МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, професор	доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____2022 р.	«___»_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ

СТУДЕНТ: Гарнатко Леонід Олегович _____
(підпис)

КЕРІВНИК: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.т.н. Щавінський Юрій Віталійович _____
(підпис)

Київ – 2022

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність 125 Кібербезпека
Спеціалізація Управління інформаційною та кібернетичною безпекою
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу

студенту Гарнатку Леоніду Олеговичу

Тема роботи: «ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ», затверджена наказом по університету № 122 від «12» жовтня 2022 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 2023 р.
2. **Об'єкт дослідження:** інформаційна безпека підприємств середнього і малого бізнесу.
3. **Предмет дослідження:** виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу.
4. **Мета дослідження** полягає у вивченні засад виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу, розробці відповідних рекомендацій.
5. **Перелік питань, які мають бути розроблені:**

5.1 Проаналізувати теоретичні та нормативні засади забезпечення інформаційної безпеки підприємства.

5.2 Дослідити загрози інформаційній безпеці підприємства.

5.3 Встановити особливості виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу, розробити відповідні рекомендації.

6. **Дата видачі завдання «**15» вересня 2022 р.

Науковий керівник _____ Т.М. Мужанова
Підпис

Завдання прийнято до виконання _____ Л.О. Гарнатко
Підпис

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «15» вересня 2022 р.

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	23.09.2022	виконано
2.	Збір та аналіз літератури.	30.09.2022	виконано
3.	Аналіз теоретичних та нормативних засад забезпечення інформаційної безпеки підприємства.	17.10.2022	виконано
4.	Дослідження загроз інформаційній безпеці підприємства.	01.11.2022	виконано
5.	Встановлення особливостей виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу, розробка відповідних рекомендацій.	15.11.2022	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2022	виконано
7.	Оформлення роботи.	04.12.2022	виконано
8.	Оформлення презентації.	21.12.2022	виконано
9.	Отримання рецензії на роботу.	24.12.2022	виконано
10.	Захист у ДЕК.	17.01.2023	

Студент (підпис) Л.О. Гарнатко

Науковий керівник (підпис) Т.М. Мужанова

РЕФЕРАТ

Кваліфікаційна робота присвячена вивченню засад виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу. Робота складається зі вступу, трьох розділів, що містять 12 рисунків, 9 таблиць, висновків та списку використаних джерел, що містить 58 найменувань. Загальний обсяг роботи становить 82 аркуша, з яких 6 аркушів займає список використаних джерел.

Об'єктом дослідження інформаційна безпека підприємств середнього і малого бізнесу.

Предметом дослідження є засади виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу.

Метою роботи є вивчення засад виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу та розробка відповідних рекомендацій що до захисту програмно-апаратного комплексу підприємств.

Для цього у роботі використовуються методи класифікації, порівняння, комплексного і процесного підходів, досліджуються ключові елементи інформаційної безпеки й методи активного виявлення загроз. Визначено засоби виявлення та реагування на загрози, теорії управління та інформаційної безпеки.

Галузь застосування. Розглянуті підходи можуть бути використані при плануванні та реалізації систем управління інформаційною безпекою підприємств середнього і малого бізнесу, зокрема при впровадженні технологій захисту та реагуванні на загрози.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ, ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ASN	Access Service Network
CIA	Confidentiality, Integrity, Availability
CTI	Cyber Threat Intelligence
CTH	Cyber Threat Hunting
DLP	Data Leak Prevention
EDR	Endpoint Detection & Response
IDS	Intrusion Detection System
InfoSec	Information Security, інформаційна безпека
IOC	Indicator of Compromise
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centers
RMM	Remote Network Monitoring and Management
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
UBA	User behavior analytics
АНБ	Агентство національної безпеки США
ІБ	інформаційна безпека
СМБ	середній і малий бізнес
НСД	несанкціонований доступ
ОС	операційна система
ПВПД	планування – виконання – перевірка – дія
СУ КСІІ	системи управління ключовими системами інформаційної інфраструктури

ВСТУП

Актуальність теми. Інформаційна безпека відіграє фундаментальну роль у житті сучасного підприємства, оскільки саме інформація є найбільш цінним корпоративним ресурсом, а також найбільш вразливим об’єктом інформаційних загроз, який потребує комплексного і надійного захисту.

Як свідчить практика, підприємства середнього і малого бізнесу використовують прийнятні саме для невеликих компаній методи виявлення загроз. Зазвичай на таких підприємствах система безпеки зводиться до елементарних систем захисту й політик безпеки, які не завжди забезпечують належний рівень інформаційної безпеки. Однак, сьогодні саме інформаційні системи й ресурси невеликих підприємств через їхні обмежені фінансові можливості й меншу захищеність у сфері безпеки частіше стають об’єктами інформаційних загроз.

З огляду на зазначене вивчення засад виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу, розробці відповідних рекомендацій.

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

1. Проаналізувати теоретичні та нормативні засади забезпечення інформаційної безпеки підприємства.
2. Дослідити загрози інформаційній безпеці підприємства.
3. Встановити особливості виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу, розробити відповідні рекомендації.

Об’єкт дослідження - інформаційна безпека підприємств середнього і малого бізнесу.

Предмет дослідження – засади виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, ситуаційного та процесного підходів, визначено ключові елементи інформаційної безпеки та методи активного виявлення загроз.

Наукова новизна одержаних результатів. У роботі дана оцінка загрозам, вразливостям та потенційним ризикам інформаційній безпеці. Розглянуті підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства, зокрема при впровадженні технологій захисту та реагуванні на загрози.

Практичне значення одержаних результатів. Розроблені рекомендації щодо виявлення та протидії загрозам інформаційній безпеці, запровадження правил і політик для захисту інформації, плану дій на випадок кібератаки сприятимуть підвищенню ефективності системи управління інформаційною безпекою підприємств малого і середнього бізнесу.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА НОРМАТИВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Інформаційна безпека: поняття, терміни та визначення

З огляду на принципово важливе значення інформації в сучасних умовах інформаційної глобалізації і цифровізації сучасні підприємства незалежно від розміру, форми власності та сфери діяльності стоять перед викликом забезпечення безпеки своїх інформаційних ресурсів та даних, які перебувають у їх розпорядженні, а також інформаційного середовища підприємства загалом. Розглянемо визначення основних понять у сфері інформації та інформаційної безпеки [1].

В онлайн-словнику Мерріама-Вебстера (www.merriam-webster.com) дається таке визначення інформації:

- відомості, отримані під час дослідження, вивчення чи навчання;
- звістки, новини, факти, дані;
- команди або символи подання даних (у системах зв'язку або комп’ютерах);
- знання (повідомлення, експериментальні дані, зображення), що змінюють концепцію, отриману внаслідок фізичного чи розумового досвіду [2].

Безпека в цьому ж джерелі визначається так: захист від небезпеки, захищеність, свобода від страху чи занепокоєння. При об’єднанні двох понять ми отримаємо визначення інформаційної безпеки - заходи, вжиті для запобігання несанкціонованому використанню, зловживанню, змінам відомостей, фактів, даних чи апаратних засобів або відмови в доступі до них.

Відповідно до визначення, інформаційна безпека не забезпечує абсолютний захист, але є сукупністю запобіжних дій, які дозволяють

захистити інформацію та обладнання від загроз та використання їх уразливих місць.

Інформаційна безпека (InfoSec)– це набір процедур та інструментів, які захищають усю чутливу корпоративну інформацію від неправомірного використання, несанкціонованого доступу, псування або знищення. InfoSec включає безпеку на фізичному й корпоративному рівні, керування доступом і кібербезпеку [3]. Це рішення часто передбачає використання технологій які забезпечують захищений доступ до хмари, примусового застосування політики безпеки між корпоративними користувачами й постачальниками хмарних служб. Можуть об’єднувати безліч різних політик безпеки, зокрема автентифікацію, зіставлення облікових даних, шифрування, виявлення шкідливого ПЗ тощо, а також гарантують захист в авторизованих і неавторизованих програмах та на керованих і некерованих пристроях

Проведений аналіз тлумачення терміну «інформаційна безпека» (див. табл. 1.1) показує, що його трактування у більшості гравців ринку інформаційної безпеки, як практиків так і розробників відповідних стандартів, в цілому співпадає та не викликають протиріч.

Таблиця 1.1

Визначення терміну «інформаційна безпека»

Джерело	**Визначення**
Стандарт ISO 27001 [4]	визначає інформаційну безпеку як: збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені інші властивості, такі як справжність, неможливість відмови від авторства, достовірність. Конфіденційність – забезпечення доступності інформації лише для тих, хто має відповідні повноваження (авторизовані користувачі). Цілісність – забезпечення точності та повноти інформації, а також методів її опрацювання. Доступність – забезпечення доступу до інформації авторизованим користувачам

Джерело	Визначення
Cisco [5]	Інформаційна безпека – це процеси та інструменти, розроблені і розгорнуті для захисту конфіденційної бізнес-інформації від модифікації, порушення, знищення та перевірки.

Продовження таблиці 1.1

Джерело	Визначення
Microsoft [3]	Інформаційна безпека – це набір процедур та інструментів, які захищають усю чутливу корпоративну інформацію від неправомірного використання, несанкціонованого доступу, псування або знищення. Включає безпеку на фізичному та корпоративному рівні, керування доступом і кібербезпеку.
Електроний підручник «Безпека мереж» [6]	Інформаційна безпека - це система, що дозволяє виявляти вразливі місця організації, небезпеки, що загрожують їй, та справлятися з ними.

На нашу думку найбільш точно та стисло визначення інформаційної безпеки надано саме у останньому варіанті, хоча, слід зауважити, що всі визначення майже тотожні.

Коли ми отримали уявлення про поняття інформаційної безпеки, перейдемо до вивчення її структури. На рисунку 1.1 представлено ключові елементи інформаційної безпеки.

Рис. 1.1. Ключові елементи інформаційної безпеки

У таблиці 1.2 представлено коротку характеристику кожного з елементів інформаційної безпеки.

Таблиця 1.2

Елементи інформаційної безпеки

Елемент ІБ	**Пояснення змісту елемента**
Захист програм	Політики, процедури, інструменти й практичні поради щодо захисту програм і даних, які містяться в них
Захищеність хмари	Політики, процедури, інструменти й практичні поради щодо комплексного захисту хмари, зокрема систем, даних, програм та інфраструктури.
Криптографія	Алгоритмічний метод забезпечення захищеного спілкування, який полягає в тому, що певне повідомлення можуть переглядати й дешифрувати лише конкретні одержувачі.
Аварійне відновлення	Метод відновлення функціональних технологічних систем після стихійних лих, кібератак або інших порушень.
Реагування на інциденти	План організації для реагування на кібератаки, порушення безпеки даних та інші загрози, керування ними й усунення їхніх наслідків.
Убезпечення інфраструктури	Безпека всієї технологічної інфраструктури організації, зокрема систем апаратного й програмного забезпечення.
Керування вразливостями	Процес виявлення, оцінювання й усунення вразливостей у кінцевих точках, програмному забезпеченні та системах організації.

Складено на основі компіляції джерел [3-6]

Принципи інформаційної безпеки. При обговоренні питань інформаційної безпеки часто буває корисно мати модель, яку можна взяти за основу. В цьому випадку ми отримаємо послідовний набір термінів та концепцій, на які ми як професіонали в області безпеки можемо посилатися.

Модель CIA. Конфіденційність, цілісність і доступність – це запорука ефективного захисту даних та безпеки інфраструктури організації. Ці три поняття є основоположними принципами для впровадження плану ІБ [7].

Рис. 1.2. Модель CIA (Confidentiality, Integrity, Availability)

Конфіденційність – це основний компонент ІБ, який полягає в тому, що доступ до інформації можуть отримувати лише авторизовані користувачі. Шифрування даних, багатофакторна автентифікація та захист від втрати даних – це приклади інструментів, які підприємства можуть використовувати для забезпечення конфіденційності інформації.

*Цілісність***.** Підприємства мають підтримувати цілісність даних протягом усього їхнього життєвого циклу. Підприємства з розвинутим компонентом ІБ визнають важливість використання точних і надійних даних та не дозволять неавторизованим користувачам отримувати доступ до них, змінювати їх або керувати ними. Такі інструменти, як дозволи для файлів, керування ідентичностями й елементи керування доступом користувачів, забезпечують цілісність даних.

*Доступність***.** Інформаційна безпека включає безперервну підтримку фізичного обладнання й регулярне оновлення системи, щоб авторизовані користувачі мали надійний і узгоджений доступ до даних відповідно до своїх потреб.

Разом ці поняття складають так звану модель CIA (Confidentiality, Integrity, Availability) та багато в чому є основними елементами, яким приділяють увагу при захисті систем у ході стандартних процесів розгортання, підтримки чи оцінки захищеності.

При виявленні загроз, потрібно зрозуміти, до якої частини CIA або їх комбінації відносяться ці інциденти. Це допомагає зрозуміти її повніше, дозволяє розбивати інциденти за категоріями та вживати відповідних заходів. Розуміючи сутність моделі CIA, нескладно класифікувати за її допомогою вразливість різного масштабу.

Модель Паркера. Паркерівська гексада – це менш відома модель, яка названа на честь Донна Паркера та представлена в його книзі «Fighting Computer Crime» [8], представляє собою дещо складніший варіант класичної тріади CIA. Тріада CIA складається лише з конфіденційності, цілісності та доступності, а в гексаді Паркера додаються володіння (possession), або контроль, справжність та корисність, складаючи у сумі шість принципів (рис. 1.3).

Паркерівська гексада включає три принципи тріади CIA з тими самими визначеннями, що обговорювалися вище, та три додаткових принципи, які ми розглянемо нижче.

Володіння або Контроль — це фізичне розташування носія, на якому зберігаються дані. Ця концепція дозволяє говорити про втрату даних на фізичному носії без залучення інших факторів, таких як доступність.

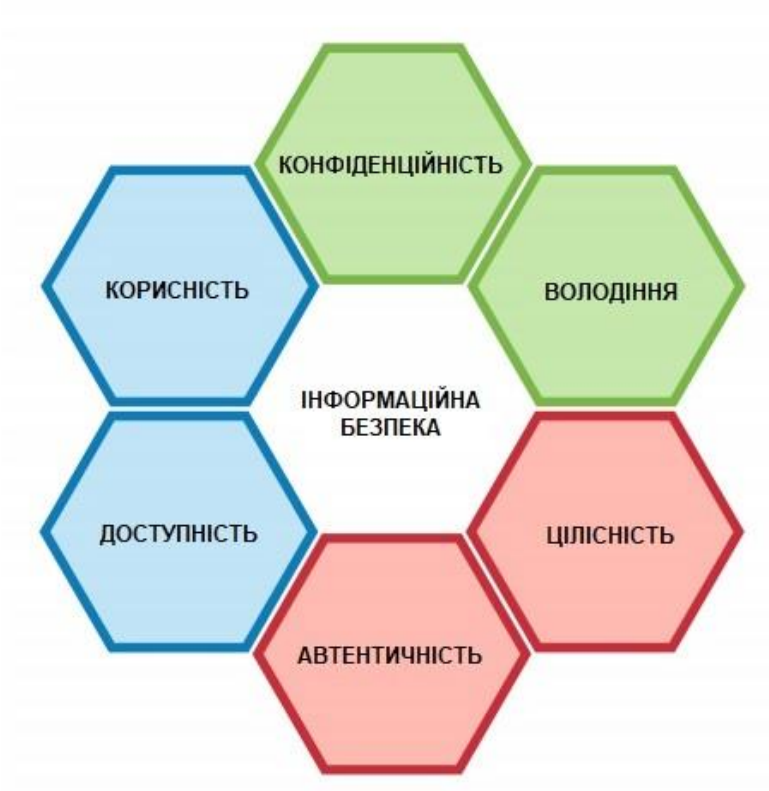

Рис. 1.3. Модель інформаційної безпеки Паркера

Автентичність. Принцип справжності дозволяє сказати, чи правильний у даних автор чи власник. Справжність можна забезпечити, наприклад, за допомогою цифрових підписів. Це підтвердить автентичність автора та належність до даних.

Корисність – це те, наскільки дані є важливими. Корисність також є єдиним принципом гексади Паркера де дані можуть мати безліч ступенів корисності залежно від змісту та формату. Це дещо абстрактна концепція, яка, однак, виявляється корисною при обговорення певних ситуацій у сфері безпеки.

Концепції, які вводяться в тріаді CIA і гексаді Паркера, дають практичну основу для обговорення того, що і як може піти не так у сфері інформаційної безпеки. Ці моделі дозволяють краще розглянути ймовірні загрози, методи та засоби, які потрібні для боротьби з ними.

