевидно, що основною внутрішньою загрозою для інформаційної безпеки організації є постійні працівники. Навіть ті з них, які мають обмежений доступ до систем згідно з робочими обов'язками, цілком можуть завдати шкоди організації. Наприклад, вони можуть скачувати конфіденційну інформацію на свої пристрої та поширювати третім сторонам або особам, встановлювати несанкціоновані програми, а також можуть стати жертвами соціальної інженерії. 90% атак є успішними саме через працівників, які порушують або нехтують правилами інформаційної безпеки.

Показовим прикладом реалізації внутрішньої загрози з боку працівника організації є випадок, який стався у травні 2022 року, коли старший науковий співробітник відомої компанії Yahoo К.Санг викрав конфіденційну інформацію про продукт Yahoo AdLearn. Скомпрометовані дані включали 570 тис. файлів, що містили вихідний код, інформацію про серверну архітектуру, секретні алгоритми та іншу інтелектуальну власність. Санг завантажив ці дані на свої особисті пристрої зберігання через кілька хвилин після отримання пропозиції про роботу від одного з конкурентів Yahoo.

Після виявлення інциденту Yahoo висунула проти Санга три звинувачення, включно з крадіжкою інтелектуальної власності, стверджуючи, що його дії розкрили комерційні таємниці компанії, даючи конкурентам значну перевагу [6].

Нерідко внутрішні загрози викликані негативним ставленням працівника до компанії, який внаслідок невдоволення, образи чи злості втручається в роботу інформаційних систем компанії та наносить шкоду.

Розглянемо ситуацію, що сталася в одній американській компанії в 2008 році, співробітниця якої видалила даних на 2,5 мільйони через те, що подумала, що її керівник планує її звільнити. Жінка почала підозрювати, що її хочуть звільнити, коли прочитала оголошення про роботу, опис вакансії був дуже схожим з її поточними задачами. Отже, вона зробила хибні висновки і, маючи доступ до серверів компанії, видалила всі малюнки та дизайни, що були зроблені за останні 7 років [7].

Варто відзначити, що особливу загрозу інформаційній безпеці становлять привілейовані користувачі, до яких відносяться адміністратори, керівники рівня C (C-level management) та інші, хто має високий рівень доступу до інформаційних систем. Привілейовані користувачі мають ключі до критично важливої інфраструктури, тому через це можуть легко завдати шкоди всій організації.

Для прикладу, в березні 2022 року, група осіб повідомила турецьку компанію Pegasus Airline про те, що 6,5 терабайт їхніх конфіденційних даних були розкриті в Інтернеті. Це сталося через те, що системний адміністратор не зміг належним чином налаштувати хмарне середовище, в якому зберігалися ці записи. Порушення могло вплинути на тисячі пасажирів і членів екіпажу. Допустивши розкриття особистих даних персоналу, авіакомпанія порушила законодавство Туреччини про захист персональних даних, що могло призвести до максимального штрафу приблизно в 183 тис. доларів США [8].

Треті сторони або постачальники, субпідрядники, бізнес-партнери, які мають доступ до IT систем або даних організації, також можуть бути джерелом загроз інформаційній безпеці організації внаслідок недотримання ними правил кібербезпеки, які прийняті в організації або їх порушення шляхом зловмисних дій. Крім того, хакери можуть отримати доступ до слабо захищених

інформаційних систем третіх сторін, щоб проникнути в організацію, яка користується послугами третьої сторони.

Розглянемо такий приклад. У лютому 2022 році компанія Toyota припинила роботу в Японії через витік даних у постачальника пластикових деталей Kojima. Оскільки Kojima мав доступ до їхніх виробничих підприємств, Toyota була змушена припинити співпрацю, щоб захистити свої дані. Через цю зупинку компанія не змогла виготовити 13 тис. автомобілів, тобто 5% місячного виробничого плану. Порушення також вплинуло на деякі операції дочірніх компаній Toyota, що призвело до скорочення виробництва та потенційно вплинуло на їхні прибутки [9].

1.2 Методи реалізації внутрішніх загроз інформаційній безпеці

Розглянемо детальніше основні методи реалізації внутрішніх загроз.

Соціальна інженерія. Методи соціальної інженерії використовуються, щоб заволодіти інформацією за допомогою обману і використання людських слабкостей щоб досягти своїх деструктивних цілей. Ця техніка використовує психологічні методи й соціальні навички для отримання конфіденційної інформації, надання незаконного доступу до систем або виконання інших дій, що можуть зашкодити інтересам особи, організації або суспільства в цілому.

Поняття соціальної інженерії введено американським консультантом з комп'ютерної безпеки Кевіном Митником. Статистика демонструє, що велика кількість людей ставиться до використання власної конфіденційної інформації недостатньо уважно. Для прикладу, далеко не всі обирають достатньо складні для зламування паролі, неуважно ставляться до умов доступу до онлайн-рахунку в банку, є необережними при вході в свої акаунти в соціальних мережах. Поняття паролю і таємного запитання здається не важливим та не має

ніякого сенсу для більшості користувачів, хоча, недооцінювати їх значення не можна.

Але сама соціальна інженерія почала зародилася дуже давно. Шахраї та аферисти використовували соціальну інженерію з незапам'ятних часів, щоб змусити жертв діяти проти їхньої волі, віддати гроші або розкрити особисту інформацію. Однак завдяки Інтернету злочинці мають доступ до зовсім нового світу потенційних жертв.

Шахрайство з передоплатою - це відмінний приклад того, як старий засіб соціальної інженерії може еволюціонувати відповідно до часів і використовувати технологічні досягнення з жахливими наслідками.

Одним із відомих прикладів використання технологій обману є конспіративні «листи з Єрусалима» кінця XVIII ст. Щоб уникнути переслідувань (або страти) після Французької революції, шахраї стверджували, що є слугами французьких дворян і за певну суму пропонували революціонерам надати карту, на якій показане місцезнаходження скарбу. Цей скарб вони нібито вкрали у своїх колишніх господарів і заховали до кращих часів. Як свідчать записи, що дійшли до нашого часу, 20% одержувачів відповідали на листи. У подальшому такі листи продовжували бути успішним знаряддям виманювання грошей [10].

Соціальна інженерія включає в себе різноманітні методи та техніки, які використовуються для маніпулювання людьми. До найбільш поширених методів соціальної інженерії відносять:

1. Фішинг (Phishing): жертві надсилають шкідливого листа, який дуже важко відрізнити від справжнього повідомлення електронної пошти або веб-сайтів. Їх мета - переконати людей передати особисті дані такі як паролі, номери кредитних карток або інші конфіденційні відомості (Рис. 1.3). Фішинг є найпоширенішим типом атаки соціальної інженерії.

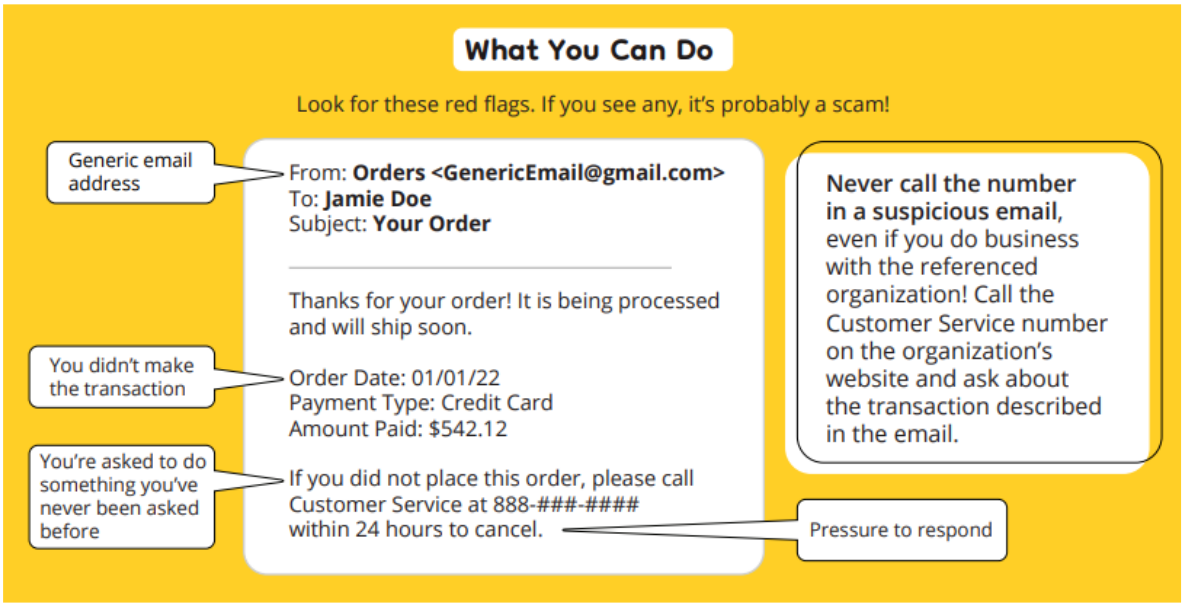

Рис. 1.3. Приклад фішингового листа

2. Виманювання інформації (Baiting): зловмисники можуть представлятися працівниками правоохоронних органів, щоб отримати необхідну інформацію. Дана атака спокушує людей привабливою пропозицією чи винагородою за отримання конфіденційної інформації або отримання несанкціонованого доступу. Цей тип атаки нагадує фішингову атаку; однак він відрізняється тим, що використовує «жадібність» як основний інструмент для маніпулювання [11].

3. Обман: шахраї представляються відомими особами, колегами, близькими друзями, родичами з метою отримання конфіденційної інформації.

4. Залякування: передбачає використання техніки погроз з метою викликати стрес у людини і змусити її видати інформацію.

5. Використання чужих облікових записів у соціальних мережах: вивчення акаунтів жертви в соціальних мережах, щоб знайти її слабкі місця для подальшої атаки.

6. Збір інформації з відкритих джерел: пошук інформації з відкритих онлайн-джерел (OSINT).

7. Трояни вказують на будь-який вид шкідливого програмного забезпечення, яке видає себе за інше програмне забезпечення. Так само, як Троянський кінь зі славетної грецької історії, комп'ютерні Трояни містять

руйнівне навантаження. Вкладені у електронні листи файли, що містять приховане шкідливе програмне забезпечення, макроси. Хитрощі, пов'язані із соціальною інженерією, виникають, коли електронний лист виглядає так, наче відправлений від надійного відправника, такого як колега, друг, родич або компанія-партнер [12].

Соціальна інженерія є багатогранним і складним способом отримання конфіденційної інформації від користувачів із застосуванням методів переконання і технологічних засобів. Будь-яка людина в сучасному світі є вразливою до соціальної інженерії, а отже, повинна залишатися постійно в курсі того, з ким вона взаємодіє як в режимі онлайн, так і віч-на-віч.

Розглянемо детальніше як працює соціальна інженерія. Існує 4 основних кроки (рис. 1.4).

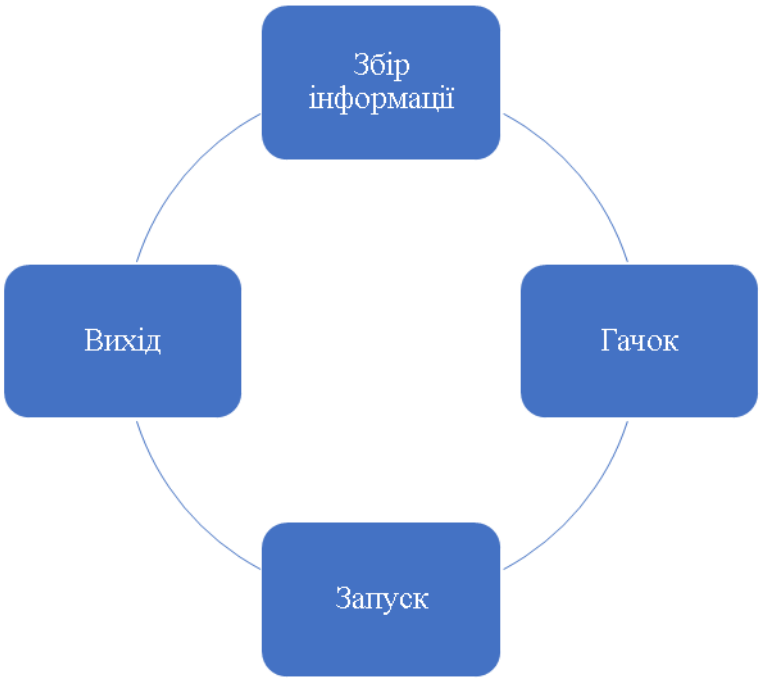

Рис. 1.4. Життєвий цикл атаки соціальної інженерії

Першим кроком виділимо збір інформації (Investigation). На цьому етапі, людина дізнається якомога більше інформації про жертву. Інформація збирається з відкритих джерел, такі як, веб-сайти компанії, соцмережі та інше.

Другий крок - це зловити жертву на гачок. За допомогою обману жертви з метою отримати контроль над взаємодією.

На третьому етапі зловмисники виконують атаку за допомогою отриманої інформації протягом певного періоду часу.

Четвертий крок - це доведення взаємодії до кінця, прибирання і замітання слідів, не викликаючи підозр.

Завдяки підвищенню обізнаності й формування навичок розпізнавання недостовірної інформації та спроб ввести користувачів в оману для розголошення секретної інформації компанія та її співробітники зможуть підтримувати безпечне корпоративне середовище, захистити власні активи, персональні дані працівників, партнерів, постачальників і клієнтів.

Витік інформації. На сьогоднішній день більшість організацій використовує багаторівневі системи обробки інформації: комп'ютери, хмарні сховища, корпоративні мережі тощо. Всі ці системи не тільки передають дані, але також є середовищем їх можливого витоку. Витік конфіденційної і секретної інформації – це процес неконтрольованого розголошення даних обмеженого доступу.

До інформації обмеженого доступу відносять державну таємницю, комерційну таємницю, персональні дані, професійні таємниці (лікарська, банківська, нотаріальна тощо), листування, телефонних розмов, відомості про винаходи (авторські права), інтелектуальна власність.

Основними категоріями конфіденційної інформації підприємства є комерційна таємниця та персональні дані. Комерційною таємницею є інформація про організацію та діяльності, технології розробки продукції, дані про фінанси, інтелектуальна власність та інші відомості, володіючи якими отримуються фінансові вигоди [2].

Персональні дані - це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [14].

Розглянемо декілька причин витоку даних.

Першою причиною є власне персонал. Кожен співробітник є потенційною загрозою для ІБ організації. Часто люди забирають роботу додому, особливо з початком пандемії та повномасштабної війни в Україні, використовують флеш-

носії для перенесення робочих даних, передають їх незахищеними каналами з'єднання, обговорюють інформацію зі співробітниками конкуруючих компаній. На рис. 1.5 показана класифікація дій працівників, що призводять до інсайдерських загроз [14].

Рис. 1.5. Класифікація дій працівників

Дії персоналу бувають навмисними і ненавмисними. Ненавмисні дії – це наслідок незнання регламенту роботи з комерційною інформацією. Ризик витоку інформації від персоналу є завжди, і його не можна виключити повністю. Служба безпеки може вжити заходів, щодо обмежень взаємодії працівників з конфіденційною інформацією та впровадити технічні заходи.

Важливою передумовою виникнення внутрішніх загроз є неналежний підбір кадрів. Часта зміна персоналу, масштабні зміни в організації роботи компанії, зменшення заробітних плат, скорочення співробітників – все це є причинами «плинності» кадрів. Таке явище часто стає причиною витоку секретної інформації. Криза, нестача коштів для видачі зарплат змушують керівництво погіршувати умови роботи персоналу. В результаті підвищується

невдоволення працівників, які можуть звільнитися або ж просто почати поширювати конфіденційні дані конкурентам.

