МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИ ЗАПОБІГАННЯ І ПРОТИДІЇ ЗАГРОЗАМ МЕРЕЖЕВІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Андрій МАКАРЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Андрій МАКАРЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к.держ.упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:

Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Макаренку Андрію Вадимовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи запобігання і протидії загрозам мережевій безпеці підприємства”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к. держ. упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *мережева безпека підприємства, загрози мережевій безпеці, методи запобігання та протидії загрозам мережевій безпеці підприємства.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні основи мережевої безпеки підприємства.
4.2. З’ясувати особливості нормативно-правових і організаційних методів мережевої безпеки.
4.3. Проаналізувати програмно-технічні засоби запобігання та протидії загрозам мережевій безпеці, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Дослідження теоретичних основ мережевої безпеки підприємства	08.04.2024	
4.	Вивчення особливостей нормативно-правових і організаційних методів мережевої безпеки.	22.04.2024	
5.	Аналіз програмно-технічних засобів запобігання та протидії загрозам мережевій безпеці, розробка практичних рекомендацій.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Андрій МАКАРЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Макаренко А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи запобігання і протидії загрозам мережевій безпеці підприємства"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач МАКАРЕНКО Андрій у кваліфікаційній роботі дослідив теоретичні основи мережевої безпеки, з'ясував особливості нормативно-правових та організаційних методів забезпечення мережевої безпеки, проаналізував програмно-технічні засоби запобігання та протидії загрозам безпеці мережі, розробив практичні рекомендації за темою дослідження.

Під час підготовки кваліфікаційної роботи МАКАРЕНКО Андрій показав високу теоретичну та практичну підготовку, вміння самостійно знаходити шляхи вирішення наукових проблем, довів володіння науково-дослідницькими методами і навичками організації дослідження. Результати дослідження апробовані на одній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача МАКАРЕНКА Андрія на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

"_____" ____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Макаренко А.В. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти МАКАРЕНКА Андрія

на тему “Методи запобігання і протидії загрозам мережевій безпеці підприємства”

Актуальність. Сучасні організації обробляють і передають величезні обсяги даних, серед яких комерційна таємниця, інтелектуальна власність, персональні дані тощо. У таких умовах мережева безпека відіграє ключову роль у захисті конфіденційної інформації і є обов’язковою складовою забезпечення інформаційної та кібербезпеки. Завдяки використанню методів мережевої безпеки, компанія може реалізувати проактивний підхід до захисту інформації, мінімізувати ризики інцидентів і обсяги потенційних збитків, сприяючи підвищенню рівня корпоративної інформаційної безпеки.

З огляду на зазначене дослідження методів запобігання і протидії мережевій безпеці підприємства є актуальним науковим завданням.

Позитивні сторони.

1. У роботі представлено комплексне дослідження нормативно-правових та організаційних методів забезпечення мережевої безпеки, а також програмно-технічних засобів запобігання та протидії мережевим загрозам, розроблено практичні рекомендації за темою дослідження.

2. Кваліфікаційна робота оформлена відповідно до вимог, структура роботи забезпечує досягнення поставленої мети. Студент показав розуміння проблеми, володіння методами дослідження і здатність вирішувати прикладні завдання.

3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовні наукові статті.

4. За результатами дослідження запропоновано рекомендації щодо використання засобів протидії мережевим загрозам (SIEM, IDS/IPS, DLP) в компаніях різного розміру і сфер діяльності.

Недоліки.

Доцільно було б приділити більше уваги вивченню й класифікації програмно-технічних засобів мережевої безпеки, представлених на ринку.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач МАКАРЕНКО Андрій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів запобігання і протидії загрозам мережевій безпеці підприємства. Робота складається зі вступу, трьох розділів, що містять 13 рисунків, 1 таблицю, висновків і списку використаних джерел із 49 найменувань. Загальний обсяг роботи становить 85 аркушів, з яких 4 аркуші займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження методів запобігання і протидії загрозам мережевій безпеці підприємства.

Об'єктом дослідження є забезпечення мережевої безпеки підприємства.

Предмет дослідження – методи запобігання і протидії загрозам мережевій безпеці підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління мережевою безпекою.

Як результат, у роботі досліджено теоретичні основи мережевої безпеки, з'ясовано особливості нормативно-правових та організаційних методів забезпечення мережевої безпеки, проаналізовано програмно-технічні засоби запобігання та протидії загрозам безпеці мережі, розроблено практичні рекомендації щодо підвищення рівня мережевої безпеки підприємства.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації комплексу заходів і засобів запобігання та протидії мережевим загрозам з метою підвищення рівня безпеки корпоративних мереж.

Ключові слова: МЕРЕЖЕВА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗИ МЕРЕЖЕВІЙ БЕЗПЕЦІ, МЕТОДИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЗАГРОЗАМ МЕРЕЖЕВІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА.

ABSTRACT

The qualification work is devoted to the study of methods of preventing and counteracting threats to enterprise network security. The work consists of an introduction, three chapters containing 13 figures, 1 table, conclusions and a list of references of 49 titles. The total volume of the work is 85 pages, of which 4 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to investigate methods of preventing and counteracting threats to enterprise network security.

The object the study is to network security of the enterprise.

The subject of the study is methods of preventing and counteracting threats to enterprise network security.

Research methods. To solve the above scientific task, the methods of analysis and synthesis, comparison, classification, expert evaluation, and a systematic approach to network security management were used in the work.

As a result, the theoretical aspects of network security were investigated in the work, the peculiarities of regulatory and organizational methods of network security were clarified, software and technical tools of preventing and countering threats to network security were analyzed, and practical recommendations were developed to increase the level of network security of the enterprise.

Field of application. The developed approaches can be used in the planning and implementation of a set of measures and tools of preventing and countering network threats in order to increase the level of security of corporate networks.

Keywords: ENTERPRISE NETWORK SECURITY, NETWORK SECURITY THREATS, METHODS PREVENTION AND COUNTERING THREATS TO ENTERPRISE NETWORK SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

BCP	Business Continuity Planning
DRP	Disaster Recovery Plan
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

ВСТУП

Актуальність теми. У сучасному світі, де підприємства й організації обробляють і передають величезні обсяги даних, серед яких інформація критичного значення, зокрема комерційна таємниця, інтелектуальна власність, персональні дані тощо. У таких умовах мережева безпека стає обов'язковою складовою забезпечення інформаційної та кібербезпеки підприємства і відіграє ключову роль у захисті конфіденційної інформації. Завдяки використанню методів мережевої безпеки, компанія може реалізувати проактивний підхід до захисту інформації, мінімізувати ризики інцидентів і обсяги потенційних збитків, сприяючи підвищенню рівня корпоративної інформаційної безпеки.

З огляду на зазначене дослідження методів запобігання і протидії мережевій безпеці підприємства є актуальним науковим завданням.

Мета роботи полягає у дослідженні методів запобігання і протидії загрозам мережевій безпеці підприємства.

Об'єкт дослідження – забезпечення мережевої безпеки підприємства.

Предмет дослідження – методи запобігання і протидії загрозам мережевій безпеці підприємства.

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

1. Дослідити теоретичні основи мережевої безпеки підприємства.

2. З'ясувати нормативно-правові й організаційні методи забезпечення мережевої безпеки.

3. Проаналізувати програмно-технічні засоби запобігання та протидії загрозам безпеці мережі, розробити практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління мережевою безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і інструментів

забезпечення мережевої безпеки відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Мережева безпека: сутність, принципи, переваги

Безпека мережі – це широкий термін, який охоплює безліч технологій, пристроїв і процесів. У найпростішому вигляді це набір правил і конфігурацій, призначених для захисту цілісності, конфіденційності та доступності комп'ютерних мереж і даних за допомогою як програмних, так і апаратних технологій. Кожній організації, незалежно від розміру, галузі чи інфраструктури, потрібен певний рівень мережевих рішень безпеки, щоб захистити її від постійно зростаючого ландшафту кіберзагроз у мережі Інтернет сьогодні.

Сучасна мережева архітектура є складною та стикається із середовищем загроз, яке постійно змінюється, і зловмисниками, які постійно намагаються знайти та використати вразливі місця. Ці вразливості можуть існувати в багатьох сферах, включаючи пристрої, дані, програми, користувачів і розташування. З цієї причини сьогодні використовується багато інструментів і програм для управління мережевою безпекою, які спрямовані на вирішення окремих загроз і експлойтів, а також невідповідності нормативним вимогам. Коли лише кілька хвилин простою можуть спричинити масштабні збої та завдати серйозної шкоди прибутку й репутації організації, вкрай важливо вжити ці заходи захисту.

Існує багато рівнів, які слід враховувати під час вирішення питань безпеки мережі в організації. Атаки можуть відбуватися на будь-якому рівні в моделі рівнів мережевої безпеки, тому апаратне забезпечення, програмне забезпечення та політики безпеки мережі повинні бути розроблені для кожного рівня [1].

Для забезпечення безпеки мережі зазвичай впроваджують три види заходів: фізичні, технічні й адміністративні. Нижче представлені короткий опис і принципи роботи кожного виду заходів.

- Фізичні – фізичні заходи безпеки стосуються фізичного стану пристроїв. Офісні пристрої можуть вимагати кілька облікових даних, перш ніж надати доступ. Компанії повинні фізично захищати сервери та інші пристрої зберігання даних за допомогою замків і засобів контролю доступу. Налаштування безпеки можуть включати використання камер і біометричних сканерів для додаткового захисту.

- Технічні – ці заходи управління мають на меті захист потоків даних через комп'ютерну мережу, а також даних, що зберігаються на мережевих пристроях. Технічні заходи охоплюють локально підключені сервери та робочі станції, а також віддалені робочі пристрої та служби SaaS, якими користуються співробітники компанії. Технічні заходи спрямовані на запобігання зовнішнім атакам без шкоди для продуктивності мережі.

- Адміністративні – ці заходи стосуються поведінки користувачів. Адміністративний контроль включає системи керування ідентифікацією та доступом, які перевіряють усі запити на доступ. Політики безпеки визначають привілеї для кожного користувача. Системи підключають нових працівників і видаляють застарілі облікові записи, щоб запобігти крадіжці облікових даних. Навчання персоналу також є важливим адміністративним завданням [2].

Мережевій безпеці притаманні такі ж принципи, що й інформаційній безпеці загалом.

Модель CIA (Confidentiality, Integrity, Availability) є найпопулярнішим способом візуалізації методів безпеки для сучасних мереж. Ця модель є основою для поглибленого захисту, що означає захист підключених активів на всіх рівнях мережі.

- Конфіденційність: означає ступінь секретності інформації, якою обмінюються відправник і одержувач. Це гарантує, що лише авторизовані сторони можуть отримати доступ до інформації, зберігаючи її прихованою від неавторизованих осіб і зловмисників. Якщо неавторизована особа отримує доступ до конфіденційного повідомлення, принцип конфіденційності порушується.

Наприклад, уявімо, що відправник А хоче поділитися конфіденційною інформацією з одержувачем В, але зловмисник С перехоплює повідомлення. У цьому сценарії конфіденційна інформація потрапляє до рук зловмисника С, порушуючи принцип конфіденційності.

- Цілісність: гарантує, що отримана інформація є незмінною і точною. Якщо під час передачі вміст повідомлення змінено або підроблено, цілісність повідомлення буде порушено. Необхідно враховувати два аспекти цілісності: цілісність системи й цілісність даних.

Цілісність системи забезпечує, що система виконує заплановану функцію без несанкціонованих маніпуляцій. Вона захищає систему від навмисних або ненавмисних змін, які можуть поставити під загрозу її функціональність.

Цілісність даних гарантує, що збережена й передана інформація залишається незмінною та непошкодженою. Це гарантує, що дані не будуть модифіковані або підроблені несанкціонованим чином.

- Доступність – передбачає, що ресурси мають бути доступними для авторизованих користувачів у будь-який час. Працівники повинні мати доступ до робочих навантажень і передавати дані з віддалених робочих станцій. Однак інструменти безпеки мають мінімізувати свободу неавторизованих користувачів.

Дотримуючись цих принципів, організації можуть створити міцну основу для безпеки своєї мережі. Крім того, існують інші важливі аспекти, які слід враховувати в безпеці мережі:

- Вимоги до веб-безпеки. Захист веб-додатків та їхніх даних за допомогою шифрування і безпечних протоколів зв’язку має важливе значення в сучасному цифровому середовищі.

- Рівень захищених сокетів: протоколи SSL/TLS забезпечують спеціальні канали зв’язку, гарантуючи, що дані, що обмінюються між системами, залишаються зашифрованими та захищеними від перехоплення.

- Алгоритм SHA. Алгоритм безпечного хешування (SHA) відіграє вирішальну роль у цілісності даних, гарантуючи, що дані залишаються незмінними та автентичними.
- Атаки на безпеку: розуміння різних векторів атак на безпеку має важливе значення для впровадження ефективних контрзаходів для захисту даних і систем.
- Важлива потреба в безпеці: ландшафт загроз, що швидко розвивається, підкреслює важливість надійних заходів безпеки для захисту від кібератак.
- Неспростовність - це механізм, який запобігає відхиленню відправником факту відправлення або отримувачем факту отримання повідомлення надісланого через мережу. Це гарантує, що відправник не зможе пізніше відмовити в надсиланні повідомлення, надаючи докази спілкування. Неспростовність має вирішальне значення в ситуаціях, коли виникають відповідальність і судові спори.
- Контроль доступу передбачає управління та контроль того, хто може отримати доступ до даних і в якому обсязі. Він охоплює управління ролями та правилами, визначаючи як осіб, уповноважених на доступ до даних, так і рівень інформації, яку вони можуть отримати. Принцип контролю доступу гарантує, що дані доступні лише авторизованим сторонам на основі їхніх ролей і дозволів.
- Автентифікація - це механізм, який використовується для перевірки ідентичності користувача, системи чи об’єкта. Це гарантує, що особа або система, які намагаються отримати доступ до інформації, є тими, за кого себе видають. Автентифікація зазвичай здійснюється за допомогою імен користувачів, паролів або інших факторів автентифікації. Підтверджуючи особу авторизованих осіб, автентифікація запобігає несанкціонованому доступу до конфіденційної інформації.

Безпека мережі охоплює широкий і складний набір технологій і процедур, реалізованих з метою захисту пристроїв і даних, підключених до домашньої, корпоративної або загальнодоступної мережі.

Різні організації можуть по-різному визначати безпеку мережі. Для одних це може означати захист усієї мережевої інфраструктури через комплексну платформу від сервера до периметра, тоді як інші можуть розглядати це як більш спеціалізований сегмент у сфері кібербезпеки, наголошуючи на захисті пристроїв, що з'єднуються з мережею, а не на захисті мережі.

Незалежно від конкретної спрямованості, мережева безпека має три універсальні ключові цілі:

- Запобігання несанкціонованому доступу до ресурсів мережі.
- Виявлення та припинення кібератак і порушень безпеки.
- Забезпечення надання доступу до мережевих ресурсів виключно авторизованим користувачам відповідно до їхніх потреб [3].

Переваги безпеки мережі

Інвестиції в мережеву безпеку - це не просто технологічне рішення, а стратегічний бізнес-вибір із численними безпосередніми й опосередкованими перевагами. Основними перевагами є такі (Рис. 1.1):

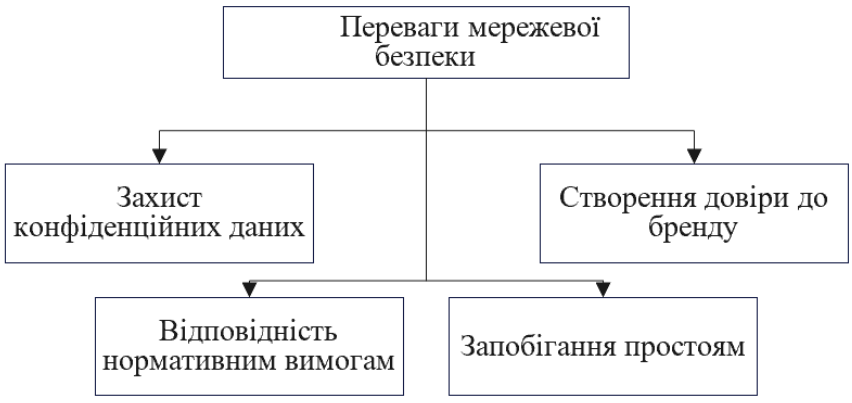

Рис. 1.1. Переваги мережевої безпеки

Захист конфіденційних даних. Безпека мережі є наріжним каменем захисту конфіденційних даних кожної організації. Ці дані можуть відрізнятися й охоплювати особисту інформацію клієнтів, їх банківські дані, результати приватних досліджень, корпоративні фінансові записи тощо. Без надійної

безпеки мережі ці цінні активи піддаються ризику несанкціонованого доступу й використання.

Яскравим прикладом важливості захисту конфіденційних даних компанії є злом T-Mobile у січні 2023 року. У T-Mobile визнали, що це порушення даних може призвести до «значних витрат», не рахуючи величезної компенсації в розмірі 350 мільйонів доларів, яку компанія має виплатити своїм клієнтам через порушення даних у серпні 2021 року.

Ця низка невдач із безпекою коштувала T-Mobile не лише значного фінансового тягаря, але й удару по їхній репутації, оскільки довіра клієнтів була підірвана послідовними витоками персональних даних. Таким чином, інвестиції в безпеку мережі – це не тільки захист даних; йдеться про запобігання потенційним фінансовим втратам.

Відповідність нормативним вимогам. У багатьох секторах, таких як охорона здоров'я, фінанси та державний сектор, нормативні стандарти вимагають суворих заходів захисту даних. Безпека мережі часто є центральною для відповідності цим стандартам. Наприклад, організації охорони здоров'я в США повинні дотримуватися Закону про перенесення та підзвітність медичного страхування (HIPAA), який вимагає надійних заходів безпеки для захисту даних пацієнтів. Невиконання вимог може призвести до великих штрафів, а також до втрати довіри пацієнтів.