1.2 Методи і технології інформаційної безпеки

Для забезпечення інформаційної безпеки підприємства комплексно використовують різні види методів, зокрема:

- нормативно-правові;
- організаційно-адміністративні;
- фізичні;
- програмні-технічні;
- морально-етичні [9].

До нормативно-правових методів інформаційної безпеки підприємства належить використання й забезпечення відповідності нормам діючого в державі законодавства (законів, постанов, указів тощо), стандартів, специфікацій та інших галузевих нормативних документів, які, зокрема, регламентують правила поводження з конфіденційною інформацією, а також розробка й дотримання вимог корпоративних документів, в тому числі у сфері інформаційної безпеки (політик, процедур, регламентів, інструкцій тощо).

Організаційно-адміністративні методи забезпечення інформаційної безпеки підприємства передбачають планування і впровадження заходів щодо:

- проектування й обладнання обчислювальних центрів та інших об'єктів ІС (облік впливу стихії, пожеж, охорона приміщень тощо);

- підбору й підготовки персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, із мірами відповідальності за порушення правил її обробки; створення умов, при яких персоналу було б невигідно допускати зловживання тощо);

- організацію внутрішнього і пропускного режиму;

- обліку, зберігання, використання та знищення документів і носіїв з конфіденційною інформацією;

- управління доступом (паролів, повноважень тощо);

- контролю за роботою користувачів і персоналу;

- сертифікації наявних у використанні технічних і програмних засобів, розгляд і затвердження змін, перевірка на відповідність вимогам захисту тощо.

До програмно-технічних методів інформаційної безпеки відносять застосування різноманітних електронних пристроїв та спеціальних програм, які унеможливлюють витік, знищення та блокування інформації, порушення цілісності та режиму доступу до неї; використання засобів ідентифікації та аутентифікації суб'єктів ІС, розмежування доступу до інформаційних ресурсів, контролю цілісності даних та забезпечення їх конфіденційності; резервного копіювання ресурсів та ІС, аудиту інформаційної безпеки тощо.

Фізичні методи інформаційної безпеки включають застосування різних механічних, електро і електромеханічних пристроїв або споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу порушників (турнікети, колючий дріт, кодові замки, системи охоронно-пожежної сигналізації тощо).

До морально-етичних методів відносять розробку й забезпечення дотримання норм поведінки, які традиційно складаються в компанії, формування культури інформаційної безпеки персоналу. Ці норми можуть бути як неписаними (загальновизнані норми чесності, корпоративної відданості тощо), так і оформленими в формально затверджений кодекс поведінки, звід правил чи приписів.

Технології ІБ. Створення ефективної стратегії інформаційної безпеки потребує застосування різноманітних інструментів та технологій. У більшості стратегій використовують певну комбінацію наступних технологій (таблиця 1.3).

При чому реальна практика свідчить проте, що саме комбінація збалансованих технологій програмного, апаратного та організаційного рівня дає найкращій результат. Балансування технологій відбувається на основі наявних ресурсів, доступних компетенцій, технологій та рішень. Задача

балансування технологій забезпечення ІБ – одна з основних у роботі адміністратора системи або вповноваженого з інформаційної безпеки.

Таблиця 1.3

Технології реалізації інформаційної безпеки

Технологія	**Короткий опис**
Брандмауери	Рівень захисту, який можна застосувати до мереж або програм. Ці інструменти дозволяють фільтрувати трафік і передавати дані про трафік у системи моніторингу та виявлення. Брандмауери часто використовують встановлені списки дозволеного чи не дозволеного трафіку та політики, що визначають швидкість або обсяг дозволеного трафіку.
Технології управління інцедентами, SIEM (Security Information and Event Management)	Рішення для управління інцидентами та подіями безпеки дозволяють вам отримувати та зіставляти інформацію з різних систем. Таке об'єднання даних дозволяє командам ефективніше виявляти загрози, керувати попередженнями й забезпечувати кращий контекст для розслідувань. Рішення SIEM також корисні для реєстрації подій, що відбуваються в системі, або для складання звітів про події та продуктивність. Потім можна використовувати цю інформацію для підтвердження відповідності або оптимізації конфігурацій.
Захист від втрати даних DLP (Data Leak Prevention)	Включає політики, процедури, інструменти й практичні поради, які дають змогу запобігти втраті або неправомірному використанню делікатних даних. До ключових інструментів DLP належать шифрування або перетворення звичайного тексту на зашифрований за допомогою алгоритму та визначення смислових одиниць або призначення набору випадкових чисел певному фрагменту даних і використання бази даних сховища маркерів для збереження зв’язку між ними.
Перевірка системи безпеки для DevOps	Процес інтеграції спеціальних заходів упродовж усього періоду розробки системи безпеки. Це рішення дає змогу пришвидшити процеси реалізації задач

Технологія	Короткий опис
(DevSecOps)	інформаційної безпеки й оптимізувати їх.

Продовження таблиці 1.3

Технологія	Короткий опис
Технології протидії загрозам у кінцевих точках, EDR (Endpoint Detection & Response)	Дозволяють відстежувати активність кінцевих точок, виявляти підозрілі дії та автоматично реагувати на погрози. Ці рішення призначені для покращення видимості кінцевих пристроїв і можуть бути використані для запобігання проникненню загроз у мережі або витоку інформації. Рішення EDR засновані на безперервному зборі даних кінцевих точок, механізмах виявлення та реєстрації подійних.
Мікросегментація	У процесі мікросегментації центри обробки даних діляться на кілька деталізованих і захищених зон або сегментів, що знижує рівень ризику.
Поведінкова аналітика користувачів UBA (User Behavior Analytics)	Рішення UBA збирають інформацію про дії користувачів та співвідносять їхню поведінку з базовим рівнем. Потім рішення використовують цей базовий рівень для порівняння з новими моделями поведінки з метою виявлення невідповідностей. Аналітичним методом визначаються невідповідності які можуть бути ознаками потенційної небезпеки.
Технологія Блокчейн	Технологія, яка спирається на транзакційні події, що не змінюються. У блокчейн-технологіях розподілені мережі користувачів перевіряють справжність транзакцій та забезпечують підтримку їх цілісності.
Система запобігання вторгненням (IPS – Intrusion Prevention System)	Рішення, що реагують на трафік, ідентифікований як підозрілий чи шкідливий, блокуючи запити або завершуючи сеанси користувача. IPS-рішення використовують для керування мережевим трафіком відповідно до певних політик безпеки.

Складено на основі компіляції джерел [4-7]

Якщо уважно проаналізувати технології реалізації задач інформаційної безпеки, то можна помітити, що лише частина цих задач виконується за

допомогою інформаційних технологій. Тому у сфері інформаційних технологій виділено спеціальне поняття *кібербезпеки*. До кібербезпеки відносяться лише технологічні задачі інформаційної безпеки, які вирішуються виключно засобами інформаційних технологій.

Кібербезпека. *Кібербезпека*– це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи та мережу від кібератак [10]. Оскільки об’єм даних збільшується й усе більше користувачів працюють і спілкуються звідусіль, кіберзлочинці розробляють складні методи, щоб отримувати доступ до ресурсів, викрадати дані, саботувати роботу компаній або вимагати гроші. Щороку кількість атак збільшується, а зловмисники розробляють нові методи для уникнення виявлення. Ефективна програма з кібербезпеки включає фахівців, процеси та технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак.

Кібербезпека – це частина інформаційної безпеки. InfoSec охоплює велику кількість інформаційних областей і задач, зокрема фізичних пристроїв та серверів, а кібербезпека стосується лише технологічної безпеки.

1.3 Стандарти з інформаційної безпеки

Важливу роль у регламентації процесів забезпечення інформаційної безпеки підприємства відіграють міжнародні стандарти, які є узагальненням кращого світового досвіду у цій сфері.

Найбільш відомою інституцією у сфері стандартизації є Міжнародна організація зі стандартизації (ISO), яка була створена в 1926 році для впровадження загальних стандартів різних країн. До основних видів діяльності ISO належать: заходи, які сприяють координації та уніфікації національних стандартів; розроблення і затвердження міжнародних стандартів; обмін інформацією з проблем стандартизації; співробітництво з

іншими міжнародними організаціями, які зацікавлені у вирішенні суміжних проблем, і на їх прохання, вивчає проблеми стандартизації [11].

Серія ISO 27000 щодо управління інформаційною безпекою містить понад 60 стандартів, які поділяють на три категорії (Рис.1.4) [12]:

− стандарти, які визначають термінологію (ISO 27000);

− стандарти, які встановлюють загальні вимоги (ISO 27001, ISO 27006);

− стандарти, які дають загальні вказівки (ISO 27002, ISO 27005 та інші).

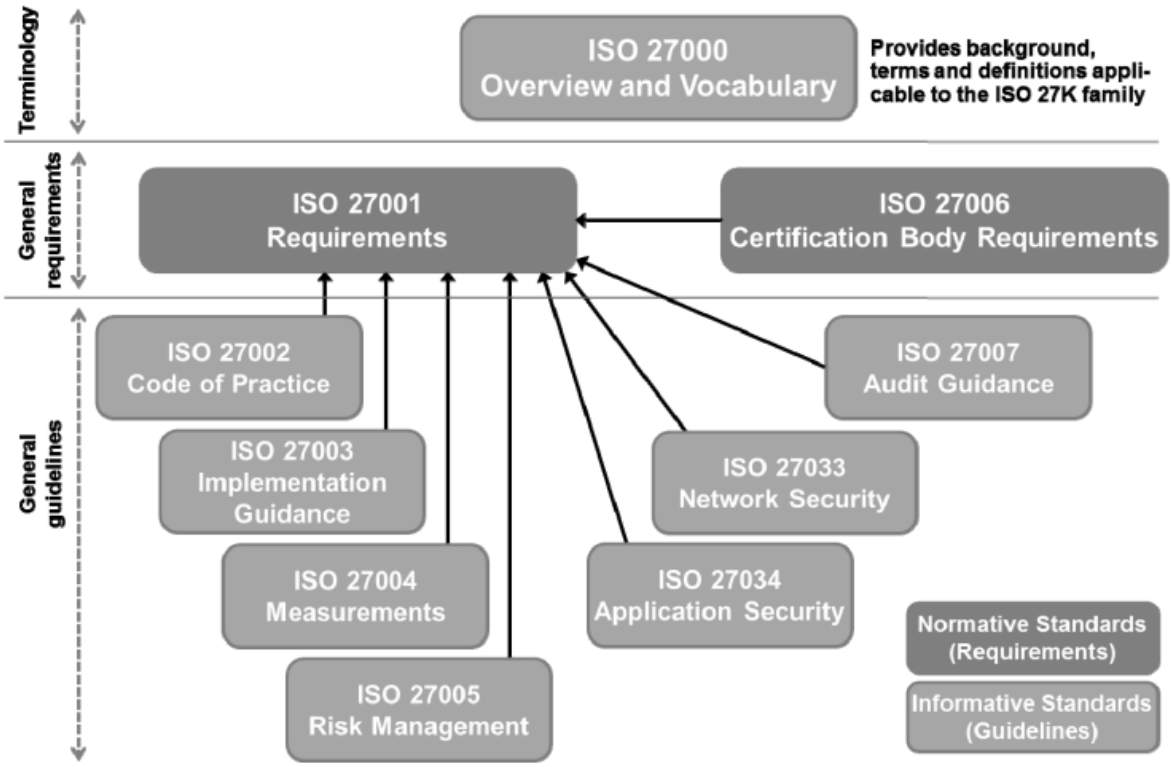

Рис. 1.4. Стандарти серії ISO 27000.

Основоположними стандартами є:

− ISO 27000 - «Системи управління інформаційною безпекою. Огляд та основні терміни». У цій серії стандартів ISO описані системи управління інформаційною безпекою (далі - СУІБ), задачі ІБ, рекомендації щодо управління безпекою активів організації. У цих документах викладені (відносно) передові методи управління ризиками, контролю, конфіденційності, технічні питання й інші особливості управління ІБ.

− ISO/IEC 27001 - «Інформаційні технології. Методи безпеки. Системи керування інформаційною безпекою. Вимоги». ISO 27001 описує структуру системи управління інформаційною безпекою (скорочено СУІБ) для компаній незалежно від організаційної структури, розміру або орієнтації. Стрижнем тут є управління ризиками. Мінливі кіберзагрози постійно використовують нові потенційні вразливості в компаніях з метою атаки та компрометації інформаційних потоків, а отже, і бізнес-процесів. Ризики, що виникають внаслідок цього механізму для трьох основних цілей захисту інформаційної безпеки - конфіденційності, цілісності та доступності - повинні бути ідентифіковані та керовані.

− ISO/IEC 27002 - «Зведення правил для заходів контролю інформаційної безпеки». В оновленому стандарті ISO/IEC 27001:2022 розглядаються кращі практики управління цими ризиками інформаційної безпеки. Перелік можливих засобів контролю інформаційної безпеки в нормативному Додатку А нового стандарту ISO/IEC 27001:2022 ідентично походить з переглянутого керівництва ISO/IEC 27002:2022.

28 жовтня 2022 року було опубліковано нову покращену версію серії стандартів ISO/IEC 27000:2022, а саме ISO/IEC 27001:2022.

Насамперед хотілося б зазначити, що оновлена версія ISO 27001:2022 суттєво не відрізняється від попередньої 2013 року, проте є деякі помітні поправки, які розглянемо нижче.

Почнемо з того, що в новому виданні ISO 27001 35 елементів управління залишилися без змін, 23 – були перейменовані, 56 – об'єднані у 24 і лише 1 (18.2.3. Аналіз технічної відповідності) було поділено на два: управління технічними вразливостями; відповідність політикам та стандартам інформаційної безпеки (скор. ІБ) організації, до якої додано ще 11 нових елементів контролю (оцінка загроз, інформаційна безпека для хмарних сервісів, готовність інформаційно-комунікаційних технологій (англ. ICT - Information and Communications Technology) до забезпечення безперервності бізнесу, моніторинг фізичної безпеки та ін.).

Модернізований ISO 27002 скоротився приблизно на 20%, заходи щодо безпеки в ньому об'єднані в 4 глави замість колишніх 14, а кількість засобів управління зменшилася до 93 [13].

Настанова з впровадження вже була прийнята в лютому цього року з більш простою таксономією та сучасними засобами контролю безпеки. З появою нового стандарту ISO/IEC 27001:2022 успішний тандем стандартів ISO 27001/27002 з його цінними рекомендованими заходами знову відповідає сучасному рівню розвитку.

До основоположних відносять такі стандарти з інформаційної безпеки:

- ISO/IEC 17799:2002 - один із найвідоміших стандартів, створений на основі BSI та розглядає практичні питання з управління інформаційною безпекою;
- BSI - стандарт розроблений у Німеччині і присвячений, на відміну від попереднього, більш повному висвітлення питань приватності;
- ISO 15408 - стандарт створений на основі досвіду фахівців із США та Канади, описує загальні критерії безпеки інформаційних технологій.

Державні стандарти України в сфері інформаційної безпеки. Відповідно наказу Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (яке виконує функції національного органу стандартизації) №312 від 16.10.2019 «Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів» прийняті національні стандарти в сфері інформаційної безпеки, гармонізовані з європейськими та міжнародними стандартами, методом підтвердження з наданням чинності з 01 листопада 2019 року [14]:

- ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) – Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (на заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT);

– ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT);

– ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) – Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. (на заміну ДСТУ ISO/IEC TR 27008:2018 ISO/IEC TR 27008:2011, IDT);

– ДСТУ ISO/IEC 27018:2019 (ISO/IEC 27018:2019, IDT) – Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII. (на заміну ДСТУ ISO/IEC 27018:2016, ISO/IEC 27018:2014, IDT);

– ДСТУ ISO/IEC TS 27034-5-1:2019 (ISO/IEC TS 27034-5-1:2018, IDT) – Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних керування протоколами та захистом застосунків. Схеми XML (вперше).

– ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT) – Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;

– ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT) – Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки;

– ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) / Поправка № 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT) – Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002.

Як бачимо, вітчизняний законотворець пішов по простому та прагматичному шляху: відмовився від складання власних стандартів, як від невиправдано складної та витратної процедури, і прийняв рішення про

впровадження міжнародних стандартів, які містять кращий світовий досвід, у правове поле держави.

Висновки до розділу 1

У результаті дослідження встановлено, що інформаційна безпека підприємства – це система, що дозволяє виявляти вразливі місця організації, небезпеки, що загрожують їй, та справлятися з ними. До основних методів інформаційної безпеки відносять нормативно-правові; організаційно-адміністративні; програмно-технічні; фізичні та морально-етичні.