Проблема зміни персоналу особливо важлива для керівних посад. Загрозу поширення таємниці можуть нести не тільки ті співробітники, які звільнилися, але і діючі працівники, рівень мотивації яких знижений.

Співпраця з іншими компаніями також є одним із чинників виникнення інсайдерських загроз. Більшість захисних автоматизованих систем здатні обмежувати доступ до корпоративної інформації в межах лише однієї будівлі чи підприємства (в разі, коли кілька філій використовують спільний сервер для зберігання даних). Під час колективної реалізації проєкту декількома компаніями служби безпеки не можуть повністю контролювати, як реалізується доступ до корпоративної таємниці кожного з підприємств.

1.3 Навмисна шкідлива активність інсайдерів

Інсайдерська загроза в інформаційній безпеці є однією з найскладніших у боротьбі, так як вона походить від осіб, які вже мають легальний доступ до внутрішніх ресурсів та конфіденційної інформації організації. Навмисна шкідлива активність інсайдерів може призвести до серйозних наслідків для конфіденційності, цілісності та доступності інформації. Розглянемо основні аспекти інсайдерської загрози та стратегії захисту від неї [15].

Розглянемо основні 4 типи інсайдерів:

1. Необережний інсайдер. Недбалі інсайдери є поширеним типом інсайдерів в більшості організацій. Ці інсайдери не мають злих намірів щодо компанії, однак їхні недбалі дії створюють хаос та шкоду компанії. Шкідливі, але ненавмисні дії необережного інсайдера включають натискання/ завантаження шкідливих вкладень, реагування на фішингові приманки та залишення флеш-накопичувачів, що містять конфіденційні дані, без нагляду.

2. Неуважний інсайдер. Неуважні інсайдери мають доступ до конфіденційних даних компанії, що робить їх основною мішенню для фішерів. Зловмисники часто обманюють цих інсайдерів за допомогою соціальної інженерії, щоб отримати конфіденційні дані або розгорнути зловмисне ПЗ всередині організації.

3. Зловмисний інсайдер. Це особа або співробітник організації, який діє навмисно та зловживає своїми внутрішніми привілеями і правами доступу для завдання шкоди організації. Це може включати в себе викрадення чутливої інформації, руйнівні дії, внутрішні атаки або інші шкідливі дії, які можуть призвести до втрати даних або порушення безпеки інформаційних систем.

4. Інсайдер-диверсант. До цієї категорії належать інсайдери, які змінюють часто компанії. Диверсанти навмисно намагаються завдати шкоди репутації своєї поточної компанії, щоб показати своє розчарування. Інсайдери-диверсанти мають на меті помститися своїй теперішній компанії, надаючи хакерам корпоративні дані та використання вразливостей, що існують в компанії.

Інсайдерські атаки можуть приймати різні форми. Також, їх сценарії залежать від мотивації інсайдера, його ролі в організації та доступу до ресурсів. Розглянемо декілька найпоширеніших сценаріїв інсайдерських атак:

1. Витік конфіденційної інформації: Історично, подібні витоки мали серйозні глобальні наслідки, як у випадку з Е. Сноуденом, що викликав міжнародні дебати про приватність і масовий нагляд. Сноуден був співробітником американської розвідки та інформатором, який у 2013 році розкрив існування таємних широкомасштабних програм збору інформації, які проводило Агентство національної безпеки. Справа висвітлила низку проблем, зокрема таємне використання урядової влади, конфіденційність у цифрову епоху, етику інформування та роль Інтернету та анонімних браузерів у даркнеті. В Україні, згідно з законодавством, такі дії можуть тягнути за собою серйозні юридичні наслідки, включаючи кримінальну відповідальність, що підкреслює важливість суворого дотримання корпоративних політик конфіденційності.

2. Видалення або зміна даних: Це може спричинити катастрофічні збитки для компанії, як це було в разі атаки NotPetya, що нанесла значні збитки компаніям по всьому світу. Українське законодавство, а саме ЗУ «Про основні засади забезпечення кібербезпеки України», чітко регулює відповідальність за такі дії, вказуючи на потребу високого рівня захисту даних і регулярного моніторингу систем [16].

3. Саботаж інфраструктури: Акти саботажу можуть включати знищення обладнання, відключення критичних систем або втручання в роботу мережевих ресурсів. Згідно з Кримінальним кодексом України, саботаж критичної інфраструктури вважається серйозним злочином.

4. Фінансові махінації: Цей сценарій може призвести до значних фінансових втрат та пошкодження репутації підприємства. Українські закони забезпечують чіткі правила щодо фінансових операцій і накладають відповідальність за їх порушення, що підсилює необхідність строгого контролю за фінансовими процесами.

Враховуючи дані сценарії, для компаній важливо впроваджувати стратегії управління ризиками, які включатимуть як технічні засоби захисту, так і комплексні програми навчання персоналу. Експерти з інформаційної безпеки наголошують, що особливу увагу слід приділяти кібербезпеці та фізичній безпеці, а також створенню етичного робочого середовища для зниження внутрішніх загроз.

1.4 Ненавмисні внутрішні загрози безпеці підприємства

Розглянемо більш детально ненавмисні внутрішні загрози. Ненавмисна загроза є похідною від недбалості.

Недбалий інсайдер наражає організацію на небезпеку через свою необережність. Недбалі інсайдери, як правило, знайомі з політикою безпеки

та/або ІТ-політиками, але ігнорують їх, чим створюють ризик для організації. До прикладів таких загроз можемо віднести наступне: дозвіл співробітникам обійти засоби інформаційної безпеки через захищену точку входу, неправильне розміщення або втрату портативного пристрою зберігання конфіденційної інформації, та ігнорування повідомлень про встановлення нових оновлень і виправлень безпеки.

Також існує наступний підвид ненавмисного інсайдера – випадковий інсайдер. Цей тип помилково створює ненавмисний ризик для організації. Наприклад, це може включати неправильне введення адреси електронної пошти та випадкове надсилання конфіденційного ділового документа конкуренту, несвідоме чи випадкове натискання гіперпосилання, відкриття вкладення у фішинговому електронному листі, яке містить вірус, або неналежну утилізацію конфіденційних документів. Організації можуть успішно працювати над мінімізацією інциденту, але позбутися цього ризику повністю неможливо, його можна тільки пом’якшити.

Ненавмисні інсайдери прискорюють зовнішні загрози, такі як фішингові атаки, поширення програм-вимагачів, шкідливі програми. Через це є необхідним розуміння ризику для виявлення загрози.

Один із прикладів ненавмисних внутрішніх загроз є наступна історія. У 2017 році HSBC вибачилася після того, як відправили особисту інформацію про клієнтів іншим власникам рахунків по електронній пошті. У листах були вказані імена, електронні адреси, країни проживання, імена менеджерів та ідентифікаційні номери клієнтів HSBC.

Пізніше у цьому ж році HSBC була оштрафована на суму 5,3 мільйона доларів США за втрату незашифрованого диска поштою, на якому були дані понад 1,9 тис. учасників пенсійних програм, включаючи адреси, дати народження та номери національного страхування; тоді як у лютому 2008 року HSBC втратила незашифрований компакт-диск із даними 180 тис. держателів полісів поштою.

Варто відзначити, що повторне порушення інформаційної безпеки, пов’язане із захистом персональних даних свідчить про те, що компанія не усвідомила важливість збереження особистої інформації та небезпеки шахрайства і не покращила захист даних своїх клієнтів.

Розглянемо ще один приклад інциденту, що стався через ненавмисну дію. Під час розгляду справи Гарі Сіндербранда, адвокат колишнього працівника Wells Fargo, викликав банк в суд у рамках справи про наклеп проти працівника банку, як і сам Сіндербранд, вони очікували отримати від банку вибірку електронних листів та документів, пов'язаних із справою. Проте те, що потрапило в їх руки, вийшло далеко за межі того, що просив його адвокат: компанія Wells Fargo випадково, за словами адвоката банку, відправила незашифрований CD із конфіденційною інформацією приблизно 50 000 найзаможніших клієнтів банку.

1,4 гігабайта файлів, які адвокат Анджела Туріано з Wells Fargo відправила, включали обширні таблиці з іменами клієнтів та їхніми номерами соціального страхування, поруч із фінансовими деталями, такими як розмір їхніх інвестиційних портфелів та вартість послуг банку, яку їм нараховували. Більшість з них є клієнтами Wells Fargo Advisors, відділу банку, який обслуговує клієнтів з високим рівнем чистих активів [17].

Отже, як свідчить статистика порушень інформаційної безпеки, людська необережність призводить до багатьох проблем в компаніях різного розміру й популярності.

Висновки до розділу 1

Встановлено, що внутрішня загроза – це загроза безпеці, яка походить зсередини цільової організації. Зазвичай це пов’язано з поточним або колишнім співробітником або діловим партнером, який має доступ до конфіденційної

інформації або привілейованих облікових записів у мережі організації та зловживає цим доступом. Аналіз показав, що основними причинами внутрішніх загроз в організації є: непрофесійні дії персоналу; низький стан виховної і профілактичної роботи; недосконала системи заробітної плати і стимулювання праці; порушення правил кадрової роботи; психологічні й комунікативні особливості працівників.

З’ясовано, що ключову роль у здійсненні внутрішніх загроз відіграє соціальна інженерія, які використовує психологічні методи й соціальні навички для введення особи в оману з метою подальшого отримання конфіденційної інформації, надання незаконного доступу до систем або виконання інших деструктивних дій. Найбільш поширеними й успішними атаками з використанням методів соціальної інженерії є: фішинг, виманювання інформації (байтинг), обман і залякування.

Виділяють два типи внутрішніх загроз: навмисні та ненавмисні. Навмисний інсайдер – працівник організації, здатний на недобросовісні дії чи злочинну діяльність, який загрожує безпеці організації, конфіденційності та/або доступності інформації та ресурсам з метою отримання особистої вигоди або помсти організації. Ненавмисний внутрішній порушник – працівник, який внаслідок своєї непрофесійної або недбалої поведінки, випадково порушує інформаційну безпеку організації, ставлячи під загрозу її інформаційні ресурси та системи.

РОЗДІЛ 2
ТЕХНОЛОГІЇ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВНУТРІШНІМ ЗАГРОЗАМ

Залежність від використання цифрових активів створює реальний виклик щодо їх безпеки. Такі активи існують в межах організацій на ПК, USB-пристроях, електронній пошті, внутрішніх ресурсах та мережах. Безпека чутливих цифрових активів має велике значення для неперервності та розвитку організацій. Щоб запобігти внутрішнім загрозам, деякі компанії приймають радикальні заходи, такі як перевірка співробітників, механізми аутентифікації, навчання, спостереження, розділення обов'язків та інші. Виявлення внутрішніх загроз є найбільш складним завданням, через це традиційні методи не завжди зменшують їх ризики виникнення.

Виявлення загроз – це здатність організації відстежувати події в інформаційному середовищі та виявляти реальні випадки порушення безпеки. Запобігання загрозам – це можливість блокувати загрози до того, як вони проникнуть в середовище чи нанесуть шкоду.

Функції та завдання захисту інформації визначають склад та структуру методів і систем захисту. Перелік основних методів захисту інформації представлений в таблиці 2.1.

Різні підходи до захисту від внутрішніх загроз можна розділити на три класи:

- підходи до виявлення,
- підходи до виявлення та запобігання,
- підходи до запобігання.

Перший клас виявляє внутрішні загрози під час або після виникнення загрози. У другому класі внутрішні загрози виявляються, а потім їм

запобігають, але під час або після появи деяких частин загроз. У третьому класі внутрішнім загрозам запобігають до того, як вони будуть реалізовані [18].

Таблиця 2.1

Основні методи захисту інформації

Метод	**Опис**	**Приклади**
Шифрування	Шифрування даних для забезпечення їх незрозумілості без спеціального ключа.	AES, RSA, SSL/TLS
Брандмауери	Блокування несанкціонованого доступу до приватної мережі або з неї.	Апаратні та програмні брандмауери, брандмауери NGFW
Антивірусне ПЗ	Захист від шкідливого ПЗ, в т.ч. віруси, черв'яки та трояни.	Norton, McAfee
Системи виявлення вторгнень (IDS)	Моніторинг мережевого трафіку на предмет підозрілої активності та відомих загроз.	Snort, Suricata
Контроль доступу	Обмеження доступу до даних і систем лише для авторизованих осіб.	Паролі, біометрична верифікація
Фізична безпека	Захист апаратного забезпечення і приміщень, де зберігаються дані.	Замки, системи відеоспостереження
Безпечне резервне копіювання	Створення копій даних для захисту від втрати даних.	Хмарне сховище, сервери резервного копіювання
Політика безпеки	Норми та практики для обробки та захисту конфіденційної інформації.	Політика доступу користувачів, плани реагування на інциденти

2.1 Технології виявлення внутрішніх загроз

Технології захисту конфіденційної інформації від внутрішніх загроз (Information Protection and Control, IPC) – це рішення, призначені для захисту інформації від внутрішніх загроз, запобігання різних видів витоків інформації, корпоративного шпигунства та бізнес-розвідки [19]. У системах такого типу комбінується два основні підходи до захисту: шифрування носіїв даних у всіх вузлах мережі та здійснення контролю, в інформаційних системах, витоку інформації із залученням технологій DLP.

Також розглянемо додаткові завдання системи:

- Запобігання передачі не лише конфіденційної, але й іншої небажаної інформації назовні.
- Запобігання передачі небажаної інформації не лише зсередини назовні, але й ззовні всередину інформаційної системи організації.
- Запобігання використанню працівниками Інтернет-ресурсів та ресурсів мережі в особистих цілях.
- Захист від спаму та вірусів.
- Оптимізація завантаження каналів та зменшення нецільового трафіку.
- Облік робочого часу і присутності працівників на робочому місці.
- Архівування інформації для випадків випадкового видалення або пошкодження оригіналу.
- Захист від випадкового або навмисного порушення внутрішніх політик.
- Забезпечення відповідності стандартам інформаційної безпеки та законодавству.

IPC використовують DLP-системи для моніторингу потоків інформації. Основною метою DLP-систем є запобігання неправильній передачі конфіденційної інформації за межі інформаційної системи. Такі передачі, або витоки, можуть бути як навмисними, так і не навмисними. Більшість витоків відбувається не через зловмисні дії, а через помилки, неуважність,

безтурботність та недбалість працівників. Інша частина витоків пов'язана із зловмисними намірами співробітників і користувачів інформаційних систем. Очевидно, що інсайдери, як правило, намагаються обійти заходи захисту, які забезпечують DLP-системи.

Розглянемо для початку базовий захист інформаційних систем організації.

Firewall (міжмережевий екран) – це пристрій безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік на основі попередньо встановлених політик безпеки організації. За своєю суттю брандмауер — це, бар’єр, який стоїть між приватною внутрішньою мережею та загальнодоступним Інтернетом. Основна мета брандмауера - пропускати незагрозливий трафік і запобігати небезпечному трафіку.