Запобігання простоям. Кібератаки можуть спричинити значні збої в роботі організації, призводячи до дорогих простоїв, поки проблема не буде вирішена, а системи відновляться. Так, атака програм-вимагачів WannaCry у 2017 році призвела до очікуваних простоїв у всьому світі, які коштували компаніям 4 мільярди доларів. Запобігаючи таким атакам, заходи безпеки мережі допомагають забезпечити безперебійну роботу бізнесу, підтримуючи продуктивність і надання послуг.

Створення довіри до бренду. Нарешті, як ілюструє наведена вище історія про T-Mobile, безпека мережі є невід'ємною частиною підтримки та підвищення

довіри до бренду. В епоху, коли витоки даних регулярно потрапляють у заголовки газет, клієнти все більше цінують і вимагають від компаній захисту своїх даних. Компанія, відома своєю надійною мережевою безпекою, сприятиме міцнішим відносинам із клієнтами та їх лояльності [4].

Незахищена мережа в сучасному Інтернеті може привести до катастрофи. І витрати на персонал і засоби захисту, необхідні для встановлення та підтримки безпеки корпоративної мережі, не підлягають обговоренню.

Отже, безпека мережі - це не витрати, а інвестиція в захист активів організації, забезпечення дотримання нормативних вимог, мінімізацію простою та підвищення репутації корпоративного бренду. Відповідно безпека мережі має бути стратегічним пріоритетом для будь-якої перспективної компанії.

1.2 Статистика загроз мережевій безпеці

У сучасному глобалізованому світі мережева безпека має вирішальне значення і повинна забезпечити ефективний захист від загроз, що постійно еволюціонують, і нових методів атак. Як свідчить статистика, показники атак на корпоративні мережі і обсяги збитків внаслідок руйнівної діяльності хакерів постійно зростають.

Розглянемо результати спостережень, експертні оцінки й прогнози щодо динаміки загроз безпеці мережі [5-8].

Вартість і частота кібератак.

1. За оцінками, витрати на кіберзлочинність у всьому світі досягнуть 10,5 трильйонів доларів США щорічно до 2025 року, що підкреслює необхідність посилених заходів кібербезпеки.

2. Очікується, що кіберзлочинність обійдеться світові в 9,5 трильйонів доларів США в 2024 році, що трохи нижче прогнозованих темпів зростання.

3. Очікується, що глобальні збитки від кіберзлочинності зростатимуть на 15% на рік протягом наступних двох років, досягнувши 10,5 трильйонів доларів США на рік до 2025 року.

4. У 2023 році Сполучені Штати продовжують мати найвищу вартість витоку даних – 5,09 млн доларів США.

5. 75% спеціалістів із безпеки помітили збільшення кількості кібератак за останній рік.

6. Середня глобальна вартість витоку даних у 2023 році становила 4,45 мільйона доларів США, що на 15% більше за три роки, що підкреслює зростаючий фінансовий тягар для організацій.

7. Страхові внески в США зросли на 50% у 2022 році, досягнувши 7,2 млрд доларів премій, зібраних з полісів, написаних страховими компаніями.

8. Коли віддалена робота є фактором, що спричиняє порушення даних, середня ціна за порушення становить на 173 074 доларів США вище, що підкреслює проблеми кібербезпеки в робочому середовищі, що розвивається.

9. 12-й рік поспіль Сполучені Штати мають найвищу вартість витоку даних – 5,09 млн доларів.

10. Крадіжка даних була причиною 19% усіх інцидентів, підкреслюючи зростаючу стурбованість інформаційною безпекою.

Отже, статистичні показники свідчать, що вартість і частота кібератак упродовж останніх років постійно зростає, що, зокрема, пов’язано з розширенням обсягів віддаленої роботи.

Статистика щодо програм-вимагачів.

1. У 2023 році 72,7% усіх організацій стали жертвами атаки програм-вимагачів.

2. Очікується, що до 2031 року витрати на програмне забезпечення-вимагач досягнуть близько 265 мільярдів доларів США щорічно, що значно більше порівняно з 20 мільярдами доларів у 2021 році.

3. Майже половина (47%) компаній зараз мають політику виплати викупів, пов’язаних із загрозами кібербезпеці, що на 13% більше, ніж у попередньому році.

4. Програми-вимагачі названо головною проблемою керівників у 62% опитаних організацій, що на 44% більше, ніж у 2022 році.

5. Середня вартість атаки програм-вимагачів склала 4,54 мільйона доларів.

6. Середня вартість відновлення після атаки програм-вимагачів у 2023 році склала 1,82 мільйона доларів без урахування викупу.

7. Лише 8% підприємств, які платять викуп хакерам, отримують усі свої дані натомість.

8. Бекдори були розгорнуті в 21% усіх інцидентів, виправлених у 2022 році, тоді як програми-вимагачі становили 17% інцидентів.

9. У 2023 році 66% організацій повідомили, що стали мішенню програм-вимагачів, а середня виплата викупу зросла з 812 380 доларів США у 2022 році до 1 542 333 доларів США.

10. 81% опитаних організацій стикалися з атаками програм-вимагачів у 2023 році, а 48% заплатили викуп.

Таким чином, статистика показує зростання кількості атак програм-вимагачів, витрат на атаки та відновлення. Багато організацій готові платити викуп, але це не гарантує відновлення даних. Необхідно вживати заходів для захисту від програм-вимагачів, таких як резервне копіювання даних, навчання персоналу та впровадження систем захисту мережевою безпеки.

Статистика фішингу.

1. Фішинг продовжує залишатися найпоширенішим методом атаки електронною поштою, на нього припадає 39,6% усіх загроз електронної пошти.

2. 94% зловмисного ПЗ доставляється електронною поштою.

3. Фішингові вкладення використовувалися в 62% фішингових атак, а посилання використовувалися в 33% і як послуга в 5%.

4. У 2022 році лише 29% наборів для фішингу перевірили дані кредитної картки, що на 52% менше, ніж у 2021 році.

5. Компрометація бізнес-електронної пошти (BEC), яка часто включає фішингові посилання, спричинила 6% інцидентів, причому в половині цих випадків використовувалися прямі фішингові посилання.

6. У 80% організацій, де сталася атака BEC, до інциденту не було застосовано рішення багатофакторної автентифікації (MFA).

7. Фішинг був визначений як основний вектор зараження в 41% випадків кібербезпеки.

8. У 2022 році кількість спроб захоплення потоків подвоїлася порівняно з 2021 роком.

Відповідно до результатів спостережень фішинг залишається найпоширенішим методом атаки електронною поштою та однією з найбільш поширених і небезпечних мережевих загроз.

Штучний інтелект, IoT та DDoS-атаки.

1. 85% фахівців з кібербезпеки пояснюють збільшення кількості кібератак використанням зловмисниками генеративного ШІ.

2. Близько 46% респондентів вважають, що інтеграція генеративного ШІ в бізнес-операції збільшить вразливість до кібератак.

3. Занепокоєння з приводу ШІ в кібербезпеці охоплюють можливість посилення проблем із конфіденційністю (39%), невиявлених фішингових атак (37%) і збільшення загального обсягу та швидкості атак (33%).

4. 85% фахівців з кібербезпеки пов’язують зростання кількості кібератак зловмисниками, які використовують генеративний штучний інтелект [9].

5. У грудні 2022 року було зареєстровано понад 10,54 мільйона атак Інтернету речей.

6. У другому кварталі 2023 року кількість атак DDoS (розподілена відмова в обслуговуванні) зросла на 15%.

7. У 2022 році було зареєстровано 6248 DDoS-атак.

8. У першому кварталі 2023 року зафіксовано збільшення на 600% кількості кіберінцидентів, націлених на криптовалютні фірми, що супроводжувалося значним зростанням на 15% DDoS-атак HTTP.

Як свідчить статистика, через зростання популярності штучного інтелекту, AI, IoT та DDoS-атаки стають дедалі більш витонченими та руйнівними, що підкреслює потребу в комплексних стратегіях кібербезпеки**.**

Переривання діяльності та інвестиції в безпеку.

1. 45% експертів кажуть, що кіберінциденти є найстрашнішою причиною переривання бізнесу, перевершуючи стихійні лиха чи проблеми з енергетикою.

2. Очікується, що витрати на інформаційну безпеку, продукти та послуги з управління ризиками зростуть на 14,3% у 2024 році та досягнуть понад 215 мільярдів доларів.

3. 53% організацій вимагають перевірки кібербезпеки перед розгортанням будь-якого рішення, демонструючи проактивний підхід до управління кіберризиками.

4. 35% організацій впроваджують засоби безпеки в усі ініціативи трансформації з самого початку, тоді як 18% запровадили безпеку після події, що вказує на різні підходи до кібербезпеки в цифровій трансформації.

5. 44% бізнес-лідерів підкреслюють важливість CISO у передачі технічних аспектів кібербезпеки керівникам і радам, що відображає зростаючу стратегічну важливість кібербезпеки в процесі прийняття організаційних рішень.

6. Експлуатація загальнодоступних програм спричинила 26% інцидентів.

Отже, збільшення загроз кібербезпеці ставить під загрозу не лише функціонування бізнесу, а й вимагає значних інвестицій у безпеку. Дані підтверджують, що кіберінциденти найчастіше стають причинами переривання діяльності, перевершуючи навіть стихійні лиха чи енергетичні проблеми.

1.3 Типи й етапи реалізації загроз мережевій безпеці

Загрози мережевій безпеці - це спеціальні методи атак, які використовують вразливості фізичних пристроїв або програмного забезпечення мережі [10].

Для ідентифікації та запобігання кібервторгненням розроблена модель Cyber Kill Chain® [11], яка визначає, що зловмисник має зробити, щоб досягти своєї мети. Сім кроків підвищують видимість атаки і покращують розуміння аналітиком тактики, методів і процедур зловмисника. Проявом кібератаки є успішне виконання взаємопов'язаних кроків (Рис. 1.2):

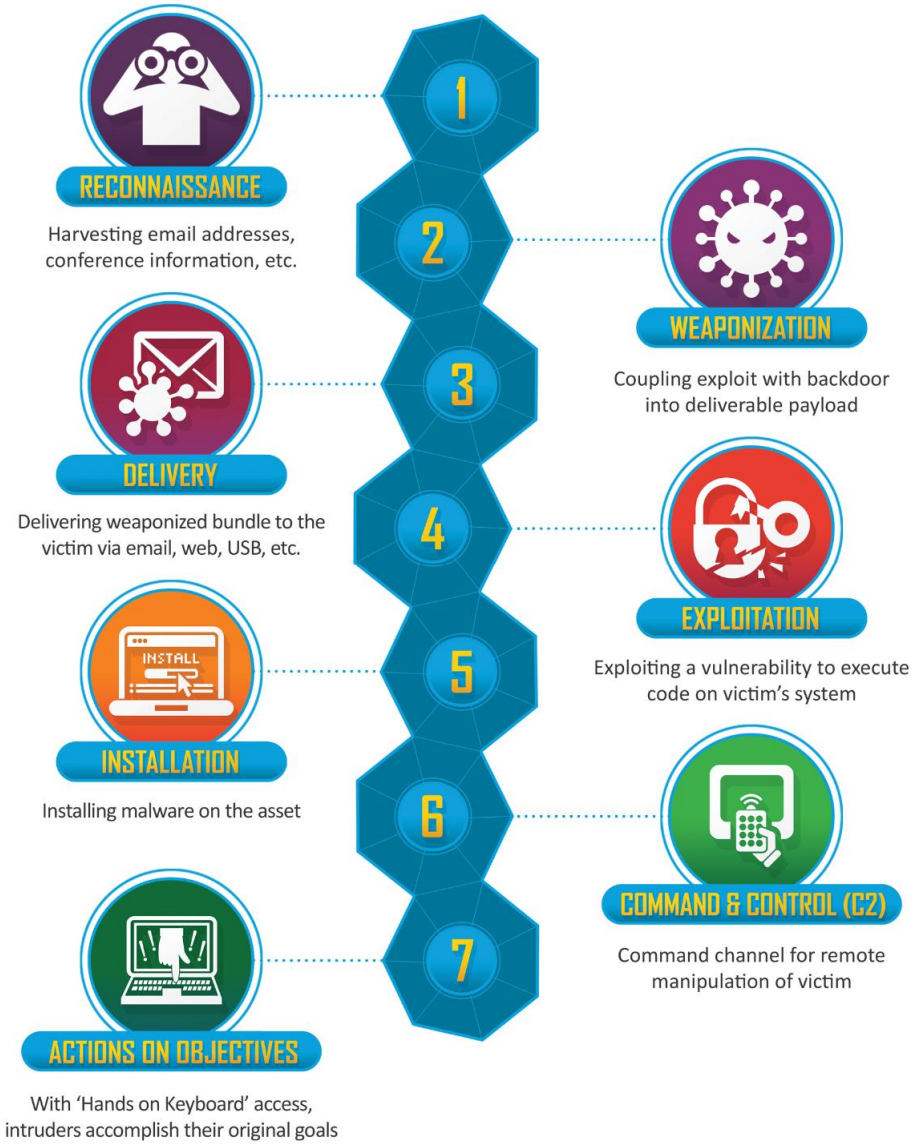

Рис. 1.2. Модель реалізації кібератаки Cyber Kill Chain

Етап 1. Розвідка

Цей етап охоплює вибір мети, виявлення особливостей організації, специфічних вимог у цій галузі, вибір технологій, вивчення активності підприємства у соцмережах чи через розсилки. Фактично, зловмисник намагається отримати відповіді на такі питання: «Які методи атаки працюватимуть із найбільшим ступенем успіху?» або «Які з них найлегше здійснити з погляду інвестицій і ресурсів?»

Етап 2. Озброєння та упаковка

На цьому етапі можливі різні форми: експлуатація веб-додатків, стандартні або спеціально виготовлені шкідливі програми, уразливості у документах різних форматів (PDF, Office тощо) або атаки типу watering hole. Зазвичай вони готуються відповідно до мети атаки з урахуванням специфіки організації-жертви.

Етап 3. Доставка

Передача необхідного (шкідливого) контенту відбувається з ініціативи хакера (SQL-ін'єкція або компрометація мережевої служби) або жертви (наприклад, користувач заходить на шкідливий сайт, внаслідок чого передається шкідлива програма, або він відкриває шкідливий PDF-файл).

Етап 4. Зараження

Після доставки на комп'ютер або пристрій користувача шкідливий контент розгортається, встановлюючись в оточенні. Зазвичай, це відбувається через використання відомої вразливості, для якої раніше було наявне виправлення. У більшості випадків (залежно від мети) зловмисник не витрачає додаткових ресурсів на пошук і експлуатацію невідомих уразливостей.

Етап 5. Встановлення

Часто установка (використання) відбувається на тлі певних зовнішніх з'єднань. Зазвичай шкідлива програма приховується у таких операціях, непомітно проникаючи на кінцеві точки, до яких можна отримати доступ. Потім порушник має можливість контролювати цю програму без відома жертви.

Етап 6. Отримання контролю

На цьому етапі хакери починають контролювати активи жертви за допомогою таких переважно віддалених методів, як DNS, Internet Control Message Protocol (ICMP), веб-сайти та соціальні мережі.

У результаті зловмисник передає контрольованим «активам» необхідні команди щодо подальших дій і збору інформації. Для збору даних використовуються такі методи: знімки екрана, контроль натискання клавіш, злом паролів, моніторинг мережі на облікові дані, збір чутливого контенту й документів. Нерідко призначається проміжний хост, куди копіюються всі дані, а потім стискаються/шифруються для подальшого відправлення.

Етап 7. Виконання дій щодо жертви

На фінальному етапі порушник відправляє зібрані дані та/або виводить з ладу IT-активи під час свого перебування в мережі жертви. Потім проводяться заходи щодо виявлення інших цілей, розширення своєї присутності всередині організації та вилучення даних [12].

Залежно від мети (наприклад, компанії, державні установи, окремі особи, тощо) і цілей зловмисника складність успішного проникнення (без ідентифікації) значно відрізняється. За атаками стоять кіберзловмисники: окремі особи або групи, націлені на інфраструктури, комп’ютерні мережі та системи разом із їхніми аналогами в Інтернеті речей (наприклад, мобільними телефонами, IP-камерами, розумними будинками тощо). Зловмисний намір порушника залежить від його типу й мотивації. Виділяють три категорії зловмисників відповідно до місця їх перебування по відношенню до цільової організацію і рівня знань про неї [13]:

• Внутрішні або інсайдери - мають високий рівень знань про цільову мережу, системи, безпеки, політики та процедури. За даними Інституту комп’ютерної безпеки (CSI) [14], існує два вектори внутрішніх загроз, а саме працівники організації, які мають (1) зловмисні наміри (наприклад, розкрити та/або продати непублічну інформацію); (2) незловмисні наміри (наприклад, шляхом здійснення ненавмисної помилки). Більшість втрат припадає на останній вектор загрози.

• Зовнішні - порівняно з внутрішніми загрозами, таким зловмисникам перед нападом доводиться витрачати багато часу на збір інформації про ціль через їх обмежені попередні знання.

• Змішані групи - складаються з внутрішніх і зовнішніх зловмисників.

Кіберзловмисників також розрізняють за їхніми навичками, мотивами й потенційними цілями. Виходячи з цілей і навичок, кіберзловмисникам потрібна різна «зброя», як-от уразливості нульового дня, експлойти й набори експлойтів, а також ботнети для розподілених атак типу «відмова в обслуговуванні» (DDoS), і в той же час їм потрібне фінансування. У більшості випадків фінансування надходить з викрадених кредитних карток і біткойн-гаманців, які часто отримують за допомогою фішингових електронних листів, шахрайства, програм-вимагачів та оренди своїх навичок «злочин як послуга».

Успішне профілювання кіберзловмисників може значно підвищити технічну й освітню готовність організації, а також допомогти пом’якшити й зменшити наслідки атаки. Профілювання кіберзловмисників також може мінімізувати час, зусилля та ресурси, необхідні для їх виявлення. Крім того, це дозволяє розробляти точніші й адаптовані моделі загроз [15].