Зроблено висновок, що для створення ефективної системи інформаційної безпеки підприємства необхідним є комплексне застосування різноманітних технологій, зокрема міжмережевого екранування, запобігання вторгненням (IPS) та втраті даних (DLP), управління інформацією та подіями безпеки (SIEM), виявлення і протидії загрозам у кінцевих точках (EDR), поведінкової аналітики (UEBA), управління інцидентами та інших.

Розглянуто основні положення стандартів серії ISO 27000, які пропонують рішення щодо впровадження й удосконалення системи управління інформаційною безпекою (СУІБ) на основі узагальнення кращого світового досвіду у цій сфері.

В Україні методом підтвердження прийняті такі національні стандарти в сфері інформаційної безпеки, гармонізовані з міжнародними стандартами методом підтвердження з наданням чинності з 01 листопада 2019 року серії ISO 27000: 27000-27002, 27005, 27008, 27011 та інші.

РОЗДІЛ 2
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

2.1 Ризики, загрози та вразливості у сфері інформаційних технологій

Розглянемо докладніше поняття ризик та його складові: загрозу та вразливість. Ці поняття не надто складні, але в них легко заплутатися. У спрощеному вигляді можна відзначити наступне: найкраще сприймати *ризик* як те небажане, що ви намагаєтеся запобігти, *загрозу* – як те, що може це, небажане, зробити, і *вразливість* – як щось, здатне дозволити зробити те, що ви хочете запобігти. Відповідні зусилля можна докласти до зниження рівня загрози або усунення вразливість, тим самим зменшити рівень ризику (Рис 2.1).

У обчислювальному середовищі ми часто говоримо про потенційні, але малоймовірні атаки. Однак найкраще витратити свій час на усунення ймовірної атаки. Якщо витратити ресурси на спроби передбачити всі можливі атаки, то не вистачить захисту там, де він справді потрібний [15].

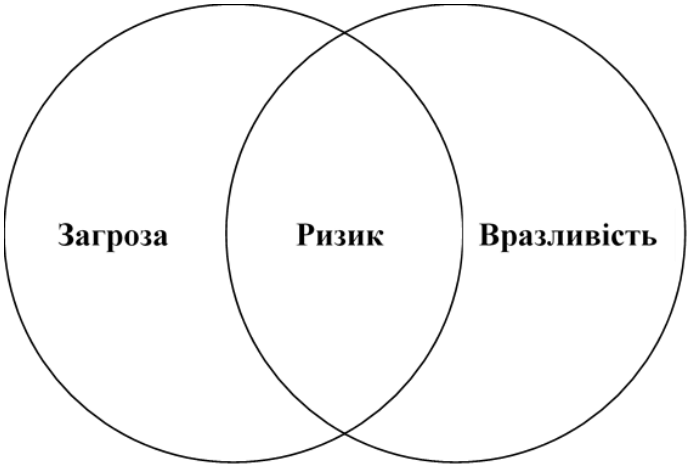

Рис. 2.1. Схема взаємозв’язків понять загроза, вразливість та ризик у сфері інформаційної безпеки

Такі організації, як Агентство національної безпеки США (АНБ), додають до рівняння «загроза – вразливість – ризик» ще один параметр – вплив. Цей фактор враховує вартість активу, якому загрожує небезпека і вартість використовується для розрахунку ризику. Наприклад, якщо інформація до якої може отримати доступ не містять нічого конфіденційного, то ніякого ризику ви не наражаєтеся, особливо коли у вас є резервна копія цих даних.

Процеси управління ризиками компенсують ризики у інформаційному середовищі. На рис. 2.2 показаний типовий процес управління ризиками високому рівні [16].

Потрібно визначити, які активи потенційно важливі, з'ясувати ймовірні загрози, оцінити вразливості, а потім вжити заходів для зниження цих ризиків.

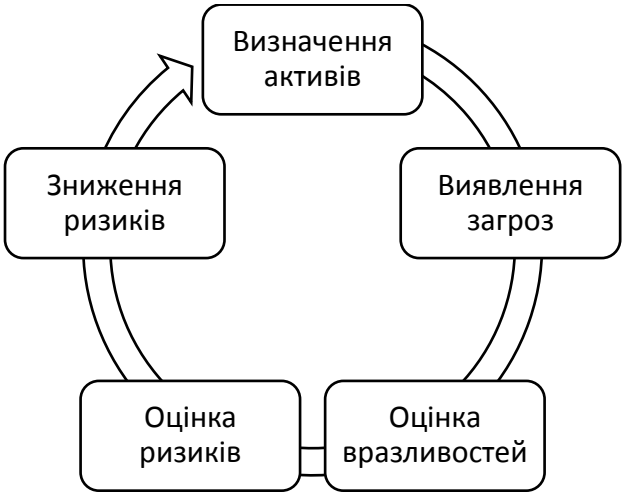

Рис. 2.2. Процес управління ризиками ІБ

Визначення активів. Одна з перших і, можливо, найважливіших частин процесу управління ризиками – це визначити, які активи потребують захисту. Якщо неможливо перерахувати потенційні активи та оцінити важливість кожного з них, то й захистити їх буде справді важко. Завдання здається простим, але лише на перший погляд, особливо якщо йдеться про великі підприємства. У багатьох організацій можливо обладнання різних поколінь, активи від придбання інших компаній, що знаходяться невідомо де, та безліч незареєстрованих віртуальних хостів, які можуть бути критично важливими для безперервної роботи підприємства.

Коли визначено використовувані активи, потрібно буде вирішити, які з них є критично важливими для бізнесу. Зазвичай визначення того, які активи дійсно важливі для бізнесу, потрібно зрозуміти, для яких задач вони використовується, які ресурси він вимагає для роботи і які ще особи або організації впливають на його роботу.

Виявлення загроз. Визначивши критично важливі активи, потрібно перейти до виявлення загроз, які можуть на них вплинути. Часто буває корисно мати основу для обговорення природи загрози – для цього підійде тріада CIA чи гексада Паркера.

Оцінка вразливостей. Виконувати оцінку вразливостей слід у контексті потенційних загроз. Будь-який актив може містити тисячі чи мільйони загроз,

які можуть вплинути на нього, але тільки невелика частина з них матиме значення.

Використовуємо гексаду Паркера та спробуємо вивчити загрози та відповідні їм вразливості, з якими ви можете зіткнутися, на прикладі додатку, який обробляє платежі за кредитних карток (Таблиця 2.1).

Таблиця 2.1

Потенційні загрози та відповідні їм вразливості активу (на прикладі додатку, який обробляє платежі по кредитним карткам)

Елемент	**Потенційна загроза**
Конфіденційність	Загроза**:** Якщо дані розкриваються неналежним чином, можливі порушення безпеки. Вразливість: Конфіденційні дані знаходяться без руху та зашифровані. Системи захисту регулярно тестуються компанією на предмет проникнень. Ризику немає.
Цілісність	Загроза**:** Якщо дані пошкоджені, можливе неправильне оброблення платежу. Вразливість: Уважно перевіряйте правильність платіжних даних у рамках робочого процесу. Неправильні дані призводять до відхилення транзакції. Ризику немає.

Продовження таблиці 2.1

Елемент	**Потенційна загроза**
Доступність	Загроза**:** Якщо система або програма вийде з ладу, буде неможливо виконувати обробку платежів. Вразливість: Втрата резервної копії бази даних на внутрішній стороні системи обробки платежів. Якщо база даних вийде з ладу, буде не можливо її відновити та обробляти платежі. Ризик є.
Володіння (Possession)	Загроза**:** Якщо втратити резервний носій, можливі порушення безпеки. Вразливість: Резервні копії мають бути зашифровані та зберігатися з обмеженим

	доступом. Ризику немає.
Справжність	Загроза**:** Якщо немає достовірної інформації про клієнта, можливо, буде опрацьовано транзакцію шахрая. Вразливість: Важко гарантувати, що інформація про платіж дійсна і що вона належить особі, яка проводить транзакцію. Не має способу верифікації. Ризик є.
Корисність	Загроза**:** некоректні або застарілі дані мають низьку корисність. Вразливість: Щоб захистити корисність даних, потрібно регулярно оновлювати дані, слідкувати за актуальністю інформації перевіряти контрольну суму даних, щоб переконатися в коректності. Ризику немає.

Це досить спрощена оцінка загроз системи, але вже зараз ми виділили кілька проблемних областей. Важливо подумати про втрату контролю над даними, стежити за точністю даних та підтримувати систему в робочому стані. Маючи цю інформацію, можливо вивчити області вразливості та потенційного ризику.

Оцінка ризиків. Визначивши загрози та вразливості для цього активу, можна оцінити загальний ризик. Як уже говорилося, ризик – це поєднання загрози та вразливості. Вразливість без відповідної загрози або загроза без відповідної вразливості не викликають ризику.

Наприклад, наступний елемент у категорії Доступність (табл. 2.1) був одночасно потенційною загрозою та вразливістю: Загроза – система або програма вийде з ладу, буде неможливо виконувати обробку платежів, Вразливість – втрата резервної бази даних на внутрішній стороні системи обробки платежів – буде неможливо обробляти платежі.

У цьому випадку є і загроза, і відповідна вразливість, а це означає, ризик втратити можливість обробляти платежі за кредитними картками через

відмову в серверній частині бази даних. Пропрацювавши таким чином загрози та вразливості, буде можливо пом'якшити ризики.

2.2 Види загроз інформаційній безпеці підприємства

Зупинимося детальніше на визначенні сутності поняття «загроза інформаційній безпеці».

Загроза (в загальному) - це потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди інтересам певного суб’єкта, в тому числі організації чи підприємства.

Під загрозою інтересам суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта [17].

У свою чергу, загроза інформаційній безпеці є сукупністю умов і факторів, що створюють ризик порушення інформаційної безпеки. На рис. 2.3 класифіковано загрози інформаційній безпеці за певними ознаками.

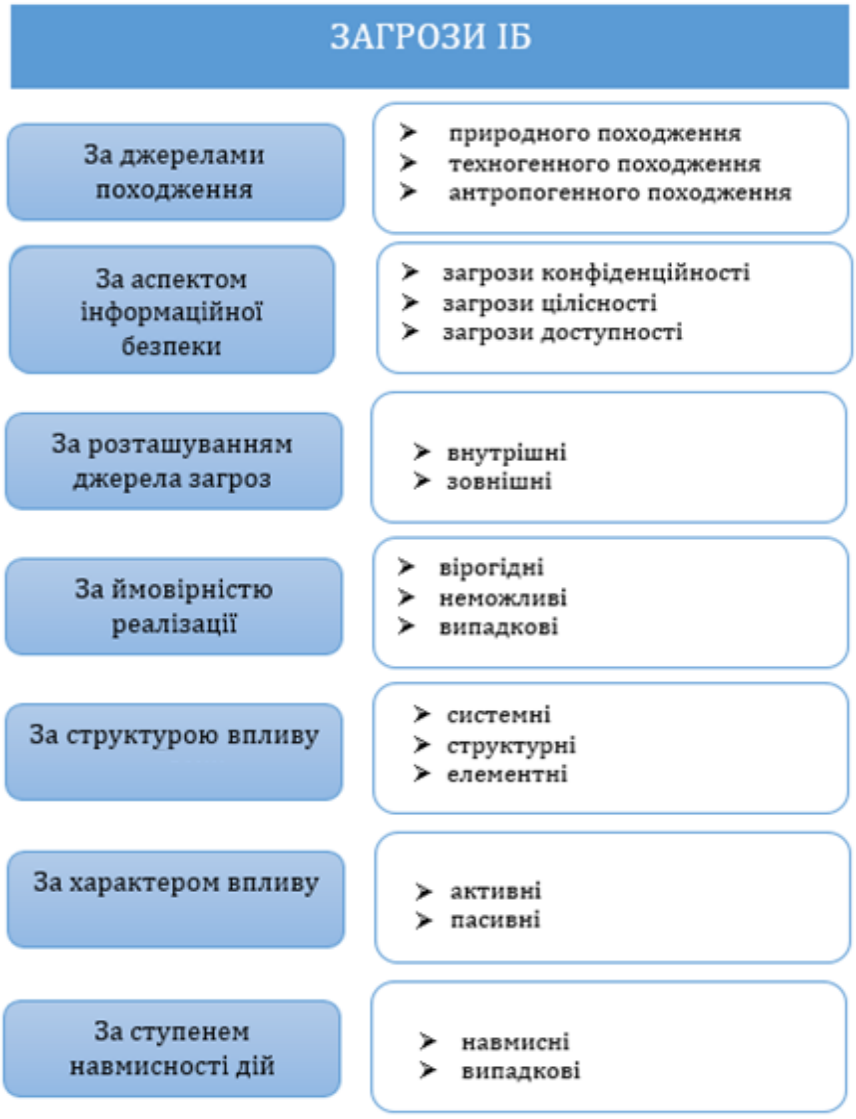

Рис 2.3. Класифікації загроз інформаційній безпеці

Загрози інформаційній безпеці за джерелами походження поділяються на три основні групи:

Обумовлені діями суб'єкта (антропогенні джерела) — суб'єкти, дії яких можуть призвести до порушення безпеки інформації, дані дії можуть бути кваліфіковані як навмисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми, так і внутрішніми. Ці джерела можна спрогнозувати, і прийняти адекватні заходи.

Обумовлені технічними засобами (техногенні джерела) — ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і

тому вимагають особливої уваги. Дані джерела загроз інформаційній безпеці, також можуть бути як внутрішніми, так і зовнішніми.

Стихійні джерела — дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, які неможливо передбачити або запобігти чи можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до захищеного об'єкта і під ними, як правило, розуміються природні катаклізми.

За аспектом інформаційної безпеки, на який спрямовані загрози:

Загрози конфіденційності (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, телефонних переговорів, поштових відправлень, та ін).

Загрози цілісності (неправомірна зміна даних). Загрози порушення цілісності — це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками — від умисних дій персоналу до виходу з ладу обладнання.

Загрози доступності (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

Загрози інформаційній безпеці за розташуванням поділяються на внутрішні та зовнішні. Зовнішні загрози – це такі загрози, джерела яких знаходяться поза системою. До зовнішніх загроз інформаційної безпеки підприємства можна віднести:

а) промислове і економічне шпигунство, шантаж, дезінформацію, атаки на систему захисту з метою крадіжки, знищення, спотворення інформації, підриву нормальної роботи підрозділів;

б) відсутність на ринку достатньої кількості сертифікованих засобів захисту інформації; неповноцінність існуючої нормативно-правової бази інформаційної безпеки;

в) діяльність недобросовісних партнерів, клієнтів.

Внутрішні загрози інформаційної безпеки підприємства – це такі загрози, джерела яких розташовуються усередині системи. До внутрішніх загроз інформаційної безпеки підприємства можна віднести:

а) застарілі програмно-технічні засоби зберігання і обробки даних;

б) недосконаліть використовуваної системи захисту інформації;

в) використання «піратського» програмного забезпечення;

г) саботаж персоналу;

д) низьку кваліфікацію співробітників;

е) недостатню пожежну, технічну безпеку приміщень, будівель підприємства [18].

Класифікація загроз може бути проведена за безліччю ознак. Найбільш поширені з них наведені в таблиці 2.2 [17].

Таблиця 2.2

Класифікація загроз інформаційній безпеці

Критерій	**Види загроз**
За походженням	антропогенні; техногенні; природні
За видом властивості інформації, що порушується	загрози конфіденційності (витік, перехват, зняття, копіювання, викрадання, розголошення); загрози цілісності (втрата, знищення, модифікація); загрози доступності (блокування)
За характером порушення	порушення конфіденційності даних; порушення працездатності серверів, мережевого обладнання, робочих станцій; незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій, тощо
За тяжкістю порушення	незначні помилки; дрібне хуліганство; серйозний злочин; природні і техногенні катастрофи
За мотивами порушника	умисне порушення; ненавмисне порушення
За мотивацією	зловмисне порушення; незловмисне порушення
За закінченістю	закінчені; незакінчені
За причиною виникнення	загрози, які виникли через недостачу засобів технічного захисту; загрози, які виникли через недостачу організаційних заходів
За розміром нанесеної шкоди	незначні; значні; критичні
За типовими об’єктами інформатизації	загрози безпеці інформації на базі автономної ЕОМ (без підключення до обчислювальної мережі); загрози безпеці інформації на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі); загрози безпеці інформації для СУ, підключеної до розподіленої обчислювальної мережі;

Продовження таблиці 2.2

Критерій	Види загроз
За об’єктом дії	загрози, націлені на всю інформаційну систему; загрози, націлені на окремі компоненти АСУ
За способом реалізації загроз безпеці інформації	1) загрози спеціальної дії на інформацію: механічної; хімічної; акустичної; біологічної; радіаційної; термічної; електромагнітної (електричні імпульси, електромагнітні випромінювання, магнітне поле); 2) загрози не санкціонованого доступу в системи управління критичної інфраструктури; 3) загрози витоку інформації технічними каналами; (по радіоканалу; електричному каналу; оптичному каналу; по змішаним (параметричним) каналам.