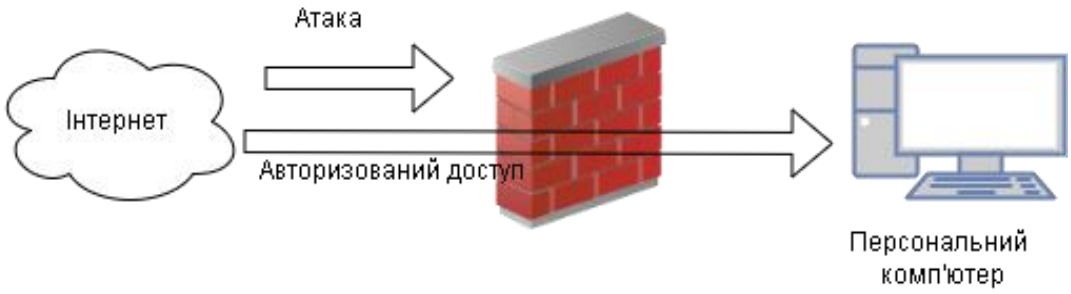

Рис. 2.1. Атака через брандмауер

VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером [20]. Дані в ньому надійно зашифровані. Це необхідно для захисту даних при їх передачі. VPN-сервіси дозволяють користуватися ресурсами, доступ до яких заборонено з метою захисту інформації від неавторизованих осіб. VPN-підключення типу «мережа-мережа» (логічне з’єднання) дозволяє організаціям встановлювати маршрутизовані підключення між окремими офісами або між організаціями по публічній мережі, при цьому забезпечуючи захищеність зв’язку (рис.2.2) [21].

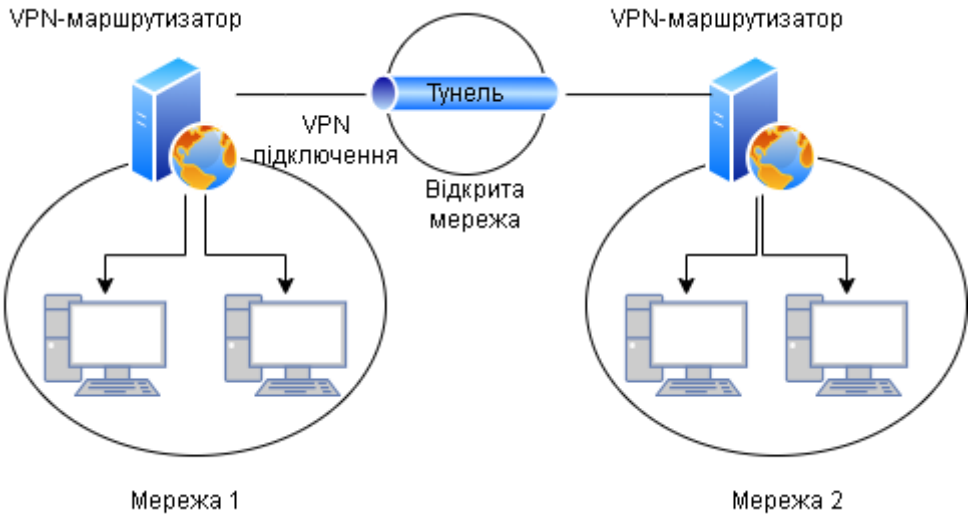

Рис. 2.2. З’єднання двох віддалених мереж

IDS/IPS (Intrusion Detection and Prevention System) – це програмні або апаратні системи виявлення та запобігання вторгненням, що забезпечують мережеву та комп'ютерну безпеку. IDS – це пасивна система виявлення, яка у режимі реального часу аналізує весь трафік і за необхідності повідомляє про можливі загрози. Вона ніяк не модифікує мережеві пакети даних і не впливає на роботу мережевої інфраструктури, в той час як IPS здатна запобігти доставці пакетів подібно до того, як це робить брандмауер. IPS, будучи системою запобігання вторгненням, також націлена на постійний аналіз трафіку, але повноваження служби більше – може відхиляти отримання пакетів, якщо системний аналіз виявить загрозу. Для виявлення загроз використовується актуальна база даних сигнатур, через що, рекомендується регулярно її оновлювати, з метою належного виконання системою своїх функцій [22]. На рис. 2.3 зображено практичне використання двох технологій та різниця між ними.

Здатність IDS лише виявити загрозу та сповістити адміністратора про подію. Але подальші дії це відповідальність адміністратора. В роботі розглянемо дві наступні архітектури IDS: на рівні мережі NIDS та окремого хоста HIDS.

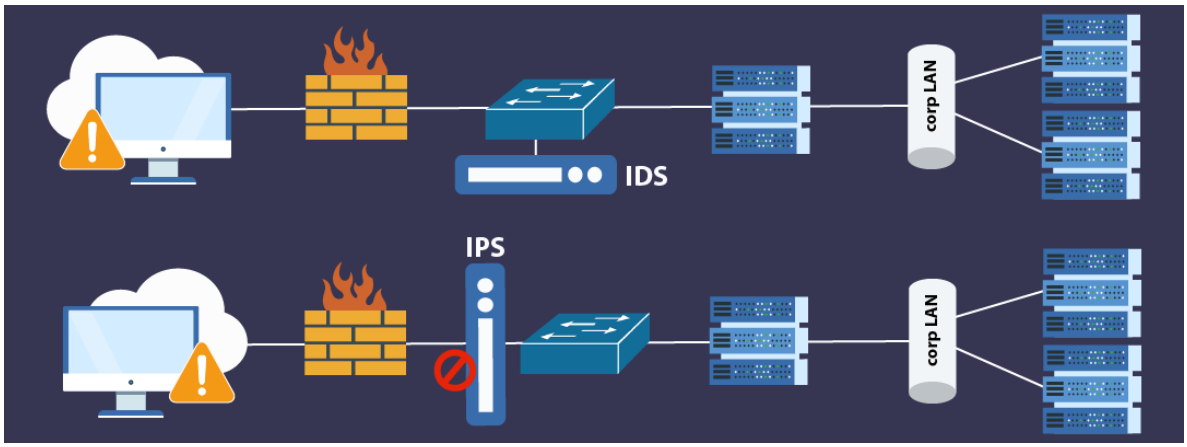

Рис. 2.3. Різниця в роботі технологій IDS та IPS

NIDS, або системи виявлення мережевих вторгнень, забезпечують безперервний моніторинг мережі в локальній і хмарній інфраструктурі для виявлення зловмисної активності, наприклад, порушення політик викрадання даних.

Технології безпеки NIDS є «пасивними», що означає, що вони призначені виключно для сповіщення про підозрілу активність. Тому, їх необхідно розгортати разом із системами запобігання вторгненням (IPS), які вважаються «активними».

Для організацій, які прагнуть ще більше підвищити видимість загроз, системи NIDS зазвичай використовуються разом із системами виявлення вторгнень на основі хосту (HIDS) і рішеннями SIEM, які збирають і аналізують події безпеки з багатьох джерел [23].

HIDS - це система виявлення вторгнень, що аналізує трафік і реєструє зловмисну поведінку саме на хостах. HIDS забезпечує точне бачення того, що відбувається у критично важливих системах безпеки. За його допомогою виявляють зловмисну чи аномальну діяльність у середовищі. Самостійно виявлення вторгнень на хості не надає повної картини про стан безпеки, однак правильне співвідношення даних журналу HIDS з іншими критично важливими даними безпеки дає можливість слідкувати за тим, що відбувається в повному обсязі.

Ці технології також корисні для виявлення й обмеження внутрішніх атак. Розглянемо кілька прикладів використання їх саме у випадках внутрішніх загроз.

IDS/IPS можуть аналізувати поведінку користувачів та систем. Якщо користувач або система раптово починає вести себе аномально (наприклад, збільшується обсяг передачі даних або надмірно запитує доступ до певних ресурсів), це може вказувати на внутрішню атаку, яку слід виявити та зупинити.

Якщо співробітник отримає винагороду від експлуатації відомих вразливостей в системі, IPS може допомогти заблокувати спроби використання цієї вразливості, що дозволяє запобігти атакам.

Ще одна із можливих ситуацій, IPS може виявляти та блокувати витік конфіденційної інформації. Якщо співробітник намагається незаконно отримати доступ до конфіденційних даних, IPS може перешкоджати цьому та захистити критичні ресурси.

Підсумуємо, IPS та IDS допомагають підвищити рівень безпеки мережі та системи, гарантуючи виявлення, блокування та реагування потенційних загроз в реальному часі, що є ключовим для захисту від внутрішніх атак та забезпечення стійкості інформаційних систем.

2.2 Системи управління правами доступу

Управління доступом – це основний елемент кібербезпеки, який визначає, хто може отримувати доступ до визначених даних, програм та ресурсів згідно з робочими обов’язками та за певних умов. Як ключі та попередньо затверджені списки гостей забезпечують фізичний захист, так і політики управління доступом забезпечують захист цифрового середовища, дозволяючи доступ відповідним користувачам і забороняючи всім іншим. Політики управління доступом в основному ґрунтуються на таких методах як автентифікація та авторизація, що дають змогу організаціям перевіряти правдивість даних користувачів та їхнє право на доступ до певних ресурсів на основі пристроїв, розташування, ролей тощо.

Завдяки управлінню доступом неавторизовані користувачі не можуть викрасти клієнтські дані або інтелектуальну власність, а також зменшується ризик викрадення даних (exfiltration data) працівниками. Замість того, щоб управляти дозволами вручну, більшість організацій із високим рівнем захисту використовують рішення для управління ідентичністю і доступом [24].

Основними й найбільш відомими методами є: мандатне управління доступом (Mandatory Access Control, MAC); управління доступом на основі ролей (Role-based Access Control, RBAC); вибіркове управління доступом (Discretionary Access Control, DAC).

Mandatory Access Control (MAC)

Передусім, мандатне управління доступом є найсуворішим методом контролю, за якого налаштування й конфігурації управління доступом доступні лише адміністратору. Це включає конкретні ролі та дозволи, потрібні кожному користувачу. MAC діє від рівня операційної системи або ядра безпеки організації. Практично це означає, що користувачі не можуть змінити призначені їм права доступу.

Для прикладу, якщо в організації працює 100 користувачів, необхідно налаштувати 100 різних ролей і дозволів в системі для використання MAC.

З огляду на те, що MAC вважають одним із найбільш надійних методів контролю доступу через його простоту, а також найменш гнучким методом, оскільки кожна зміна повинна відбуватися на дуже детальному рівні, цю модель контролю доступу здебільшого використовують урядові організації, військові та правоохоронні установи.

Так, уряд США використовує MAC для захисту секретної інформації та підтримки багаторівневих політик безпеки та програм. Компанії страхової галузі та банківської сфери використовують MAC для контролю доступу до даних облікових записів клієнтів, кращого захисту даних і забезпечення нормативної відповідності. Ця недискреційна модель контролю доступу може також захистити доступ до баз даних. Розумно використовувати MAC в організаціях, які цінують безпеку даних більше, ніж операційну гнучкість і

витрати. Впровадження MAC у приватних компаніях зустрічається рідко через складність і негнучкість такої системи. Чиста модель MAC забезпечує високий і деталізований рівень безпеки.

З іншого боку, його важко налаштувати та підтримувати. Ось чому зазвичай поєднують MAC з іншими моделями контролю доступу. Наприклад, поєднання його з RBAC прискорює налаштування профілів користувачів. Замість того, щоб визначати права доступу для кожного користувача, адміністратор може створювати ролі користувачів зі схожими ролями та правами доступу, однаковою посадою тощо.

Адміністратор може налаштувати ролі для цих груп замість того, щоб налаштовувати окремі профілі користувачів з нуля. Іншою популярною комбінацією є MAC і дискреційна модель контролю доступу, або DAC. MAC можна використовувати для захисту конфіденційних даних, тоді як DAC дозволяє колегам обмінюватися інформацією в корпоративній файловій системі [25].

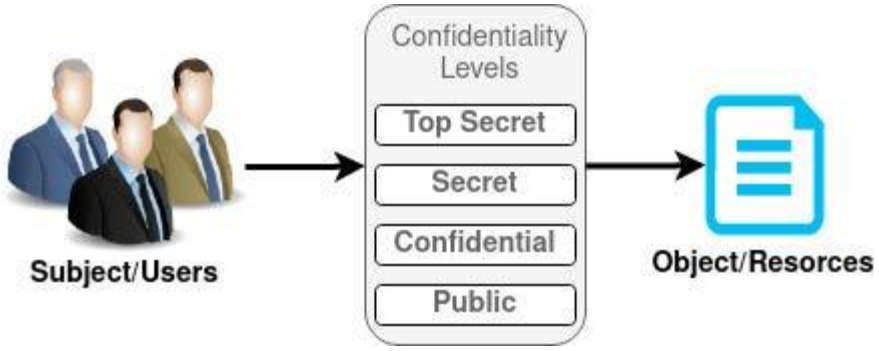

Рис. 2.4. Схема роботи MAC

Discretionary Access Control (DAC)

Дискреційний контроль доступу - це модель контролю доступу на основі ідентичності, яка надає користувачам певний контроль над своїми даними. Власники даних (творці документів або будь-які користувачі, уповноважені контролювати дані) можуть визначати права доступу для окремих користувачів або груп користувачів. Іншими словами, власник ресурсу на свій розсуд вирішує, кому надати доступ і привілеї.

Права доступу до кожної частини даних зберігаються в списку контролю доступу (ACL). Адміністратор створює цей список, коли користувач надає

комусь доступ. Список може формуватися автоматично. ACL включає користувачів і групи, які можуть отримувати доступ до даних, та їхні рівні доступу. Системний адміністратор може застосувати ACL. У цьому випадку ACL діє як політика безпеки, і звичайні користувачі не можуть редагувати або скасовувати його (рис. 2.5) [26].

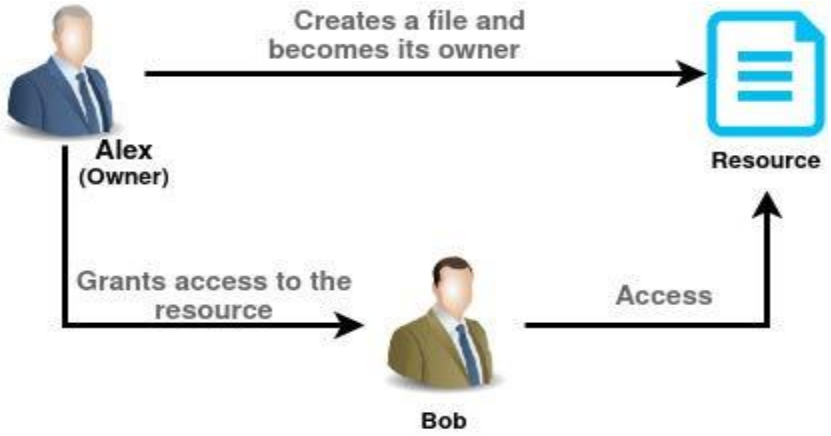

Рис. 2.5. Схема роботи DAC

Основні принципи DAC:

1. Характеристики об’єкта (розмір, назва, шлях до каталогу) невидимі для неавторизованих користувачів.

2. Кілька невдалих спроб доступу застосовують додаткову багатофакторну автентифікацію або забороняють доступ.

3. Користувачі можуть передавати право власності на об’єкт іншим користувачам. Також власник визначає тип доступу інших користувачів. На основі цих привілеїв доступу операційна система вирішує, чи надавати доступ до файлу.

Role-based Access Control

Контроль доступу на основі ролей (RBAC) - це метод обмеження доступу до мережі на основі ролей окремих користувачів. Організації використовують RBAC для аналізу рівнів доступу на основі ролей і обов’язків конкретного працівника.

Обмеження доступу до мережі є важливим для організацій, які мають багато співробітників, підрядників або дозволяють третім сторонам, таким як

клієнти та постачальники, мати доступ до мережі, оскільки ефективний моніторинг доступу до мережі може бути складним. Компанії, які залежать від RBAC, краще можуть захистити свої конфіденційні дані та критично важливі програми. RBAC гарантує, що користувачі отримують доступ лише до інформації, необхідної для виконання своєї роботи, запобігаючи доступу до інформації, яка їх не стосується.

Роль працівника в організації визначає дозволи, які надаються особі, гарантуючи, що працівники нижчого рівня не зможуть отримати доступ до конфіденційної інформації або виконувати завдання високого рівня.