Розглянемо основні типи загроз мережевій безпеці (Рис.1.4).

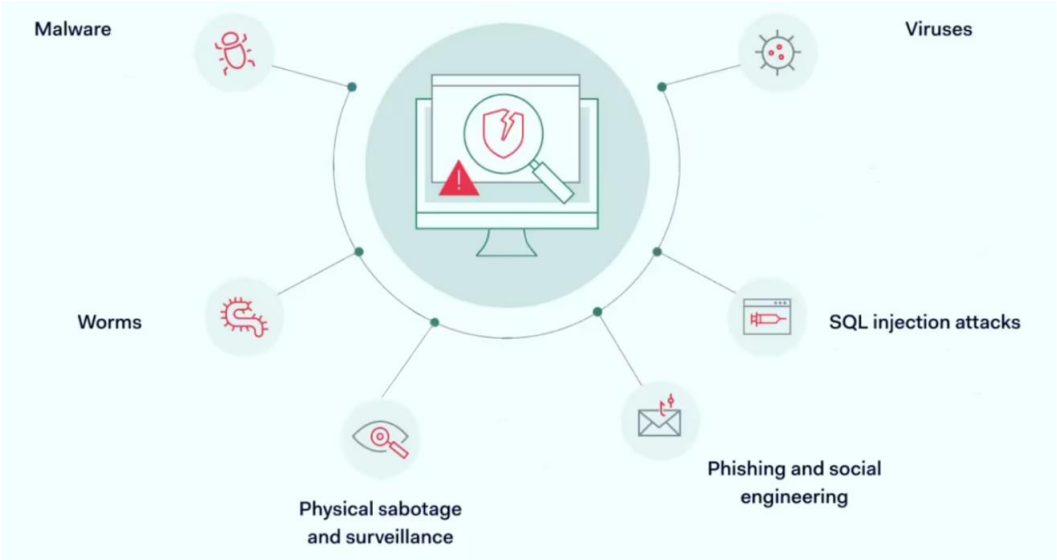

Рис. 1.3. Типи загроз мережевій безпеці

Шкідливе або зловмисне програмне забезпечення - це категорія комп’ютерних програм (або, загалом, коду), розроблених з метою заподіяти шкоду комп’ютерній мережі, комп’ютерній системі або її користувачам шляхом навмисного порушення одного чи кількох ключових аспектів комп’ютерної безпеки (тріади CIA) [16] або виконати будь-які дії проти волі й основних інтересів користувачів або власників обчислювальної системи.

Інфекція. Зараження включає в себе самовідтворення програми (або її частини) і вставку її копій в інші програми, файли або структури пам'яті. Інфекція, якщо вона не використовується на початковому етапі впровадження шкідливого ПЗ, часто запускається через взаємодію з користувачем (зазвичай, використовуючи трюки соціальної інженерії) або автоматизованими засобами (наприклад, експлуатацію вразливості).

Віруси - категорія шкідливого програмного забезпечення, що поширюється переважно через інфікування. Залежно від середовища їх виконання, вони можуть бути додатково класифіковані як: (a) скомпільовані, якщо вони знаходяться в оброблюваній формі процесора (тобто машинний код) або (b) інтерпретовані, якщо вони вимагають скриптового/макрорушія для їх виконання.

Уразливості - це недоліки, наявні в апаратному або програмному забезпеченні системи, які можуть дозволити противнику виконувати дії або використовувати систему ненавмисно. Експлойти - це програми або код, створені й використані для експлуатації вразливості [17]. Нерозкриті уразливості, невідомі дизайнеру або вразливій системі, називаються вразливостями нульового дня. У контексті атак шкідливого ПЗ, експлуатація вразливостей передбачає використання експлойтів для досягнення виконання довільного коду.

Черв'яки - категорія автономного шкідливого програмного забезпечення, яке поширюється автономно через комп'ютерну мережу. Як і у випадку з вірусами, вони можуть бути спочатку викликані взаємодією користувача. Вони можуть поширювати: (a) використовуючи вразливості, наявні в системі, або (b)

реалізуючи інші доступні варіанти зв'язку (повідомлення електронної пошти, підключення до неправильно налаштованих систем тощо).

Соціальна інженерія охоплює маніпулятивні психологічні методи, які використовуються зловмисним актором проти інших, щоб вплинути на них, щоб діяти проти їх власної волі і кращих інтересів [18].

Два найпопулярніші комунікаційні вектори в контексті атак шкідливих програм: (а) фішинг, коли зловмисник віддалено спілкується з обраними цілями, наприклад, за допомогою електронних листів, служби коротких повідомлень (SMS) та миттєвих повідомлень (IM) тощо, і (б) персоніфікація, коли зловмисник контактує з обраними цілями або через голосовий зв'язок (наприклад, телефонні дзвінки), або особисто.

Трояни або троянські коні: категорія зловмисного ПЗ, яке використовує методи соціальної інженерії, щоб виглядати доброякісними або бажаними, щоб спонукати їхню ціль запустити їх. Зазвичай вони додаються до існуючих, доброякісних, надійних або інших бажаних (до цільових) файлів або ПЗ.

Системні пошкодження включають дії, які порушують цілісність системи, шляхом маніпулювання або знищення її даних, програмного чи апаратного забезпечення. Метою таких дій є скомпрометувати доступність системи й максимізувати особисту вигоду зловмисника від наслідків цих дій.

Програми-вимагачі (Ransomware) - категорія шкідливого програмного забезпечення, що використовує криптографічні методи й алгоритми для блокування доступу до системи (шляхом націлювання на критичні файли або її ОС) або до її даних (шляхом націлювання на створені користувачем файли), або тимчасово, поки викуп не буде сплачений, або назавжди, якщо його метою є пошкодження системи.

Логічні бомби: категорія зловмисного коду або ПЗ, навмисно вставленого в систему або її програмне забезпечення, зі здатністю ініціювати зловмисне корисне навантаження, коли виконуються певні умови (наприклад, досягнуто певної дати або визначений обліковий запис користувача було видалено).

Заходи приховування. Шкідливе ПЗ часто використовує засоби приховування, щоб уникнути їх виявлення системами моніторингу безпеки (включаючи рішення для захисту від зловмисного ПЗ, моніторинг процесів, системи виявлення/запобігання вторгненням тощо), ОС або власниками/ користувачами системи.

Руткіти: категорія зловмисного програмного забезпечення, призначеного для маскування або повного приховування своєї присутності від власників/ користувачів системи або будь-якого існуючого програмного забезпечення моніторингу шляхом зміни внутрішніх функцій ОС і структур пам'яті або програмного забезпечення низького рівня (ПЗ пристрою або драйвери тощо).

Таємний доступ (backdoor): категорія шкідливого програмного забезпечення, встановленого в системі для забезпечення легкого доступу (локального чи віддаленого) до неї та полегшення виконання довільного коду. Зразки зловмисного ПЗ можуть використовувати кілька методів, наприклад:

• Хуки, інструкції переходу, які використовуються для перенаправлення потоку виконання програми до певного сегмента коду, а потім назад у вихідне місце. Їх можна розмістити в таблицях імпорту/експорту надійного виконуваного файлу або шляхом переписування частини його коду.

• Двійкові файли ОС і структури пам'яті можуть бути змінені для виконання зловмисного корисного навантаження або для приховування його існування.

• Звичайні мережеві протоколи зв'язку (наприклад, протокол передачі гіпертексту HTTP) і шифрування також можна використовувати для маскування вмісту й наявності мережевих з'єднань, таким чином уникаючи систем виявлення вторгнень, які використовують мережу виявлення аномалій або глибоку перевірку пакетів.

• Зворотні з'єднання, ініційовані цільовою системою до системи, контрольованої зловмисником, можуть успішно обійти правила фільтрації мережі, які забороняють вхідні з'єднання.

Крадіжка інформації передбачає збір і вилучення даних (наприклад, конфіденційної інформації, облікових даних або файлів) із цільової системи назад до зловмисника, що зазвичай досягається за допомогою таких засобів як:

• Викрадачі облікових даних: програми, розроблені для вилучення облікових даних із системи шляхом сканування структур у пам’яті, файлів ОС або застосування трюків соціальної інженерії (наприклад, показ фальшивого екрана входу).

• Кейлоггери: програми, які записують натискання клавіш (і, можливо, інформацію про графічний інтерфейс системи) для збору введеної конфіденційної інформації.

• Сніфери: програми, що перехоплюють канали зв'язку для збору інформації.

• Інструменти віддаленого адміністрування/доступу (RAT): категорія шкідливого ПЗ, що використовується для дистанційного керування низкою систем. Більшість RAT не обов’язково розробляються для зловмисних цілей, що ускладнює їх виявлення та приписування інциденту, оскільки існують дійсні, доброякісні способи використання RAT.

• Шпигунське програмне забезпечення: категорія зловмисного ПЗ, яке діє без згоди користувача як для встановлення, так і для дій, розроблене спеціально для збору та вилучення інформації користувача.

Атаки на відмову в обслуговуванні (DoS-атаки) спрямовані на доступність залучених систем і головним чином мережевих служб, які на них працюють. Відповідно до Посібника з обробки інцидентів комп’ютерної безпеки Національного інституту стандартів і технологій (NIST) [19], DoS-атака визначається як дія, яка виснажує обчислювальні ресурси, як-от центральний процесор (CPU), пропускну здатність, пам’ять і дисковий простір у порядку, щоб запобігти або порушити авторизоване використання систем, мереж і програм.

На основі цього визначення можна виділити три основні категорії DoS-атак, спрямованих відповідно на ширину смуги пропускання мережі, системні ресурси й ресурси додатків. Крім того, DoS-атаки можна класифікувати за

кількістю потенційних зловмисників. Тільки один або невелика кількість кібер-зловмисників можуть запускати безпосередньо DoS-атаки, які не вимагають величезного обсягу мережевого трафіку. З іншого боку, кілька кібер-зловмисників можуть співпрацювати, щоб сформувати розподілену відмову в обслуговуванні (DDoS) або атаки посилення.

Розподілені атаки на відмову в обслуговуванні (DDoS-атаки) є більш ефективними, оскільки їх здійснюють багато хакерів або скомпрометованих машин, а ймовірність перевантаження цілі значно зростає. Зазвичай у цьому випадку зловмисник компрометує інші машини, які називаються «зомбі» або ботами, які згодом використовуються для підтримки DDoS-атаки. Велика кількість ботів утворює ботнет. Зазвичай такі атаки проводяться в ієрархічній манері, де для керування «зомбі» використовуються машини-обробники. Ця ієрархія пропонує численні переваги, оскільки головний зловмисник може давати конкретні вказівки машинам-обробникам щодо того, як поводитись із ботами, які знаходяться під їхнім контролем.

Ін'єкційні атаки за допомогою мови структурованих запитів (SQL) спрямовані на використання вразливостей веб-додатків для доступу до неавторизованої інформації. Сьогодні, на відміну від статичних веб-сайтів, більшість веб-додатків використовують бази даних для належної обробки свого динамічного вмісту. Зазвичай такі програми використовують SQL-запити, щоб отримати інформацію, таку як особиста інформація, місцезнаходження та інформація про кредитну картку.

Основною метою атак SQL-ін'єкцій є масове вилучення даних. Наприклад, зловмисник спробує отримати файл зі вмістом таблиць бази даних, включаючи особисту інформацію клієнтів. Однак атаки SQL-ін'єкцій також можна використовувати для зміни або видалення вмісту бази даних, виконання DoS-атак або запуску зловмисних команд ОС. Зокрема, ці атаки можуть бути життєздатними, коли зловмисні команди SQL помилково фільтруються на екрановані символи або типи різних полів у базі даних SQL не надто надійні, що

дозволяє зловмисникам створювати комбінації, здатні повертати або змінювати неавторизований вміст. Типова атака SQL-ін’єкції складається з таких кроків:

1. Зловмисник виявляє вразливу веб-програму до атак SQL-ін’єкцій і надсилає зловмисну команду SQL.

2. Веб-сервер отримує шкідливу команду SQL і пересилає її до бази даних.

3. Шкідлива команда SQL виконується над базою даних, таким чином витягуючи відповідний вміст.

4. Веб-сервер створює сторінку, яка містить результат виконання шкідливої команди SQL.

Висновки до розділу 1

Встановлено, що мережева безпека - це набір правил і конфігурацій, призначених для захисту цілісності, конфіденційності й доступності комп’ютерних мереж і даних за допомогою як програмних, так і апаратних технологій. Мережева безпека забезпечує досягнення таких універсальних цілей: запобігання несанкціонованому доступу до ресурсів мережі; виявлення та припинення кібератак і порушень безпеки; забезпечення надання доступу до мережевих ресурсів авторизованим користувачам.

Дослідження показало, що безпека мережі забезпечує низку переваг для організації, серед яких захист конфіденційних даних у мережі; відповідність нормативним вимогам безпеки; запобігання збоям у наданні послуг; створення довіри до організації як надійного партнера й надавача послуг.

Аналіз статистики засвідчив, що показники атак на корпоративні мережі і обсяги збитків внаслідок руйнівної діяльності хакерів постійно зростають; серед найбільш деструктивних загроз виділяють атаки фішингу, програм-вимагачів, DDoS-атаки, використання методів штучного інтелекту. З огляду на це інвестиції у кібербезпеку загалом і мережеву безпеку зокрема продовжуватимуть зростати.

Загрози мережевій безпеці - це спеціальні методи атак, які використовують вразливості фізичних пристроїв або програмного забезпечення мережі.

Відповідно до моделі Cyber Kill Chain реалізації кібератаки є послідовністю семи етапів, які дозволяють зловмиснику досягти поставленої мети: розвідка (збір інформації про жертву); озброєння та упаковка (вибір методів впливу); доставка засобів впливу у цільову систему; зараження (експлуатація відомої вразливості системи); інсталяція шкідливих засобів впливу; отримання віддаленого контролю над роботою системи; виконання дій щодо жертви (захоплення даних, збій, виведення з ладу системи).

У результаті дослідження виділено такі основні типи загроз мережевій безпеці: шкідливе або зловмисне програмне забезпечення, вразливості експлуатації, соціально інженерія, системні пошкодження, заходи приховування, таємний доступ, крадіжка інформації, атаки на відмову в обслуговуванні, розподілені атаки на відмову в обслуговуванні та атака SQL-ін'єкції.

Розділ 2 НОРМАТИВНО-ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ МЕРЕЖЕВОЇ БЕЗПЕКИ

2.1 Розробка комплексної стратегії забезпечення мережевої безпеки підприємства

Стратегія мережевої безпеки – це план високого рівня захисту активів компанії протягом наступних 3-5 років. Оскільки технології та мережеві загрози постійно змінюються, керівництву компанії, ймовірно, доведеться переглядати їй стратегію раніше ніж через 3 роки. Стратегія мережевої безпеки не повинна бути ідеальною; скоріше, це добре обґрунтована ставка на те, що слід робити. Оскільки компанії та світ навколо змінюються, стратегія також має змінюватися. Корпоративні активи будуть краще захищені, якщо буде створена і впроваджена ефективна стратегія мережевої безпеки.

Зазвичай це передбачає перехід від реактивної до проактивної позиції безпеки, зосередженої на запобіганні мережевим нападам та інцидентам, а не реагуванні на них постфактум. З іншого боку, надійна стратегія мережевої безпеки краще підготує компанію до реагування на будь-які події, допоможе захистити її репутацію та зменшити шкоду для її співробітників, клієнтів, партнерів та інших зацікавлених сторін, запобігаючи переростанню незначних проблем у серйозні. Стратегія мережевої безпеки має бути ефективною, тобто забезпечувати досягнення поставлених цілей з оптимальним використанням ресурсів, мати належну підтримку серед керівництва компанії, її працівників та партнерів, і постійно вдосконалюватися [20]. Чотири кроки, щоб досягти цього відображені на рисунку 2.1.

1. *Розпізнавання мережевих загроз* передбачає:

- вивчення типів мережевих атак, з якими зараз стикається компанія для того, що зрозуміти мережеву загрозу;

- визначення типів ризиків, які зараз є найбільш поширеними і серйозними у компанії: зловмисні програми, фішинг, інсайдерські загрози тощо;
- аналіз конкурентів, які нещодавно стикалися з великими інцидентами;

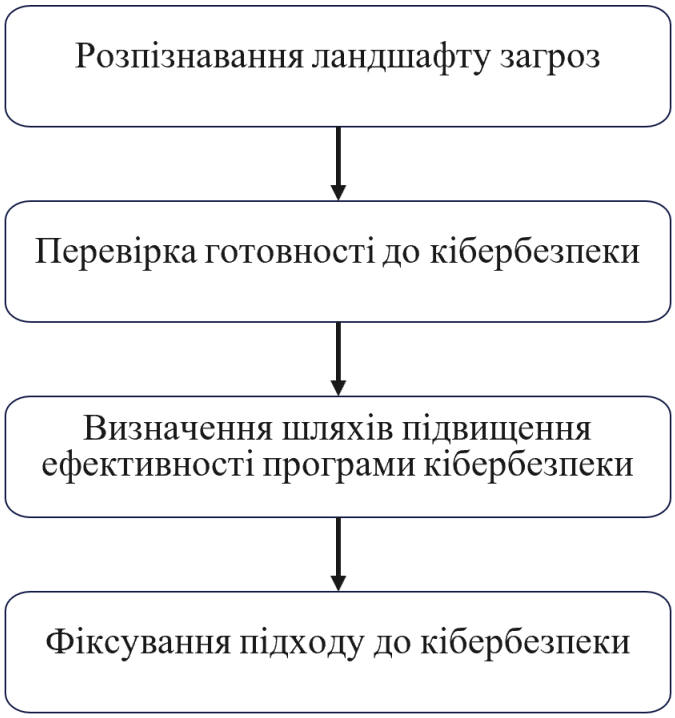

Рис. 2.1. Етапи розробки стратегії мережевої безпеки компанії

- ознайомлення з очікуваним розвитком мережевих загроз, які можуть вплинути на компанію в майбутньому.