Класифікація загроз несанкціонованого доступу в системи критичної інфраструктури може бути проведена за ознаками, які наведені у таблиці 2.3.

Таблиця 2.3

Класифікація загроз несанкціонованого доступу

Критерій	Види загроз
За джерелом загрози	1) створені порушником: внутрішнім; зовнішнім; 2) створені апаратною закладкою: вбудованою; автономною; 3) створені шкідливими програмами: програмні закладки типу «Троянський кінь»; програмні віруси; шкідливі програми, що поширюються мережею (мережеві черви); інші шкідливі програми для здійснення НСД;

Продовження таблиці 2.3

Критерій	**Види загрози**
За використаною вразливістю системи	1) з використанням вразливості ПЗ; 2) з використанням вразливості, викликаної наявністю апаратної вкладки в СУ КСІІ; 3) з використанням вразливості, пов’язаної з реалізацією протоколів мережевої взаємодії і каналів передачі даних; 4) з використанням вразливості, викликаної недоліками технічного захисту інформації від НСД; 5) з використанням вразливості системи захисту інформації; 6) з використанням вразливості програмно-апаратних засобів при збоях і позаштатних ситуаціях
За об’єктом взаємодії	1) НСД до інформації, яка обробляється на ЕОМ (вузли обчислювальної мережі): на відчужених носіях інформації; на вбудованих носіях довготривалого зберігання; у засобах обробки і зберігання оперативної інформації; у засобах (портах) вводу (виводу) інформації
	2) НСД до інформації залежно від її рівня мережевої взаємодії: на фізичному рівні; на канальному рівні; на мережевому рівні; на транспортному рівні; на сеансовому рівні; на презентаційному рівні; на прикладному рівні
	3) НСД до інформації користувачів або технологічної інформації залежно від способу доступу: загрози НСД до операційного середовища (до команд, інструкцій); загрози дії на технологічну інформацію, не пов’язані з допуском порушника до команд операційної системи (відмова в обслуговуванні при перевантаженні, збій операційної системи); загрози програмно-математичної дії

Отже, система забезпечення інформаційної безпеки підприємства розглядається як цілісний комплекс прийнятих управлінських рішень, спрямованих на виявлення і запобігання інформаційним загрозам. Ефективність вжитих заходів ґрунтується на визначенні таких факторів як ступінь і характер загрози, аналітична оцінка кризової ситуації і розгляд інших несприятливих моментів, які становлять небезпеку для розвитку підприємства, і досягнення поставлених цілей [19].

2.3 Засади виявлення і реагування на загрози інформаційній безпеці підприємства

Наведемо спрощену класифікацію, яка відображає найбільш типові атаки на розподілені автоматизовані системи. Цю класифікацію було запропоновано Пітером Меллом (Peter Mell) [20].

Віддалене проникнення. Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. Приклади програм, що реалізують цей тип атак: NetBus, BackOrifice.

Локальне проникнення. Атаки, що призводять до отримання несанкціонованого доступу до вузлів, на яких вони ініційовані. Приклад програми, що реалізує цей тип атак: GetAdmin.

Віддалена відмова в обслуговуванні. Атаки, що дають можливість порушити функціонування системи або перенавантажити комп'ютер через мережу (зокрема, через Інтернет). Приклади атак цього типу: Teardrop, trinOO.

Локальна відмова в обслуговуванні. Атаки, що дають змогу порушити функціонування системи або перенавантажити комп'ютер, на якому їх ініційовано. Приклади атак цього типу: аплет, який перенавантажує процесор (наприклад, відкривши багато вікон великого розміру), що унеможливлює оброблення запитів інших програм.

Класифікація атак (за способом здійснення)

Сканування мережі. Аналіз топології мережі та активних сервісів, доступних для атаки. Атака може бути здійснена за допомогою службового програмного забезпечення, наприклад за допомогою утиліти nmap.

Використання сканерів вразливостей. Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Такі сканери системні адміністратори застосовують як діагностичні інструменти, але їх також можна використовувати для розвідки та здійснення атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus.

Злам паролів. Для цього використовують програмні засоби, що добирають паролі користувачів. Залежно від надійності системи зберігання паролів, застосовують методи зламу або підбору пароля за словником. Приклади програмних засобів: LOphtCrack для Windows і Crack для UNIX.

Методика класифікації загроз STRIDE. Методика STRIDE розроблена, обґрунтована та активно пропагується фахівцями з корпорації Майкрософт. Фактично, це ще один варіант класифікації загроз за їхніми наслідками. Методику використовують для побудови моделі загроз під час розроблення ПЗ. Назву методики утворено з перших літер назв категорій загроз.

Підміна об'єктів. Крім згаданих вище загроз, які виникають через недоліки мережних протоколів, до цього класу належить також загроза, викликана підміною особи користувача, її здійснюють, скориставшись слабкістю системи автентифікації або здобувши автентифікаційні дані шляхом крадіжки чи шахрайства (так звана соціальна інженерія).

Модифікація даних. До цього класу належать загрози впливів (атак), мета яких — навмисне псування даних. Атаки можуть бути спрямовані на інформаційні об'єкти, що перебувають у стані зберігання (файли, бази даних), і такі, що передаються мережею.

Відмова від авторства. Загрози цього класу дають змогу порушнику відмовитися від здійснених ним дій (або бездіяльності). Причиною існування

такої загрози є відсутність або слабкість механізмів реєстрації подій і слабкі механізми автентифікації.

Розголошення інформації. Загрози цього класу не потребують коментарів.

Відмова в обслуговуванні. Ми вже обговорювали загрози цього класу. Атаки, що спричиняють відмову в обслуговуванні, порівняно легко здійснити в розподілених системах і дуже важко їм протидіяти. Особливо небезпечними є атаки розподіленої відмови в обслуговуванні (DDoS), які здійснюють на один об'єкт одразу з кількох вузлів мережі.

Перевищення привілеїв. До цього класу належать загрози, які дають можливість порушнику підвищити свої привілеї у системі. Наприклад, звичайний користувач отримує повноваження адміністратора, або порушник, що підключився без автентифікації до будь-якого мережного сервісу, виконує дії як авторизований користувач.

Моніторинг усіх подій у корпоративній мережі відіграє важливу роль для кожної компанії. Будь-які події що описані вище, відслідковуються та відбуваються на робочих станціях, серверах, маршрутизаторах, комутаторах та інших об’єктах інфраструктури у мережі підприємства створюють журнали подій, які швидко перетворюються у великі об’єми даних для аналізу.

Неминучим є ряд певних подій, які можуть спричинити негативні наслідки для безпеки компанії, проте не кожна небажана подія потребує розгляду повною командою реагування на загрози й інциденти інформаційної безпеки. У таких випадках велику роль в управлінні ресурсами та часом, які доступні для корпоративної IT-безпеки, відіграють автоматизовані процеси реагування. Тому часто достатньо одного IT-адміністратора, який має базові інструменти реагування, щоб успішно уникнути небезпеки від небажаної події.

Однак, у випадку виявлення більш підступної схеми та намірів скористатися поодинокими небажаними подіями або у разі раптового збою

системи, ймовірно, відбулася кібератака та без сумніву необхідне звернення до команди реагування на інциденти інформаційної безпеки. На підприємстві має бути план дій для таких випадків та ефективна команда реагування на інциденти, то такі кібератаки не стануть проблемою для підприємства.

Системна і якісна діяльність з виявлення загроз і обробки інцидентів інформаційної безпеки може допомогти компанії забезпечити успішне повернення до звичайних бізнес-операцій. Основні кроки виявлення та протидії загрозам інформаційної безпеки представлені на рис. 2.4 [21].

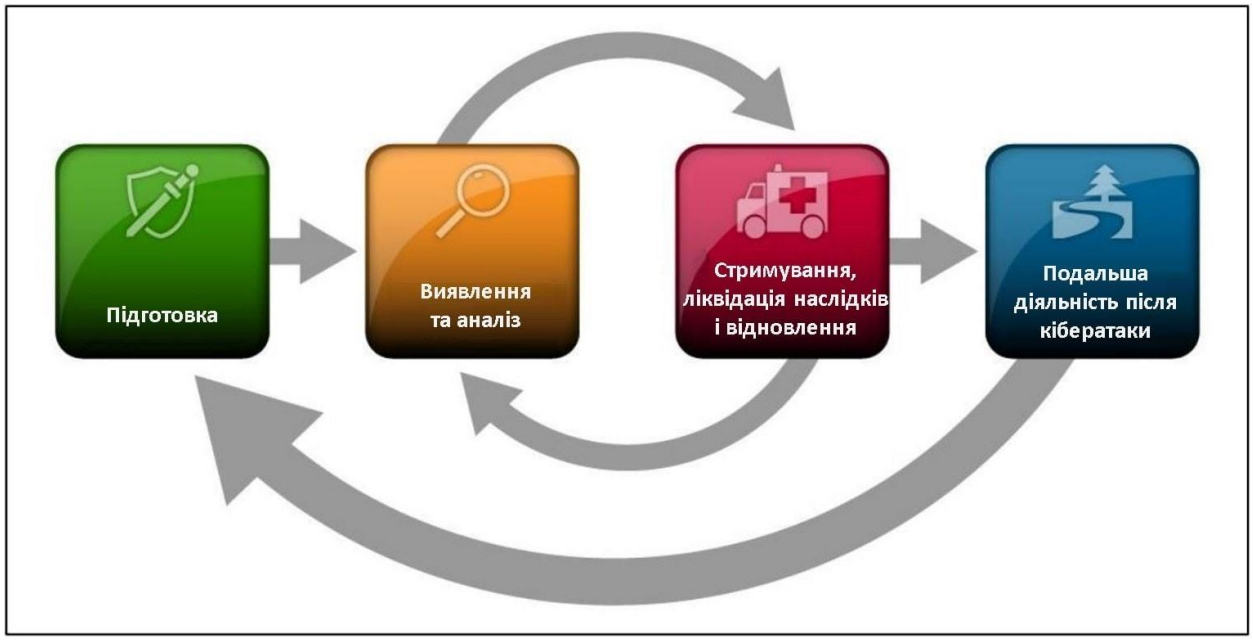

Рис 2.4. Основні кроки виявлення та реагування на загрози інформаційній безпеці

Розглянемо дії в межах наведених кроків детальніше.

1 Крок. Підготовка

Перш ніж реалізується загроза інформаційній безпеці і станеться інцидент, важливо встановити належні заходи безпеки для зменшення ризиків інфікування вже відомими загрозами. Зокрема, це оновлення серверів, операційних систем та додатків до актуальних версій, налаштування посиленого захисту від шкідливих програм. Також корпоративна мережа має бути захищена через брандмауери і VPN. Крім цього, варто не забувати про покращення обізнаності співробітників у галузі

інформаційної безпеки для зменшення кількості інцидентів, оскільки саме вони часто піддаються на маніпуляції хакерів.

Важливою частиною налаштування мережі є наявність всіх необхідних інструментів моніторингу та введення журналів для збору та аналізу подій у внутрішній мережі. Доступні різні варіанти: інструменти віддаленого моніторингу та управління (RMM), інструменти управління інформаційною безпекою та подіями безпеки (SIEM), інструменти організації та автоматизації процесів реагування на інциденти безпеки (SOAR), системи виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS), а також рішення для виявлення та реагування на події безпеки на робочих станціях (EDR).

Ще одним важливим кроком є створення та навчання команди реагування на інциденти інформаційної безпеки відповідно до вимог підприємства. Компанії малого бізнесу можуть створити тимчасову команду, яка буде складатися з існуючих IT-адміністраторів. Однак організації більших розмірів повинні мати постійну команду, яка буде залучати інших IT-адміністраторів компанії виключно для допомоги в певних атаках, наприклад, адміністратора бази даних, щоб допомогти проаналізувати атаку типу SQL injection.

Альтернативою є залучення команди реагування на інциденти інформаційної безпеки на аутсорсингу, хоча це може коштувати дорожче. Якщо розглядати варіант аутсорсингу, треба бути готовим до більш тривалого часу для реагування. Деяких членів команди реагування на інциденти, можливо, доведеться чекати з інших регіонів, що значно збільшує час для впливу загроз на мережу підприємства.

Найголовніше, що у складі будь-якої команди повинні бути співробітники, які розуміють, як саме будується корпоративна мережа, що є нормальним для неї, а що - незвичним.

Керівництво також має відігравати активну роль, зокрема надавати необхідні ресурси та засоби для ефективного виконання роботи команди реагування на інциденти. Це означає забезпечення інструментами та

пристроями, які необхідні команді реагування, а також прийняття жорстких управлінських рішень стосовно інциденту.

Команда реагування на інциденти інформаційної безпеки виявляє компрометацію сервера електронної комерції, що є важливим елементом введення бізнесу, та потребує його відключення. Керівництво компанії має швидко зрозуміти вплив на бізнес-процеси у разі відключення або ізоляції сервера та повідомити команду реагування на інциденти.

Інші співробітники і відділи компанії також надають важливу підтримку команді реагування. IT-спеціалісти можуть допомогти вимкнути і замінити сервери, відновити дані з резервних копій та очистити систему відповідно до вимог команди. Юристи та відділ зі зв'язків з громадськістю необхідні для управління будь-якими комунікаціями щодо інциденту, наприклад, зі ЗМІ, партнерами, клієнтами та правоохоронними органами.

2 Крок. Виявлення та аналіз

На цьому етапі аналітики за допомогою своїх знань та потрібних інструментів мають виявити, що відбувається в мережі та яких заходів потрібно вжити. Завдання аналітика — співставити події, щоб відтворити їх послідовність до моменту інфікування, та визначити основну причину, щоб якомога швидше перейти до дій етапу 3.

Однак, як показано на схемі вище, 2 та 3 етапи мають циклічний характер, що означає реагування на інциденти може переключитися назад на другий етап для проведення подальшого аналізу причин. Наприклад, знаходження і аналіз деяких даних на етапі 2 призводить до необхідності вжити конкретних заходів щодо пом'якшення наслідків на етапі 3. Потім на 3 етапі можуть виявитися певні додаткові дані, які потребують аналізу, тобто перехід до етапу 2.

Варто зазначити, що інструменти для виявлення та відслідковування подій на робочих станціях дозволяють автоматично визначити підозрілу активність, дослідити та миттєво відреагувати на інцидент інформаційної безпеки, що допомагає спеціалістам на 2 етапі.

3 Крок. Стримування, ліквідація наслідків і відновлення

На 3 етапі команда реагування на інциденти інформаційної безпеки повинна прийняти рішення з метою уникнення поширення виявлених загроз, наприклад, відключення сервера, ізоляція робочої станції або припинення використання деяких сервісів. Обрана стратегія стримування має враховувати можливу шкоду у майбутньому, зберігання доказів компрометації та тривалість стримування. Як правило, це означає ізолювати скомпрометовані системи, сегментувати частини мережі або розмістити уражені пристрої в пісочниці.

У випадку виявлення шкідливого програмного забезпечення потрібно видалити його зі скомпрометованих систем. Після цього потрібно буде відключити, закрити чи скинути облікові записи користувачів. Також слід виправити уразливості, відновити системи та файли з чистих резервних копій, змінити паролі, посилити правила брандмауера тощо.

Повне повернення до звичайних бізнес-операцій в певних випадках може зайняти місяці залежно від кібератаки. Для початку слід встановити покращену систему ведення журналів та моніторингу, щоб IT-адміністратори могли запобігти повторенню тієї ж кібератаки. У перспективі потрібно прийняти більш масштабні зміни, які допоможуть зробити корпоративну мережу безпечнішою.

4 Крок. Подальша діяльність після кібератаки

Команда реагування на інциденти інформаційної безпеки повинна фіксувати та надавати дані щодо зміни подій та їх хронологію. Це допомагає зрозуміти основну причину кібератаки та запобігти повторному чи подібному інциденту безпеки. Крім цього, всі команди мають переглянути ефективність процесів та операцій, які виконуються, виявити недоліки у спілкуванні та співпраці та знайти можливості для покращення поточного плану реагування на подібні інциденти.

Важливим моментом є визначення політики збереження доказів, зібраних під час інциденту інформаційної безпеки. Тому перед очищенням жорстких дисків доцільно звернутися до юридичного відділу. Як правило, більшість компаній зберігають записи про такі випадки протягом двох років відповідно до норм.