RBAC базується на концепції ролей і привілеїв. Доступ залежить від таких факторів, як повноваження, компетентність і відповідальність. Доступ до мережі та інших ресурсів, як-от доступ до певних файлів або програм, може обмежувати працівник. Наприклад, певні файли можуть бути доступними лише для читання, але до певних файлів або програм можна надати тимчасовий доступ для виконання завдання. Організації можуть визначити, чи є користувач кінцевим користувачем, адміністратором чи спеціалістом. Ці ролі також можуть збігатися або давати різні рівні дозволів для окремих ролей. На рис. 2.6. можемо побачити на прикладі деяких ролей як збільшується кількість їх обмежень [27].

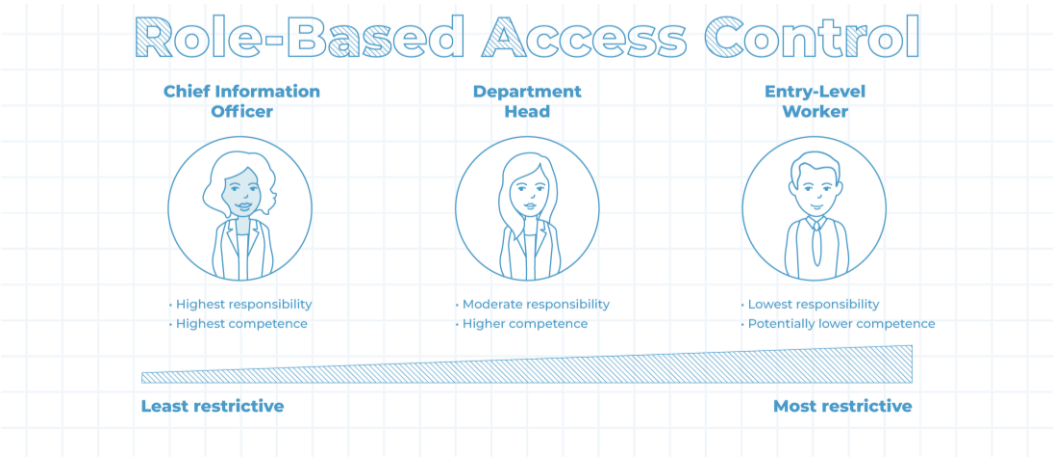

Рис. 2.6. Збільшення обмежень відповідно до обов’язків

Після надання доступу новим працівникам відповідно до робочих обов’язків необхідно зробити так, аби доступ до ресурсів організації був безпечним. Ці завдання виконує управління ідентифікацією. Програмне

забезпечення для управління ідентифікацією та доступом (IAM) надає інструменти, які допомагають організаціям перевіряти особистість людей і пристроїв, які намагаються ввійти, та гарантує, що перевірені користувачі мають доступ до потрібних ресурсів [28].

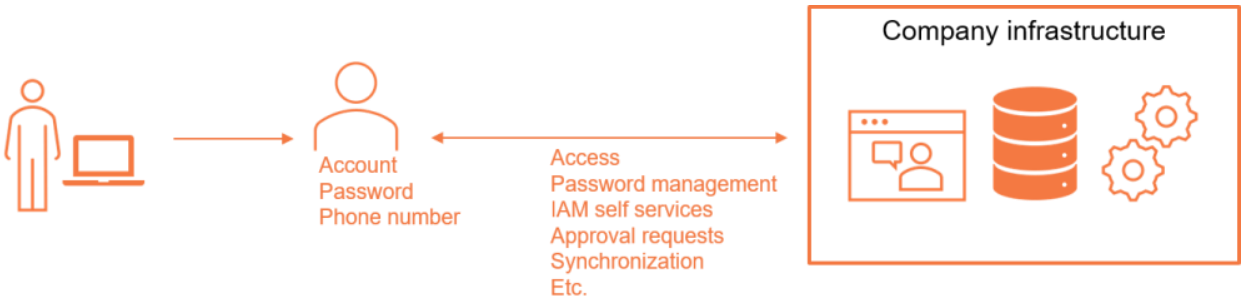

Рис. 2.7. Схема цифрової ідентифікації працівника

Управління доступом - це компонент IAM, що працює в реальному часі. Він охоплює процеси, які є критично важливими для захисту корпоративних ресурсів і безпеки цифрового бізнесу. Архітектура управління доступом контролює планування, проектування та розробку відповідних технологій, незалежно від того, чи йдеться про надання клієнтам доступу до електронної комерції чи забезпечення ресурсів для третіх сторін для безпечного ведення бізнесу [29].

Управління ідентифікацією перевіряє спробу входу в базу даних управління ідентифікацією, яка є постійним записом усіх, хто має мати доступ. Ця інформація постійно оновлюється, коли люди приєднуються до організації або залишають її, змінюються їхні ролі та проекти, а також розвивається сфера діяльності організації.

Приклади типу інформації, яка зберігається в базі даних управління ідентифікацією, включають імена співробітників, посади, керівників, прямих підпорядкованих, номери мобільних телефонів і особисті адреси електронної пошти. Зіставлення чиєїсь реєстраційної інформації, як-от ім’я користувача та пароль, з ідентифікацією в базі даних називається автентифікацією.

Для додаткової безпеки багато організацій вимагають від користувачів перевіряти свою особу за допомогою багатофакторної автентифікації (MFA). Також відома як двостороння перевірка або двофакторна автентифікація (2FA),

MFA є більш безпечною, ніж використання лише імені користувача та пароля. Це додає крок до процесу входу, де користувач повинен підтвердити свою особу за допомогою альтернативного методу перевірки. Ці методи підтвердження можуть включати номери мобільних телефонів, особисті адреси електронної пошти або встановлений спеціальний додаток на мобільному телефоні. Система управління ідентичністю та доступом IAM (Identity and Access Management) зазвичай надсилає одноразовий код до альтернативного методу перевірки, який користувач повинен ввести на порталі входу протягом встановленого періоду часу.

Управління доступом є другою половиною IAM. Після того, як система IAM перевірила, що особа, яка прагне отримати доступ до ресурсу, відповідає заявленій особистості, управління доступом відстежує, до яких ресурсів ця особа має доступ. Більшість організацій надають різні рівні доступу до ресурсів і даних, і ці рівні визначаються такими факторами, як посада, термін роботи, дозвіл безпеки та проект.

Надання правильного рівня доступу після автентифікації користувача називається авторизацією. Метою систем IAM є переконатися, що автентифікація та авторизація відбуваються правильно та безпечно під час кожної спроби доступу.

На рисунку 2.8 бачимо найвідоміші рішення та їх оцінку IAM по квадрату Gartner. Лідер серед запропонованих на ринку IAM рішень - це Okta, на другому місці знаходиться Microsoft, а на третьому – Ping Identity [30].

Системи IAM можуть бути не структурованими й потребувати багато ресурсів відділу IT, щоб управляти акаунтами і доступом до кожного застосунку, сервісу тощо. Чим більше користувачів, тим більше потрібно ресурсів і часу для забезпечення надійного рівня безпеки [31].

Рис. 2.8. Найпопулярніші IAM за оцінкою Gartner

IAM рішення фокусуються на управлінні доступом всіх користувачів до ресурсів, наданні й забезпеченні зручного та безпечного доступу, управлінні доступом до користувачів на основі ролей залежно від їх посадових функцій та обов'язків, а також управлінні ідентифікаторами користувачів, атрибутами та правами доступу в кількох системах і додатках [32].

2.3 Системи моніторингу й аналізу поведінки користувачів

Без своєчасного моніторингу та запобігання несанкціонованих дій втрачається сенс усіх систем захисту інформації, що вже впроваджені в організації. Для цього фахівці з безпеки використовують рішення SIEM - Security Information and Event Management.

Поєднуючи SIM і SEM, SIEM пропонує моніторинг і аналіз подій у реальному часі, а також відстеження та реєстрацію даних безпеки для цілей

відповідності або аудиту. На рисунку 2.9 представлено розвиток систем внутрішнього моніторингу.

Рис. 2.9. Розвиток систем моніторингу

Іншими словами, SIEM - це рішення безпеки, яке допомагає організаціям розпізнавати потенційні загрози безпеці та вразливості до того, як вони зашкодять організації. Він виявляє аномалії поведінки користувачів і використовує штучний інтелект для автоматизації багатьох ручних процесів, пов’язаних із виявленням загроз і реагуванням на інциденти, і став основним продуктом сучасних операційних центрів безпеки (SOC) для випадків використання управління безпекою та відповідністю стандартам та нормативним документам.

З роками SIEM став не лише інструментом управління журналами, які йому передували. Сьогодні SIEM пропонує розширену аналітику поведінки користувачів і об’єктів (UEBA) завдяки потужності ШІ та машинного навчання. Це високоефективна система оркестровки даних для управління загрозами, що постійно розвиваються, а також для дотримання нормативних вимог.

SIEM-система дозволяє зібрати всі події та інциденти інформаційної безпеки в єдиному місці, з різних джерел, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи з інформаційної безпеки. Крім цього, система моніторингу інформаційної безпеки виконує реєстрацію та зберігання всіх інцидентів інформаційної

безпеки, на час який вибере адміністратор цієї системи, що робить можливим використання отриманої інформації в якості доказів при виконанні розслідувань інцидентів та побудови можливої атаки.

Робота SIEM дозволяє побачити більш повну картину активності мережі і інцидентів інформаційної безпеки. Цю систему використовують як додатковий спосіб захисту від цілеспрямованих атак на корпоративну мережу. SIEM-система повинна збирати, аналізувати, моніторити і представляти інформацію із мережевих пристроїв і систем безпеки. Функції SIEM-системи спрямовані на моніторинг основних подій і станів інформаційної безпеки всередині компанії та її діяльності [33].

За формою впровадження SIEM можна поділити на 3 категорії - хмарні, внутрішні та керовані.

Хмарна SIEM — це система керування інформацією та подіями безпеки, яка пов’язана з хмарними обчисленнями. Цей варіант став популярним після глобального поширення хмарних обчислень в організаціях. Це забезпечує функціональність SIEM з набагато меншими затратами на розгортання. Однак він трохи менш адаптований для потреб кожної окремої організації. Але є велика загроза – збільшення поверхні атак: дані, зібрані й оброблені системою SIEM, можуть просочуватися не лише від компанії-клієнта, а й від третьої сторони хмарних послуг, а також перехоплені на шляху до сервера. Але є і переваги в гнучких тарифах і відсутності необхідності купувати та обслуговувати обладнання.

Внутрішня SIEM передбачає впровадження системи на власному апаратному та програмному забезпеченні. Це забезпечує максимальну інтеграцію, оскільки зазвичай in-home модель передбачає розширену адаптацію програмного забезпечення під потреби певної компанії. Така інтеграція підходить компаніям, які використовують всеохоплюючі заходи захисту, які утворюють комплексний центр безпеки. Цей підхід потребує участі великої кількості кваліфікованих спеціалістів, але вартість набагато більша, проте є дуже ефективним.

Керована SIEM – це тип системи, яка може базуватися як на внутрішній, так і на хмарній формі, але за допомогою команди аналітиків стороннього підрядника. Постачальник технологій пропонує обчислювальну потужність і кваліфікований персонал, який прийматиме рішення постійно або на вимогу. Ця форма обслуговування приваблива для компаній, які не мають відповідного персоналу і не хочуть його наймати, а також не мають можливості для придбання та обслуговування відповідного апаратного забезпечення.

Робота SIEM відбувається наступним чином: спочатку збирається інформація з різних джерел, приводиться до одного виду, аналізується в режимі реального часу та/або аналізує поведінку на основі попередніх спостережень і генерує повідомлення про попередження (Рис. 2.10).

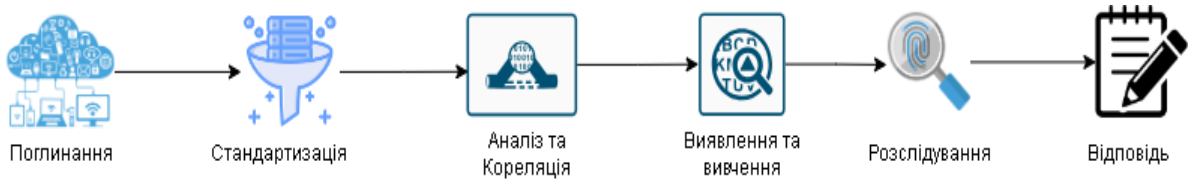

Рис. 2.10. Діаграма роботи SIEM

Ця схема реалізується за допомогою наступних компонентів:

- Агенти (збір даних з різних джерел).
- Сервери-колектори (акумуляція інформації, що надійшла від агентів).
- Сервер баз даних (зберігання інформації).
- Сервер кореляції (аналіз інформації).

Для SIEM-систем вхідною може бути будь-яка інформація. Збір даних може виконуватися за допомогою програм – це спеціальні агенти, що локально збирають журнали подій і за можливості передають їх на сервер. Для стандартизації того чи іншого джерела даних агент використовує колектори – бібліотеки для розуміння журналу подій або системи. Колектори відіграють важливу роль, адже різні джерела можуть іменувати одну і ту саму подію по-різному. Наприклад, Firewall одного виробника може записувати у звіт «deny», іншого «discard», третього «drop». Колектори допомагають привести всі ці події

до одного виду. Якщо ж для джерела нема відповідного колектора, події можна спробувати відправляти як SYSLOG, при умові, що це можливо. Але тут можна зіткнутися з «проблемою синонімів» та необхідністю написати додаткову програму обробки для приведення даних у єдиний формат. Також інформацію можливо збирати віддалено за допомогою з'єднання за різними протоколами такі як NetBIOS, RPC, TFTP, FTP. Однак і тут може виникнути проблема з навантаженням на мережу, тому що частина систем дає можливість передавати тільки журнал цілком, а не «свіжі» записи [34].

SIEM наступного покоління має нові можливості для покращення видимості безпеки та виявлення загроз, а також процес керування робочим навантаженням команд безпеки. Деякі основні компоненти SIEM наступного покоління включають:

– Відкрита та масштабована архітектура: можливість оптимізувати дані з розрізнених систем за допомогою локальних, хмарних і мобільних технологій в одному об'єкті.

– Інструменти візуалізації в режимі реального часу: функції, які допомагають командам безпеки візуалізувати відповідні події безпеки, щоб точно.

– Архітектура великих даних: можливість збирати великі, складні набори даних і керувати ними для індексування структурованого й неструктурованого пошуку.

– UEBA: рішення для моніторингу поведінкових змін у даних користувачів для виявлення аномальних випадків.

– SOAR: технологія, яка автоматизує звичайні ручні дії аналітиків для підвищення ефективності роботи в процесі реагування на інциденти [35].

Розглянемо більш детально засоби аналізу поведінки користувачів і суб'єктів (UEBA). Адже, рішення UEBA є доповненням до рішень SIEM для організацій, які бажають дізнатися більше про те, як користувачі взаємодіють із конфіденційними корпоративними даними. Крім того, така комбінація

забезпечує більш швидке виявлення інцидентів і можливості реагування, таким чином підвищуючи загальну кібербезпеку організації.

UEBA – рішення безпеки, яке виявляє кіберзагрози шляхом ідентифікації активності, яка відхиляється від звичайного базового рівня. Хоча відомі рішення UEBA включають також інші функції: моніторинг і виявлення незвичайних шаблонів трафіку, несанкціонований доступ до даних та їх переміщення, а також підозрілу чи шахрайську діяльність у комп'ютерній мережі чи кінцевих точках.

UEBA надає інформацію, необхідну для виявлення та дослідження нерегулярних моделей у режимі реального часу, дозволяючи аналітикам безпеки перевіряти та усувати загрози, перш ніж вони завдадуть ще більшої шкоди. Рішення UEBA використовують різноманітні аналітичні підходи, такі як детальна статистика, зіставлення шаблонів і правила, які використовують сигнатури, щоб шукати аномалії, які можуть вказувати на потенційно зловмисну поведінку чи дії.