Багато аналітиків безпеки вважають, що найближчим часом зростатимуть загрози з боку програм-вимагачів, а також проблеми ланцюга постачання, такі як отримання зіпсованих компонентів і використання їх усередині компанії або включення їх у споживчі товари. Розуміння того, з якими небезпеками компанія зіткнетеся в майбутньому, а також усвідомлення серйозності кожної з цих загроз є критично важливим для розробки успішної стратегії мережевої безпеки.

2. *Перевірка готовності до мережевої безпеки*. Після визначення мережевих загроз, з якими стикається компанія, необхідно провести аналіз рівня зрілості її системи мережевої безпеки. Для цього можна використовувати різні підходи, зокрема концепцію NIST Cybersecurity Framework [19].

Цей документ дозволяє оцінити зрілість організації в сотнях категорій і підкатегорій, що охоплюють політики, управління, технології безпеки, навички відновлення після інцидентів тощо. Оцінка має охоплювати всі технології компанії, включаючи традиційні IT, операційні технології, IoT та кіберфізичні системи.

На основі оцінки та з використанням цього підходу визначають, до якого рівня зрілості в кожній категорії та підкатегорії прагне дійти компанія протягом наступних 3-5 років. Наприклад, якщо розподілені атаки типу "відмова в обслуговуванні" становлять серйозну небезпеку, компанія може інвестувати в більш складні можливості мережевої безпеки. Якщо ж програми-вимагачі є головною проблемою безпеки, важливо переконатися, що належним чином розроблені системи резервного копіювання й відновлення. Тимчасові інструменти, запроваджені під час пандемії COVID-19, потрібно буде посилити, якщо політики віддаленої роботи стануть постійними. Ці нові стратегічні цілі стають цільовим рівнем зрілості для компанії.

3. *Визначення способів підвищення ефективності програми мережевої безпеки*. Після визначення поточного рівня зрілості й цільових показників мережевої безпеки, необхідно визначити, які технології та кращі практики можуть допомогти в досягненні поставлених цілей. Цей етап передбачає розробку програми мережевої безпеки, яка відповідає стратегічним цілям компанії.

Важливо розуміти, що будь-яке вдосконалення потребує витрат ресурсів, включаючи фінанси, час, персонал тощо. Тому слід ретельно проаналізувати різні підходи до досягнення цілей, враховуючи їх переваги та недоліки. Одним із варіантів може бути часткове або повне передання завдань з мережевої безпеки на аутсорсинг. Після вибору оптимальних варіантів, їх необхідно представити вищому керівництву для отримання оцінки, відгуку та, можливо, підтримки. Важливо зазначити, що зміни в програмі мережевої безпеки можуть вплинути на ведення бізнесу. Тому керівництво компанії має бути проінформованим про це і

сприймати це як необхідний ризик, якщо компанія прагне належним чином захистити себе від мережевих атак.

4. *Документування та вдосконалення стратегії мережевої безпеки*. Після отримання схвалення керівництва на впровадження програми мережевої безпеки, необхідно ретельно задокументувати всі аспекти підходу до мережевої безпеки. Це передбачає:

- створення або оновлення оцінок ризиків, які описують ймовірні мережеві загрози, вразливі місця та потенційні наслідки кіберінцидентів;
- розробку або оновлення стратегії мережевої безпеки, яка визначає цілі та пріоритети мережевого захисту, а також шляхи їх досягнення;
- створення або оновлення правил, інструкцій і процедур мережевої безпеки, які чітко визначають ролі та відповідальності персоналу в питаннях мережевої безпеки;
- оновлення інших документів, пов'язаних з мережевою безпекою, таких як план реагування на інциденти, політика мережевої безпеки тощо.

Важливо, щоб всі зацікавлені сторони, включаючи керівництво, персонал і постачальників послуг мережевої безпеки, чітко розуміли свої ролі й відповідальності. Під час розробки та оновлення документів з мережевої безпеки необхідно активно залучати співробітників, які будуть їх використовувати. Це допоможе їм краще зрозуміти важливість мережевої безпеки та сприятиме кращому виконанню своїх обов'язків.

Важливо також проводити регулярні навчання з питань мережевої безпеки для всіх співробітників, щоб вони були в курсі нових загроз та методів захисту. Корпоративна культура мережевої безпеки має постійно розвиватися і вдосконалюватися, щоб відповідати мінливим мережевим загрозам. Це передбачає регулярний перегляд і оновлення документів з мережевої безпеки, а також проведення навчання та тренінгів для співробітників. Оскільки кожен працівник відіграє важливу роль у забезпеченні мережевої безпеки компанії,

важливо, щоб весь колектив розумів свою відповідальність за мережеву безпеку і вживав заходів для захисту мережевих активів компанії.

Аналіз прогалин. Ландшафт мережевих загроз постійно змінюється, і процедури безпеки, які діяли вчора, можуть бути неадекватними сьогодні. Кожну секунду відбувається мережева атака, і порушення безпеки може призвести до втрати особистої інформації клієнта, що призведе до фінансових санкцій і заплямованої репутації. Організації можуть використовувати аналіз прогалин в мережевій безпеці, щоб знайти вразливі місця в своїх заходах мережевої безпеки, забезпечуючи стабільність і ефективність мережі. Порівнюючи поточну діяльність компанії із найкращими галузевими практиками, аналіз прогалин у безпеці демонструє, що слід робити, і дає зрозуміти, як бізнес може запровадити належну структуру та засоби контролю [21].

Аналіз прогалин у мережевій безпеці може надати численні переваги, якщо його виконати належним чином. Розглянемо, як це зробити.

Вибір системи (фреймворку) безпеки, що відповідає галузевим стандартам

Використання системи безпеки, що відповідає галузевим стандартам, надає ряд переваг:

- Базові кращі практики: Ці розробки надають базові кращі практики, які можна використовувати для вимірювання й порівняння корпоративної програми безпеки.
- Охоплення важливих аспектів безпеки: Фреймворки безпеки охоплюють важливі аспекти безпеки, такі як оцінка ризиків, контроль доступу, фізична безпека, управління змінами тощо.

Один із найпоширеніших фреймворків - ISO/IEC 27002. Цей стандарт слугує чудовим орієнтиром для оцінки політик безпеки і засобів управління мережею.

Платформи мережевої безпеки

Однак для аналізу плану безпеки й забезпечення відповідності заходів

безпеки галузевим нормативам рекомендується використовувати платформи мережевої безпеки. Це пов'язано з тим, що платформи мережевої безпеки мають автоматизовані алгоритми, які часто можуть виявляти слабкі місця, які люди, що щоденно користуються мережею, можуть не помітити. Таким чином, використання галузевих стандартів і платформ мережевої безпеки може допомогти компаніям створити та підтримувати ефективну програму мережевої безпеки. Деякі з основних платформ мережевої безпеки:

Брандмауер:

- Cisco ASA: пропонує розширений захист мережі з гнучкими можливостями керування трафіком.
- Palo Alto Networks: забезпечує глибокий огляд трафіку та виявлення загроз на рівні додатків.
- Fortinet FortiGate: інтегрує мережеві функції з функціями безпеки, включаючи IPS, VPN, та веб-фільтрацію.

Системи виявлення та запобігання вторгнення (Intrusion Detection and Prevention Systems IDS/IPS):

- Snort: відкрите джерело IDS, яке використовує правила для аналізу мережевого трафіку.
- Suricata: платформа, яка забезпечує IDS, IPS та мережевий моніторинг.

Інформація про безпеку та керування подіями (Security Information and Event Management):

- Splunk: збирає, аналізує та візуалізує дані з різних джерел для виявлення інцидентів.
- IBM QRadar: пропонує комплексний підхід до управління подіями безпеки з використанням аналітики та кореляції подій.
- ArcSight (Micro Focus): система для збору, аналізу та кореляції подій безпеки.

Контроль доступу до мережі (Network Access Control):

- Cisco ISE: забезпечує контроль доступу до мережі та динамічне управління політиками безпеки.
- Aruba ClearPass: пропонує інтегроване рішення для контролю доступу до мережі та управління автентифікацією.

Виявлення та реагування кінцевих точок (Endpoint Detection and Response):

- CrowdStrike Falcon: хмарна платформа для виявлення та реагування на загрози на кінцевих точках.
- Carbon Black: забезпечує моніторинг активності на кінцевих точках для виявлення підозрілої поведінки.

Моніторинг та аналіз мережі (Network Monitoring and Analysis):

- SolarWinds Network Performance Monitor: пропонує інструменти для моніторингу продуктивності мережі та виявлення проблем.
- Nagios: відкрите джерело для моніторингу мережі та серверів з можливістю розширення.

Управління вразливостями (Vulnerability Management):

- Qualys: хмарна платформа для управління вразливостями та відповідності стандартам.
- Nessus: сканер вразливостей, що допомагає виявляти потенційні загрози у мережах.

Оцінка персоналу та процедур

Оскільки людські помилки, такі як ненавмисне натискання на фішинговий лист, є причиною багатьох мережевих інцидентів, важливо провести оцінку персоналу та процедур для виявлення й усунення потенційних слабких місць.

Керівництво компанії має забезпечити:

- проведення навчання працівників з питань мережевої безпеки, щоб інформувати їх про нові загрози та методи захисту;
- наявність набору процедур та схвалень, які необхідно виконати перед впровадженням будь-яких змін до системи безпеки;

- розробку чітких процесів для відмови у випадку виявлення проблем під час впровадження змін, а також надання та скасування доступу до систем і даних для нових співробітників та звільнених осіб.

Проведення ретельного аналізу мережевої безпеки з урахуванням цих факторів допоможе компаніям краще зрозуміти ризики, пов'язані з людським фактором, та вжити заходів для їх мінімізації. Важливо зазначити, що це лише деякі з питань, які слід враховувати при оцінці персоналу та процедур. Кожна компанія має свої унікальні потреби та ризики, тому важливо провести всебічну оцінку, щоб виявити всі потенційні слабкі місця.

Збір інформації

Метою збору даних як люди отримують доступ до мережі організації та які засоби контролю мережевої безпеки застосовуються є з'ясування, наскільки добре поточна програма мережевої безпеки працює в технічній архітектурі компанії:

- визначити ефективність роботи поточної програми безпеки в рамках технічної архітектури;
- порівняти використовувані засоби контролю з передовими стандартами (ISO 27002, NIST 800-53) та галузевими вимогами;
- провести порівняльну оцінку процедур безпеки з іншими успішними практиками;
- виявити прогалини і слабкі місця в системі безпеки компанії шляхом вибіркового аналізу мережевих пристроїв, серверів і програмного забезпечення.

Результатами збору даних з питань мережевої безпеки є формування вичерпної картини технічного середовища компанії; наявності переліку механізмів безпеки; оцінка загальної ефективності системи мережевої безпеки.

Збір даних є важливим етапом для оцінки поточної позиції компанії з точки зору мережевої безпеки, визначення пріоритетів для покращення програми безпеки та розробки ефективних стратегій захисту від мережевих загроз.

Перевірка системи мережевої безпеки

Останнім кроком у процесі покращення мережевої безпеки є детальна перевірка програми безпеки. Використання платформи мережевої безпеки може допомогти в цьому процесі, оскільки дозволяє: автоматично співвідносити дані за всіма критеріями для створення профілю IT-безпеки; визначити сильні сторони та сфери, які потребують покращення; розробити рекомендації щодо плану безпеки, який відповідає потребам конкретного бізнесу.

Комплексний план безпеки повинен включати:

- Оцінку мережевих загроз.
- Визначення кадрових потреб.
- Оцінку фінансових потреб.
- Визначення часових рамок для впровадження заходів з покращення мережевої безпеки.

Перевірка системи безпеки допоможе гарантувати, що програма безпеки відповідає поточним потребам і ризикам; визначити пріоритети для покращення; ефективно використовувати ресурси; забезпечити стійкість до мережевих загроз. Важливо зазначити, що перевірка системи безпеки - це постійний процес. Оскільки з часом з'являються нові загрози та вразливості, важливо регулярно перевіряти й оновлювати програму безпеки [22].

2.2 Розробка політики мережевої безпеки. Впровадження стандартів та практик безпеки

Політика мережевої безпеки - це документ/набір документів, які розробляє організація на основі власних вимог, щоб створити структуру безпеки з загальним наміром захистити дані. Політика безпеки спрямовує компанію на прийняття рішень щодо мережевої безпеки (зокрема впровадження процесів, технологій, закупівель, укомплектування персоналу тощо) і накладає певні обов’язки й відповідальності щодо захисту інформації на працівників.

Створення ефективної політики є першим кроком у формуванні структури мережевої безпеки організації. Однак слід дотримуватися прагматичного підходу та мати варіанти для всіх можливих сценаріїв, які відповідають вимогам бізнесу. Політика має бути практичною та доступною для виконання. Політики мережевої безпеки відіграють важливу роль у захисті даних та активів організації. Ось деякі з ключових причин їх впровадження:

1. Встановлення вимог мережевої безпеки: політики чітко визначають вимоги, яких повинні дотримуватися співробітники й організація в цілому, щоб гарантувати безпеку інформації. Це включає правила щодо використання паролів, доступу до даних, обробки конфіденційної інформації та інших аспектів безпеки.

2. Визначення напрямку побудови структури безпеки: політики безпеки слугують орієнтиром для створення структури захисту даних і активів організації. Ця структура може включати технічні й організаційні заходи, такі як навчання з питань мережевої безпеки й чіткий розподіл відповідальності, використання брандмауерів, систем виявлення вторгнень, забезпечення відеонагляду тощо.

3. Демонстрація вразливостей компанії до ризиків і підтримки керівництва: політики відображають основні ризики безпеки, притаманні конкретній організації, напрями їх запобігання і протидії, і підтверджують відповідальне ставлення до безпеки з боку вищого керівництва компанії.

4. Підтримка юридичних та етичних зобов'язань: політики безпеки допомагають організації дотримуватися юридичних та етичних зобов'язань щодо захисту даних, зокрема положень законів про захист даних, галузевих стандартів і специфікацій.

5. Визначення ролей і відповідальності з мережевої безпеки: політики безпеки сприяють створенню механізму для визначення чіткої структури посад і повноважень за мережеву безпеку, наприклад з використанням моделі RACI (Responsible, Accountable, Consulted, Informed). Це допомагає гарантувати, що

кожен працівник знає свої ролі й обов'язки, а також міру відповідальності щодо досягнення очікуваних результатів [23].

Впровадження та дотримання політик безпеки є важливою складовою всебічної програми мережевої безпеки. Ці політики допомагають захистити дані й активи організації, а також гарантують відповідність юридичним та етичним зобов'язанням.

Структура політики мережевої безпеки

Визначаючи політику мережевої безпеки, варто розуміти, що цей документ відображає консолідоване уявлення про екосистему й сукупність вимог і обмежень з мережевої безпеки в організації. Хоча політика може бути як завгодно широкою, вона в першу чергу залежить від вимог бізнесу і нормативних зобов’язань, а її дотримання є ключовим елементом забезпечення мережевої безпеки. Структуру політики мережевої безпеки показано на рисунку 2.2.

Рис. 2.2. Структура політики інформаційної безпеки

Призначення політики мережевої безпеки

Перед розробкою політики безпеки важливо чітко визначити її мету, що дозволить створити загальний підхід до програми безпеки та її складових.

Метою політики мережевої безпеки є:

- створення загального підходу до мережевої безпеки, який охоплює визначення загальних принципів і правил, які регулюють захист інформаційних активів організації;
- виявлення та прогнозування порушень безпеки шляхом впровадження заходів для виявлення і прогнозування потенційних загроз та інцидентів. Це може включати такі заходи, як моніторинг мереж, систем і даних, а також оцінка ризиків [24]
- підтримка бренду та репутації, сприяючи захисту бренду та репутації організації в результаті запобігання витоку даних, мережевих атак та інших інцидентів, які можуть завдати шкоди авторитету компанії;
- дотримання етичних норм і правил відповідності, гарантуючи, що компанія дотримується всіх етичних норм, законів і правил, пов'язаних з мережевою безпекою та захистом даних;
- повага до прав клієнтів шляхом визначення їхніх прав, пов’язаних з персональними даними та іншою приватною інформацією, а також розробки процесу розгляду скарг, проблем і випадків невиконання вимог з боку клієнтів.

Цільова аудиторія

Потрібно ідентифікувати та визначити аудиторію, на яку поширюється політика мережевої безпеки. Щоб визначити правильну аудиторію й очікування, доцільно виокремити цільові групи, які входять у сферу дії політики, а також ті, які не входять до неї.

Визначення цілей

Важливим етапом розробки політики безпеки є чітке визначення її цілей, які мають бути узгоджені з цілями організації загалом і відображати принципи тріади CIA (конфіденційність, цілісність, доступність).

Для того, щоб політика мережевої безпеки відповідала стратегії та пріоритетам організації рекомендується обговорити її цілі з керівництвом організації. Політика має гарантувати, що конфіденційна інформація доступна лише уповноваженим особам; інформація є точною та повною, не була змінена

або пошкоджена в несанкціонований спосіб; уповноважені користувачі мають доступ до інформації та систем, коли це їм потрібно.

Визначені цілі політики повинні відповідати кінцевій меті програми мережевої безпеки, яка має чітко визначати бажаний результат, якого хоче досягти організація за допомогою своєї програми мережевої безпеки [25].

Класифікація даних

Політика мережевої безпеки має спочатку визначити дані, які входять до сфери її дії (на основі визначення власника даних, бізнес- і нормативних вимог), а потім класифікувати їх за кількома категоріями на основі критеріїв чутливості даних і їх доступності для різних аудиторій.

Традиційна схема класифікації даних виділяє такі категорії:

- загальнодоступні;
- для внутрішнього використання;
- конфіденційні;
- з обмеженим доступом.