На мою думку, представлену вище схему виявленні реагування на загрози інформаційній безпеці доцільно використовувати на підприємствах середнього й малого бізнесу, тому що запропонований системний підхід та якісна діяльність з виявлення загроз і обробки інцидентів інформаційної безпеки може допомогти компанії забезпечити успішне повернення до звичайних бізнес-операцій.

Висновки до розділу 2

У другому розділі детально розглянуто поняття ризику та його складових: загрози і вразливості. Встановлено, що методи зниження ризиків пропорційні зниженню загроз та усуненню вразливостей, а ризик – це поєднання загрози та вразливості. Вразливість без відповідної загрози або загроза без відповідної вразливості не викликають ризику.

З’ясовано, що загроза інформаційній безпеці є сукупністю умов і факторів, що створюють ризик порушення інформаційної безпеки. Загрози ІБ класифіковано за такими основними ознаками: джерелами походження (природні, технічні, антропогенні); аспектами інформаційної безпеки (загрози конфіденційності, цілісності та доступності); розміщенням джерела загрози (внутрішні і зовнішні); наявністю злого умислу (навмисні, випадкові) тощо.

Відповідно до розробленого плану дій на випадок кібератак, основними кроками виявлення та протидії загрозам інформаційної безпеки та реагування на інциденти визначено такі: 1) підготовка; 2) виявлення та аналіз; 3)

стримування, ліквідація наслідків і відновлення; 4) подальша діяльність після кібератаки.

РОЗДІЛ 3
ОСОБЛИВОСТІ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СЕРЕДНЬОГО І МАЛОГО БІЗНЕСУ

3.1 Оцінка вразливостей та аналітичні моделі виявлення загроз інформаційній безпеці

Після впровадження усіх заходів інформаційної безпеки, важливо переконатися, що вони справді захищають систему. Як відзначено в попередньому розділі, дотримання законів, стандартів, рекомендацій і постанов ще не означає, що задіяно якісне забезпечення інформаційної безпеки. Світ динамічно змінюється і сфера інформаційної безпеки змінюється разом з ним, це означає, що зловмисники, які також володіють знаннями про стандартні засоби захисту, шукають нестандартні шляхи їх подолання.

Для виявлення реального рівня інформаційної безпеки підприємства є два методи: оцінка вразливості й тестування на проникнення [22].

Оцінка вразливостей. При оцінці вразливостей використовують спеціально розроблені інструменти для пошуку вразливостей – сканери вразливостей. Прикладом таких сканерів можуть служити два популярні інструменти оцінки вразливості – Qualys (https://www.qualys.com) і Nessus (https://www.tenable.com/products/nessus). Щоб створити ці інструменти, постачальники виконують величезну роботу зі збору й каталогізації відомих вразливостей, в рамках каталогу вразливості групуються за платформою, механізмом роботи та ступенем небезпеки. Найбільш цінним, у цій діяльності

є той факт, що бази даних вразливостей систематично оновлюються, тобто мають актуальний стан, також постачальники цих інструментів часто надають додаткову інформацію про особливості вразливості, способи її усунення тощо.

Вразливості постійно змінюються, постачальникам необхідно постійно стежити за цими змінами і виправленнями, появою нових варіантів вразливостей і за безліччю інших чинників, що постійно змінюються. Без постійних оновлень ці інструменти швидко втрачають свою корисність і здатність виявляти нові вразливості або надавати точну інформацію. Але навіть при цьому, результати оцінки вразливості не є запорукою надійності захисту: оцінка може виявити лише відомі на поточний час вразливості, а не вразливості взагалі.

Відображення та виявлення. Щоб сканувати вразливості, потрібно знати, які пристрої є у корпоративному середовищі. Зазвичай потрібно виконувати сканування груп або діапазон хостів, які згодом змінюються. Якщо в компанії немає можливості підтримувати актуальність списків хостів, є ризик отримати неповні результати сканування або взагалі просканувати неправильні хости. Особливо ця проблема зачіпає хости, розташовані у хмарі.

Відображення середовища. Роботу зі сканування вразливостей починають із створення карти середовища, на якій буде видно, які пристрої є в мережі. Більшість інструментів сканування вразливостей дозволяють безпосередньо створювати таку карту, і іноді можна імпортувати інформацію про хост з інструментів, створених спеціально з цією метою, на зразок Nmap (https://nmap.org/).

Часто інструменти створюють такі карти, опитуючи кожну окрему IP-адресу в діапазоні мережі, для якої збудована картка. Для великих діапазонів адрес у мережі це може тривати багато часу, а за цей час може з'явитися та зникнути якийсь хост. Наприклад, внутрішня мережа класу A, зазвичай розпізнається IP-адресами в діапазоні від 10.0.0.0 до 10.255.255.255, може містити понад 16 мільйонів IP-адрес. Інша поширена схема внутрішньої мережі, мережа класу B, у якій зазвичай використовуються IP-адреси типу

192.168.0.0, може містити більше 65 000 хостів. У середовищі для цілей сегментації нерідко використовуються мережі класу A та кілька мереж класу B [23].

Оскільки більшості інструментів для опитування кожної IP-адреси потрібно кілька секунд, весь процес може зайняти багато часу.

Якщо сканування буде надто швидко, це також може створити навантаження на мережну інфраструктуру. Під час відображення мережі можуть бути перевантажені мережні пристрої, такі як маршрутизатори, і в результаті вони взагалі можуть перестати відповідати.

Відкриття нових хостів. Крім відображення, яке допомагає з'ясувати, що знаходиться на хості, також необхідно оновлювати списки хостів. Якщо розташування нових пристроїв у корпоративних мережах відоме, компанія може переглянути саме ці місця, але може пропустити деякі хости, якщо вони не там, де очікується, особливо якщо вони були навмисно приховані [24].

Нові хости шукають активно чи пасивно:

− Активне виявлення — це процес, аналогічний відображенню мережі: для цього необхідно перейти за IP-адресою і опитати кожну з них, щоб дізнатися, чи наявна відповідь. Тут є ті ж проблеми, що й у відображення, але можна виконувати оновлення тільки в тих частинах мережі, де є нові пристрої. У цьому випадку прохід через мережу буде виконуватися швидше та з більш короткими інтервалами.

− Пасивне виявлення – часто пов'язане з розміщенням пристрою (маршрутизатора або комутатора) у вузьких точках мережі з метою моніторингу трафіку, що проходить через корпоративну інфраструктури. Таким чином, можна автоматично виявити пристрої, коли вони починають спілкуватися в мережі, й автоматично додавати їх у списки хостів для сканування.

Сканування. Як тільки фахівці отримують інформацію про хости компанії, вони можуть просканувати їх на наявність вразливостей. Можна

виконувати кілька сканувань різних типів, а використовувати для кожного з них різні способи:

− *сканування без автентифікації*. Найпростіше сканування хоста на вразливості – це зовнішнє сканування без автентифікації. Для такого сканування не потрібно жодних облікових даних для сканованого хоста або будь-якого доступу, крім мережевого підключення до хоста. Метод дозволяє сканувати практично будь-який пристрій. Залежно від налаштувань сканування він часто показує, які порти на хості, що розглядається, відкриті, виявляє служби, які прослуховують ці порти, та визначає встановлені програми та операційну систему на основі іншої зібраної інформації.

− *Сканування з автентифікацією*. Можна також сканувати вузли з автентифікацією. У цьому випадку сканування проводиться з використанням дійсного для сканованої системи набору облікових даних, зазвичай з правами адміністратора. Наявність облікових даних для входу на хост дозволяє збирати внутрішню інформацію (встановлене ПЗ, вміст файлів конфігурації, дозволи для файлів і каталогів, виправлення вразливостей, які необхідні системі, але яких на даний час немає, та іншу інформацію. Це дає більш повне уявлення про пристрій та його потенційні вразливості, ніж зовні. Таким чином, можна створити значно точнішу картину безпеки пристрою. Сканування з автентичністю вимагає, щоб ваші облікові дані для автентифікації були актуальними як на стороні інструменту сканування вразливостей, і на самих хостах. Для деяких перевірок також буде потрібний адміністративний доступ до пристрою, і не всі адміністратори систем погодяться надати вам облікові записи з таким широким рівнем доступу.

− *Агентне сканування*. Агентне сканування дозволяє уникнути деяких недоліків сканування з автентифікацією. Агент – це невеликий програмний продукт, встановлений кожному хості. ПЗ працює так, якби воно було користувачем у системі, тому воно відразу буде автентифіковане, але не потребує окремого набору облікових записів на пристрої або в інструменті пошуку вразливостей. Ще однією перевагою використання агентів є те, що

хости, налаштовані з їх допомогою, зазвичай самостійно передають звіти керуючим пристроям, що усуває потребу в індивідуальному пошуку пристроїв у ваших мережах. Метод не усуває необхідність пошуку повністю, тому що деякі пристрої не дозволяють запустити агент, проте він повинен полегшити вашу роботу, оскільки майже всі пристрої, які відобразяться, повинні ідентифікувати себе автоматично.

− *Сканування програмних додатків*. Деякі інструменти дозволяють сканувати певні програми. Є добре розроблені сканери, призначені виключно для сканування веб-застосунків. Ці типи сканування специфічні для веб-технологій та вразливостей і можуть значно глибше шукати проблеми в додатку, ніж сканування, призначене безпосередньо для хостів. Найчастіше сканери веб-застосунків є одними з найбільш якісно розроблених сканерів вразливостей, і дійсно існує безліч сканерів, призначених лише цієї конкретної мети. Один з поширених таких сканерів - Burp Suite (https://portswigger.net/burp/) який відмінно підходить як для автоматичного, так і ручного тестування веб-додатків.

Вразливості нульового дня. Варто пам’ятати, що навіть якщо зловмисник просканує систему і не знайде жодних відомих вразливостей, він матиме змогу отримати доступ до неї за умови виявлення нової, ще невідомої вразливості, так званої вразливості нульового дня.

Пошук вразливості нульового дня часто починається з виявлення помилки у коді програмного забезпечення. Виявивши таку помилку, хакер може використати її у своїх інтересах, наприклад для крадіжки даних, порушення роботи додатків або отримання контролю за системою [25].

Для відповіді на запитання щодо методів виявлення хакерами таких помилок допоможуть наявні дослідження, зокрема в роботі [26] приведено опис знаходження та експлуатації вразливості Heartbleed (CVE-2014-0160). Це помилка типу buffer over-read у криптографічному програмному забезпеченні OpenSSL, що дозволяє несанкціоновано читати пам'ять на сервері чи клієнті, зокрема для вилучення закритого ключа сервера.

Інформація про вразливість була опублікована у квітні 2014 року, помилка існувала з кінця 2011 року. На момент оголошення про помилку кількість вразливих веб-сайтів оцінювалася в півмільйона, а це становило близько 17% захищених веб-сайтів Інтернету.

У день виявлення вразливості TOR Project випустив повідомлення, яке радило усім бажаючим «надійної анонімності чи приватності в Інтернеті» «триматися подалі від Інтернету кілька днів, доки все не владнається». Власники сайтів і платформ порадили своїм користувачам змінити паролі [27].

Інтернет-платформи системно займаються виявленням вразливостей у своїх системах [28]. Так, у Google є ціла команда, яка займається пошуком уразливостей нульового дня у рамках проекту Project Zero. Вона публікує дані про виявлені вразливості у своєму блозі на https://googleprojectzero.blogspot.com/

Обговоримо низку інструментів та методів, які зловмисники та фахівці з інформаційної безпеки використовують для виявлення таких помилок як Heartbleed (див. таблицю 3.1).

Таблиця 3.1

Методи виявлення вразливостей нульового дня

Технологія	**Коротка характеристика**
Фазинг	Полягає у генеруванні різних варіантів вхідних даних для перевірки реакцій програми з метою виявити ті, які можуть викликати її збій чи змусити її діяти у невластивий спосіб. Вперше цей метод був запропонований в 1988 Б.Міллером, професором Вісконсінського університету. З того часу такі компанії, як Google та Microsoft, розробили власні фазери й використовують цю техніку для тестування своїх систем.
Символьне виконання	Дозволяє використовувати символи замість реальних даних для статичного аналізу програми. У ході цього процесу досліджуються шляхи виконання коду і складаються їх рівняння у вигляді деревоподібного графу, вирішення яких дозволяє визначити, коли буде

	обрано ту чи іншу гілку. Щоб програмно вирішити цю систему, використовується засіб доказу теорем.
Динамічний символьне виконання (Dynamic Symbolic Execution, DSE)	Поєднує методи динамічного тестування, такі як фазинг, з деякими аспектами символьного виконання. Крім символьних змінних та обмежень шляху, DSE відстежує конкретні значення, надані програмі як вхідні дані, та досліджує весь шлях, який проходять ці конкретні змінні. Обмеження шляху, які є результатом цього дослідження, потім використовуються для створення нових конкретних змінних, застосовуваних для дослідження нових шляхів.

Наведена вище процедура автоматичного виявлення вразливостей є складною, вимагає значних інтелектуальних ресурсів для розробки відповідного інструментарію та обчислювальних ресурсів для роботи. Використання подібних технологій є обґрунтованим для крупних IT-компаній або для спеціалізованих компаній, які надають відповідні послуги за контрактом. Для забезпечення безпеки інформаційних систем підприємств середнього і малого бізнесу розробка або експлуатація подібних систем, на мою думку, є економічно невигідною.

Тестування на проникнення. Тестування на проникнення (*пентестинг* або *етичний злом)* – це процес тестування системи на наявність вразливостей, які може використати зловмисник [29]. Тестування на проникнення – це набагато глибший процес, ніж сканування вразливостей, і в більшості випадків він не піддається автоматизації, тому часто виконується вручну.

Мета тестування на проникнення - знайти вразливості, щоб виправити їх до того, як їх виявить зловмисник. У тестах на проникнення використовуються ті ж самі інструменти й методи, які використовують реальні хакери. У табл. 3.2. дано пояснення особливостей діяльності хакерів трьох видів.

Таблиця 3.2

Деякі особливості тлумачення терміну «хакер»

Тип хакерів	Характеристика діяльності
Black Hat	зловмисники, які мають глибокі знання в області інформаційної безпеки, але використовують їх з метою розкрадання і псування даних.
Grey Hat	фахівці, які забезпечують безпеку, але здатні за ситуацією виконати компрометацію системи без дозволу (в цьому випадку також стають зловмисниками).
White Hat (пентестери або етичні хакери)	фахівці в галузі інформаційної безпеки (ентузіасти, співробітники компаній), мета яких – захистити IT-систему від зловмисників.

Слід зауважити, щоб будь-які тести на проникнення, проведені без відповідного дозволу вповноважених осіб компанії щодо корпоративних активів, будуть вважатися актом кіберзлочинності і матимуть відповідні правові наслідки.

Поняття червоної та синьої команди (Red/Blue Team) не є новим. Початкова концепція була введена під час Першої світової війни та, як і багато термінів, що використовуються в інформаційній безпеці, з'явилася у військовій сфері. Загальна ідея полягала в тому, щоб продемонструвати ефективність нападу за допомогою симуляції: коли червона команда грає роль зловмисника, оцінюючи безпеку систем організації настільки реалістично, наскільки це можливо, з урахуванням необхідної безпеки та розумності тесту, а синя відповідно їй протистоїть [30].

Червона команда має складатися з висококваліфікованих фахівців з різними наборами навичок, причому вони мають бути повністю обізнані про існуючий ландшафт загроз для організації. Команда має бути в курсі тенденцій, а також їй потрібно розуміти, як відбуваються поточні атаки. У деяких обставинах і залежно від вимог організації члени червоної команди повинні мати навички кодування, щоб створити свій власний експлойт і

налаштувати його для більш ефективної експлуатації відповідних вразливостей, які можуть стосуватися організації.

Червона команда повинна провести тестування на проникнення шляхом реалізації атаки на систему і проникнення у середовище, намагаючись прорвати поточні засоби захисту. Мета місії – знайти вразливість та експлуатувати їх для отримання доступу до ресурсів компанії.

Результати тестування на проникнення тобто ефективність роботи червоної команди, або ефективність системи захисту протистояти її роботі оцінюється наступними показниками:

− *середній час компрометації* (відлік починається з моменту, коли червона команда розпочала атаку, до того моменту, коли вона змогла успішно скомпрометувати об'єкт);

− *середній час підвищення привілеїв* (починається в тій же точці, що й попередній показник, але йде до моменту повної компрометації, і саме в цей момент червона команда отримує адміністративні привілеї в системі.

Синій команді необхідно забезпечити безпеку ресурсів, і в тому випадку, якщо червона команда виявить вразливість і її експлуатуватиме, їй потрібно швидко виправити цей факт і задокументувати як частину висновків.