Перш ніж рішення UEBA зможуть належним чином виконувати аналітику поведінки для організації, потрібен повний набір даних для її технологій машинного навчання, які є водночас надійними та інтегрованими. Для більшої картини, на рисунку 2.11 зображено приклад загальної архітектури UEBA.

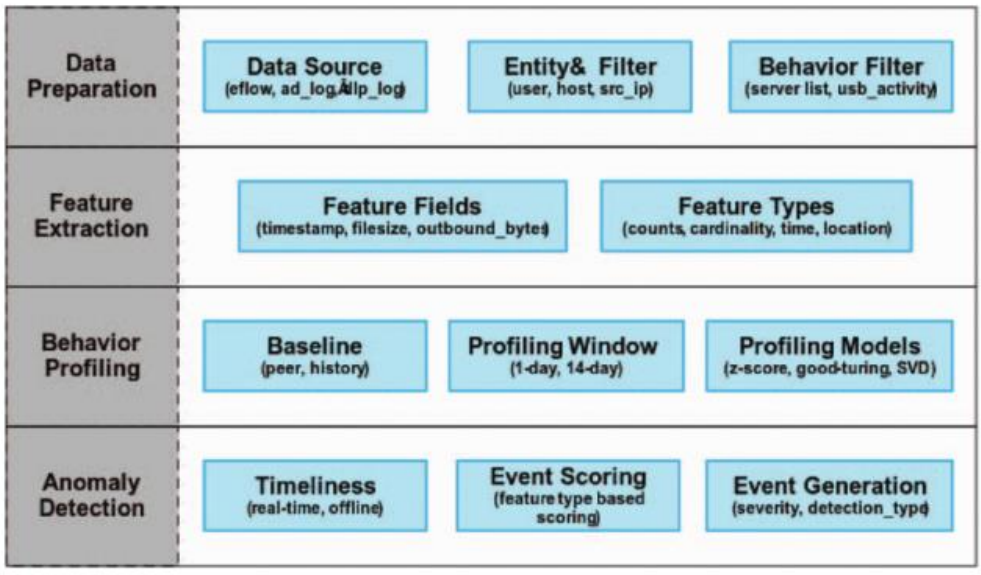

Рис. 2.11. Архітектура UEBA

Відповідно до Gartner, рішення UEBA визначається трьома основними характеристиками:

– Варіанти використання: Рішення UEBA має аналізувати, виявляти, звітувати й контролювати шаблони поведінки як користувачів, так і організацій. І, на відміну від попередніх точкових рішень, UEBA має зосереджуватися на кількох варіантах використання, а не лише на спеціалізованому аналізі, наприклад моніторингу надійних хостів або виявленні шахрайства.

– Аналітика: Рішення UEBA має пропонувати розширені аналітичні можливості, які можуть виявляти аномалії поведінки за допомогою кількох аналітичних підходів в одному пакеті. До них належать статистичні моделі та машинне навчання (ML), а також правила та підписи.

– Джерела даних: Рішення UEBA має мати можливість отримувати дані про дії користувачів і організацій як безпосередньо з джерел даних, так і через існуюче сховище даних (наприклад, управління інформацією про безпеку та подіями (SIEM), сховище даних або озеро даних) [36].

Висновки до розділу 2

У другому розділі проаналізовано мету технологій запобігання і протидії внутрішнім загрозам в організації, а саме: IPS/IDS, SIEM, UEBA.

IDS/IPS (Intrusion Detection and Prevention System) – це програмні або апаратні системи виявлення та запобігання вторгненням, що забезпечують мережеву та комп'ютерну безпеку. Встановлено, що ці системи допомагають підвищити рівень безпеки мережі та системи, гарантуючи виявлення, блокування та реагування потенційних загроз в реальному часі, що є ключовим для захисту від внутрішніх атак та забезпечення стійкості інформаційних систем. Правильне налаштування IAM і розподіл прав доступу відповідно до

обов’язків значно зменшує вірогідність отримання доступу до критичних ресурсів невповноважених працівник.

Встановлено, що методи управління доступом, основними з яких є: мандатне управління доступом MAC, управління доступом на основі ролей RBAC і дискретне управління доступом DAC, мінімізують можливості отримання несанкціонованого доступу потенційного внутрішнього порушника до інформаційних ресурсів і систем. Кожен метод використовується в різних умовах, а його використання залежить від розміру та цілей організації.

SIEM - це засіб безпеки, який використовує штучний інтелект для виявлення потенційних загроз та автоматизації реагування на них у сучасних центрах безпеки. Аналіз показав, що за формою впровадження SIEM поділяють на три категорії: хмарні, внутрішні та керовані. Роль SIEM у внутрішній інфраструктурі є дуже важливою, оскільки система не тільки адекватно реагує на вже реалізовані інциденти безпеки, але й забезпечує своєчасне виявлення неправомірних дій стосовно активів організації.

Система UEBA виявляє кіберзагрози шляхом ідентифікації активності, яка відхиляється від звичайного базового рівня. Встановлено, що типові рішення UEBA здійснюють моніторинг і виявлення незвичайних шаблонів трафіку, недозволеного доступу до даних та їх переміщення, а також підозрілої чи шахрайської діяльності в мережі чи на кінцевих пристроях. UEBA діє як система виявлення передових і внутрішніх загроз, які оминули традиційні інструменти безпеки, а також відстежує доступ користувачів до критично важливих даних і систем.

РОЗДІЛ 3
ПОРІВНЯЛЬНА ХАРАКТЕРИТИКА СУЧАСНИХ SA&T ТА DLP РІШЕНЬ ДЛЯ ПІДПРИЄМСТВ

3.1 Роль навчання персоналу у протидії інсайдерським загрозам

Незважаючи на значну роль технічних рішень у запобіганні і протидії внутрішнім загрозам інформаційній безпеці організації, вони можуть забезпечити ефективний захист від деструктивної інсайдерської діяльності тільки в комплексі з управлінськими заходами. Ключове значення для запобігання внутрішнім загрозам відіграють заходи з інформування й навчання персоналу організації та залучених третіх сторін.

Майже три з чотирьох порушень в інформаційному просторі організації пов’язані з людськими помилками, а кількість стратегічних фішингових атак, таких як компрометація корпоративної електронної пошти, з минулого року майже подвоїлася. Спеціалісти з інформаційної безпеки також помітили цю тенденцію: працівники найчастіше переходять за посиланнями в електронних листах з моделюванням фішингу, які пов’язані з корпоративними комунікаціями та контактами із зацікавленими сторонами. Багато організацій уже мають навчальні програми з питань безпеки для боротьби з цими загрозами, однак часто стикаються з наступними перешкодами:

- низька залученість співробітників у тренінги з безпеки;
- незнання персоналом процедур повідомлення про ймовірні інциденти;
- нерозуміння керівниками важливості навчання з безпеки та сприйняття навчально-просвітницьких заходів тільки як засобів дотримання вимог відповідності стандартам і нормативним документам.

На думку деяких експертів, ефективне навчання з питань безпеки - це і мистецтво, і наука, і до нього треба ставитися відповідально. Програми

навчання мають розроблятися і впроваджуватися таким чином, щоб співробітники були зацікавлені, усвідомлювали важливість дотримання вимог безпеки і знали про відповідальність за їх порушення.

Навчання з питань безпеки - це більше, ніж засіб управління ризиками і забезпечення відповідності вимогам. Це інвестиція у персонал і культуру компанії. Маючи під рукою перевірені клієнтами навчальні ресурси, компанії не тільки підвищують залученість співробітників, але й позитивно впливають на поведінку, зменшують рівень людських помилок, які можуть спричинити витік даних та зловмисне їх використання.

Навчання з безпеки не може бути універсальним для всіх. Кожен працівник перебуває на унікальному етапі своєї кар'єри у сфері кібербезпеки, а фахівці на різних посадах стикаються з різними кіберзагрозами. Водночас, виділяють загальні поради щодо корпоративного навчання з кібербезпеки, які включають проведення практично спрямованих тренінгів; оцінювання результатів навчання; використання симуляційних фішингових технологій; проведення фішингових кампаній, розповсюдження постерів, розсилання листів електронною поштою тощо (рис. 3.1) [37].

Рис. 3.1. Перелік базових порад щодо навчання

Опитування впродовж останніх трьох років показують, що двома основними змінними, які корелюють із зрілими програмами навчання й підвищення обізнаності, є підтримка керівництва та розмір команди з питань безпеки. Чим сильнішою є підтримка керівництва та чим більше штатних працівників, що підтримують програму навчання й підвищення обізнаності, тим

більш зрілою буде програма. Цьогорічне опитування SANS показало, що організації, які ефективно змінюють поведінку внаслідок навчання персоналу у сфері кібербезпеки, мали команду щонайменше з трьох штатних співробітників. Організації, які виходили за межі зміни поведінки й ефективно створювали сильну культуру інформаційної безпеки і мали систему стратегічних показників для вимірювання цих змін, мали в середньому команду з принаймні шести штатних працівників [38].

Хенш і Бененсон спробували визначити обізнаність про інформаційну безпеку як концепцію та дійшли висновку, що вона має три виміри: сприйняття, захист і поведінку.

Обізнаність про інформаційну безпеку як сприйняття передбачає знання користувачів про існування загроз, небезпек і ризиків. Кінцеві користувачі індивідуально реагують на різні загрози безпеки, і реакція залежить від того, як вони сприймають цю конкретну загрозу. Поінформованість про безпеку як сприйняття також пов’язана зі ступенем думки кінцевого користувача про безпечні й небезпечні явища.

Обізнаність про безпеку як захист включає знання користувачів не тільки про існування загроз, небезпек і ризиків безпеки, але й про наявні заходи, щоб захистити себе. Це значення поінформованості про безпеку стосується уваги користувачів до безпеки й того, наскільки добре вони розпізнають проблеми IT-безпеки, а також те, як вони мають реагувати на загрози.

Обізнаність про безпеку як поведінка є відображенням того, що головною причиною інформування з питань безпеки є прагнення до ефективного зменшення загроз. Це досягається, коли користувачі знають, які заходи безпеки вони можуть використати, щоб захистити себе та як розгортати й підтримувати програмні додатки із захисту інформації. Обізнаність про безпеку як поведінка зосереджується на тому, як користувачі діють і думають про інформаційну безпеку, як можна передати знання про різні чинники безпеки, як можна впливати на дії й поведінку користувачів [39].

Навчання з питань безпеки має на меті надати персоналу організації знання, необхідні для захисту від загроз інформаційній безпеці. Не варто очікувати, що співробітники самостійно знайдуть інформацію про те, які загрози існують або як діяти у випадку їх виникнення. Для цього необхідно проводити навчання на рівні організації, окремих відділів і категорій посад з використання різних форм навчання.

Актуальною вимогою до сучасних організацій, які хочуть досягти високого рівня обізнаності й володіння персоналом навичками у сфері інформаційної безпеки, є використання програмних продуктів SA&T (Security Awareness and Training).

На даний момент, на ринку є великий вибір додатків даного профілю, які автоматизують процес навчання й формування обізнаності персоналу з інформаційної безпеки. Відповідно до дослідження компанії Gartner кращими продуктами за чотирма категоріями є:

– OutThink, Terranova Security (рішення з високою продуктивністю);
– InfoSec, KnowBe4, NINJIO (вибір споживачів);
– Proofpoint (визнаний продукт);
– Mimecast, Security Mentor (перспективне рішення (рис. 3.2) [40].

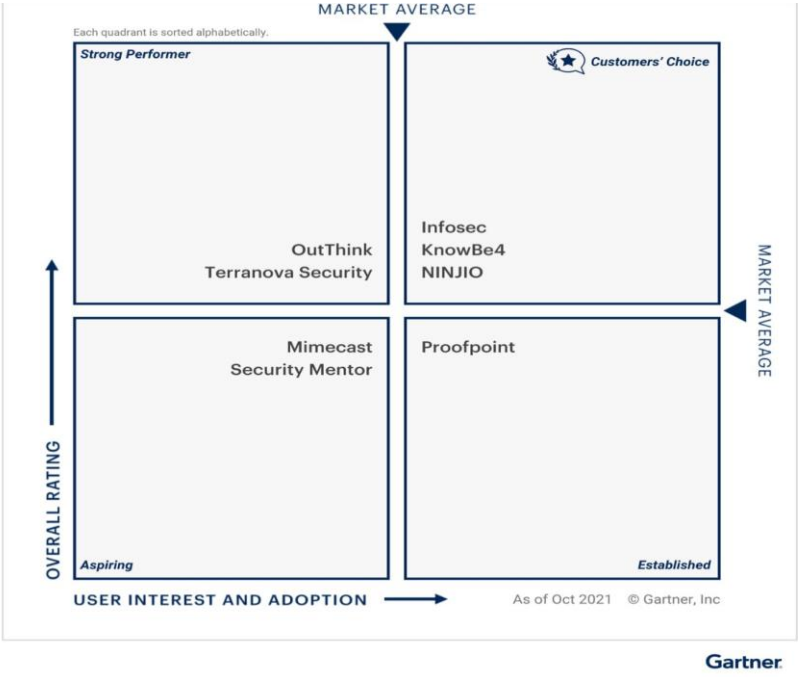

Рис. 3.2. Рішення SA&T з високою оцінкою від Gartner

Даючи загальну характеристику навчальним платформам з питань безпеки варто відзначити такі їх можливості:

– надання кінцевим користувачам онлайн-порталів для доступу до навчальних матеріалів з кібербезпеки;

– створення навчальних тренінгів з інтерактивними вікторинами й тестами, щоб переконатися, що користувачі навчаються й використовують матеріали;

– імітація фішингових кампаній, які перевіряють, наскільки добре користувачі здатні виявляти фішингові атаки;

– плагіни Outlook, які дозволяють користувачам повідомляти IT-командам про ймовірні фішингові атаки безпосередньо зі своєї електронної скриньки [41].

3.2 Порівняльний аналіз технологій SA&T

Для порівняння візьмемо два рішення від визнаних виробників: KnowBe4 та Proofpoint. Порівнюючи ці два рішення можна встановити, що KnowBe4 та Proofpoint мають подібні характеристики, але трохи різні підходи до навчання.

KnowBe4. Заглибившись у функціонал, можемо зробити висновки, що KnowBe4 має більше можливостей для навчання й надання різноманітних матеріалів. Платформа пропонує не лише проходження тренінгів на платформі, а також можливість скачувати постери, брошури для поширення за допомогою будь-яких каналів.

KnowBe4 використовує багатосторонній підхід до навчання, який починається з розуміння конкретної ситуації щодо ризиків організації, а надалі дозволяє використовувати рішення для реальних спроб фішингу [42].

На рисунку 3.3 проілюстровано підхід до навчання KnowBe4, відповідно до якого спеціалісти з інформаційної безпеки спочатку проводять тренінги з використанням відеоматеріалів та постерів, після цього налаштовують кампанії по фішингу, що вибірково надсилають листи різним групам працівників та перевіряють засвоєння навчальних матеріалів. Після цього фахівці компанії отримують результати з фішингової кампанії та аналізують їх. Якщо велика кількість учасників навчання (понад 80%) переходять за посиланням, то їм необхідно повторно пройти навчання [43].

Рис. 3.3. Підхід то навчання KnowBe4

Основні функції рішення SA&T від KnowBe4 охоплюють:

Базове тестування - для оцінки вразливих до фішингу користувачів (Phish-prone) у відсотках за допомогою симуляції фішингової атаки.

Навчання користувачів - передбачає можливості використання найбільшої у світі бібліотеки навчального контенту з питань безпеки, включаючи інтерактивні модулі, відео, ігри, плакати та інформаційні бюлетені. Рішення дозволяє проводити автоматизовані навчальні кампанії із запланованими електронними листами з нагадуваннями.