Власники даних мають нести відповідальність за їх належну класифікацію, тоді як розпорядники даних відповідають за позначення їх відповідними рівнями класифікації та захисту. Обов’язки користувачів даних включають дотримання вимог щодо захисту даних і дотримання відповідності нормативним вимогам.

Контроль доступу та мережева безпека

Рівень повноважень кожної організаційної ролі щодо даних та IT-систем має бути визначено в політиці. Користувачі можуть отримати доступ до мереж і серверів компанії лише за допомогою унікальних логінів, які вимагають автентифікації, як-от паролі, біометричні дані, ідентифікаційні картки або токени. Організація має здійснювати нагляд за всіма системами та відстежувати всі спроби входу.

Підтримка даних та операцій

Політика підтримки даних і операцій має визначати категорії різних зацікавлених сторін, їхні ролі та обов’язки щодо захисту даних. Системи та кінцеві

точки організації мають бути захищені відповідно до організаційних стандартів, кращих практик і рекомендованої конфігурації від виробника оригінального обладнання і відповідати регуляторним вимогам і галузевим стандартам відповідності. Операційна політика має включати резервне копіювання даних, механізм шифрування та захищену практику переміщення даних.

Обізнаність і навчання

Співробітники і партнери компанії відіграють ключову роль у забезпеченні мережевої безпеки. Їхня обізнаність та відповідальність є критично важливими для захисту даних та активів організації.

Для підвищення обізнаності й відповідальності персоналу з мережевої безпеки рекомендується:

- ознайомлення з політиками шляхом надання всім співробітникам доступу до документів з політиками мережевої безпеки. Це допоможе їм зрозуміти вимоги та очікування щодо захисту інформації;
- регулярне проведення навчання і тренінгів з питань мережевої безпеки для персоналу з метою ознайомлення з політиками, процедурами, методами захисту даних, вимогами до контролю доступу й обробки даних.
- навчання гігієни мережевої безпеки для надання персоналу знань і навичок, необхідних для захисту себе та організації від мережевих загроз. Тематика може охоплювати питання виявлення і протидії атакам соціальної інженерії, фішингу, шкідливих програм, а також безпечної поведінки в мережі Інтернет. Типовими рішеннями є впровадження політики чистого екрана та робочого столу, прийняття політики безпечного використання Інтернету, формування переліку заборонених ресурсів чи програм.

Ролі та обов'язки

Для того, щоб мати успішну систему забезпечення мережевої безпеки, весь залучений до цієї діяльності повинен мати визначені ролі та обов’язки. Чітко визначена матриця RACI допоможе організації зрозуміти та чітко визначити ролі та обов’язки [26].

Слід наголосити на необхідності розробки унікального підходу до створення системи забезпечення мережевої безпеки для кожної організації, в рамках якого будуть обрані для впровадження заходи і засоби безпеки, які дозволять досягти визначених цілей політики і нормативної відповідності. У таблиці 2.1 представлено характеристику основних підходів до забезпечення мережевої безпеки, з яких кожна конкретна організація може обрати найбільш прийнятний для неї варіант.

Таблиця 2.1.

Основні підходи до забезпечення мережевої безпеки

Стандарт	Чим керує	Вирівнювання бізнесу
NIST Cybersecurity Framework [27]	Об'єднуючи чинні стандарти, настанови та найкращі практики, ця система була розроблена для того, щоб надати індивідуальні рекомендації щодо управління та зменшення ризиків, пов'язаних з мережевою безпекою.	Хоча це добровільна система, вона є однією з найбільш поширених і цитованих рекомендацій, які будь-яка компанія може використовувати для зниження загального ризику безпеки.
CIS Critical Security Controls [28]	Керує впровадженням та управлінням найважливіших заходів кібербезпеки, які організації повинні вжити для захисту своїх інформаційних систем і даних. Ці заходи розроблені для того, щоб допомогти організаціям зменшити ризики від кіберзагроз шляхом впровадження конкретних дій та процедур.	Бізнес зацікавлений у посиленні безпеки Інтернету речей (IoT).

Продовження табл. 2.1

Серія стандартів ISO 27000 [29]	Призначена для управління інформаційною безпекою та захисту інформаційних активів організацій.	Ці правила мають широку сферу застосування і можуть бути застосовані до кількох компаній або будь-якою одною для оцінки своїх процедур мережевої безпеки.
Серія стандартів ISO 31000 [30]	Регулюють принципи впровадження та управління ризиками в управлінні організацією.	Ці правила мають широку сферу застосування і можуть бути застосовані до різних видів бізнесу або будь-якою компанією для оцінки своїх процедур мережевої безпеки.
PCI-DSS [31]	Це набір з 12 правил, спрямованих проти шахрайств із кредитними картками та захист даних клієнтів.	Інформація про кредитні картки обробляється підприємствами.
COBIT [32]	Поєднуючи бізнес-цілі та IT-цілі, ця система була створена, щоб допомогти підприємствам в управлінні інформаційними та технологічними процесами.	Організації, відповідальні за контроль якості інформації та бізнес-операції, що включають технології. Сфери охоплення: аудит і підтвердження достовірності, відповідність, IT-операції, управління, безпека й управління ризиками.

Оскільки нові галузеві стандарти і регуляторні акти впливають на всі компанії, дотримання вимог мережевої безпеки стає рушійним фактором ефективності бізнесу. Реагуючи на зростаючу кількість і складність мережевих загроз, уряди й організації, що займаються розробкою галузевих стандартів, намагаються впорядкувати галузі мережевої безпеки, розробляючи більш суворі критерії відповідності. З іншого боку, регуляторні норми часто відстають від середовища загроз і викликів безпеки інформації. У таких умовах, щоб не відставати від мінливих вимог середовища і змін регуляторних норм, компанії повинні розробити й постійно оновлювати узгоджену й ефективну стратегію мережевої безпеки, орієнтовану на очікування, потреби і можливості організації.

2.3 Організаційні заходи із забезпечення безпеки мережі

2.3.1 Навчання й підвищення обізнаності у сфері безпеки

Кадрове забезпечення та ресурси відіграють важливу роль у будь-якій стратегічній ініціативі, і це також стосується сфери мережевої безпеки. Люди в будь-якій організації є її найбільшим активом, тому очевидно, що вони повинні розуміти важливість безпеки [33].

Навчання й підвищення обізнаності про безпеку

У цифрову епоху, коли все більше повсякденних справ пересічного громадянина й організації переміщується в онлайн, потреба суспільства в мережевій безпеці зросла, оскільки люди працюють, спілкуються, ведуть бізнес і співпрацюються онлайн. Кіберзлочинці можуть з легкістю завдати шкоди приватному і професійному життю людей, більшість з яких залежні від Інтернету та мобільних пристроїв. Успішна мережева атака в комерційному секторі може завдати значних збитків, а в деяких ситуаціях завдати незворотної шкоди.

Для того, щоб по можливості запобігти або обмежити наслідки кіберзлочинів сучасна компанія має впроваджувати комплекс заходів, почавши з найважливішого кроку: підвищення рівня обізнаності про мережеву безпеку.

Люди залишаються найслабшою ланкою в будь-якій схемі цифрової безпеки. Вони роблять помилки, забувають речі і стають жертвами обману. Саме тут вступає в дію навчання з мережевої безпеки, яке передбачає інформування персоналу про різні ризики та загрози мережевої безпеки, а також про потенційні слабкі місця. Працівники повинні засвоїти найкращі практики та процедури для забезпечення безпеки мереж і даних, а також наслідки їхнього недотримання, які можуть заподіяти непоправної шкоди компанії.

Крім цього, персонал має знати, що у випадку недотримання вимог безпеки будуть застосовані покарання, які можуть включати в залежності від тяжкості проступку отримання догани, виплату штрафу, втрату роботи або притягнення до кримінальної відповідальності. Експерти з мережевої безпеки можуть зміцнити цю можливу вразливість, інформуючи персонал про масштаби ризиків і про те, що може бути поставлено на карту, якщо захист не спрацює.

Переваги навчання й підвищення обізнаності з безпеки

Перш за все, працівники, які пройшли навчання з мережевої безпеки, забезпечують менший ризик для загальної безпеки мережі організації. Чим менше ризиків, тим менше фінансових втрат в результаті кіберзлочинів. Таким чином, компанія, яка виділяє кошти на навчання персоналу з питань мережевої безпеки, має отримати віддачу від цих інвестицій. Крім того, якщо всі співробітники пройдуть навчання з мережевої безпеки, буде менше прогалин у безпеці, якщо хтось звільниться з компанії. Нарешті, компанія, в якій працівники дбають про безпеку, матиме міцнішу репутацію серед клієнтів, оскільки більшість людей не поспішають вести бізнес з компанією, якій вони не довіряють. Незалежно від фактичних наслідків будь-якого порушення, компанія, яка неодноразово зазнає компрометації безпеки, втрачатиме споживачів через несприятливий піар. Люди повинні знати про рекомендовані практики, щоб досягти цього вищого рівня безпеки.

Ключові фактори, які слід враховувати при проведенні навчання й підвищення обізнаності щодо мережевої безпеки

Працівники з різними рівнями технічних здібностей і знань з мережевої безпеки, а також з різними стилями навчання повинні отримати користь від ефективної програми навчання й підвищення обізнаності з мережевої безпеки.

Вона має бути багатогранною, з різноманітними уроками та можливостями для навчання, щоб залучити працівників з усіма рівнями знань і стилями навчання. Комплексна програма також включає рольовий контент, який надає навчальний матеріал, адаптований до потреб ролі працівника, а також матеріал, адаптований для сторонніх зацікавлених сторін, таких як ділові партнери та працівники за контрактом, щоб гарантувати, що окремі особи не поставлять під загрозу організацію.

Існує кілька ключових компонентів успішної програми:

– співробітники повинні мати можливість отримувати інформацію у форматах, які їм найбільше підходять (аудіо, візуальні чи ігрові сесії);

– заняття мають варіюватися за рівнями складності відповідно до можливостей і здібностей працівників;

– контент має бути доступним і відповідати спеціалізації персоналу, щоб працівники могли знайти найбільш релевантний матеріал для своєї роботи.

Подальші дії та постійна комунікація забезпечують інформування працівників про політику мережевої безпеки компанії, надання оперативних нагадувань про те, як виявляти й запобігати ризикам і порушенням безпеки, вирішувати будь-які проблеми безпеки і повідомляти їх про потенційні загрози.

Імітовані атаки, такі як спроби фішингу, анкетування й інші форми оцінювання, використовуються для перевірки того, наскільки добре працівники компанії дотримуються стандартів мережевої безпеки організації, та виявлення осіб, які не відповідають кращим практикам.

Вимірювання результативності та звітування про участь персоналу в навчальних програмах навчання й підвищення обізнаності в організації може допомогти виявити недоліки програми та сфери, які потребують посилення [34].

Ключові рекомендації щодо навчання й підвищення обізнаності з мережевої безпеки показано на рис. 2.3.

Рис. 2.3. Рекомендації щодо навчання й підвищення обізнаності з мережевої безпеки

Різноманітність підходу

Ефективна програма навчання й підвищення обізнаності з мережевої безпеки має бути адаптована до потреб і можливостей різних груп працівників. Це пов'язано з тим, що люди мають різні рівні технічних знань, досвіду і стилі навчання.

Багатогранність програми

Програма навчання має охоплювати різноманітні формати та методи навчання, щоб зацікавити й залучити всіх співробітників, зокрема лекції, семінари, онлайн-курси, ігри, рольові сценарії та інші інтерактивні методи.

Адаптований контент

Важливо, щоб навчальний матеріал був адаптований до ролей та обов'язків працівників. Це допоможе їм зрозуміти, як мережеві загрози можуть вплинути на їхню роботу, й навчить їх, як захищати себе та організацію.

Різні рівні складності

Програма тренінгу повинна пропонувати заняття різного рівня складності, щоб відповідати потребам співробітників з різним рівнем знань та досвіду. Це дозволить їм знайти матеріал, який буде для них актуальним і корисним.

Подальші дії та комунікація

Важливо не лише провести заняття, але й забезпечити подальшу підтримку й комунікацію з персоналом. Це може включати розробку політики мережевої безпеки, надання ресурсів для подальшого навчання, а також створення каналів зв'язку для повідомлення про мережеві загрози.

Імітовані атаки

Проведення імітованих атак, таких як фішингові розсилки або тестові проникнення, може допомогти перевірити рівень обізнаності й навичок працівників у сфері мережевої безпеки. Це також може допомогти виявити слабкі місця в системі безпеки та вжити заходів для їх усунення.

Вимірювання та звітування

Важливо відстежувати результативність програми навчання та звітувати про неї. Це допоможе визначити, чи є програма ефективною, та внести необхідні зміни.

Проведення ефективної програми навчання й підвищення обізнаності щодо мережевої безпеки є важливою інвестицією для будь-якої організації, яка допоможе значно знизити ризики мережевих загроз, покращити стійкість і репутацію, а також підвищити рівень обізнаності та знань персоналу з питань мережевої безпеки.

2.3.2 Перевірка й аудит безпеки

Зростаючий попит з боку громадськості та приватного сектору на інституціоналізацію управління мережевою безпекою з винятковим наглядом за програмами сприяє поширенню інформації про важливість контролю в різних галузях. Типовий аудит, спрямований на перевірку заходів безпеки організації, застосовує підхід, заснований на оцінці ризиків.

Усі члени команди аудиторів, які беруть участь у виконанні завдань з підтвердження довіри до системи управління мережевою безпекою, можуть використовувати підхід, заснований на оцінці ризиків, для обґрунтування вибору діяльності підрозділу, що підлягає перевірці.

Загальна структура системи аудиту безпеки полягає у плануванні підходу, вивченні й оцінці заходів, тестуванні та оцінці засобів безпеки, звітування про результати завдань і подальші дії за рекомендаціями. Оцінка управління мережевою безпекою є важливим елементом аудиторських послуг, що сприяє стратегічному узгодженню діяльності організації, створенню цінності, обробці ризиків, управлінню ресурсами та вимірюванню ефективності діяльності [35].

Процес планування аудиту

Аудит мережевої безпеки зазвичай має організаційний фокус. Під час організаційного аудиту системи управління мережевою безпекою досліджуються розгорнуті структури, управлінські питання і діяльність підрозділів. Однак, під час організаційного планування аудитор може виявити, що система управління не функціонує на належному рівні. У такому випадку особа, яка планує аудит безпеки має використовувати систему цілей контролю мережевих і суміжних технологій для визначення цілей завдань.

Крім того, аудит безпеки може охоплювати й інші сфери аудиту IT. За таких обставин може бути доцільним проведення "орієнтованого на результат" IT аудиту. З кількісної точки зору, аудит, орієнтований на результат, може вирішувати питання ефективності, використовуючи цільові показники й показники ефективності в якості стандартів вимірювання. З якісної точки зору, аудит, орієнтований на результат, може також забезпечити оцінку знань та практик управління сферою аудиту. Незалежно від того, які стандарти вимірювання аудиту, орієнтованого на результати, використовуються, ефективність управління мережевою безпекою є основною метою аудиту підрозділу, що підлягає аудиту.

Основними факторами планування аудиту безпеки є перевірка наявності, адекватності та стратегічного узгодження управління. Однак, як і у випадку з іншими аудитами IT, під час планування завдань необхідно отримати розуміння загального середовища контролю, мережевих систем та процедур контролю, щоб забезпечити дотримання стандартів та керівних принципів аудиту. При визначенні загальних цілей аудиту безпеки відповідальний аудитор має розглянути такі варіанти:

- звітування про систему управління;
- звітування про ефективність управління;
- залучення або вилучення фінансової інформації;
- залучення або вилучення нефінансової інформації.

Крім того, при визначенні цілей аудиту мережевої безпеки може знадобитися врахування інших зусиль і результатів діяльності підприємства із забезпечення надійності. Детальні цілі аудиту безпеки зазвичай залежать від системи управління, прийнятої вищим керівництвом компанії. Таким чином, парадигма оцінювання аудиту безпеки може відображати очікування щодо ефективності або відповідності.

На сферу аудиту безпеки можуть впливати потреби цільової аудиторії та рівні розповсюдження інформації. Відповідальний аудитор повинен враховувати окремі та об'єднані зв'язки підрозділу, що підлягає аудиту, з іншими організаціями та підрозділами, а також функціональні процеси для визначення обсягу аудиту, як показано на рисунку 2.4 [36].

Рис. 2.4. Функціональні процеси для визначення обсягу аудиту

Відповідальний аудитор повинен включити до сфери аудиту відповідні процеси планування, організації та моніторингу діяльності з безпеки. Крім того, сфера аудиту повинна включати системи контролю за використанням і захистом всього спектру ресурсів мережевої безпеки. Зокрема, люди, інформація, процеси та інфраструктура є тими ресурсами мережевої безпеки, яким необхідно приділяти увагу в рамках систем управління безпекою.

Що стосується кадрового забезпечення аудиту, то потенційні учасники завдань безпеки повинні мати відповідний стаж і кваліфікацію. Якщо завдання аудиту безпеки охоплюють широкий спектр функцій мережевої системи, призначені фахівці з аудиту повинні мати глибокі організаційні знання та розуміння пов'язаних з ними процесів. Критерії відбору персоналу аудиту можуть бути задоволені шляхом поєднання формальної освіти, відповідної сертифікації та професійного досвіду.

Після оцінки потенційних кандидатів на виконання завдань аудиту безпеки визначають, що служба аудиту не має необхідного набору навичок; аутсорсинг професійних послуг може бути варіантом для проведення аудиту безпеки.

Наприклад, співробітники служби аудиту можуть не мати відповідних бізнесових, технічних або базових знань для оперативного проведення планового аудиту безпеки. Таким чином, керівництво аудиту може розглянути можливість передачі аудиту безпеки на аутсорсинг, щоб виконати заплановане завдання.

Висновки до розділу 2

Встановлено, що для того, щоб стратегія мережевої безпеки була ефективною, вона має виконувати чотири кроки: розпізнавання мережевих загроз, перевірка готовності до мережевої безпеки, визначення способів підвищення ефективності програми мережевої безпеки, документування та вдосконалення стратегії мережевої безпеки.