Нижче наведено задачі, які виконує синя команда, коли зловмисник (у даному випадку - червона команда) може скомпрометувати систему:

− збереження доказів (реальна інформація про інцидент необхідна для аналізу, раціоналізації та вживання заходів щодо нейтралізації загроз у майбутньому);

− перевірка доказів (не кожне окреме оповіщення, або в даному випадку доказ, призведе вас до дійсної спроби зламати систему. Але якщо це станеться, необхідно каталогізувати це як індикатор компрометації);

− сортування за інцидентом (іноді синій команді може знадобитися сприяння правоохоронних органів або офіційний дозвіл для проведення

подальшого розслідування, правильне сортування допоможе у цьому процесі);

− створення плану виправлення (синя команда повинна скласти план виправлення, щоб ізолювати чи блокувати противника);

− виконання плану (після того як план буде готовий, Синій команді необхідно здійснити його та виконати відновлення після порушення.

Діяльність синьої команди також відображається у відповідних показниках, а саме:

− розрахунковий час до виявлення;

− розрахунковий час до відновлення.

Робота синьої та червоної команд не закінчується, якщо першій вдається скомпрометувати систему. Повинен бути створений остаточний спільний звіт, який відображає деталі щодо того, як сталося порушення, надає документований графік атаки, подробиці вразливостей, які зазнали експлуатації на отримання доступу до перевищення привілеїв (якщо це мало місце), та визначає рівень впливу на бізнес компанії.

Процес тестування на проникнення виконується за стандартним сценарієм: визначення обсягу, розвідка, виявлення, експлуатація та звітність (Рис. 3.1).

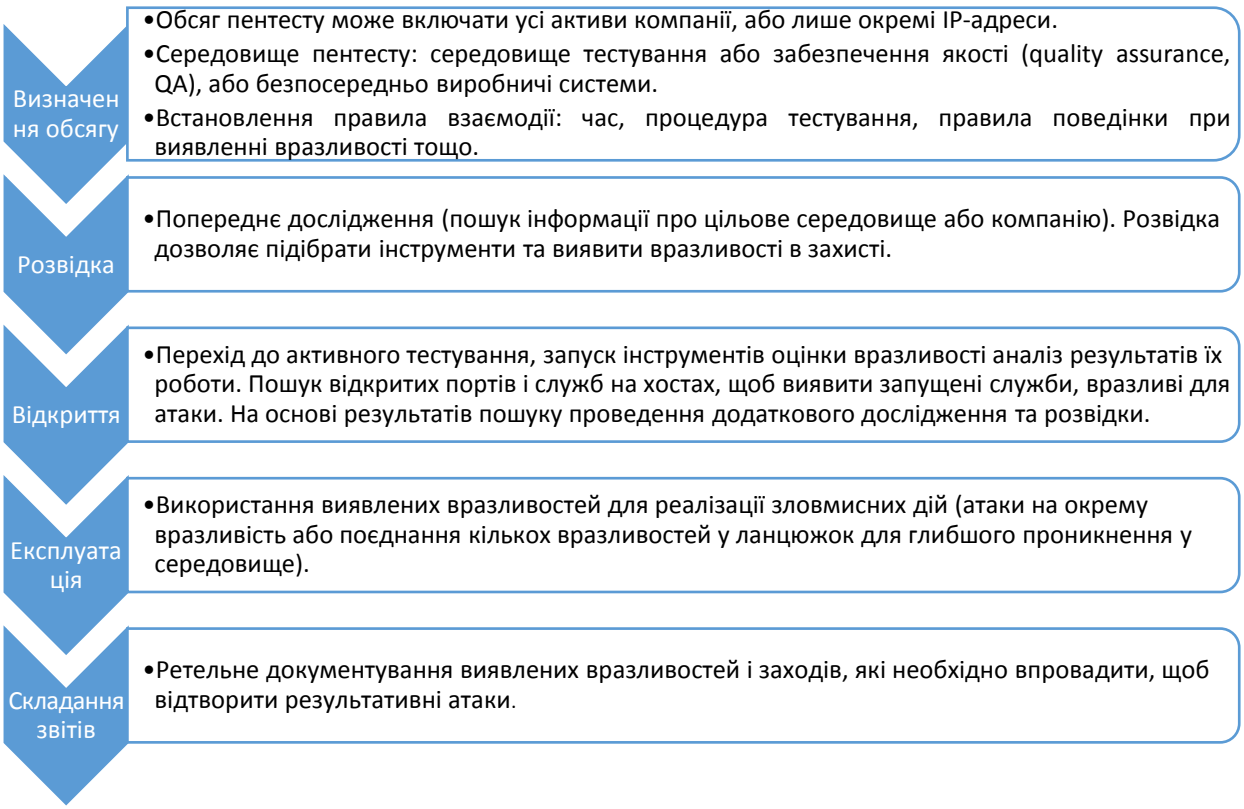

Рис. 3.1. Схема процесу тестування на проникнення.

Класифікація методів тестування на проникнення. Виконуючи тестування, можна підійти до тесту з різним рівнем знань про середовище, з різних стартових позицій чи з різними командами, які виконують конкретні частини тесту.

Методи тестування за рівнем знань про середовище або рівнем непрозорості (рівень інформації, яку тестер дає про середовище, яке підлягає тестуванню) поділяються на три типи [31]:

– Чорна скринька. При тестуванні методом чорної скриньки тестувальник нічого не знає про середовище, крім області тестування. Це схоже на реальну атаку, оскільки зовнішній зловмисник, ймовірно, почне з цього ж місця;

– Біла скринька. У тестування методом білої скриньки тестеру дають усю доступну інформацію про середовище. Швидше за все, він також отримує список усіх хостів, інформацію про ПЗ, вихідний код додатків і веб-сайтів тощо. Це не реалістична атака, оскільки у зловмисника навряд чи буде доступ до такої інформації, але вона дозволяє тестувальнику більш ретельно

зробити свою роботу й виявити проблеми, які в іншому випадку залишилися б непоміченими.

− Сіра скринька. Тестування методом сірої скриньки є комбінацією вже згаданих типів тестування. У цьому випадку тестеру надається деяка внутрішня інформація про середовище, але не в такому обсязі, як у випадку з білою скринькою. Цей один із найпоширеніших типів пентестів.

За рівнем доступу, який має тестер в середовищі, що тестується, тести поділяються на:

− внутрішні тести – якщо тестери перебувають у тій самій мережі, що й середовище, фізично або через підключення до віртуальної приватної мережі (VPN);

− зовнішні тести – якщо компанія дає пентестеру доступ до середовища тільки з її частин, що виходять в Інтернет.

Також існує аналогічна за назвою класифікація, коли терміни «внутрішній» та «зовнішній» вказують на те, яка людина чи команда проводять пентест. Зовнішнє тестування може відноситися до сторонньої компанії, найнятої для виконання пентесту, в той час як внутрішнє тестування, швидше за все, відноситься до команди, що працює в компанії.

Оцінка вразливостей та пентестинг. Ключовою відмінність між оцінкою вразливості й пентестингом є той факт, що хоча оцінка вразливості дозволяє отримати список потенційних вразливостей у середовищі, інструменти не можуть гарантувати, що зловмисник справді зможе їх використати. При пентестингу тестер повідомлятиме лише про проблеми, що призвели до реальних атак на систему або мали високі шанси на реалізацію [32].

3.2 Методика активного виявлення інформаційних загроз

Аналітичне відстеження кіберзагроз (Cyber Threat Intelligence, CTI) та активне виявлення загроз (Threat Hunting, TH) – є одними з найбільш популярних сучасних технологій забезпечення інформаційної безпеки. CTI та

TH – це процеси та методи, тісно пов'язані з традиційними процедурами безпеки (Security Operations, SecOps), які вони доповнюють та розширюють.

Полювання на кіберзагрозу (англ. Cyber Threat Hunting) або полювання на загрозу (англ. Threat Hunting) є активною діяльністю в галузі кіберзахисту. Це - процес активного та ітеративного пошуку у мережах з метою виявлення та виділення просунутих загроз, які недосяжні для наявних рішень з безпеки. Цей підхід відрізняється від традиційних заходів з управління загрозами, таких як брандмауери, системи виявлення вторгнень IDS, ізолювання шкідливих програм (англ. malware sandbox) та системи SIEM, які, зазвичай, передбачають розслідування після попередження про можливу загрозу або коли інцидент вже стався [33].

Коли ми говоримо про CTI, ми маємо на увазі процеси збору, аналізу та обробки даних для перетворення спершу на аналітичну, а потім на оперативну інформацію та підтримку заходів щодо виявлення дій, які можуть уникнути автоматичного виявлення. Аналітичне відстеження загроз направлено на пошук дій зловмисників, які не можуть бути виявлені за допомогою традиційних засобів захисту на основі сигнатур.

В основному вони включають профілювання та виявлення характерних ознак з використанням кінцевих точок та мережевої активності. Поєднання CTI і активного виявлення загроз – це процеси виявлення методів зловмисника та визначення того, наскільки вони небезпечні для мережі, яка захищається.

На основі отриманих даних генеруються профілі та шаблони, що дозволяють визначити, коли зловмисник знову намагатиметься використовувати ці потенційно можливі методи [34].

Говорячи про виявлення загроз, важливо згадати про індикатори виявлення. Коли нові загрози виявляються у природному середовищі, вони зазвичай мають якийсь поведінковий шаблон і залишають свій слід у системі жертви. Системи виявлення збирають ці індикатори та видають оповіщення при здійсненні атаки.

Існує два типи індикаторів:

− Індикатор компрометації (Indicator of Compromise, IoC) повідомляє, що відбулася дія, і система перебуваєте в режимі реагування. Цей тип IOC здійснюється шляхом перегляду корпоративних даних із журналів транзакцій або даних SIEM. Приклади IOC включають незвичний мережевий трафік, незвичайну активність привілейованого облікового запису користувача, аномалії входу, збільшення обсягів читання бази даних, підозрілі зміни реєстру чи системного файлу, незвичайні запити DNS і веб-трафік, який демонструє аномальну поведінку. Ці типи незвичайних дій дозволяють командам адміністрування безпеки виявляти зловмисників на ранніх етапах процесу кібератаки [35].

− Індикатор занепокоєння (Indicator of Concern) дозволяє використовуючи розвідку з відкритих джерел (Open-source Intelligence, OSINT), може збирати дані з загальнодоступних джерел, щоб використовувати їх для виявлення кібератак і полювання на загрози .

Для роботи з індикаторами компанія може зареєструватися на сайті OpenIOC (http://openioc.org), щоб отримати інформацію про нові індикатори, а також зробити свій внесок у спільноту, створивши власний індикатор за допомогою IoC Editor-у, який можна завантажити за посиланням у довідковому розділі сайту.

Модель Оперативний конвеєр (Intelligence Pipeline) (Рис. 3.4) [36]. Активне виявлення загроз – це більше, ніж зіставлення наданих IOC із зібраними даними та виявлення «заздалегідь поганих» ознак. Виявлення загроз, засноване на перетворенні зібраних даних спершу на аналітичну, а потім на оперативну інформацію, цей процес відомий як *оперативний конвеєр* або канал оперативної інформації. Для обробки даних, що проходять через конвеєр, застосовують кілька перевірених аналітичних моделей, які можна використовувати, щоб зрозуміти, в яку частину інфраструктури компанії проник зловмисник, куди він рухатиметься далі і як розподілити

пріоритети та ресурси (в основному час) при виявленні загроз, щоб перешкодити зловмиснику чи повністю його зупинити.

Рис. 3.2. Схема оперативного конвеєра

Ідея оперативного конвеєра полягає в тому, що оперативна інформація не надходить ззовні, а створюється на основі даних, які отримують з власного робочого середовища.

У цій моделі події проходять через такі етапи оперативного конвеєра:

1. збір та обробка подій для перетворення їх у дані;

2. додавання контексту та збагачення даних для перетворення їх на інформацію;

3. аналітична обробка сирої інформації для перетворення її на оперативну інформацію;

4. прийняття рішень, заснованих на даних (за потреби).

Діючи в рамках компанії, фахівці, як правило, обмежені у ресурсах для збирання великих обсягів даних, необхідних для розробки оперативної інформації. Крім того, додавання контексту та збагачення в такому масштабі обходиться неймовірно дорого з погляду персоналу, технологій і капіталу. Для збору інформації та пошуку загроз першорядне значення має отримання

відповідних послуг від галузевих спільнот, спільних або спеціалізованих центрів обміну інформацією та аналізу (Information Sharing and Analysis Centers, ISAC), державних органів і постачальників.

Модель Cyber Kill Chain (компанії Lockheed Martin) [37]. Lockheed Martin – високотехнологічна компанія, один з лідерів військово-промислового комплексу США. Одним із напрямків її діяльності є розробка інструментарію для кібербезпеки. Серед іншого компанія розробила модель відгуків (response model), спрямовану на виявлення дій, які противник повинен виконати для успішного завершення вторгнення. Ця модель була однією з перших, що набули широкого поширення, і надала аналітикам, операторам та фахівцям з реагування спосіб скласти схему вторгнення супротивника. Завдяки цій схемі після виявлення будь-якої шкідливої активності можна подивитися, як далеко зайшов противник, яких дій раніше не спостерігали, і під час відновлення після інциденту зробити висновок про те, які захисні технології, процеси чи навчання необхідно застосувати у майбутньому. Кіберланцюг вбивств (Cyber Kill Chain) – це високорівнева модель, яка використовується для ілюстрації дії зловмисника.

Модель Kill Chain складається із семи етапів: розвідка; озброєння; доставка; використання вразливості; встановлення; управління та контроль; дії щодо досягнення мети (рис 3.3).

Рис. 3.3. Схема моделі Cyber Kill Chain

Розглянемо кожен із них докладніше у таблиці 3.3.

Таблиця 3.3

Етапи моделі Cyber Kill Chain [38].

№	Назва	Пояснення
1	Розвідка (Reconnaissance)	Зловмисник складає карту своєї мети. Цей етап виконується як активно, так і пасивно за допомогою перерахування мереж і систем, профілювання соцмереж, виявлення можливих вразливостей, визначення конфігурації захисту цільової мережі та визначення цінних об'єктів в інфраструктурі організації.

Продовження таблиці 3.3

№	Назва	Пояснення
2	Озброєння (Weaponization)	Противник має вивчити арсенал своїх інструментів, тактик і методів, точно визначити, як використовуватиме інформацію, зібрану на попередньому етапі, для досягнення своїх цілей. Один із найдорожчих та найважливіших етапів.
3	Доставка (Delivery)	Зловмисник намагається проникнути в цільову мережу. Часто це робиться за допомогою фішингу (звичайного, цілеспрямованого або навіть через соцмережі). Це можна також зробити за допомогою інсайдера, спеціального обладнання або вразливості, яку використовують віддалено.
4	Використання вразливості, або експлойта (Exploitation)	Етап починається, коли зловмисник використовує лазівки у захисті (експлойти) та виконує код в системі. Це може бути застосування вразливості системи, користувача чи їх комбінації.
5	Установка (Installation)	Установка яка складається з кількох проміжних етапів, які інсталюють на цільову машину кілька дропперів (проміжних завантажувачів), що допоможуть зберегти надійну точку опори для взлому в системі, щоб зловмисник не втратив цінний фрагмент шкідливого ПЗ (backdoor або інші шкідливі файли), наприклад, у разі успішного спрацювання антивірусу.
6	Управління та контроль (Command & Control, C2)	Використовується для встановлення віддаленого доступу до впровадженого на попередньому етапі шкідливого коду. На цьому етапі зловмисник намагається зробити так, щоб його код міг уникнути виявлення та зберігався при нормальній роботі системи (перезавантаження, перевірка вразливостей та антивірусне сканування, взаємодія користувача із системою тощо).

Продовження таблиці 3.3

№	Назва	Пояснення
7	Досягнення мети (Action in Objectives)	Етап, на якому противник реалізує справжню мету свого вторгнення. Це може бути кінець вторгнення чи початок нового етапу: досягнення мети може запустити нову кампанію, яка почнеться з етапу розвідки зсередини мережі для збирання додаткової інформації та глибшого вивчення мети.

Завдання як аналітиків з кібербезпеки, операторів та фахівців з реагування – відтіснити супротивника якомога глибше в ланцюжок до такої міри, щоб вартість атаки переважила цінність успіху. Всі виявлені механізми та інструменти зловмисника, включаючи інфраструктуру, яка була використана для атаки, повинні бути блоковані або знешкоджені, інформація про незаконне або некоректне використання інструментів, які належать третій стороні, повинна бути доведена до власників та/або правоохоронних органів. Невідомі механізми та технології вторгнення, виявлені під час реагування інциденту повинні бути оприлюднені.