Фішинг - розгортання автоматизованих імітованих фішингових атак з багатьма шаблонами з необмеженим використанням.

Перегляд результатів - передбачає можливості ознайомлення з корпоративними звітами, які відображають статистику та графіки як для навчання з питань безпеки, так і для фішингу, а також звіти для керівництва щодо успіхів або зон, які потрібно вдосконалити.

На рис. 3.4. показані додаткові переваги рішення KnowBe4, які полегшують налаштування навчання й аналітики після проведення навчальних кампаній, зокрема: інтегрована платформа; надання випадкових атак (понад 23 тис. варіантів); безлімітне використання за трьома рівнями доступу (відповідно до підписки); технічна підтримка найвищого рівня з мінімальним терміном реагування; звітування про стан обізнаності з безпеки персоналу; інноваційна функція ідентифікації ризиків безпеки, пов'язаних з обізнаністю працівників.

Рис. 3.4. Додаткові функції, що пропонує KnowBe4

KnowBe4, який є лідером на ринку навчання з питань безпеки, пропонує низку безкоштовних і платних інструментів для навчання та імітованих фішингових кампаній; величезну бібліотеку навчального контенту з безпеки, включаючи презентації, відео, вікторини тощо; комплексну платформу моделювання фішингових атак, яка дозволяє організації створювати власні шаблони та кампанії.

KnowBe4 також пропонує звіти і статистичні дані для відстеження ефективності навчальних кампаній з підвищення рівня безпеки, зокрема звітування передбачає можливість генерувати навчальні звіти для конкретних користувачів або певних груп. Такий індивідуальний підхід дозволяє організації забезпечити участь у процесі навчання та моделювання фішингових атак

користувачів із найбільш ризикованою поведінкою. Комплексна платформа KnowBe4 є оптимальним вибором для більшості організацій, які планують використовувати навчальну платформу для навчання з інформаційної безпеки.

Proofpoint. Програмна платформа SA&T від Proofpoint пропонує постійно оновлювану бібліотеку навчального контенту, включно з модулями, відео, зображеннями плакатами і статтями, призначеними для покращення обізнаності й допомоги користувачам у виявленні фішингових атак, спроб зламу облікового запису тощо.

Proofpoint використовує комплексний підхід до навчання з питань безпеки. Структура ACE (Assess, Change Behavior, Evaluate), яка передбачає аналіз поточного стану рішення безпеки, зміну поведінки та оцінку результатів (Рис. 3.5). Завдяки такому підходу забезпечується постійне вдосконалення програми інформування навчання відповідно до потреб інформаційної безпеки.

Рис. 3.5. Підхід то навчання Proofpoint

Окрім навчальних матеріалів, Proofpoint пропонує симуляцію загроз, щоб перевірити, наскільки ефективно користувачі виявляють зловмисні електронні листи, і допомогти організації спрямувати навчання на працівників, які мають прогалини у знаннях та навиках з інформаційної безпеки.

Proofpoint надає понад 700 фішингових шаблонів для тестування різних типів зловмисних електронних листів, у тому числі зі зловмисними вкладеннями, вбудованими посиланнями та запитами на особисті дані. Навчання Proofpoint Security Awareness Training тепер доступне як частина Proofpoint Essentials, пакета безпеки електронної пошти, який включає

провідний тренінг Proofpoint щодо електронної пошти, шифрування та безпеки, що робить його ефективним рішенням для організацій, які потребують навчання інформованості разом із захистом електронної пошти.

Узагальнені результати порівняльного аналізу представлені в таблиці 3.1.

Таблиця 3.1

Порівняльна характеристика рішень SA&T від KnowBe4 та Proofpoint

Критерії порівняння	**KnowBe4**	**Proofpoint**
Методи навчання користувачів	Мультимедійне навчання	Мультимедійне навчання
Оцінка знань	Так	Так
Тип продукту	SaaS	SaaS
Персоналізована адаптація курсів	Так	Так
Фішингові кампанії	Так	Так
Виявлення користувачів, які найчастіше є об’єктами атак і які є вразливими до фішингу	Ні	Так
Автоматичне зарахування на курс	Так	Так
Інформаційна панель CISO	Так	Ні
Кнопка для повідомлення про фішинговий лист	Так	Ні
Брошури, документація, постери	Так	Так
Автоматична програма навчання	Так	Ні
Smart (розумні) групи	Так	Ні
Соціальна інженерія (QR-code, USB)	Так	Так
Забезпечення відповідності	Так	Так
Active Directory інтеграція	Так	Ні

Отже, відповідно до таблиці вище, обидва запропоновані рішення використовують один метод навчання користувачів – мультимедійне навчання, пропонують проводити фішингові кампанії й оцінювання знань користувачів.

Водночас, рішення мають незначну різницю у функціоналі. Так, KnowBe4 надає можливість налаштовувати «розумні» групи для полегшення роботи відділу безпеки, що дозволяє здійснювати автоматичне додавання і видалення

користувачів за встановленими критеріями (період роботи, посада тощо). Це дуже зручно для швидкого налаштування тренінгів у великих компаніях, які мають багато підрозділів з відмінними вимогами щодо знань з інформаційної безпеки ІБ відповідно до робочих обов'язків.

Також KnowBe4 пропонує впровадити свою кнопку для попередження служби безпеки одразу в пошті, де отриманий фішинговий лист. У той час як у Proofpoint немає даної функції. Отже, аналіз двох продуктів показав відсутність значної різниці у їхньому функціоналі і орієнтація обох рішень на забезпечення швидкого та зручного використання продукту, а також зменшення кількості працівників з інформаційної безпеки для організації та супроводу навчання.

3.3 Системи запобігання витоку даних

DLP система – це інформаційно-технічний комплекс, призначений для виявлення, моніторингу та запобігання небажаним витокам чутливої інформації з корпоративних систем та мереж. Основна мета DLP - забезпечити захист конфіденційної інформації від неправомірного використання чи розголошення. Це стратегічний підхід до захисту конфіденційної інформації в організації.

Системи DLP допомагають виявляти, відстежувати й контролювати передачу чутливої інформації, такої як фінансова інформація, персональні дані або інші конфіденційні документи, які можуть втратитися або потрапити в невірні руки. Системи DLP можуть використовувати різні методи, включаючи виявлення заборонених слів, аналіз контексту, криптографічне шифрування і багато інших [44].

Для компаній DLP системи також стали допоміжним засобом для дотримання законодавства, оскільки уряди в усьому світі ухвалили закони про захист конфіденційності та даних споживачів. Зокрема, Європейський Союз прийняв Загальний регламент захисту даних (GDPR) у 2018 році, щоб

встановити найвищі у світі стандарти щодо того, як організації мають захищати персональні дані своїх громадян, із значними фінансовими штрафами в разі їх недотримання. Регламент також надає своїм громадянам набір прав на доступ, зміну, обмеження та переміщення їхніх особистих даних між будь-якими організаціями, які обробляють їхні дані [45].

В умовах постійних змін у середовищі Інтернет-технологій і посилення державного регулювання, рішення DLP розширили обсяг «даних» і прогресували в перевірці вмісту, зосереджуючись на моніторингу, орієнтованому на користувача, як на кінцевій точці, так і в мережі.

Перевірка вмісту та виявлення даних перейшли від простих ключових слів до розширеного зіставлення шаблонів для більшої широти й точності, а метадані, як-от дані про власника файлу та місцезнаходження, враховувалися для визначення контексту. На додаток до паралельних зусиль із навчання співробітників, користувач і надалі залишався головною увагою DLP із такими функціями як сповіщення про порушення політики (спливаюче вікно у разі спроби завантажити неавторизований сайт) і постійний моніторинг мережевого трафіку і файлів передачі з кінцевої точки.

Оскільки, відповідність нормативним вимогам стало додатковою вимогою для DLP, звітування й аудит даних, насамперед персональних даних (PII), стали стандартними функціями.

DLP системи виявляють і контролюють рух даних, забезпечуючи виконання політик безпеки, які можуть включати обмеження на передачу конфіденційної інформації через електронну пошту, веб-сайти, під час обміну файлами та інші канали зв'язку. DLP системи також можуть використовувати методи шифрування, моніторингу діяльності користувачів, аналізу контексту й інші техніки для виявлення та управління ризиками втрати даних [46].

Використання DLP систем стає важливим в корпоративному середовищі, адже дотримання стандартів безпеки та захисту конфіденційної інформації є критичним завданням для усіх організацій та їх бренду.

Система створює захищений «цифровий периметр» навколо організації, аналізуючи всю вхідну, вихідну і внутрішню інформацію. Як було згадано вище, виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифу документа, спеціально введених міток, значень хеш-функції.

DLP системи забезпечують виконання таких основних завдань:

1. Виявлення та ідентифікація чутливої інформації: DLP системи визначають і класифікують конфіденційну інформацію, таку як особисті дані, фінансова інформація чи інші види конфіденційних даних.

2. Моніторинг руху даних: Системи DLP відстежують потоки даних в мережі та на комп'ютерах, щоб виявити ненормативні дії користувачів, які можуть призвести до витоку чутливої інформації.

3. Запобігання втраті даних: DLP системи призначені для управління ризиками та запобігання неправомірному чи ненавмисному витоку даних. Вони блокують або контролюють передачу інформації через різні канали зв'язку.

4. Шифрування інформації: DLP системи можуть використовувати шифрування для захисту конфіденційної інформації, що дозволяє лише авторизованим користувачам отримувати доступ до неї.

5. Моніторинг активності користувачів: DLP системи слідкують за діяльністю користувачів, виявляючи можливі порушення політик безпеки та надаючи інформацію для аудиту й аналізу.

6. Забезпечення відповідності законодавству і стандартам безпеки: DLP системи допомагають організаціям дотримуватися вимог законодавства, нормативів і стандартів безпеки, зменшуючи ризик витоку конфіденційних даних.

Сучасні DLP системи мають величезну кількість параметрів і характеристик, які необхідно враховувати при виборі рішення для організації захисту конфіденційної інформації від витоків [47]. Проте найважливішим з них є мережева архітектура, відповідно до якої DLP продукти поділяються на дві великі групи: шлюзові та хостові.

Шлюзові (Gateway) DLP системи зосереджені на мережевому рівні. Дані системи розміщені на точках входу та виходу мережі, таких як брандмауери, мережеві шлюзи або проксі-сервери.

Контроль відбувається на рівні транспортного рівня (модель OSI). Вони взаємодіють з трафіком на рівні мережі, аналізуючи та блокуючи передачу конфіденційної інформації.

Шлюзові системи здійснюють виявлення, фільтрацію і блокування спроб передачі конфіденційних даних через мережу, враховуючи правила й політики безпеки.

Хостові (Endpoint) DLP системи зосереджені на рівні кінцевого пристрою. Такі системи встановлюються на кінцевих пристроях, а саме: комп'ютерах, ноутбуках або мобільних пристроях.

Хостові системи здійснюють контроль на рівні додатків та операційної системи. Вони взаємодіють з додатками та операційною системою на кінцевому пристрої, щоб виявляти та контролювати витік конфіденційної інформації. Ще один варіант - це локальний моніторинг і контроль, який дозволяє контролювати й відстежувати дії користувачів на пристрої, а не тільки на рівні мережі.

Щоб зрозуміти, як саме працюють DLP системи розглянемо робочий процес (Рис. 3.6).

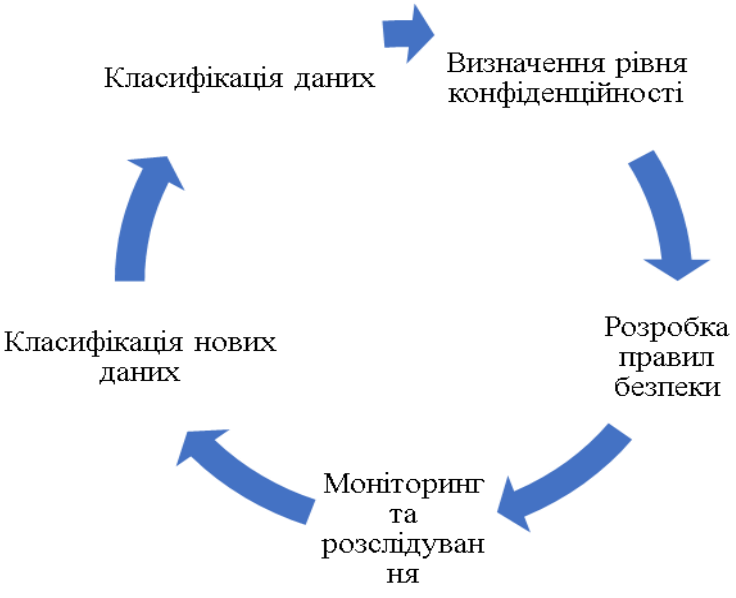

Рис. 3.6. Робочий процес DLP-систем

Перший етап – класифікація даних. Експерти з кібербезпеки використовують рішення DLP для сортування та маркування кожного елементу даних в інфраструктурі організації з певним рівнем класифікації, таким як публічний, чутливий або внутрішній. Класифікація даних є тривалим і складним процесом, який вимагає розробки відповідних політик, може виконуватися вручну або автоматизовано залежно від рішення DLP, що використовується.

Другим етапом є визначення рівня конфіденційності даних. На основі розробленої в організації класифікації керівники підрозділів інформаційної безпеки визначають конкретні фрази, що є показниками певного рівня конфіденційності для різних типів даних: приватний, конфіденційний, засекречений, фінансова інформація тощо. Залежно від компанії та її бізнес-цілей може існувати сотні або навіть тисячі маркерів конфіденційності.

На третьому етапі розробляють правила безпеки. Після обробки всіх даних організації, відділ інформаційної безпеки формує поведінку системи DLP, створюючи правила. Ці правила визначають, як система DLP реагує під час спрацювання певних маркерів конфіденційності: надсилає сповіщення-попередження, зупиняє передачу конфіденційних даних або скасовує права доступу користувача.

Четвертий етап охоплює моніторинг і розслідування інцидентів. Після встановлення правил безпеки DLP система починає відстежувати дані. Коли спрацьовує сповіщення, система реагує на подію згідно з налаштуваннями і повідомляє відповідальних за цей процес. Відділ з інформаційної безпеки аналізує подію, щоб визначити, чи це інцидент, чи помилковий сигнал.

Останнім етапом є класифікація нових даних. Якщо нові дані потрапляють в інфраструктуру організації, процес DLP починається спочатку, повертаючись на етап класифікації. Деякі рішення DLP можуть надавати певний рівень автоматизації, але воно може залишати прогалини в безпеці та впливати на робочий процес організації. Тому експерти надають рекомендації щодо детальної перевірки й налаштування DLP під потреби конкретної організації [48].

На сьогоднішній день ринок DLP поділений на DLP як функцію та DLP як рішення. Деякі продукти, зокрема рішення безпеки електронної пошти, надають базові функції DLP, але не є повними DLP. Різниця полягає в наступному:

– DLP-продукт включає централізоване управління, створення політик і робочий процес із забезпеченням їх виконання, призначений для моніторингу та захисту вмісту і даних. Інтерфейс користувача і функціональні можливості призначені для вирішення ділових і технічних проблем із захистом вмісту за допомогою його розуміння.

– Функції DLP включають деякі можливості виявлення і примусового застосування продуктів DLP, але не призначені для завдання захисту вмісту і даних.