Дослідження показало, що політика мережевої безпеки має складатися з: призначення політики мережевої безпеки, визначення цільової аудиторії, визначення цілей, класифікації даних, контролю доступу та мережевої безпеки, підтримки даних та операцій, забезпечення обізнаності і навчання персоналу, встановлення ролей та обов'язків. Основними підходами до забезпечення мережевої безпеки є: NIST Cybersecurity Framework, CIS Critical Security Controls, серія стандартів ISO 27000, серія стандартів ISO 31000, PCI-DSS, COBIT.

Кожна конкретна організація може обрати найбільш прийнятний для неї варіант, відштовхуючись від власних потреб, зокрема великим міжнародним корпораціям доцільно використовувати ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, ISO/IEC 31000; малим і середнім підприємствам - CIS Controls, ISO/IEC 31000; компаніям, що обробляють платіжні дані - PCI DSS; компаніям з розвинутою IT-інфраструктурою - COBIT, ISO/IEC 27001.

Ключовими рекомендаціями щодо навчання й підвищення обізнаності з мережевої безпеки є: різноманітність підходів програми навчання, багатогранність програми, адаптований контент, різні рівні складності, подальші

дії та комунікація, імітовані атаки, вимірювання та звітування результативності програми навчання. Організація ефективної програми навчання та підвищення обізнаності щодо мережевої безпеки є важливою інвестицією для будь-якої компанії, яка допоможе значно знизити ризики мережевих загроз, покращити стійкість та репутацію, а також підвищити рівень знань та обізнаності персоналу у питаннях мережевої безпеки.

Розділ 3. ПРОГРАМНО-ТЕХНІЧНІ ЗАСОБИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЗАГРОЗАМ БЕЗПЕЦІ МЕРЕЖІ

3.1 Превентивні методи мережевої безпеки

З кожним роком зловмисники стають все більш винахідливими та агресивними у своїх спробах використати кіберпростір для власної користі за рахунок інших. У цьому контексті превентивні методи запобігання кіберзагрозам стають критичними для забезпечення мережевої безпеки підприємства. Вони мають на меті не лише реагувати на вже існуючі загрози, а й передбачати їхнє виникнення та запобігати їм заздалегідь. Ці методи охоплюють широкий спектр заходів, від освіти користувачів до використання передових технологій мережевої безпеки.

Проте, превентивні заходи ніколи не будуть на 100% ефективними, тому система захисту мережевої безпеки повинна мати розширені можливості для швидкого виявлення сучасного шкідливого ПЗ, якщо воно проникає крізь передову лінію захисту.

3.1.1 Фізичний захист мережі

Фізичний захист мережі - це комплекс заходів та стратегій, спрямованих на захист фізичної інфраструктури мережі від несанкціонованого доступу, пошкодження або її знищення.

Системи контролю доступу гарантують, що тільки уповноважені особи можуть увійти в певні зони або об'єкти, і передбачають використання таких методів, як ключ-картки, біометрична автентифікація (відбитки пальців або розпізнавання обличчя), PIN-коди або залучення співробітників служби безпеки для перевірки та надання доступу.

Засоби фізичного контролю доступу можуть включати ворота, турнікети, замки, а також охорону на входах і в чутливих зонах. Політика та процедури контролю доступу визначають, кому, коли та за яких умов надається доступ.

Вони також містять протоколи управління відвідувачами для відстеження й моніторингу відвідувачів у приміщенні [37].

Системи відеоспостереження допомагають контролювати та реєструвати діяльність всередині та навколо об'єктів. Вони діють як стримуючий фактор і надають докази в разі інцидентів. Системи відеоспостереження еволюціонували з такими вдосконаленими функціями, як камери високої чіткості, можливості панорамування, нахилу та масштабування, а також відеоаналітика.

Технології відеоаналітики аналізують відеоматеріали в режимі реального часу, автоматично виявляючи підозрілу поведінку, покинуті об'єкти або спроби несанкціонованого доступу. Це зменшує потребу в постійному ручному моніторингу. Хмарні системи відеоспостереження забезпечують віддалений моніторинг, зберігання та доступ до відеозаписів з будь-якого місця з будь-якого місця, підвищуючи обізнаність про ситуацію та полегшуючи розслідування.

Системи виявлення вторгнень виявляють і попереджають персонал служби безпеки про несанкціоновані спроби доступу до зон з обмеженим доступом або про порушення фізичної безпеки. Системи сигналізації можуть включати датчики, детектори руху, детектори розбиття скла або датчики дверей або вікон, які запускають звукові або беззвучні сигнали тривоги у відповідь на несанкціонований доступ або підозрілу діяльність[38].

Політика та процедури безпеки встановлюють чіткі правила для персоналу, підрядників і відвідувачів, які визначають прийнятну поведінку, протоколи контролю доступу та процедури повідомлення про інциденти. Системи управління відвідувачами можуть використовуватися для реєстрації та відстеження відвідувачів, видачі тимчасових посвідчень доступу і ведення журналів обліку. Для запобігання несанкціонованому доступу до конфіденційної або чутливої інформації слід запровадити безпечні процедури утилізації документів, такі як подрібнення або використання захищених контейнерів.

Плани реагування на інциденти визначають конкретні кроки, яких слід вжити під час інцидентів, включаючи канали зв'язку, процедури ескалації та

координацію з аварійними службами. Готовність до надзвичайних ситуацій передбачає регулярні тренування, симуляції або настільні вправи для перевірки ефективності планів реагування й ознайомлення персоналу з процедурами на випадок надзвичайних ситуацій. Системи оповіщення про надзвичайні ситуації, такі як системи масового оповіщення або екстреного мовлення, можуть бути використані для швидкого розповсюдження критично важливої інформації серед працівників під час надзвичайних ситуацій.

Контроль навколишнього середовища включає заходи для підтримки оптимальних умов для обладнання та захисту даних. Системи виявлення та гасіння пожеж, включаючи детектори диму, пожежну сигналізацію, спринклерні установки або системи очищення, допомагають мінімізувати ризик пошкоджень, пов'язаних з пожежею. Системи моніторингу температури та вологості можуть бути використані для забезпечення належних умов навколишнього середовища для чутливого обладнання або складських приміщень [39].

Фізична безпека охоплює інвентаризацію та управління активами для відстеження та захисту цінних активів, таких як IT-обладнання, конфіденційні документи тощо. Системи відстеження активів, маркування активів та обмежений доступ до місць їхнього зберігання допомагають запобігти крадіжкам або несанкціонованому вилученню.

Зовнішні фахівці можуть проводити тестування на фізичне проникнення, оцінку вразливостей або огляд системи безпеки, щоб виявити потенційні слабкі місця та рекомендувати вдосконалення.

Отже, впровадження заходів фізичної безпеки, таких, як системи контролю доступу, системи відеоспостереження, системи виявлення вторгнень, контроль навколишнього середовища, інвентаризацію й управління активами, політики та процедур безпеки, планів реагувань на інциденти допомагають підприємству захистити фізичну інфраструктуру мережі від несанкціонованого доступу, пошкодження або знищення.

3.1.2 Технічні засоби мережевого захисту

Безпека мереж і комунікацій є критично важливим компонентом надійної архітектури мережевої безпеки. Вона передбачає вжиття заходів для захисту конфіденційності, цілісності та доступності даних під час їх передачі мережами.

- *Брандмауери* діють як перша лінія захисту, відстежуючи і контролюючи вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки. Вони можуть бути реалізовані як на рівні мережі, так і на рівні хоста [40].

- *Віртуальна приватна мережа (VPN)* створює безпечні, зашифровані тунелі через загальнодоступні мережі, такі як Інтернет, для забезпечення конфіденційного й автентифікованого зв'язку між віддаленими користувачами або між різними офісами [41].

- *Сегментація мережі* - це стратегічний підхід, який передбачає поділ мережі на окремі сегменти або зони, кожна з яких має свої заходи безпеки та контроль доступу. Ця практика спрямована на мінімізацію наслідків порушення мережевої безпеки шляхом ізоляції критично важливих ресурсів від решти мережі. Таким чином, сегментація мережі ефективно обмежує несанкціоноване бічне переміщення всередині мережі, забезпечуючи додатковий рівень захисту від потенційних мережевих загроз.

Для забезпечення конфіденційності й цілісності даних, що передаються мережею, вкрай важливо впроваджувати безпечні протоколи та методи шифрування. Основними методами є:

- Захист на транспортному рівні (TLS) та рівні захищених сокетів (SSL). Протоколи TLS і SSL відіграють життєво важливу роль у забезпеченні безпечних каналів зв'язку в Інтернеті. Шифруючи дані й перевіряючи автентичність сторін, що спілкуються, ці протоколи створюють надійну основу безпеки для різних мережевих додатків. Від безпечного перегляду веб-сторінок до зашифрованої передачі електронної пошти, TLS і SSL широко використовуються для захисту

конфіденційної інформації та захисту користувачів від потенційних мережевих загроз [42].

- Безпечна оболонка (SSH): SSH - це криптографічний мережевий протокол, який використовується для безпечного віддаленого адміністрування, передачі файлів і безпечного доступу до інтерфейсів командного рядка. Він забезпечує надійні механізми шифрування та автентифікації.

Механізми контролю доступу до мережі гарантують, що тільки авторизовані суб'єкти можуть отримати доступ до мережі та її ресурсів. Ось деякі з ключових аспектів:

- Списки контролю доступу (Access Control List, ACL): ACL визначають правила, які фільтрують і контролюють мережевий трафік на основі певних критеріїв, таких як IP-адреси, протоколи або порти. Вони забезпечують обмеження доступу і дозволяють здійснювати ретельний контроль мережевої взаємодії.
- Мережева автентифікація й авторизація: багатофакторна автентифікацію (MFA) є надійним механізмом автентифікації, який гарантує, що користувачі є тими, за кого себе видають.

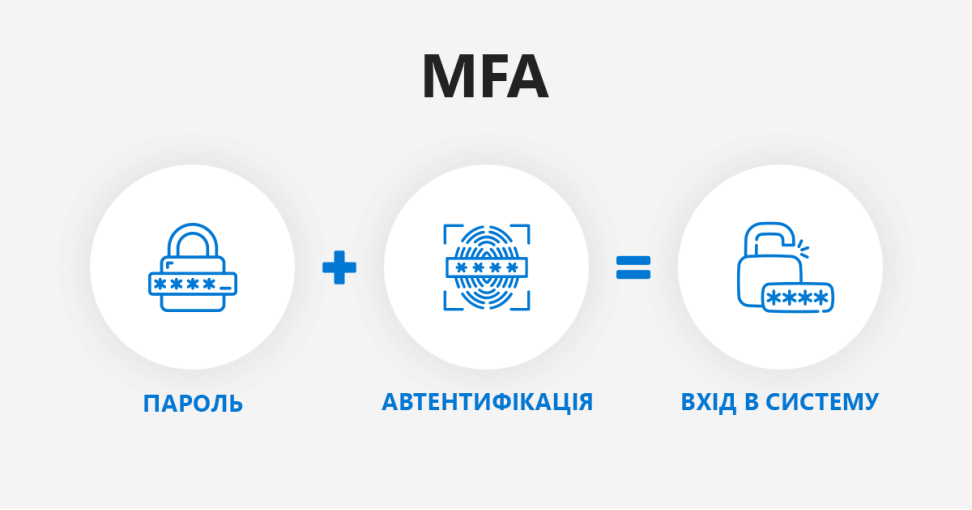

Рис. 3.1. Модель багатофакторної автентифікації

Крім того, належні процеси авторизації гарантують, що користувачі мають відповідні дозволи та привілеї відповідно до їхніх ролей та обов'язків.

Встановлено, що технічні заходи мережевої безпеки, такі як: брандмауер, VPN, сегментація мережі, протоколи TLS, SSL та SSH, списки контролю

доступу, мережева автентифікація й авторизація необхідні для забезпечення мережевої безпеки підприємства і створення безпечної та надійної мережевої інфраструктури організації.

3.2 Технології виявлення та реагування на мережеві загрози

Щоб протистояти мережевим загрозам, організації повинні впроваджувати надійні системи моніторингу та виявлення вторгнень. Ці системи відіграють вирішальну роль у виявленні та реагуванні на потенційні порушення, забезпечуючи мережеву безпеку та безпеку цінної інформації. Основними методами для виявлення та реагування на мережеві загрози є:

1. Впровадження моніторингу в режимі реального часу: моніторинг в режимі реального часу дозволяє організаціям виявляти будь-які підозрілі дії в момент їх виникнення. Постійно відстежуючи мережевий трафік, системні журнали та поведінку користувачів, компанії можуть виявляти потенційні мережеві загрози на ранніх стадіях. Такий проактивний підхід дозволяє оперативно реагувати та пом'якшувати наслідки, мінімізуючи потенційну шкоду, спричинену кібератаками.

2. Використання системи виявлення вторгнень (IDS): системи виявлення вторгнень є життєво важливими компонентами інфраструктури безпеки організації. Ці системи аналізують шаблони мережевого трафіку, виявляють аномальну поведінку і попереджають команди безпеки про потенційні загрози. IDS також можна налаштувати на автоматичне блокування або карантин підозрілих дій, ефективно нейтралізуючи загрози до того, як вони зможуть завдати шкоди.

3. Використання машинного навчання та штучного інтелекту: зростаюча складність мережевих загроз вимагає використання передових технологій, таких як машинне навчання і штучний інтелект (ШІ). Ці технології можуть аналізувати великі обсяги даних, визначати закономірності й виявляти аномалії, які можуть

свідчити про потенційний злам. Постійно навчаючись на нових даних, алгоритми машинного навчання можуть адаптуватися та вдосконалювати свої можливості виявлення з часом, залишаючись на крок попереду мережевих загроз, що еволюціонують.

4. Проведення регулярної оцінки вразливостей: для забезпечення ефективності систем моніторингу та виявлення вторгнень, організації повинні регулярно оцінювати свій загальний стан безпеки. Це включає в себе проведення оцінки вразливостей для виявлення потенційних слабких місць в інфраструктурі, додатках і системах. Оперативно усуваючи ці вразливості, компанії можуть проактивно знижувати ризики та зміцнювати свій захист від потенційних мережевих загроз.

5. Залучення експертів з безпеки: впровадження ефективних систем моніторингу та виявлення вторгнень може бути складним завданням, що вимагає досвіду в галузі мережевої безпеки. Співпраця з експертами з мережевої безпеки або партнерство з постачальниками керованих послуг мережевої безпеки може допомогти організаціям ефективніше орієнтуватися в цьому середовищі. Ці експерти можуть надати цінну інформацію, допомогти у впровадженні та налаштуванні системи, а також запропонувати постійну підтримку для забезпечення оптимальної роботи систем моніторингу та виявлення вторгнень.

Отже, моніторинг та виявлення вторгнень є важливими компонентами будь-якої комплексної стратегії мережевої безпеки. Впроваджуючи моніторинг у режимі реального часу, використовуючи системи виявлення вторгнень, застосовуючи машинне навчання та штучний інтелект, проводячи регулярну оцінку вразливостей та співпрацюючи з експертами з безпеки, організації можуть ефективно виявляти мережеві загрози та реагувати на них. В умовах постійно мінливого ландшафту мережевих загроз інвестиції в надійні технології моніторингу та виявлення вторгнень є проактивним кроком на шляху до захисту цінних даних і зниження ризиків.

3.2.1 Система управління інформацією та подіями безпеки (SIEM)

SIEM - це комплексний підхід до управління мережевою безпекою, який поєднує в собі управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM). Він передбачає збір, аналіз та співставлення даних про події мережевої безпеки з різних джерел в IT-інфраструктурі організації. Це дозволяє аналітикам з мережевої безпеки виявляти та реагувати на потенційні загрози в режимі реального часу, мінімізуючи наслідки вторгнень. Процес дії SIEM-системи показано на рис. 3.2.

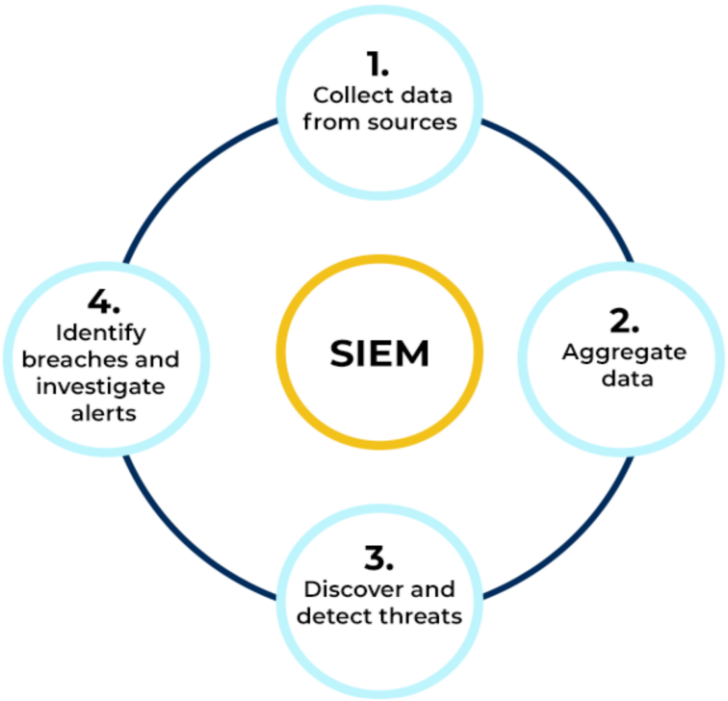

Рис. 3.2. Процес дії SIEM-системи

Впровадження рішення SIEM надає кілька переваг для організацій, які прагнуть посилити свою мережеву безпеку. По-перше, SIEM забезпечує централізовану видимість всього IT-середовища, дозволяючи командам мережевої безпеки відстежувати мережевий трафік, системні журнали й поведінку користувачів з єдиної консолі. Таке цілісне бачення дозволяє швидко виявляти підозрілі дії або аномалії, які можуть свідчити про вторгнення.