Матриці ATT&CK MITRE [39]. Американська корпорація MITRE виконує дослідження та розробки для кількох державних установ та фінансується з державного бюджету. MITRE зробила помітний внесок у кібербезпеку, і одне з досягнень – це серія докладних тактичних матриць, які використовуються для опису дій противника, відомих як матриці змагальної тактики, методів і загальних знань (Adversarial Tactics, Techniques and Common Knowledge, ATT&CK).

Існує три основні матриці:

1. Матриця Enterprise (корпоративна) включає тактику і прийоми, орієнтовані на підготовчі етапи (аналогічні етапам розвідки та озброєння з Lockheed Martin Cyber Kill Chain), традиційні операційні системи, системи ICS та тактику противника, націленого на мережі.

2. Матриця Mobile (мобільна) включає тактику і методи, спрямовані на виявлення дій зловмисників, націлених на мобільні операційні системи Apple iOS і Android і які реалізують проникнення за допомогою експлойтів.

3. Матриця ICS (Internet Control Server, сервер управління доступом в Інтернет) включає тактику і методи, спрямовані на виявлення дій зловмисників після проникнення через експлойт, націлених на мережу ICS.

Усі матриці побудовані на єдиній платформі MITRE, відомій як Cyber Analytics Repository (CAR), яка орієнтована виключно на аналітику зловмисних дій. Матриці ATT&CK – це абстракція, яка дозволяє переглядати аналітику з техніки та методів.

Усі матриці використовують схему угруповання тактики, методів і, у випадку матриці Enterprise, субметоди. Якщо говорити про відмінності між тактикою, методами й аналітикою, ці три елементи описують поведінку агресора у різних, але пов'язаних контекстах:

- тактика – це вищий рівень поведінки дійової особи (чого вона хоче досягти: початковий доступ, виконання коду тощо);
- методи – більш детальні і містять контекст тактики (що зловмисник збирається використовувати для досягнення своєї тактики: технології, інструментарій, методика тощо);
- аналітика – це дуже докладний опис поведінки, який включає контекст методів.

MITRE використовує 14 тактик і методів/субметодів, специфічних для матриці:[40]

1. розвідка – методи збору інформації про мету;
2. розвиток ресурсів – методи вторгнення в інфраструктуру та розвитку можливостей;
3. початковий доступ – методи, що дозволяють закріпитися в цільовому середовищі;
4. виконання – методи виконання коду в цільовому середовищі;

5. збереження доступу – методи, що забезпечують постійний доступ до цільового середовища;

6. перевищення привілеїв – методи підвищення рівня доступу в цільовому середовищі;

7. маскування й ухилення – методи, що дозволяють уникнути виявлення;

8. доступ до облікових даних – методи отримання внутрішніх/додаткових облікових даних;

9. вивчення середовища – методи отримання додаткових відомостей про цільове середовище (мережі, служби тощо);

10. розширення охоплення – методи розширення доступу за межі початкової точки входу;

11. збирання інформації про середовище – методи збору інформації або даних для наступної діяльності;

12. управління та контроль – методи управління впровадженими шкідливими об'єктами в цільовому середовищі;

13. витік даних – методи крадіжки зібраних даних із цільового середовища;

14. дія – методи відключення, погіршення, порушення або знищення активів, процесів або інших шкідливих операцій з цільовим середовищем.

Матриці MITRE ATT&CK набагато більш деталізовані, ніж Lockheed Martin Cyber Kill Chain, але це не означає, що один підхід обов'язково кращий за інший; обидва мають своє застосування. Наприклад, при складанні технічного звіту чи інструкції корисно мати можливість сказати, що тактика розвитку ресурсів противника включала певний метод розвитку його можливостей та, зокрема, експлойтів; проте якщо ваша аудиторія не має технічних знань, буде простіше заявити, що противник використав для атаки певний перелік інструментів (використовуючи Lockheed Martin Kill Chain).

Діамантова модель (The Diamond Model of Intrusion Analysis) [41] була розроблена некомерційною організацією Center for Cyber Intelligence Analysis

and Threat Research (CCIATR) у 2013 р. з метою сформувати стандартизований підхід до характеристик вторгнення, диференціювання різновидів вторгнень, відстежування їх життєвих циклів і, нарешті, розробити контрзаходи для їхнього пом'якшення.

Діамантова модель - це просте образне уявлення шести елементів, цінних для відстеження вторгнення (рис. 3.4): противник (adversary), інфраструктура (infrastructure), жертва (victim), можливості (capability), мотивація (motivation) та тактика/методи/процедури (tactics, techniques and procedures, TTP).

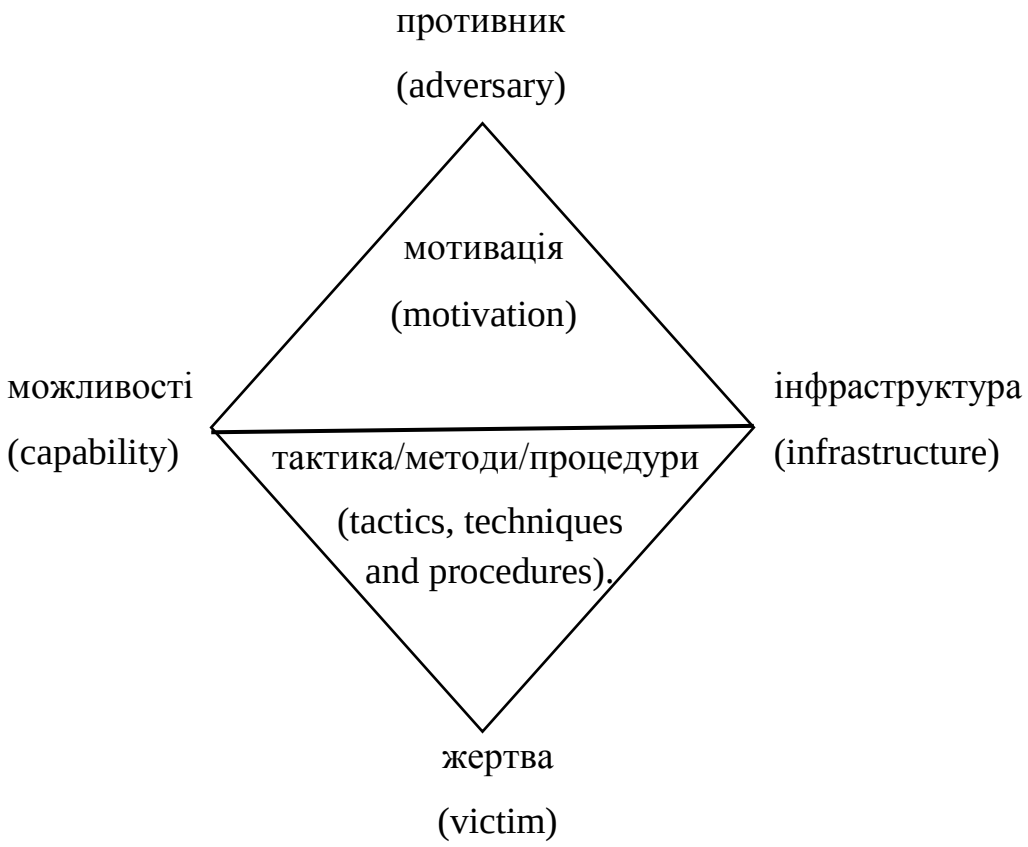

Рис. 3.4. Схема Діамантової моделі

Дамо пояснення відносно елементів моделі:

− *противник (adversary)* – елемент описує сутність, яка є суб'єктом загрози, прямо чи опосередковано причетним до вторгнення. Сюди відносяться окремі імена, організації, прізвиська, дескриптори, профілі в соціальних мережах, кодові імена, адреси (фізичні, електронна пошта тощо),

номери телефонів, роботодавці, мережеві ресурси тощо. По суті це особливі прикмети, які можна використовувати для опису зловмисника;

– *інфраструктура (infrastructure)* – елемент описує керовану зловмисником інфраструктуру, що використовується для вторгнення (IP-адреси, імена хостів, домени, адреси електронної пошти, комп'ютери, підключені до мережі тощо);

– *жертва (victim)* – елемент описує об'єкт, який є жертвою вторгнення. Він може описувати ті ж сутності, що і елемент «Противник», але в контексті ставлення жертви до противника, так що знову ж таки йдеться про конкретні імена, організації тощо. Крім контексту, сюди входять підключені до мережі ресурси жертви, якщо вони мають відношення до вторгнення, тоді як ресурси, контрольовані мережею зловмисника, можуть бути розглянуті як частина вузлів противника або інфраструктури в залежності від контексту.

– *можливості (capability)* – елемент описує можливості, доступні під час вторгнення. Безперечно, дуже добре, якщо аналітики компанії заздалегідь складуть каталог всіх можливостей, потенційно доступних зловмиснику, але загалом цей елемент описує можливості, які спостерігаються при вторгненні.

– *мотивація (motivation)* – елемент описує спонукальні мотиви зловмисників. Вони дуже важливі при описі цілей вторгнення і використовуються для опису того, як можливості та інфраструктура співвідносяться один з одним та використовуються атакуючим. Мотивація, як правило, визначається на основі шаблону MICE (гроші (Money), ідеологія (Ideology), примус (Coercion), его (Ego)).

– *тактика/методи/процедури (tactics, techniques and procedures)* - елемент описує дії та засоби досягнення мети. Може включати аналітичні здібності та алгоритмічні дії зловмисника для використання можливостей що доступні для вторгнення.

Отже, розглянуто декілька аналітичних моделей, які допомагають визначити рамки стратегічних, оперативних та тактичних операцій, чи то

аналітика, активне виявлення чи традиційні заходи SecOps. Варто відзначити важливість не тільки розуміння кожної з концепцій, але також формування загальної картини того, як вони пов'язані і яким чином кожна модель може бути накладена на іншу.

Оцінка ефективності активного виявлення загроз. Активне виявлення загроз – це комплекс заходів щодо виявлення дій зловмисників, коли автоматичний захист або виявляє підозрілі події, або, що буває частіше, не вважає їх підозрілими. Як будь-яка діяльність, активне виявлення вимог вимагає критеріїв оцінки своєї ефективності.

Існує багато комплексних технічних показників для оцінки того, наскільки успішно працює команда з кібербезпеки, але, на наш погляд, їх усі можна розділити на три групи:

1. *середній час виявлення* – скільки часу знадобилося компанії, щоб виявити загрозу.

2. *середній час відгуку* – скільки часу знадобилося компанії для відповіді на атаку з моменту виявлення.

3. *коефіцієнт рецидивів* – через який час, після того як компанія перешкодила зловмисникам, вони повертаються з новою атакою.

Існує безліч показників, пов'язаних з операціями щодо забезпечення інформаційної безпеки, але виявлення загроз і аналіз загроз, хоч і тісно пов'язані з операціями щодо забезпечення безпеки, є окремим видом діяльності й потребують окремої оцінки.

3.3 Рекомендації щодо виявлення загроз інформаційній безпеці підприємств середнього і малого бізнесу

Підприємства можуть використовувати системи управління інформаційною безпекою, щоб стандартизувати корпоративні засоби захисту, налаштовуючи спеціальні або галузеві стандарти для забезпечення інформаційної безпеки і керування ризиками. Системний підхід допоможе

ефективно захищати організацію від невиправданих ризиків і дасть команді фахівців із безпеки змогу ефективно усувати загрози щойно вони виникатимуть.

Захистити внутрішню інфраструктуру підприємства та допоможуть наступні сили та засоби, зокрема, це оновлення серверів, операційних систем та додатків до актуальних версій, налаштування посиленого захисту від шкідливих програм, оновлення сигнатур антивірусів. Також корпоративна мережа має бути захищена через брандмауери і VPN.

Основними загальновідомими недоліками процесів забезпечення інформаційної безпеки підприємств середнього і малого бізнесу (СМБ) є:[42]

- Нестача фінансових ресурсів.
- Відсутність кваліфікованих спеціалістів.
- Неможливість систематичної оцінки й коригування стану інформаційної безпеки компанії.

Ситуація у сфері безпеки СМБ посилюється відсутністю нормативів, які враховують особливості цього сектора бізнесу у сфері інформаційної безпеки. Тому доцільно вивчити закордонний досвід у цій сфері. Національним інститутом стандартів та технологій США (NIST) видано рекомендаційний документ про основи інформаційної безпеки підприємств малого та середнього бізнесу NISTIR 7621. У ньому зазначаються такі «абсолютно необхідні» дії щодо забезпечення безпеки підприємств малого та середнього бізнесу [43]:

- Захист інформації, систем чи мереж від вірусів, шпигунських програм та іншого шкідливого коду.
- Забезпечення безпеки при підключенні до Інтернету.
- Встановлення та налаштування програми засобів захисту ЕОМ.
- Своєчасне оновлення операційних систем та додатків.
- Регулярне резервне копіювання важливих для бізнесу даних та інформації.

- Розмежування фізичного доступу до комп'ютерів і мережевих комунікацій.
- Захист бездротової мережі та точки доступу.
- Навчання співробітників основним принципам забезпечення безпеки.
- Створення окремих облікових записів користувачів кожного співробітника на робочих комп'ютерах й у бізнес-додатках.
- Розмежування доступу співробітників до даних та інформації та обмеження повноважень для встановлення програмного забезпечення

Рис. 3.5. Дії що до забезпечення безпеки підприємств СМБ відповідно до NISTIR 7621

Також варто звернути увагу на те, що в даному документі особлива увага приділяється загрозам, пов'язаним із людським фактором. Якщо в рамках програмного та апаратного захисту більшістю вітчизняних підприємств СМБ вживаються хоча б мінімальні заходи, то цю частину загроз, як правило, ігнорують.

Необхідно приділити увагу і захисту від соціальної інженерії. Соціальна інженерія є способом особисто чи дистанційно отримати неавторизований доступом до інформації, системам, послуг чи важливим аспектам діяльності підприємства, маніпулюючи людьми. Соціальний інженер досліджує організацію, щоб дізнатися імена, посади, обов'язки та публічно доступну особисту ідентифікаційну інформацію. Потім соціальний інженер зазвичай використовує отримані дані на підприємстві і за допомогою правдоподібних, але вигаданих відомостей, намагається переконати персонал, що хтось (зловмисник) пов'язаний з організацією і потребує інформації або доступу в системи, які працівник організації може надати, при цьому у працівника створюють відчуття, що він зобов'язаний зробити це.

Для захисту від соціальної інженерії працівники мають бути спеціально проінструктовані. Працівник зобов'язаний спочатку ідентифікувати абонента, запитавши таку ідентифікаційну інформацію, яку знатиме лише людина, пов'язана з організацією. Якщо таку інформацію не можуть надати, то працівник повинен ввічливо, але твердо відмовити в її наданні, оскільки велика ймовірність того, що інформація була запитана соціальним інженером [44].

Важливою частиною налаштування мережі є наявність всіх необхідних інструментів моніторингу та введення журналів для збору й аналізу подій у внутрішній мережі. Доступні різні варіанти захисних технологій, розглянемо найпоширеніші [45]:

Антивіруси – спеціальні програми для виявлення та видалення вірусів, а також блокування спаму. Розрізняють такі різновиди антивірусних програм: детектори, ревізори, лікарі, сканери, фільтри, імунізатори та блокувальники.

Міжмережеве екранування (Firewall) - програмний або програмно-апаратний елемент комп'ютерної мережі, який захищає інформаційну систему через фільтрацію інформації, а також ігнорування неавторизованих запитів із зовнішнього середовища.

Системи виявлення вторгнень (IDS) — програмний продукт або пристрій для виявлення несанкціонованої та шкідливої активності на адресу мережі, що захищається.

DLP-системи - технології та технічні пристрої, які формують цифровий периметр навколо організації, запобігають витоку конфіденційної інформації з інформаційних систем, виявляють корпоративне шахрайство.

Аналіз захищеності інформаційних систем – перевірка інфраструктури підприємства на наявність вразливостей, наприклад у вихідному коді чи програмному забезпеченні.

Модулі довіреного завантаження - комплекс апаратно-програмних засобів, призначених контролювати цілісність ПЗ та реалізовувати завантаження з довіреного носія.

Системи криптографії – інструменти, які перетворюють, тобто шифрують дані. Подальше розшифрування може бути виконане лише за допомогою шифрів. Використовується для шифрування даних, мережевого трафіку, транзакцій, тощо.

Проксі-сервер — серверний додаток, який є посередником між клієнтом, який запитує ресурс, і сервером, який цей ресурс надає.

Рішення SIEM – система управління інформаційною безпекою. поєднує інструменти для керування інформаційною безпекою, а також засоби для керування подіями безпеки в одне рішення. Воно допомагає краще керувати системою безпеки. Технологія SIEM збирає дані журналу подій із низки джерел, визначає нетипові дії за допомогою аналізу в реальному часі та вживає відповідних заходів.