Захист конфіденційних даних, зокрема персональних даних, комерційної таємниці, фінансових даних та інтелектуальної власності, сьогодні є головним пріоритетом для кожної організації [49]. Унаслідок використання нових технологій організації можуть постраждати від нових методів розкриття конфіденційних даних:

– Внаслідок впровадження гібридних форм роботи корпоративні дані переміщаються за межі традиційних кордонів, у хмарних службах і скрізь, де користувач бажає підключитися, локально та за межами організації (Рис. 3.7).

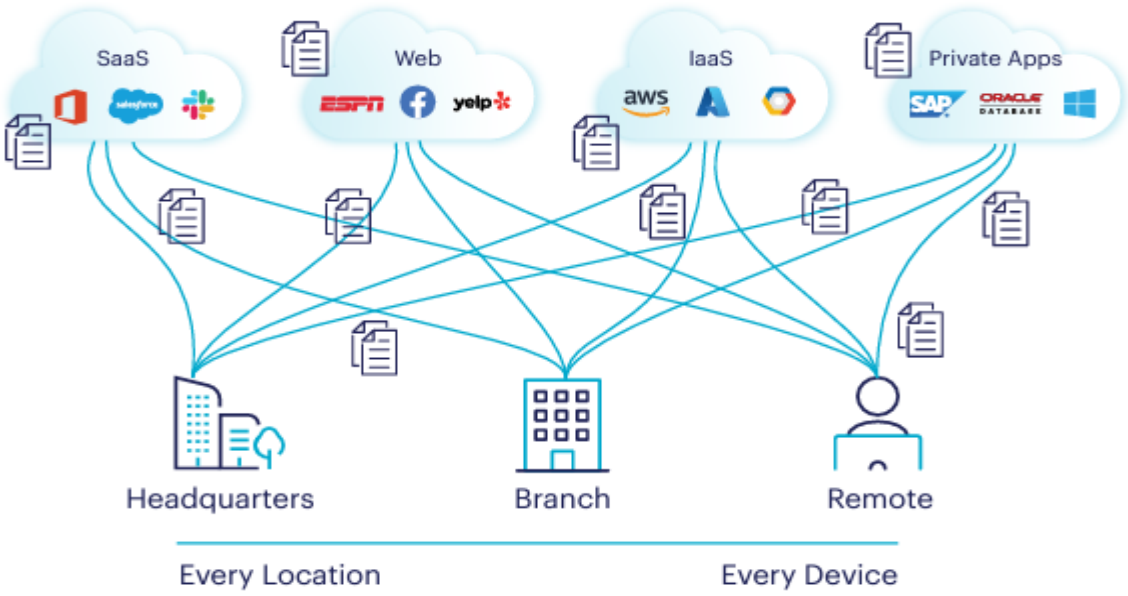

Рис. 3.7. Потік даних з різних організацій до різних систем

– Дані зберігаються та обмінюються все більшою кількістю SaaS-додатків, до яких може отримати прямий доступ будь-який користувач і будь-який пристрій.

– Обсяг, різноманітність і швидкість даних стрімко зростають. У результаті конфіденційні дані все важче ідентифікувати, а отже, й захистити [50].

На даний момент, на ринку представлено дуже багато рішень DLP з різним функціоналом. За оцінкою SoftwareReviews, кращими продуктами за трьома з чотирьох категорій є:

– Trellix DLP, Avanan, Veeam Availability Suite, Safetica, Proofpoint Enterprise DLP, CommVault Backup&Recovery (лідери ринку);

– Forcepoint DLP, Endpoint Protector, Trend Micro Apex One, Check Point Quantum DLP (претенденти на лідерство);

– Fortra Digital, Guardian, Symantec Enterprise Cloud, Better Cloud (інноваційні рішення) (рис. 3.8) [51].

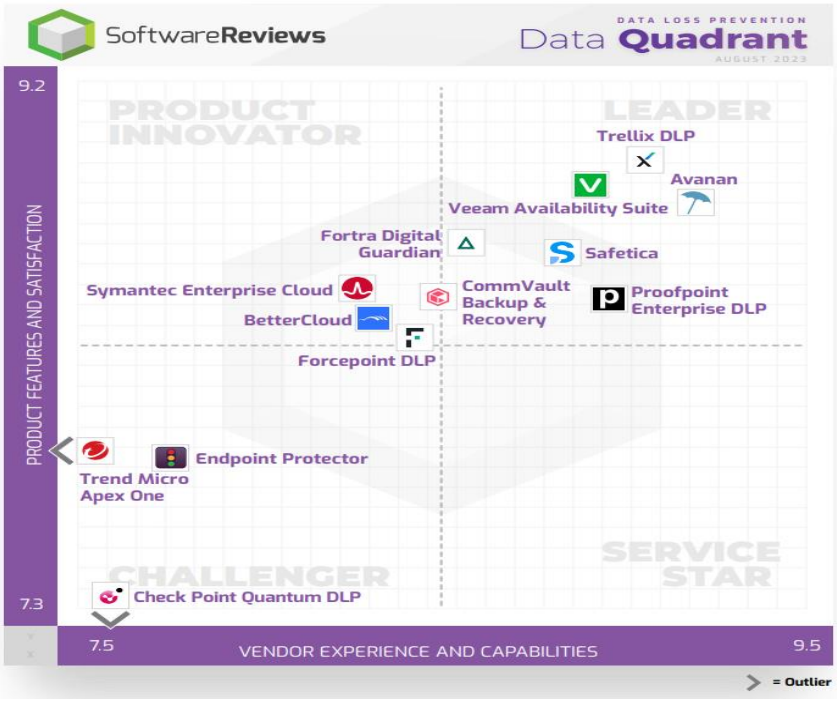

Рис. 3.8. Рішення DLP з високою оцінкою від SoftwareReviews

3.4 Порівняльна характеристика DLP систем

Управління ризиком втрати даних залишається серйозною проблемою для сучасних підприємств і організацій. Компанії обирають DLP системи з різних причин, зокрема для дотримання положень щодо конфіденційності, а також через занепокоєння з приводу можливого витоку особистих даних або інші проблеми інтелектуальної власності, такі як захист вихідного коду, комерційної таємниці або патентної інформації. Це призвело до складного набору архітектурних та операційних проблем, які мають вирішити архітектори інформаційної безпеки, адже кожна організація використовує різні операційні системи, додатки, підхід до побудови інфраструктури тощо. Та через бажання не втрачати репутацію, дані клієнтів, інтелектуальну власність важливість можливостей DLP для організації зросла, а кількість постачальників DLP збільшилася.

Деякий час інтегровані DLP-рішення, були значно слабшими, ніж корпоративні, але сьогодні можливості перших є багатообіцяючими. Інтегрована DLP-система — це рішення або постачальник послуг, у яких DLP є підмножиною інших функцій, пов’язаних з безпекою. Наприклад, брандмауер для електронної пошти може мати функції DLP. Таким чином, він зможе забезпечити автоматизацію класифікації даних з урахуванням вмісту та перевірки вмісту в режимі реального часу, а також запобігти втраті персональних даних, інтелектуальної власності та інших конфіденційних даних, що передаються електронною поштою. З іншого боку, це не допомогло б при витоку даних через портативні носії або переміщення даних через месенджери.

Недоліки інтегрованого DLP не обмежуються середовищем, яким проходять дані. Наприклад, CASB (Cloud Access Security Broker) з інтегрованим DLP може запобігти витоку даних через неправильне налаштування хмарної служби SaaS. Однак, рішення не допоможе при навмисній активності

користувача, внутрішній загрозі, або втраті конфіденційної інформації через фішингові листи [52].

Правильний підбір архітектури DLP для певної ситуації значною мірою залежатиме від мети організації в сфері ІБ.

Як відзначалося вище, сьогодні на ринку представлено дуже багато рішень DLP з різним функціоналом. Візьмемо для порівняння два DLP рішення: Trellix DLP та Forcepoint DLP, які, за оцінкою SoftwareReviews, вони мають різний рейтинг. Це і стало причиною такого вибору. Крім того, Gartner показує, що Forcepoint та Trellix мають однаковий загальний рейтинг – 4,4. Проте кількість оцінок, залишених користувачами, значно відрізняється. Рішення Forcepoint отримало 468 відгуків, а у Trellix – 252 [53, 54]. Можемо зробити висновок, що при різній кількості наданих відгуків, важко однозначно вибрати лідера без детального огляду функцій даних рішень (Рис. 3.9).

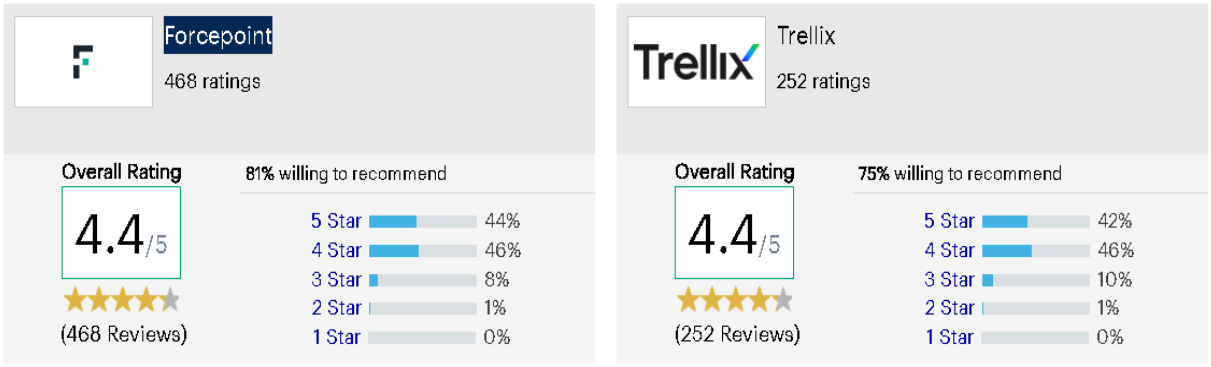

Рис. 3.9. Рейтинг від користувачів продуктів Trellix і Forcepoint

Отже, Forcepoint DLP зосереджено на уніфікованих політиках і ризиках користувачів за рахунок автоматизації, щоб гарантувати безперебійну та інтуїтивно зрозумілу безпеку бізнес-даних. Forcepoint пропонує інструменти для управління глобальними політиками в усіх основних каналах, включаючи кінцеву точку, мережу, хмару, Інтернет або електронну пошту.

Forcepoint DLP - це перевірене рішення, яке підходить для організацій будь-якого розміру, незалежно від того, чи потрібна їм базова відповідність, чи більш складна пропозиція. Це рішення рекомендується для запобігання втраті

даних організаціям, які шукають проактивний захист своїх критичних даних та об’єктів інтелектуальної власності.

Система Trellix DLP складається з DLP Discover, DLP Endpoint, DLP Monitor і DLP Prevent, є хорошим вибором як для локальних, так і для гібридних середовищ, особливо в поєднанні з можливостями SASE Skyhigh.

Secure Access Service Edge (SASE) – це стратегія безпеки мережі, яка об'єднує безпеку й мережеві функції в єдиному рішенні. Ця концепція призначена для захисту користувачів і даних у хмарному середовищі, спрощуючи інфраструктуру та забезпечуючи безпеку доступу до різних ресурсів. SASE в першу чергу надається як послуга й забезпечує нульовий довірчий доступ на основі ідентичності пристрою чи об’єкта в поєднанні з контекстом у реальному часі та політиками безпеки і відповідності вимогам [55].

DLP Discover виявляє та захищає конфіденційні дані у місцях зберігання. DLP Discover має такі функції: інвентаризація всіх даних; перевірка вмісту файлів і таблиць баз даних з метою виявлення конфіденційних даних; надання дозволів щодо переміщення і шифрування даних для унеможливлення зберігання конфіденційного контенту в несанкціонованих місцях; створення правил захисту за допомогою відбитків, що генеруються, з використанням технології сканування файлів [56].

DLP Endpoint – розповсюджує захист даних на кінцеві точки і виконує такі функції: запобігання несанкціонованому підключенню зовнішніх пристроїв до корпоративної мережі; відстеження та захист конфіденційних даних (даних платіжних карток, персональних даних, медичної інформації тощо) на кількох можливих векторах атак на кінцеву точку; виявлення конфіденційних файлів; надання повідомлень користувачам у відповідь на їхні дії та, за потреби, запиту на бізнес-обґрунтування [56, 57].

DLP Monitor – забезпечує моніторинг даних у режимі реального часу при передачі через мережу, електронну пошту та Інтернет і виконує такі функції: інтеграція з пристроями на виході за допомогою технологій SPAN або TAP; аналіз мережевих пакетів з метою визначення типу та змісту даних; збір

інформації для проведення комп'ютерно-технічної експертизи і створення політик; підтримка протоколів SMTP, IMAP, POP3, HTTP, LDAP, Telnet, FTP, IRC, SMB тощо [58].

DLP Prevent – забезпечує активне застосування мережевих політик, а також: інтеграцію з будь-яким доступним на ринку сервісом електронної пошти або інтернет-шлюзом за допомогою протоколів SMTP або ICAP; належне реагування після перевірки всіх електронних листів через протокол ICAP; запобігання переміщенню конфіденційних даних; збір інформації для проведення комп'ютерно-технічної експертизи і створення політик [59].

У нашому огляді ми зосередимося на розширенні DLP Discover через його основну роль у виявленні й захисті конфіденційних даних. Цей продукт інвентаризує дані, шукає конфіденційну інформацію та допомагає розробити правила її захисту. Але весь пакет Trellix є хорошим вибором для команд, які зосереджені на моніторингу та запобіганні загрозам в повному обсязі з усіх точок обробки, зберігання та передачі інформації [60].

Єдиним недоліком є те, що для отримання всіх можливостей DLP розширень, які пропонує Trellix, потрібні чотири продукти DLP, що часто не є економічно вигідним для невеликих компаній. Однак, для підприємств, яким потрібна багатофункціональна платформа DLP, Trellix є сильним рішенням [61].

Узагальнені результати порівняльного аналізу представлені в таблиці 3.2.

Таблиця 3.2

Порівняльна характеристика рішень DLP від Trellix і Forcepoint

Критерій	**Trellix**	**Forcepoint**
Тип продукту	Локально На основі хмари	На основі хмари
Попередньо налаштовані правила	Так	Так
Клієнтський компонент	Так	Так
Обмін файлами PST (пошта), даними у стані спокою через мережу	Так	Так

Продовження табл.3.2

Сумісність з різними ОС	Windows, MacOS	Windows, MacOS
Примусове застосування DLP на кінцевій точці	Ні	Так
Оптичне розпізнавання символів (OCR)	Ні	Так
Виявлення даних у всіх середовищах	Так	Так
Контроль відповідності	Так	Так
Фільтр DLP виявлення	Так	Так
Класифікація даних	Ні	Так
Машинне навчання	Так	Так
Моніторинг мережі	Так	Так
Трекінг інтелектуальної власності	Ні	Так
Звіти для відповідності нормативним документам	Так	Ні
Блокування (Blacklisting)	Так	Ні
Захист від загроз	Так	Ні

У результаті порівняння обох рішень, встановлено, що вони мають багато спільних характеристик. При виборі оптимального рішення кожне підприємство має орієнтуватися на свій бюджет, бізнес-цілі та можливості інфраструктури. Відповідно, й вартість рішень буде відрізнятися.

Так, Trellix для використання всіх функцій DLP вимагає придбання чотирьох рішень, тобто, ціна буде на порядок вища. Отже, для малого бізнесу даний продукт не є рентабельним. Натомість, Forcepoint має більш приємні ціни та його функціоналу буде повністю достатньо для невеликих компаній. Крім того, сам виробник Trellix більш направляє розробку свого продукту на великий бізнес.

Аналіз коментарів фахівців, які працюють з цими системами, на онлайн-ресурсах показав, вони надають більшу перевагу Trellix через якісну технічну

підтримку, виписану документацію та високі характеристики, перевірені на практиці у фінансовому секторі.