Інструменти SIEM використовують передову аналітику й алгоритми машинного навчання для виявлення закономірностей та аномалій у величезних обсягах даних. Безперервно відстежуючи та аналізуючи журнали подій, SIEM

може виявляти потенційні загрози в режимі реального часу. Наприклад, якщо користувач несподівано намагається отримати доступ до конфіденційних даних з незвичного місця або в неробочий час, система SIEM може спровокувати тривогу, що дозволить фахівцям служби мережевої безпеки оперативно розслідувати інцидент.

SIEM не тільки допомагає виявляти вторгнення, але й відіграє вирішальну роль у реагуванні на інциденти та їх розслідуванні. При виявленні вторгнення SIEM може автоматично запускати заздалегідь визначені дії реагування, такі як блокування IP-адреси або ізоляція скомпрометованих систем. Крім того, рішення SIEM можуть надавати детальний криміналістичний аналіз, що дозволяє командам мережевої безпеки зрозуміти першопричину інциденту, масштаби порушення і кроки, необхідні для його усунення.

Для збільшення ефективності SIEM в моніторингу та виявленні вторгнень, організаціям потрібно:

- забезпечити належне управління журналами: збирати та централізувати журнали з усіх відповідних джерел, щоб мати повне уявлення про IT-середовище;
- визначити чіткі сценарії використання та оповіщення: налаштувати правила та оповіщення SIEM відповідно до конкретних вимог мережевої безпеки організації та ландшафту загроз;
- регулярно оновлювати й налаштовувати правила SIEM: вивчати нові мережеві загрози і відповідно коригувати правила SIEM, щоб підтримувати високу точність виявлення;
- проводити регулярні тренінги для аналітиків мережевої безпеки: забезпечувати постійне навчання персоналу служби мережевої безпеки, щоб підвищити їхню обізнаність з інструментами SIEM та покращити можливості реагування на інциденти.

Дослідження показало що, SIEM є критично важливим інструментом для виявлення та обробки інцидентів в будь-якій організації. Завдяки централізованому управлінню безпекою, виявленню загроз у режимі реального

часу, звітності про відповідність нормативним вимогам та вбудованим можливостям, інструменти SIEM можуть допомогти організаціям посилити заходи безпеки.

3.2.2 Системи виявлення вторгнень (IDS)

Системи виявлення вторгнень (Intrusion Detection System, IDS) - це рішення для забезпечення безпеки, призначені для моніторингу мережевого трафіку та виявлення будь-яких підозрілих або зловмисних дій. Вони діють як захисний механізм, постійно аналізуючи мережеві пакети та системні журнали для виявлення потенційних вторгнень. IDS можуть бути розгорнуті як апаратні пристрої або програмні рішення, залежно від вимог та інфраструктури організації [43].

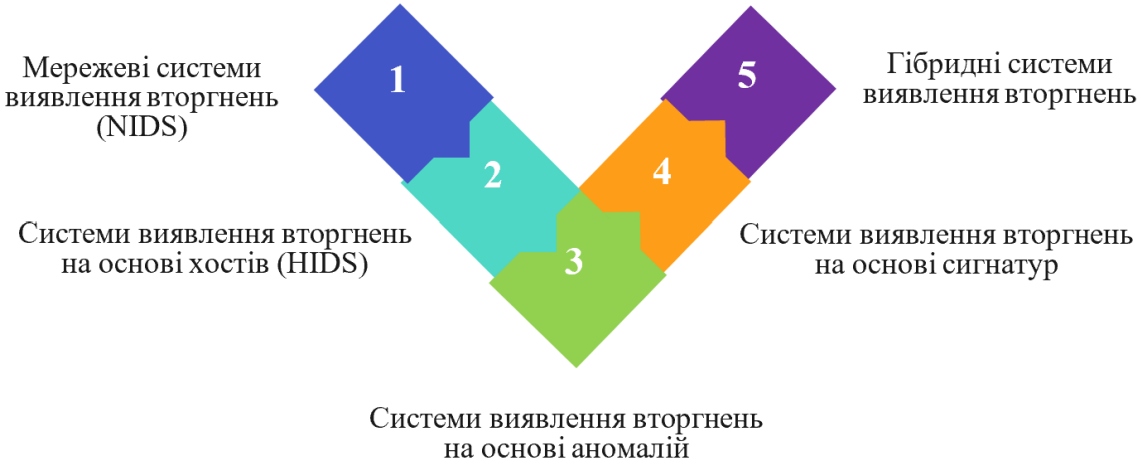

Рис. 3.3. Типи систем виявлення вторгнення

1. *Мережеві системи виявлення вторгнень* (Network Intrusion Detection System, NIDS) призначені для моніторингу мережевого трафіку та виявлення будь-яких підозрілих дій або шаблонів, які можуть вказувати на триваючу атаку. Ці системи аналізують мережеві пакети, шукаючи відомі сигнатури атак або аномальну поведінку. Наприклад, якщо NIDS виявляє велику кількість невдалих спроб входу з однієї IP-адреси, він може позначити це як потенційну атаку грубої сили. NIDS зазвичай розміщують у стратегічних точках мережі, наприклад, на периметрі або в критичних сегментах для контролю вхідного й вихідного трафіку.

2. *Системи виявлення вторгнень на основі хостів* (Host-Based Intrusion Detection Systems, HIDS), на відміну від NIDS, зосереджені на моніторингу активності на окремих хостах або кінцевих точках, таких як сервери або робочі станції. HIDS аналізують системні журнали, цілісність файлів та інші дані, що стосуються конкретного хоста, щоб виявити ознаки несанкціонованого доступу або зловмисних дій. HIDS можуть бути особливо корисними для виявлення внутрішніх загроз або атак, спрямованих на конкретні хости. Наприклад, якщо HIDS виявляє несанкціоновану модифікацію критично важливого системного файлу, він надає попередження для подальшого розслідування [44].

3. *Системи виявлення вторгнень на основі аномалій* застосовують інший підхід, встановлюючи базову лінію нормальної поведінки, а потім визначаючи будь-які відхилення від цієї базової лінії. Ці системи вивчають закономірності мережевого трафіку або поведінки хостів з плином часу і відзначають будь-які аномалії, які можуть свідчити про атаку. IDS на основі аномалій ефективно виявляють раніше невідомі атаки або атаки нульового дня, оскільки вони не покладаються на відомі сигнатури атак. Наприклад, якщо IDS на основі аномалій виявляє раптовий сплеск вихідного мережевого трафіку з хоста, який зазвичай має низький рівень, це може вказувати на скомпрометовану систему [45].

4. *Системи виявлення вторгнень на основі сигнатур*, також відомі як IDS на основі правил, покладаються на базу даних відомих сигнатур атак або шаблонів для виявлення зловмисних дій. Ці сигнатури виводяться на основі аналізу попередніх атак та їхніх характеристик. IDS на основі сигнатур порівнюють вхідний мережевий трафік або поведінку хостів з цими сигнатурами і генерують сповіщення, коли знаходять збіг. Наприклад, якщо система IDS на основі сигнатур виявляє мережевий трафік, що містить певну послідовність байт, яка, як відомо, пов'язана з певним експлойтом, вона видає сповіщення.

5. *Гібридні системи виявлення вторгнень* поєднують в собі сильні сторони декількох методів виявлення, часто інтегруючи методи, засновані на сигнатурах і аномаліях. Ці системи мають на меті забезпечити більш комплексний підхід до

виявлення вторгнень, використовуючи як відомі сигнатури атак, так і виявлення аномальної поведінки. Поєднуючи ці методи, гібридні IDS можуть підвищити точність виявлення та зменшити кількість хибних спрацьовувань. Наприклад, гібридна IDS може використовувати сигнатури для виявлення відомих атак, а виявлення аномалій - для виявлення нових або складних атак, які не мають відомих сигнатур [46].

3.2.3 Системи запобігання вторгненням (IPS)

Виявлення аномалій є критично важливим компонентом систем запобігання вторгненням (Intrusion Prevention System, IPS), який допомагає захистити мережі від зловмисних дій. Це процес виявлення шаблонів або подій, які не відповідають очікуваній поведінці або нормам. Існують різні типи методів виявлення аномалій, що використовуються в IPS, кожен з яких має свій унікальний підхід до виявлення аномалій [47]. Ці методи включають статистичне виявлення аномалій, виявлення аномалій на основі машинного навчання та виявлення аномалій на основі правил.

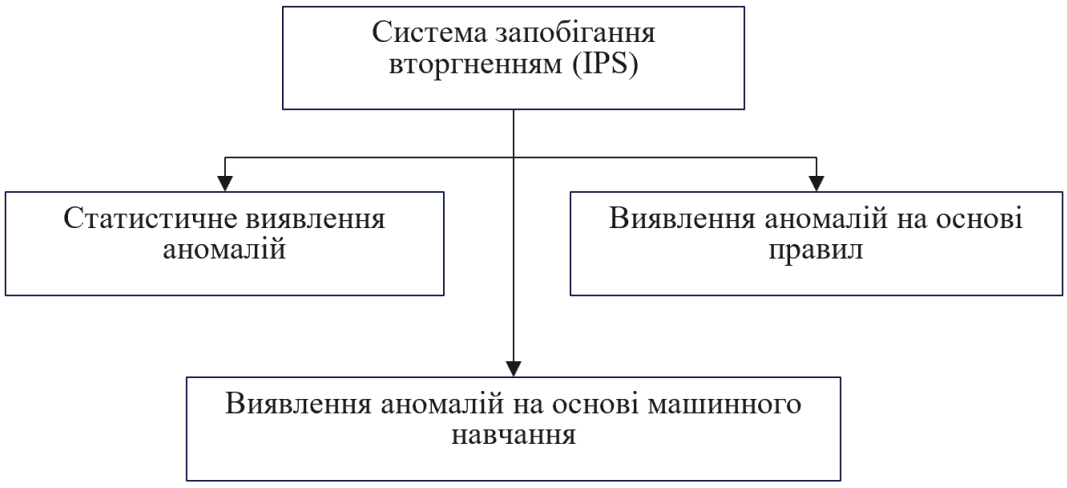

Рис. 3.4. Методи виявлення аномалій системи запобігання вторгненням

- *Статистичне виявлення аномалій* - це метод, який використовує статистичні алгоритми для виявлення аномалій в мережі. Цей метод передбачає збір даних про мережевий трафік і встановлення базової лінії нормальної поведінки. Потім система порівнює нові дані з базовою лінією і позначає будь-

які дані, які відхиляються від норми. Наприклад, якщо користувач раптом починає надсилати надмірну кількість даних, система позначає це як аномалію.

- *Виявлення аномалій на основі машинного навчання* використовує алгоритми машинного навчання для виявлення аномалій. Цей метод передбачає навчання системи на основі історичних даних для виявлення шаблонів, які вказують на нормальну поведінку. Після того, як система вивчила, що є нормальним, вона може ідентифікувати будь-які відхилення від норми. Наприклад, якщо користувач раптово починає отримувати доступ до ресурсів, до яких він ніколи раніше не звертався, система позначить це як аномалію.
- *Виявлення аномалій на основі правил* передбачає визначення правил, які встановлюють, що вважається нормальною поведінкою, а що ні. Наприклад, правило може визначати, що якщо користувач намагається увійти в систему більше трьох разів за хвилину, це слід позначити як аномалію. Цей метод часто використовується в поєднанні зі статистичними методами і методами машинного навчання для підвищення точності.

Встановлено, що використання системи запобігання вторгненням (IPS) є ефективним способом захисту мереж від кібератак. IPS забезпечує захист в режимі реального часу, виявляє і запобігає відомим і невідомим загрозам, знижує ризик витоку даних і підвищує продуктивність мережі. Впровадивши IPS, організації можуть забезпечити комплексну мережеву безпеку.

3.3 Засади планування безперервності бізнесу й аварійного відновлення

Планування безперервності бізнесу (Business Continuity Planning, BCP) та планування аварійного відновлення (Disaster Recovery Plan, DRP) є критично важливими процесами, які організації здійснюють для забезпечення своєї здатності продовжувати діяльність та відновлюватися після руйнівних інцидентів або катастроф. Вони включають в себе розробку стратегій, процедур

і політик для мінімізації впливу потенційних збоїв і підтримки бізнес-операцій в несприятливих умовах [48].

Планування безперервності бізнесу зосереджується на підтримці основних бізнес-функцій під час і після руйнівної події. Ключовими елементами BCP є (Рис. 3.5):

- *Аналіз впливу на бізнес* (Business Impact Analysis, BIA) визначає критичні бізнес-процеси, ресурси й залежності, а також оцінює потенційні наслідки збоїв. Це допомагає визначити пріоритетність зусиль з відновлення й ефективно розподілити ресурси.

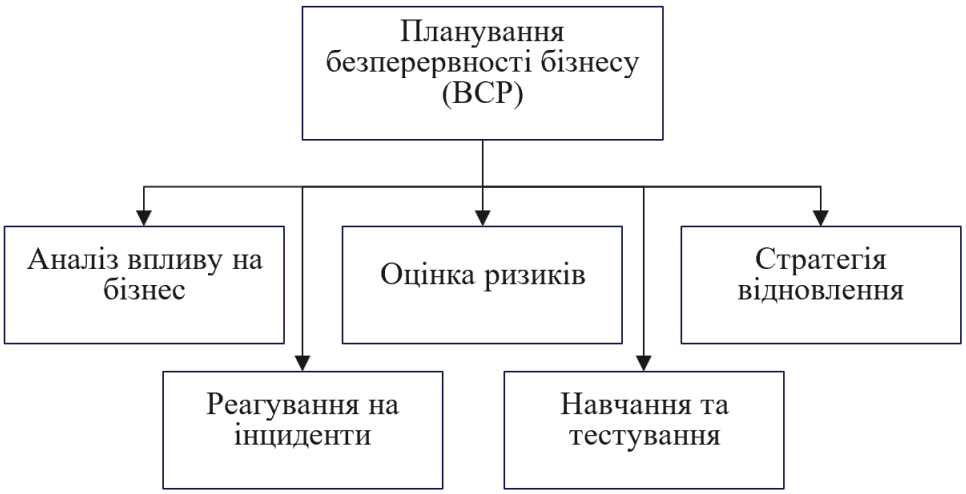

Рис. 3.5. Ключові елементи планування безперервності бізнесу

- *Оцінка ризиків* проводиться організацію для виявлення потенційних загроз і вразливостей, які можуть вплинути на бізнес-операції. Сюди входять стихійні лиха, кібератаки, системні збої, перебої в ланцюжку постачання та інциденти, спричинені людиною.

- *Стратегії відновлення* передбачають розробку планів і процедур для пом'якшення наслідків збоїв. Сюди входить визначення альтернативних об'єктів, впровадження систем резервного копіювання, створення резервних копій й організація роботи з альтернативними постачальниками або провайдерами послуг.

- *Реагування на інциденти* - процедури реагування на інциденти та плани комунікації для забезпечення своєчасного та ефективного реагування на інциденти визначаються в рамках планування безперервності бізнесу й охоплюють створення груп реагування на надзвичайні ситуації, визначення протоколів ескалації та впровадження каналів зв'язку для зацікавлених сторін, персоналу, клієнтів та ЗМІ.

- *Навчання та тестування* - регулярні тренінги і тестування проводяться для перевірки ефективності заходів з планування безперервності бізнесу. Вони включають настільні вправи, симуляції та повномасштабні навчання для оцінки готовності організації реагувати на різні сценарії та відновлюватися після них.

Планування аварійного відновлення фокусується на відновленні критично важливих IT-систем та інфраструктури після збоїв. Ключові елементи DRP показані на рис. 3.6.

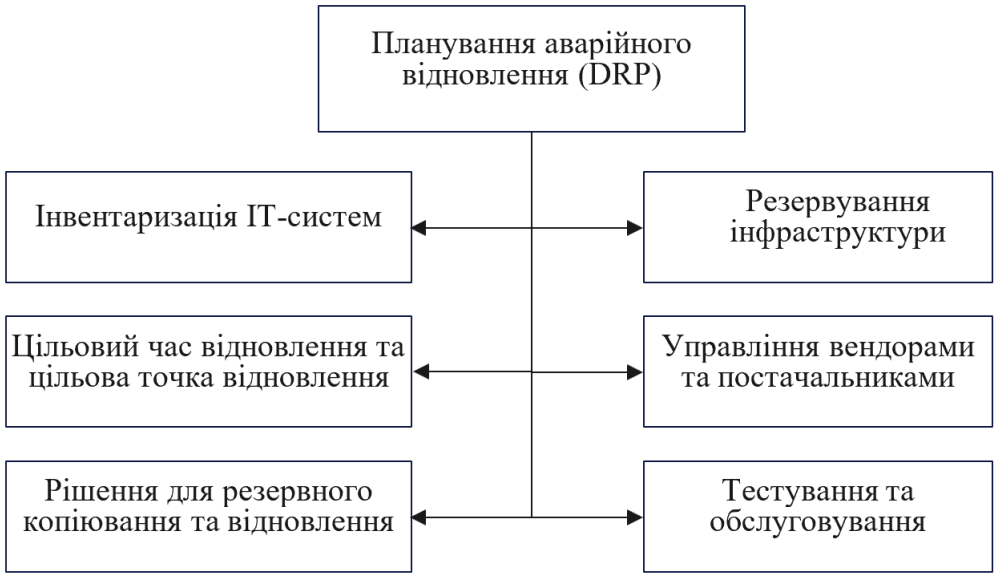

Рис. 3.6. Ключові елементи планування аварійного відновлення

- *Інвентаризація IT-систем* організації має на меті визначити критичні IT-системи, додатки, бази даних і компоненти інфраструктури, які є важливими для бізнес-операцій. Ця інвентаризація допомагає визначити пріоритетність зусиль з відновлення та ефективно розподілити ресурси.