Управління положенням хмарної безпеки (CSPM) – комплекс технологій, які дозволяють оцінювати безпеку хмарних ресурсів, а також порівнювати засоби захисту із еталонними показниками.

Використовувати такі технології захисту інформації необхідно у комплексі, обираючи ті, що відповідають вимогам компанії, регулярно оновлюються та ефективно реагують на будь-які загрози. До рекомендованих

комплексних рішень можна віднести CrowdStrike Falcon, Panda Adaptive Defence, Lepide Remote Worker Monitoring, Cisco AMP, Sophos Intercept X, Symantec Endpoint Detection and Response, Check Point Endpoint Security. Кожне з перечислених вище рішень має свої переваги, що до функціональності, рівнів захисту, підтримки та вартості.

Крім цього, варто не забувати про покращення обізнаності співробітників у галузі інформаційної безпеки для зменшення кількості інцидентів, оскільки саме вони часто піддаються на маніпуляції хакерів.

Впровадження кращих міжнародних практик допоможе підприємствам СМБ зменшити витрати, пов'язані з інформаційною безпекою. Також це буде корисно як інструмент зв'язків з громадськістю, щоб представляти бізнес в очах клієнтів, як такий, в якому безпека даних клієнтів має першорядне значення.

Висновки до розділу 3

У розділі 3 досліджено технологію тестування на проникнення та зроблено оцінювання вразливостей спеціально розробленими інструментами для пошуку вразливостей – сканерами вразливостей. Визначено сценарій, за яким виконується тестування на проникнення.

Методологія активного виявлення інформаційних загроз що описана в роботі, включає методологію аналітичного відстеження (CTI) та активного виявлення загроз (CTH). Розглянуто моделі активного виявлення загроз, серед яких моделі Оперативного конвеєра та Кіберланцюга вбивств, Діамантова модель та Матриці ATT&CK MITRE.

Для використання підприємствами СМБ рекомендовані основні технології виявлення загроз безпеці (антивіруси, міжмережеве екранування, IDS/IPS, DLP-системи, криптографічні засоби, проксі-сервер, системи SIEM та CSPM), а також ряд комплексних рішень, що їх поєднують.

Дано практичні рекомендації щодо забезпечення безпеки підприємств СМБ згідно з нормативами NISTIR 7621, зокрема щодо застосування засобів захисту від шкідливого коду; безпечного підключення до Інтернету; захисту бездротової мережі та точок доступу; безпеки ЕОМ; оновлення операційних систем і додатків; резервного копіювання важливих для бізнесу даних; розмежування доступу; навчання персоналу з питань безпеки тощо.

ВИСНОВКИ

У результаті дослідження встановлено, що інформаційна безпека підприємства – це система, що дозволяє виявляти вразливі місця організації, небезпеки, що загрожують їй, та справлятися з ними. До основних методів інформаційної безпеки відносять нормативно-правові; організаційно-адміністративні; програмно-технічні; фізичні та морально-етичні.

Зроблено висновок, що для створення ефективної системи інформаційної безпеки підприємства необхідним є комплексне застосування різноманітних технологій, зокрема міжмережевого екранування, запобігання вторгненням (IPS) та втраті даних (DLP), управління інформацією та подіями безпеки (SIEM), виявлення і протидії загрозам у кінцевих точках (EDR), поведінкової аналітики (UEBA), управління інцидентами та інших.

Розглянуто основні положення стандартів серії ISO 27000, які пропонують рішення щодо впровадження й удосконалення системи управління інформаційною безпекою (СУІБ) на основі узагальнення кращого світового досвіду у цій сфері. Відзначено, що в Україні адаптовані кращі міжнародні практики у сфері ІБ. Так методом підтвердження прийняті такі національні стандарти, гармонізовані з міжнародними стандартами серії ISO 27000 методом підтвердження з наданням чинності з 01 листопада 2019 року: 27000-27002, 27005, 27008, 27011 та інші.

У дослідженні проаналізовано поняття ризику та його складових: загрози і вразливості. Встановлено, що методи зниження ризиків пропорційні зниженню загроз та усуненню вразливостей, а ризик – це поєднання загрози

та вразливості. Вразливість без відповідної загрози або загроза без відповідної вразливості не викликають ризику.

З’ясовано, що загроза інформаційній безпеці є сукупністю умов і факторів, що створюють ризик порушення інформаційної безпеки. Загрози ІБ класифіковано за такими основними ознаками: джерелами походження (природні, технічні, антропогенні); аспектами інформаційної безпеки (загрози конфіденційності, цілісності та доступності); розміщенням джерела загрози (внутрішні і зовнішні); наявністю злого умислу (навмисні, випадкові) тощо.

Розроблено план дій на випадок кібератак, відповідно до якого основними кроками виявлення та протидії загрозам, а також реагування на інциденти ІБ є: 1) підготовка; 2) виявлення та аналіз; 3) стримування, ліквідація наслідків і відновлення; 4) подальша діяльність після кібератаки.

У роботі розглянуто технологію тестування на проникнення та зроблено оцінювання вразливостей спеціально розробленими інструментами для пошуку вразливостей – сканерами вразливостей. Визначено сценарій, за яким виконується тестування на проникнення.

За результатами дослідження підприємствам СМБ рекомендовано застосовувати такі основні технології виявлення загроз безпеці (антивіруси, міжмережеве екранування, IDS/IPS, DLP-системи, криптографічні засоби, проксі-сервер, системи SIEM та CSPM), а також ряд комплексних рішень, що їх поєднують.

Дано практичні рекомендації щодо забезпечення безпеки підприємств СМБ згідно з нормативами NISTIR 7621, зокрема щодо застосування засобів захисту від шкідливого коду; безпечного підключення до Інтернету; захисту бездротової мережі та точок доступу; безпеки ЕОМ; оновлення операційних систем і додатків; резервного копіювання важливих для бізнесу даних; розмежування доступу; навчання персоналу з питань безпеки тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.

2. Dictionary by Merriam-Webster: America's Most-Trusted Online Dictionary. URL: https://www.merriam-webster.com/ (дата звернення: 22.12.2022)

3. Що таке інформаційна безпека (INFOSEC)? Захисний Комплекс Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec (дата звернення: 22.12.2022)

4. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. URL: https://www.iso.org/standard/54534.html (дата звернення: 22.12.2022)

5. What Is Information Security (INFOSEC)? Cisco, 16 Aug. 2022. URL: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html (дата звернення: 22.12.2022)

6. Мейволд, Э. (2016). Безпека мереж: навчальний посібник. https://bstudy.net/812091/informatika/opredelenie_informatsionnoy_bezopasnosti (дата звернення: 22.12.2022)

7. Рафаэль Х., Джим Г., Мати А. Kali Linux от разработчиков. 2019. 320 с. URL: https://www.pdfdrive.com/ (дата звернення: 22.12.2022)

8. Parker, D.B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. URL: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad (дата звернення: 22.12.2022)

9. Галатенко В.А. Стандарти інформаційної безпеки. М.: Інтернет-університет інформаційних технологій. 2004. 328 с.

10. Андресс, Дж. Основи інформаційної безпеки: простий вступ. Сан-Франциско, 2019. 222 с.

11. Матвієнко В. М., Ковтун О. Ю. Міжнародна організація зі стандартизації. К.: Знання України, 2004. Т.2. 812с.

12. Міжнародна організація по стандартизації. URL: https://www.iso.org/ru/standard/73906.html (дата звернення: 22.12.2022)

13. Центр сприяння експорту. URL: https://export-center.by/blogpost/new-iso-27001-2022 (дата звернення: 22.12.2022)

14. Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів: Наказ ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» №312 від 16.10.2019. URL: https://zakon.rada.gov.ua/rada/show/v0312774-19#Text (дата звернення: 22.12.2022)

15. Загрози інформаційної безпеки. Wikimedia Foundation, 18 June 2022. URL: https://uk.wikipedia.org/wiki/Загрози_інформаційної_безпеки (дата звернення: 22.12.2022)

16. Вішняков Я.Д., Радаев Н.Н. Загальна теорія ризиків: навч. посібник для студ. вищ. навч. закладів. 2-е вид., Видавничий центр «Академія». 2008. 368 с.

17. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції. 2006. URL: https://www.dut.edu.ua/ua/lib/1/category/1181/view/1350 (дата звернення: 22.12.2022)

18. Скиба В., Курбатов В. Керівництво по захисту від внутрішніх загроз інформаційної безпеки. К.: Видавництво Либідь, 2008. 320 с.

19. Кавун С. В., Пилипенко А. А., Ріпка Д. О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації: Навчальний посібник. Х. : Вид. ХНЕУ, 2013. 364 с.

20. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. К.: Видавнича група ВНУ, 2009. 608 с.

21. Від інциденту до вирішення: основні кроки. Блог компанії Eset.

URL: https://eset.ua/ua/blog/view/83/ot-intsidenta-k-resheniyu-osnovnyye-shagi-protivodeystviya-i-vosstanovleniya-v-sluchaye-kiberataki (дата звернення: 22.12.2022)

22. ISO 15408 Загальні критерії оцінки безпеки інформаційних технологій. URL: http://ni.biz.ua/6/6_14/6_14221_mezhdunarodniy-standart-ISO---obshchie-kriterii.html (дата звернення: 22.12.2022)

23. Хоменко В.Г., Павленко М.П. Комп'ютерні мережі: Навч. посібник. Донецьк : Ландон-XXI, 2011. 316 с. URL: https://vasylkiv-litsei.com.ua/media/library/book/1614070458.978003.pdf (дата звернення: 22.12.2022)

24. Яцків В.В. Тестування комп'ютерних систем на проникнення: опорний конспект лекцій для студентів спеціальності 125 «Кібербезпека». Тернопіль : ТНЕУ, 2019. 119 с.

25. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: Навчальний посібник. Дніпро, 2020. 144с.

26. Half a Million Widely Trusted Websites Vulnerable to Heartbleed Bug. Netcraft News, 8 Apr. 2014. URL: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (дата звернення: 22.12.2022)

27. OpenSSL Bug CVE-2014-0160: Tor Project. The Tor Project, 7 Apr. 2014. URL: https://blog.torproject.org/openssl-bug-cve-2014-0160/ (дата звернення: 22.12.2022)

28. Блог компанії Google. URL: https://googleprojectzero.blogspot.com/ (дата звернення: 22.12.2022)

29. Приватна компанія «DataMi». Блог з кібербезпеки. URL: https://datami.ua/shho-take-pentest-test-na-proniknennya/ (дата звернення: 22.12.2022)

30. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны : практическое руководство; пер. с анг. Д. А. Беликова, 2020. 326 с. URL: https://znanium.com/catalog/product/1908427 (дата звернення: 22.12.2022)

31. Фетісов В.С. Комп'ютерні технології в тестуванні: Навчально-методичний посібник. Ніжин, 2011. 140 с. URL: https://moodle.ndu.edu.ua/file.php/1/Fetisov_komp_tehnol_v-testuvanni.pdf (дата звернення: 22.12.2022)

32. Aileen G Bacudio, Xiaohong Yuan, Bei Tseng Bill Chu, Monique Jones. An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 2011. P. 19-38. DOI:10.5121/ijnsa.2011.3602 (дата звернення: 22.12.2022)

33. Касснер М. Полювання за кіберзагрозами: як ця стратегія виявлення вразливостей дає перевагу аналітикам. Блог TechRepublic, 18 квітня. 2016. URL: https://www.techrepublic.com/article/cyber-threat-hunting-why-this-active-strategy-gives-analysts-an-edge/ (дата звернення: 22.12.2022)

34. Деніел Г. Грем. Етичний хакінг. Практичний посібник по взлому. 2022. 384 с. URL: https://coollib.com/b/568035-deniel-g-grem-etichnyiy-haking-prakticheskoe-rukovodstvo-po-vzlomu (дата звернення: 22.12.2022)

35. Загальні відомості про індикатор компроментації (IoC). Компанія Microsoft. URL: https://learn.microsoft.com/ru-ru/microsoft-365/security/defender-endpoint/manage-indicators?view=o365-worldwide (дата звернення: 22.12.2022)

36. Е. Піз. Полювання на загрози за допомогою Elastic Stack. Вирішуйте складні проблеми безпеки за допомогою інтегрованого запобігання, виявлення та реагування; пер. с англ. В. С. Яценкова. 2022. 326 с. URL: https://dmkpress.com/files/PDF/978-5-93700-116-0.pdf (дата звернення: 22.12.2022)

37. Lockheed M. Cyber Kill Chain®. 29 June 2022. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.htm (дата звернення: 22.12.2022)

38. Hutchins E. M., Cloppert M. J., Amin R. M. IntelligenceDriven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin, 29 June 2022. URL: https://www.lockheedmartin.com/

content/dam/lockheed-martin/rms/ documents/ cyber/LM-White-Paper-Intel-Driven-Defense.pdf (дата звернення: 22.12.2022)

39. Matrix - Enterprise Enterprise Matrix. | MITRE ATT&CK®. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 22.12.2022)

40. Як моделювання зломів та атак полегшує взаємодію з MITRE ATT&CK. iIT Distribution. https://iitd.com.ua/news/jak-modeljuvannja-zlomiv-ta-atak-polegshuie-vzaiemodiju-z-mitre-att-ck/ (дата звернення: 22.12.2022)

41. Caltagirone S., Pendergast A. & Betz C. The Diamond Model of Intrusion Analysis. US Department of Defense. 2013. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf (дата звернення: 22.12.2022)

42. Ортинський В.Л., Керницький І.С., Живко З.Б., Керницька М.І., Гук О.В., Шимечко Г.І., Живко М.О. Економічна безпека підприємств: Підручник. Київ: Алерта, 2011. 704 с.

43. Paulsen C., Toth P. Small Business Information Security: the Fundamentals: NIST Interagency Report 7621. Revision 1. 2016. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7621.pdf (дата звернення: 22.12.2022)

44. Соколов В. Курбанмурадов Д. Методика протидії соціальному інжинірингу. Кібербезпека: освіта, наука, техніка. 2018. Т.1. № 1. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/15 (дата звернення: 22.12.2022)

45. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: Навчальний посібник. Харків. Вид. ХНЕУ, 2013. 476 с. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf (дата звернення: 22.12.2022)

46. McCarthy, C. Digital Libraries : Security and Preservation Considerations. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management. 2016. Vol. 3. Free SANS Information Security Resources: https://www.sans.org/security-resources (дата звернення: 22.12.2022)

47. Blakley Bob, Ellen McDermott, Dan Geer. Information security is information risk management. URL: https://dl.acm.org/doi/10.1145/508171.508187 (дата звернення: 22.12.2022)

48. Заплотинський Б.А. Основи інформаційної безпеки.Конспект лекцій. –КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

49. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О. О. Комп'ютерна безпека. Захист інформації у комп'ютерних системах. 2020. 236 с.

50. Безпека бізнесу: як захистити компанію від кібератак 2022. URL: https://biz.ligazakon.net/analitycs/209010_bezpeka-bznesu-yak-zakhistiti-kompanyu-vd-kberatak (дата звернення: 22.12.2022)

51. Vault A. 4 SIEM Use Cases That Will Dramatically Improve Your Enterprise Security. Infocorp Security&Networking. URL: https://www.infocorp.cl/ver-mas-articulos/145-4-siem-use-cases-that-will-dramatically-improve-your-enterprise-security (дата звернення: 22.12.2022)

52. Johnson Arnold, Dempsey Kelley, Ross Ron, Gupta Sarbari, Bailey Dennis (October 2019). Guide for security-focused configuration management of information systems. URL: https://csrc.nist.gov/publications/detail/sp/800-128/final (дата звернення: 22.12.2022)

53. Марущак А. Захист інформації з обмеженим доступом та право на інформацію: проблеми правового регулювання. URL: https://ela.kpi.ua/ bitstream/123456789/10959/1/13_p108.pdf. (дата звернення: 22.12.2022)

54. Євсеєв С. Управління інформаційною безпекою, 2016. URL: http://s-byte.com/useful/27002.pdf (дата звернення: 22.12.2022)

55. Campbell Tony. Practical Information Security Management. A Complete Guide to Planning and Implementation. 2016. 270 с.

56. Waschke Marvin. Personal Cybersecurity How to Avoid and Recover from Cybercrime. 2017. 379 с.

57. Mangat M. 19 Cybersecurity Best Practices to Protect Your Business. URL: https://phoenixnap.com/blog/cybersecurity-best-practices (дата звернення: 22.12.2022)

58. Protect your business with practical steps to prevent a cyber attack. URL: https://www.telappliant.com/blog/improve-cyber-security/ (дата звернення: 22.12.2022)