Forcepoint має велику перевагу в тому, що попередньо визначає політики відповідно до класифікації (фінанси, IT, документація тощо), а також є гнучким у класифікації політик для різних хмарних рішень, таких як Google Drive, OneDrive, а також має функцію карантину (Block), яка допомагає відстежувати інцидент і реагувати на нього. Ще одна функція, яку позитивно оцінює більшість практиків, - це автоматичне надсилання користувачеві та його менеджеру звітів у випадку виявлення інциденту DLP, що допоможе зменшити ручне втручання у створення звітів та інформування відповідних команд. Як свідчить аналіз відгуків, цей продукт частіше використовують промислово-виробничі компанії.

Таким чином, кожна організація, обираючи найбільш прийнятне для неї рішення, має з’ясувати призначення DLP системи, обсяги її застосування, перелік інформаційних систем, які будуть підлягати моніторингу щодо витоку даних, а також врахувати свої фінансові можливості і спроможність забезпечити підтримку й обслуговування DLP систем.

Висновки до розділу 3

Встановлено, що організація може забезпечити ефективний захист від деструктивної інсайдерської діяльності, тільки поєднуючи застосування технічних рішень з управлінськими заходами. Ключове значення для запобігання внутрішнім загрозам відіграють заходи з інформування й навчання персоналу, які на сучасному етапі мають відповідати таким вимогам: використання різних форм і методів інформування й навчання; забезпечення практичної спрямованості навчання; використання симуляційних технологій; оцінювання результативності навчальних заходів. Доцільним є застосування

програмних платформ для формування обізнаності й навчання у сфері інформаційної безпеки (SA&T).

Порівняльний аналіз технологій SA&T від визнаних виробників KnowBe4 та Proofpoint показав, що дані рішення мають схожі підходи до навчання. Водночас, KnowBe4 дає більше можливостей і векторів проведення навчання, не обмежуючись переглядом мультимедійного матеріалу і фішинговими кампаніями, але й, зокрема, забезпечуючи налаштування «розумних» груп і спрощене повідомлення адміністратора про можливий фішинговий лист за допомогою кнопки, вбудованої в поштові сервіси.

Одним із перевірених засобів протидії витокам конфіденційної інформації з вини персоналу організації є системи DLP, які призначені виявляти, відстежувати й контролювати передачу критичних даних з використанням різних методів, включаючи аналіз вмісту і контексту, моніторинг активності користувачів, криптографічне шифрування тощо. Завдяки використанню DLP систем організація може забезпечувати відповідність законодавчим і нормативним вимогам безпеки, зменшуючи ризик витоку персональних даних, інтелектуальної власності, комерційної та інших видів таємниць.

У результаті порівняльної характеристики DLP систем від Trellix і Forcepoint встановлено, що Trellix пропонує свої рішення з розширеним функціоналом переважно для великого бізнесу та фінансових установ. Відповідно, це рішення у повній комплектації включає чотири окремі розширення і має значно вищу вартість. Натомість, для невеликих компаній функціоналу Forcepoint буде цілком достатньо, а ціна рішення буде прийнятною.

Підсумовуючи, варто зазначити, що кожна організація, обираючи найбільш прийнятне рішення для зменшення ризиків внутрішніх загроз, має з’ясувати призначення і функціональність продукту, обсяги застосування та кількість об’єктів охоплення, а також врахувати свої фінансові можливості і спроможність забезпечити підтримку й обслуговування таких систем.

ВИСНОВКИ

У результаті дослідження встановлено, що внутрішня загроза – це загроза безпеці, яка походить від діючого або колишнього працівника або ділового партнера, який має доступ до конфіденційної інформації або привілейованих облікових записів у мережі організації та зловживає цим доступом.

Внутрішні загрози поділяють на навмисні та ненавмисні, а основними причинами внутрішніх загроз безпеці організації є: непрофесійні дії персоналу; низький стан виховної і профілактичної роботи; недосконала системи заробітної плати і стимулювання праці; порушення правил кадрової роботи; психологічні й комунікативні особливості працівників.

Аналіз показав що найбільш результативними технологіями запобігання і протидії внутрішнім загрозам безпеці організації є засоби IPS/IDS, управління доступом, SIEM, UEBA. Системи IDS/IPS допомагають підвищити рівень безпеки мережі та системи, гарантуючи виявлення, блокування та реагування потенційних загроз в реальному часі. Методи управління доступом мінімізують можливості отримання несанкціонованого доступу потенційного внутрішнього порушника до інформаційних ресурсів і систем. SIEM системи забезпечують виявлення потенційних загроз та автоматизують реагування на них у сучасних центрах безпеки. UEBA здійснюють моніторинг і виявлення недозволеного доступу до даних та їх переміщення, а також підозрілої чи шахрайської діяльності в мережі чи на кінцевих пристроях.

Дослідження показало, що організація може забезпечити ефективний захист від деструктивної інсайдерської діяльності, тільки поєднуючи застосування технічних рішень з управлінськими заходами. Ключове значення для запобігання внутрішнім загрозам відіграють заходи з інформування й навчання персоналу, які на сучасному етапі використовують різні форми і методи інформування й навчання, забезпечують практичну спрямованість навчання, використовують симуляційні технології, оцінювання результативності

навчальних заходів. Доцільним є застосування програмних платформ для формування обізнаності й навчання у сфері інформаційної безпеки (SA&T).

Порівняльний аналіз технологій SA&T від визнаних виробників KnowBe4 та Proofpoint показав, що дані рішення мають схожі підходи до навчання. Водночас, KnowBe4 дає більше можливостей і векторів проведення навчання, не обмежуючись переглядом мультимедійного матеріалу і фішинговими кампаніями, але й, зокрема, забезпечуючи налаштування «розумних» груп і спрощене повідомлення адміністратора про можливий фішинговий лист за допомогою кнопки, вбудованої в поштові сервіси.

З’ясовано, що одним із перевірених засобів протидії витокам конфіденційної інформації з вини персоналу організації є системи DLP, які призначені виявляти, відстежувати й контролювати передачу критичних даних з використанням різних методів, включаючи аналіз вмісту і контексту, моніторинг активності користувачів тощо.

У результаті порівняльної характеристики DLP систем від Trellix і Forcepoint встановлено, що Trellix пропонує свої рішення з розширеним функціоналом переважно для великого бізнесу та фінансових установ. Відповідно, це рішення у повній комплектації включає чотири окремі розширення і має значно вищу вартість. Натомість, для невеликих компаній функціоналу Forcepoint буде цілком достатньо, а ціна рішення буде прийнятною.

Підсумовуючи, варто зазначити, що кожна організація, обираючи найбільш прийнятне рішення для зменшення ризиків внутрішніх загроз, має з’ясувати призначення і функціональність продукту, обсяги застосування та кількість об’єктів охоплення, а також врахувати свої фінансові можливості і спроможність забезпечити підтримку й обслуговування таких систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. Ефективна економіка №5 2014. URL: http://www.economy.nayka.com.ua/?op=1&z=3304

2. Гребенюк А., Рибальченко Л. Основи управління інформаційною безпекою. Дніпро, 2020. 144 с

3. NIST 800-53. Security and Privacy Controls for Information Systems and Organizations. Effective from 2020-10-12. Official edition.

4. Чернега В., Кацалап В., Войтко О. Методика оцінки загроз інформаційній безпеці України у воєнній сфері. *Theoretical Foundations of Information Technologies Creation and Use*. 2018.

5. What are insider threats? URL: https://www.ibm.com/topics/insider-threats.

6. Yahoo Employee Stole 570,000 Pages of Source Code the Day He Quit to Join a Competitor. URL: https://www.cyberhaven.com/blog/yahoos-lawsuit-alleged-engineer-stole-sensitive-data

7. Angry Employee Deletes All of Company's Data. Fox News. URL: https://www.foxnews.com/story/angry-employee-deletes-all-of-companys-data.

8. Turkish based airline’s sensitive efb data leaked. URL: https://www.safetydetectives.com/news/pegasus-leak-report/.

9. The Toyota Data Breach: What Could Have Been Done to Prevent It. URL: https://www.advantio.com/blog/protecting-your-company-from-a-data-breach-lessons-from-toyotas-incident

10. What is social engineering? URL: https://www.malwarebytes.com/social-engineering.

11. Social engineering attacks: recognizing and preventing manipulative techniques. URL: https://medium.com/@the_neelguy/social-engineering-attacks-recognizing-and-preventing-manipulative-techniques-a779787d79cb

12. What is social engineering? URL: https://www.malwarebytes.com/social-engineering

13. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

14. Шевченко С. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Кібербезпека: освіта, наука, техніка. Т. 3, № 2022. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/347.

15. Types of Insiders You Need to Know. URL: https://cisomag.com/4-types-of-insiders-you-need-to-know/.

16. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

17. Insider threats: from malicious to unintentional. *SentinelOne*. URL: https://www.sentinelone.com/blog/insider-threats-from-malicious-to-unintentional/ .

18. Techniques and countermeasures for preventing insider threats. *PubMed Central (PMC)*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9044369/#ref-66

19. Information protection and control (IPC) in Office 365 with Azure Rights Management. *Cloud References*. URL: https://novacontext.com/information-protection-and-control-ipc-in-office-365-with-azure-rights-management/index.html

20. Що таке VPN, і як ним безпечно користуватись. URL: https://cip.gov.ua/ua/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis.

21. Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. Київ : НТУУ «КПІ». 2015. С. 195-198.

22. ЩО таке IPS/IDS і де застосовується. *HostZealot*. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya

23. NIDS. Network Intrusion Detection System. *Redscan*. URL: https://www.redscan.com/services/nids/.

24. ЩО таке керування доступом? Захисний комплекс Microsoft. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-access-control.

25. Mandatory (MAC) vs Discretionary Access Control (DAC) Differences | Ekran System. *Ekran System*. URL: https://www.ekransystem.com/en/blog/mac-vs-dac#id-when-to-use-mac.

26. Discretionary and Mandatory Access Control. URL: https://ganganichamika.medium.com/mandatory-access-control-vs-discretionary-access-control-ade64b2a0f1c

27. What is Role-Based Access Control (RBAC)? | Okta. *Employee and Customer Identity Solutions | Okta*. URL: https://www.okta.com/identity-101/what-is-role-based-access-control-rbac/.

28. What is identity and access management (IAM)? URL: https://cutt.ly/GwHuURrB

29. Introduction to IAM architecture (v2). *IDPro Body of Knowledge*. URL: https://bok.idpro.org/article/id/38/.

30. 2023 Gartner® Magic Quadrant™ for access management | Okta. *Employee and Customer Identity Solutions | Okta*. URL: https://www.okta.com/resources/gartner-magic-quadrant-access-management/.

31. Identity and Access Management або система управління обліковими даними. Рішення Microsoft Azure AD. *GlobalLogic Ukraine*. URL: https://www.globallogic.com/ua/insights/blogs/identity-and-access-management-azure-ad/.

32. PAM vs IAM: у чому різниця і чому це важливо. URL: https://wiseit.com.ua/pam-vs-iam.

33. What is Security Information and Event Management (SIEM)? *IBM*. URL: https://www.ibm.com/id-en/topics/siem.

34. Крижановський В., Сергієнко С. Апаратно-програмні засоби захисту інформації у корпораціях. Вінниця : Дон. ім. Василя Стуса, 2019. 36 с.

35. What is SIEM? And how does it work? *LogRhythm*. URL: https://logrhythm.com/blog/what-is-siem/

36. What is User and Entity Behavior Analytics (UEBA)? *OpenText*. URL: https://www.opentext.com/what-is/ueba

37. Security awareness training. URL: https://resources.infosecinstitute.com/globalassets/downloads/infosec-iq-outcomes-ebook-2023.

38. Security awareness training | SANS Security Awareness. *Cyber Security Training. SANS Courses, Certifications & Research*. URL: https://www.sans.org/security-awareness-training/.

39. Top 10 security awareness training topics for your employees in 2023 and beyond. *Infosec Resources - IT Security Training & Resources by Infosec*. URL: https://resources.infosecinstitute.com/topics/security-awareness/top-10-security-awareness-training-topics-for-your-employees/.

40. Security awareness training reviews, ratings & features 2023. Gartner Peer Insights. *Gartner*. URL: https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/global-learning-systems/product/security-awareness-training

41. Find out how effective our security awareness training is. URL: https://www.knowbe4.com/

42. Enterprise security awareness training. *Security Awareness Training | KnowBe4*. URL: https://www.knowbe4.com/en/products/enterprise-security-awareness-training/.

43. Security awareness training & simulated phishing platform. *KnowBe4*.

44. DLP системи - що це, як DLP система запобігає витоку інформації? *ESET*. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/dlp/

45. Data Loss Prevention (DLP). URL: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

46. Data Loss Prevention (DLP) Systems: what they are & key benefits. *Ekran System*. URL: https://www.ekransystem.com/en/blog/dlp-systems-pros-and-cons.

47. Kranz G., Patrizio A. What is Data Loss Prevention (DLP)? Everything you need to know. *WhatIs*. URL: https://www.techtarget.com/whatis/definition/data-loss-prevention-DLP.

48. Balaban D. Capabilities of modern DLP systems. *Forbes*. URL: https://www.forbes.com/sites/davidbalaban/2023/02/02/capabilities-of-modern-dlp-systems/?sh=869a5ef29b2e.

49. What is network Data Loss Prevention vs endpoint DLP? *Digital Guardian*. URL: https://www.digitalguardian.com/blog/network-dlp.

50. Market guide for Data Loss Prevention. *Gartner*. *Delivering Actionable, Objective Insight to Executives and Their Teams*. URL: https://www.gartner.com/doc/reprints?id=1-2EYKQ8XI&ct=230911&st=sb

51. Top Data Loss Prevention software awards 2022. Software Reviews. *SoftwareReviews*. URL: https://www.softwarereviews.com/awards/data-quadrant-awards-2022-data-loss-prevention

52. Куди зник Gartner DLP Magic Quadrant?. URL: https://corewin.ua/blog/gartner-dlp-magic-quadrant/

53. Forcepoint DLP vs Trellix Data Loss Prevention (DLP) Endpoint 2023. Gartner Peer Insights. *Gartner*. URL: https://www.gartner.com/reviews/market/data-loss-prevention/compare/product/forcepoint-dlp-vs-trellix-data-loss-prevention-dlp-endpoint.

54. Data Loss Prevention (DLP). *Trellix. Revolutionary Threat Detection and Response*. URL: https://www.trellix.com/ru-ru/products/dlp/.

55. What is Secure Access Service Edge (SASE). *Skyhigh Security*. URL: https://www.skyhighsecurity.com/cybersecurity-defined/what-is-sase.html.

56. Trellix agent product guide. URL: https://docs.trellix.com/bundle/trellix-agent-5.8.x-product-guide/page/GUID-5E541B16-055D-434E-ACE7-E600104D166E.html

57. McDade M. Top 10 Data Loss Prevention software | Expert Insights. *Expert Insights*. URL: https://expertinsights.com/insights/top-10-data-loss-prevention-software/.

58. *Trellix. Revolutionary Threat Detection and Response*. URL: https://www.trellix.com/assets/solution-briefs/trellix-data-protection-solution-brief.pdf.

59. The top 5 Forcepoint DLP alternatives and competitors in 2023. *Cyberhaven*. URL: https://www.cyberhaven.com/guides/forcepoint-dlp-alternatives-competitors.

60. Forcepoint Data Loss Prevention (DLP). *Forcepoint. Security Simplified*. URL: https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_dlp_en.pdf.

61. The Radicati Group Inc. Data Loss Prevention -- Market Quadrant 2023. URL: https://static.fortra.com/digital-guardian/pdfs/misc/Licensed-Data-Loss-Prevention-Market-Quadrant-2023.pdf.