- *Цільовий час відновлення* (Recovery Time Objective, RTO) та *цільова точка відновлення* (Recovery Point Objective, RPO): RTO визначає допустимий час простою систем і встановлює цільовий час відновлення, тоді як RPO визначає максимально допустиму втрату даних у разі збою. Ці показники допомагають вибрати відповідні стратегії та технології відновлення.

- *Рішення для резервного копіювання та відновлення* в організації мають бути надійними, щоб забезпечити цілісність даних і полегшити відновлення систем. Вони можуть охоплювати регулярне резервне копіювання, віддалене зберігання, реплікацію, створення знімків і хмарні варіанти відновлення.

- *Резервування інфраструктури* передбачає реалізацію таких заходів як впровадження системи відмовостійкості, кластеризація, віртуалізація та географічне розмежування центрів обробки даних. Вони допомагають забезпечити високу доступність і мінімізувати час простою під час системних збоїв або катастроф.

- *Управління відносинами з вендорами та постачальниками* технологій і послуг мають на меті забезпечити наявність необхідних ресурсів, підтримки та експертизи під час відновлювальних робіт. Угоди про рівень обслуговування (Service Level Agreement, SLA) та контракти визначають очікування й обов'язки обох сторін.

- *Тестування й обслуговування* - регулярне тестування і планування аварійного відновлення DRP та інфраструктури має вирішальне значення для виявлення та усунення будь-яких вразливостей або прогалин. Організації проводять навчання, тести на відмовостійкість і вправи з відновлення системи, щоб підтвердити ефективність своїх DRP і внести необхідні вдосконалення [49].

Отже планування безперервності бізнесу і аварійного відновлення - це безперервні процеси, які вимагають постійного моніторингу, оцінки та вдосконалення. Організації повинні проводити регулярні огляди, аудити та оновлення, щоб реагувати на зміни в мережевому середовищі, нові загрози, технологічні досягнення та досвід, отримані в результаті інцидентів.

Висновки до розділу 3

Встановлено, що впровадження заходів фізичної безпеки, таких як системи контролю доступу, відеоспостереження, виявлення вторгнень, контроль навколишнього середовища, інвентаризація та управління активами, а також політики та процедури безпеки й плани реагування на інциденти, допомагає підприємству захистити фізичну інфраструктуру мережі від несанкціонованого доступу, пошкодження або знищення. Крім того, ці заходи сприяють виявленню потенційних загроз на ранніх етапах, мінімізують ризики втрат даних і забезпечують безперебійну роботу мережевих систем. Вони також допомагають у дотриманні нормативних вимог і стандартів безпеки, що є важливим для уникнення юридичних проблем і підвищення довіри клієнтів та партнерів.

Дослідження показало, що вибір відповідної системи виявлення вторгнень залежить від конкретних потреб і вимог до мережевої інфраструктури організації. Мережеві, хостові, на основі аномалій, на основі сигнатур та гібридні IDS пропонують унікальні переваги у виявленні та реагуванні на потенційні мережеві загрози. Впроваджуючи правильну комбінацію типів IDS, організації можуть значно підвищити свою здатність виявляти та пом'якшувати атаки, посилюючи загальний рівень мережевої безпеки.

Виявлення інцидентів є критично важливою частиною процесу обробки інцидентів у будь-якій організації. Для виявлення інцидентів безпеки організації можуть використовувати різні інструменти і методи, включаючи SIEM та аналіз мережевого трафіку. Найкращий підхід до виявлення інцидентів залежить від потреб і ресурсів організації у сфері мережевої безпеки. Проактивне виявлення зазвичай вважається найкращим підходом, але реактивне виявлення може бути більш прийнятним для організацій з обмеженими ресурсами або досвідом.

Підсумовуючи, слід зазначити, що SIEM підходить для великих корпорацій та підприємств, які зазвичай мають складні IT-інфраструктури та велику кількість подій безпеки, які потребують аналізу; організацій з високими

вимогами до нормативної відповідності: банків, фінансових установ, медичних закладів, які повинні відповідати таким стандартам, як PCI DSS, HIPAA, GDPR; компаній, які працюють з конфіденційними даними і потребують високого рівня захисту та моніторингу для запобігання витокам даних.

IDS підходить для малих і середніх підприємств, які можуть використовувати IDS для моніторингу мережевих загроз без значних інвестицій у складніші системи; організацій з обмеженими ресурсами, які не можуть собі дозволити повноцінні SIEM або IPS рішення, але потребують базового рівня захисту від вторгнень; компаній, які тільки починають розбудову своєї системи мережевої безпеки, де IDS може бути першим кроком у створенні комплексної системи захисту.

IPS підходить для великих підприємств, які обробляють критично важливі дані, не можуть дозволити собі жодних компромісів у безпеці і потребують автоматичного блокування загроз; організаціям, що обробляють великі обсяги транзакцій: наприклад, фінансові установи або e-commerce платформи, де критично важлива швидка реакція на загрози; хостинг-провайдерів і дата-центрів, оскільки вони забезпечують безпеку для великої кількості клієнтів і потребують високого рівня автоматизації захисту.

Встановлено, що BCP і DRP тісно пов'язані між собою та доповнюють один одного. BCP зосереджується на забезпеченні безперервності всіх бізнес-процесів організації, тоді як DRP конкретно націлений на відновлення мережевої інфраструктури після катастрофи. Разом ці плани забезпечують цілісну стратегію реагування на надзвичайні ситуації, яка дозволяє організації мінімізувати втрати, швидко відновити критичні функції та забезпечити безперебійне надання послуг клієнтам.

Отже, всі ці методи допомагають у забезпеченні комплексної мережевої безпеки підприємства, дотриманні нормативних вимог і стандартів безпеки, що є важливим для уникнення юридичних проблем і підвищення довіри клієнтів та партнерів.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що мережева безпека забезпечує досягнення таких універсальних цілей як: захист конфіденційних даних у мережі; запобігання несанкціонованому доступу до мережевих ресурсів; виявлення та припинення кібератак і порушень безпеки; надання доступу до мережевих ресурсів авторизованим користувачам; відповідність нормативним вимогам безпеки; запобігання збоям у наданні послуг; створення довіри до організації як надійного партнера й надавача послуг.

Аналіз статистики засвідчив, що показники атак на корпоративні мережі і обсяги збитків внаслідок руйнівної діяльності хакерів постійно зростають; серед найбільш деструктивних загроз виділяють атаки фішингу, програм-вимагачів, DDoS-атаки, використання методів штучного інтелекту. З огляду на це інвестиції у кібербезпеку загалом і мережеву безпеку зокрема продовжуватимуть зростати.

Встановлено, що для того, щоб стратегія мережевої безпеки була ефективною, вона має передбачати чотири кроки: розпізнавання мережевих загроз, перевірка готовності до мережевої безпеки, визначення способів підвищення ефективності програми мережевої безпеки, документування та вдосконалення стратегії мережевої безпеки. Політика мережевої безпеки має складатися з таких елементів: призначення політики, визначення цільової аудиторії, визначення цілей, класифікації даних, контролю доступу та мережевої безпеки, підтримки даних та операцій, забезпечення обізнаності і навчання персоналу, встановлення ролей та обов'язків.

Основними підходами до забезпечення мережевої безпеки є: NIST Cybersecurity Framework, CIS Critical Security Controls, серія стандартів ISO 27000, серія стандартів ISO 31000, PCI-DSS, COBIT. Кожна конкретна організація може обрати найбільш прийнятний для неї варіант, відштовхуючись від власних потреб.

З’ясовано, що організаційні заходи мережевої безпеки охоплюють,

зокрема, навчання й підвищення обізнаності з питань мережевої безпеки і проведення аудиту безпеки. Програми навчання й підвищення обізнаності мають впроваджуватися із дотриманням принципів різноманітності навчальних підходів, багатогранності й адаптованості контенту до потреб персоналу, використання ігрових і симуляційних методів навчання, вимірювання та звітування результативності програми навчання.

З’ясовано, що впровадження заходів фізичної безпеки, таких як системи контролю доступу, відеоспостереження, виявлення вторгнень, контроль навколишнього середовища, інвентаризація й управління активами, а також політики та процедури безпеки й плани реагування на інциденти, допомагає підприємству захистити фізичну інфраструктуру мережі від несанкціонованого доступу, пошкодження або знищення. Крім того, ці заходи сприяють виявленню потенційних загроз на ранніх етапах, мінімізують ризики втрат даних і забезпечують безперебійну роботу мережевих систем.

Результати аналізу засвідчили, що вибір відповідної системи виявлення вторгнень IDS залежить від конкретних потреб і вимог до мережевої інфраструктури організації. Мережеві, хостові, на основі аномалій, на основі сигнатур та гібридні IDS пропонують унікальні переваги у виявленні та реагуванні на потенційні мережеві загрози. Впроваджуючи правильну комбінацію типів IDS, організації можуть значно підвищити свою здатність виявляти та пом'якшувати атаки, посилюючи загальний рівень мережевої безпеки.

Дослідження показало, що виявлення інцидентів є критично важливою частиною процесу обробки інцидентів у будь-якій організації. Для виявлення інцидентів безпеки організації можуть використовувати різні інструменти і методи, включаючи SIEM та аналіз мережевого трафіку. Найкращий підхід до виявлення інцидентів залежить від потреб і ресурсів організації у сфері мережевої безпеки. Проактивне виявлення зазвичай вважається найкращим

підходом, але реактивне виявлення може бути більш практичним підходом для організацій з обмеженими ресурсами або досвідом.

Встановлено, що планування безперервності бізнесу BCP та аварійного відновлення DRP тісно пов'язані між собою та доповнюють один одного. BCP зосереджується на забезпеченні безперервності всіх бізнес-процесів організації, тоді як DRP конкретно націлений на відновлення мережевої інфраструктури після катастрофи. Разом ці плани забезпечують цілісну стратегію реагування на надзвичайні ситуації, яка дозволяє організації мінімізувати втрати, швидко відновити критичні функції та забезпечити безперебійне надання послуг клієнтам.

Отже, всі ці методи допомагають у забезпеченні комплексної мережевої безпеки підприємства, дотриманні нормативних вимог і стандартів безпеки, що є важливим для уникнення юридичних проблем і підвищення довіри клієнтів та партнерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ultimate Guide to Data Security: Data security empowers your team to safely. *Forcepoint*. URL: https://www.forcepoint.com/cyber-edu/data-security

2. Network security basics. NordLayer. URL: https://nordlayer.com/learn/network-security/basics/

3. Kimachia K. What Is Network Security? Definition, Types, and Benefits. *Enterprise Networking Planet*. URL: https://www.enterprisenetworkingplanet.com/security/network-security/

4. Understanding Network Security: The Different Tools & Types of Protection. IR. URL: https://www.ir.com/guides/understanding-network-security

5. 2023 Official Cybercrime Report. *Esentire*. URL: https://www.esentire.com/resources/library/2023-official-cybercrime-report

6. Ene C. 10.5 Trillion Reasons Why We Need A United Response To Cyber Risk. *Forbes*. URL: https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=613705d33b0c

7. Cost of a Data Breach Report 2023. *IBM*. URL: https://www.ibm.com/reports/data-breach

8. Zaki A. 85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat. *CFO*. URL: https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/

9. Singh S.K., Gibbs P.W., and Bultz G.A. Nuclear Security: Threat Characterization, *National Nuclear Security Administration*, 2014.

10. Network security threats and vulnerabilities. *NordLayer*. URL: https://nordlayer.com/learn/network-security/threats/?gad_source=1&gclid=CjwKCAjw8diwBhAbEiwA7i_sJZ9cpohrLfnEjWB3HWNMI-P0dYmGGgxe9kPs1BN-K74P2d8ejZhReBoCUccQAvD_BwE

11. Cyber Kill Chain. *Lockheed Martin*. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

12. What Is The Cyber Kill Chain? A Comprehensive Guide 101. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/

13. T. Mouroutis, A. Lioumpas Use–cases definition and threat analysis. RERUM FP7 project, 2014.

14. Computer Security Institute, 2010/2011 Computer Crime and Security Survey, 2011.

15. A. Magar "*State-of-the-Art in Cyber Threat Models and Methodologies*, Sphyrna Security", 2016.

16. Souppaya M., Scarfone K. "*Guide to Malware Incident Prevention and Handling for Desktops and Laptops (SP 800-83 Rev. 1)*", National Institute of Standards and Technology (NIST), Jul. 2013.

17. *Discovering and Exploiting Security Holes*, John Wiley & Sons, 2011.

18. C. Hadnagy, "*Social Engineering: The Science of Human Hacking*", Wiley Publishing, 2018.

19. The NIST Cybersecurity Framework (CSF) 2.0. *NIST*. https://doi.org/10.6028/NIST.CSWP.29

20. D. Bodeau and G. Richard, "Cyber Prep 2.0: Motivating organizational cyber strategies in terms of threat preparedness," *MITRE*, 2016.

21. J. Espenschie and G. Angela, "*Threat genomics: An evolution and recombination of best-a available models and techniques for characterizing and understanding computer network threats*," Microsoft Corporation, 2012.

22. J. Meakins, "A zero–sum game: The zero–day market in 2018," *Journal of Cyber Policy*, vol. 4, no. 1, pp. 60–71, 2019.

23. D. Gritzalis, "Zero–day vulnerabilities: A primer," in *Infosec*, Athens, 2017.

24. FIRST, "Common Vulnerability Scoring System Version 3.1," Specification Document, Revision 1, Jun. 2019. URL: https://www.first.org/cvss/v3.1/specification-document

25. M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, “Sphinx: detecting security attacks in software–defined networks,” in Proceedings of the Network and Distributed System Security Symposium (NDSS 2015), pp. 1–15, 2015.

26. M. Cotton, L. Eggert, J. Touch, M. Westerlund, and S. Cheshire, “Internet Assigned Numbers Authority (IANA) procedures for the management of the service name and transport protocol port number registry (RFC 6335),” 2011. [Online]. Available: https://tools.ietf.org/html/rfc6335.

27. Cybersecurity Framework. *NIST*. URL: https://www.nist.gov/cyberframework

28. CIS Critical Security Controls. *CIS*. URL: https://www.cisecurity.org/controls

29. ISO/IEC 27000:2018Information technology - Security techniques - Information security management systems - Overview and vocabulary. *ISO*. URL: https://www.iso.org/standard/73906.html

30. ISO 31000 Risk management. *ISO*. URL: https://www.iso.org/iso-31000-risk-management.html

31. PCI Data Security Standard (PCI DSS). *PCI Security Standards Council*. URL: https://www.pcisecuritystandards.org/standards/pci-dss/

32. COBIT Foundation Certificate. *ISACA*. URL: https://www.isaca.org/credentialing/cobit-foundation

33. P. Yosifovich, A. Ionescu, M.E. Russinovich, and D.A. Solomon, *Windows Internals, Part 1: System Architecture, Processes, Threads, Memory Management, and More*, Microsoft Press, 2017.

34. S. Iannucci and S. Abdelwahed, “A probabilistic approach to autonomic security management,” Proceeding of 13th IEEE International Conference on Autonomic Computing, Jul. 2016, pp. 157–166.

35. Octotrike, “Trike,” Octotrike. URL: http://www.octotrike.org/

36. P. Calderon, *Nmap: Network Exploration and Security Auditing Cookbook—Second Edition: Network Discovery and Security Scanning at Your Fingertips*, 2nd ed., Packt Publishing, 2017.

37. M. Naga Surya Lakshmi and Y. Radhika, “A comparative paper on measuring the per- formance of snort and suricata with variable packet sizes and speed,” *International Journal of Engineering and Technology*, vol. 8, no. 1, pp. 53–58, 2018, doi: 10.14419/ ijet.v8i1.20985.

38. A. H. Vu, N. Tippenhauer, B. Chen, D. Nicol, and Z. Kalbarczyk, “Cybersage: a tool for automatic security assessment of cyber-physical systems,” in: G. Norman, W. Sanders (Eds.), *Quantitative Evaluation of Systems (QUEST 2014*). Lecture Notes in Computer Science, vol. 8657, Springer, Cham, 2014.

39. Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, “Physical layer security game: interaction between source, eavesdropper, and friendly jammer,” *EURASIP Journal on Wireless CommunIcations and Networking*, vol. 2009, Art. no. 452907, 2010.

40. K. Neupane, R. Haddad, and L. Chen, “Next generation firewall for network security: a survey,” in *SoutheastCon 2018*, pp. 1–6, Apr. 2018, doi: 10.1109/SECON.2018.8478973.

41. A. Hay, K. Hay, and P. Giannoulis, *Nokia Firewall, VPN, and IPSO Configuration Guide*, Syngress Publishing Inc., 2009.

42. NIST, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, 2019.

43. M. Cotton, L. Eggert, J. Touch, M. Westerlund, and S. Cheshire, “Internet Assigned Numbers Authority (IANA) procedures for the management of the service name and transport protocol port number registry (RFC 6335),” 2011. URL: https://tools.ietf.org/html/rfc6335.

44. R. Oliveira, L. Sihyung, and H. Kim, “Automatic detection of firewall misconfigura- tions using firewall and network routing policies,” in *IEEE DSN Workshop on Proactive Failure Avoidance, Recovery, and Maintenance (PFARM)*, 2009.

45. H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: a com-prehensive review,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, Jan. 2013, doi: 10.1016/j.jnca.2012.09.004.

46. P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly- based network intrusion detection: techniques, systems and challenges,” *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, Feb. 2009, doi: 10.1016/j.cose.2008.08.003.

47. G.F. Lyon, “Detecting and Subverting Firewalls and Intrusion Detection Systems,” in *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, 1st ed., Insecure.com LLC, p. 464, 2009.

48. V. Jyothsna, V.V. Rama Prasad, and K. Munivara Prasad, “A review of anomaly based intrusion detection systems,” *International Journal of Computer Application*, vol 28, no. 7, pp. 26–35, Sep. 2011, doi: 10.5120/3399-4730.

49. Business continuity vs. disaster recovery: Which plan is right for you? *IBM*. URL: https://www.ibm.com/blog/business-continuity-vs-disaster-recovery-plan/