МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ТЕХНОЛОГІЇ БЕЗПЕКИ КОМП 'ТЕРНОЇ МЕРЕЖІ 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

_____ Вадим КОМАР
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Вадим КОМАР
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., проф. Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., проф. 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

Комару Вадиму Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технології безпеки комп’ютерної мережі підприємства”, керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., проф.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “27“ лютого 2024 р. №36.

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

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, інформація про технології забезпечення безпеки у корпоративних мережах, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати особливості технологічної безпеки підприємства.
   4.2. Дослідити основні методи технологічної безпеки в комп’ютерних мережах.
   4.3. Вивчити інструменти та методи покращення технологічної безпеки на підриємстві.

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	Виконано
2.	Збір та аналіз літератури.	29.03.2024	Виконано
3.	Аналіз особливостей технологічної безпеки підприємства	08.04.2024	Виконано
4.	Дослідження основних методів технологічної безпеки в комп’ютерних мережах	22.04.2024	Виконано
5.	Вивчення інструментів та методів покращення технологічної безпеки на підриємстві	08.05.2024	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	Виконано
7.	Оформлення роботи.	22.05.2024	Виконано
8.	Оформлення презентації.	03.06.2024	Виконано
9.	Отримання рецензії на роботу.	03.06.2024	Виконано
10.	Захист в ЕК.	13.06.2024	Виконано

Здобувач вищої освіти _____ Вадим КОМАР
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(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 Комар В.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології безпеки комп'ютерної мережі підприємства"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КОМАР Вадим у кваліфікаційній роботі проаналізував особливості технологічної безпеки підприємства, дослідив основні методи технологічної безпеки в комп'ютерних мережах, вивчив інструменти та методи покращення технологічної безпеки на підприємстві.

КОМАР Вадим показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

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

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Комар В.С. 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 КОМАРА Вадима
на тему “ Технології безпеки комп’ютерної мережі підприємства ”

Актуальність. У сучасну цифрову епоху безпека комп'ютерних мереж має першорядне значення для підприємств. Кіберзагрози стають все більш витонченими, націленими як на уряди, корпорації, так і на приватних осіб. Стрімкий розвиток IT-сектору призводить до зростання інформаційних ризиків та вразливостей. Забезпечення надійної мережевої безпеки має вирішальне значення для захисту конфіденційних даних і підтримки операційної цілісності. Крім того, фінансові наслідки та репутаційні збитки від кібератак підкреслюють необхідність використання передових технологій безпеки. Це дослідження спрямоване на нагальну потребу в ефективних заходах безпеки в корпоративних комп'ютерних мережах, що робить його важливим науковим дослідженням.

З огляду на зазначене дослідження проблеми технології безпеки комп’ютерної мережі є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено тесхонології та системи захисту інформації у комп’ютерній мережі.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 40 публікацій, в тому числі англомовних.
4. Автор розглянув технології забезпечення безпеки комп’ютерної мережі на прикладі реального підприємства.

Недоліки.

Доцільно було б надати практичні рекомендації з використання досліджених технологій забезпечення комп’ютерної безпеки у підприємстві.

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 КОМАР Вадим заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій безпеки комп'ютерної мережі підприємства. Робота складається зі вступу, трьох розділів, що містять 7 рисунків, висновків та списку використаних джерел з 46 найменувань. Загальний обсяг роботи становить 75 сторінок, з яких 5 сторінок займають перелік умовних скорочень та список використаних джерел.

Мета роботи полягає у розробці та оцінці ефективних технологій безпеки для захисту комп'ютерних мереж підприємств від сучасних кіберзагроз.

Об'єкт дослідження – процес захисту комп'ютерних мереж підприємств, що охоплює різні технології та стратегії мінімізації кіберзагроз.

Предмет дослідження – технології та методи захисту, що використовуються для підвищення безпеки корпоративних комп'ютерних мереж.

Методи дослідження. Для вирішення зазначеної вище наукової задачі в роботі були використані методи літературного огляду, аналізу конкретних ситуацій, практичного впровадження та оцінки. Огляд літератури містить огляд сучасних загроз та технологій безпеки. Тематичні дослідження ілюструють реальні застосування та ефективність різних заходів безпеки. Практичне впровадження включає застосування та оцінку технологій безпеки на підприємстві-партнері. Оцінка включає аналіз показників ефективності, оцінку вразливостей та опитування співробітників для вимірювання впливу впроваджених рішень.

В результаті роботи було проаналізовано поточні загрози, що впливають на комп'ютерні мережі підприємств, оцінено різні технології безпеки, включаючи брандмауери, системи виявлення та запобігання вторгнень (IDS/IPS), рішення для захисту від шкідливого програмного забезпечення, методи шифрування та контроль доступу до мережі (NAC). Практичне впровадження цих технологій було проведено на підприємстві-партнері, Business-Tech, під час стажування. Основні заходи включали модернізацію брандмауерів, впровадження IDS/IPS, проведення навчальних програм для співробітників,

вдосконалення протоколів шифрування та розробку комплексного плану реагування на інциденти. Оцінка виявила значні покращення у сфері мережевої безпеки, зокрема зменшення кількості інцидентів безпеки, посилення захисту даних, покращення обізнаності працівників та пришвидшення реагування на інциденти.

Галузь застосування. Розроблені підходи можуть бути використані для підвищення безпеки комп'ютерних мереж на різних підприємствах, зокрема у фінансовому секторі. Рекомендації містять практичні вказівки щодо впровадження та підтримки надійних заходів мережевої безпеки.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА, МЕРЕЖЕВА БЕЗПЕКА, КІБЕРЗАГРОЗИ, МІЖМЕРЕЖЕВІ ЕКРАНИ, IDS/IPS, АНТИВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ШИФРУВАННЯ, КОНТРОЛЬ ДОСТУПУ ДО МЕРЕЖІ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, НАВЧАННЯ СПІВРОБІТНИКІВ.

ABSTRACT

The qualification work is devoted to the study of security technologies of an enterprise computer network. The work consists of an introduction, three chapters containing 7 figures, conclusions, and a list of references containing 46 titels. The total volume of the work is 75 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop and evaluate effective security technologies for protecting enterprise computer networks from modern cyber threats.

The object of the study is the process of protecting enterprise computer networks, which includes various technologies and strategies for minimizing cyber threats.

The subject of the study is the specific security technologies and methods of protection used to enhance the security of enterprise computer networks.

Research methods. To solve the mentioned higher scientific task, the methods of literature review, case study analysis, practical implementation, and evaluation were used in the work. The literature review provides an overview of current security threats and technologies. Case studies illustrate real-world applications and effectiveness of different security measures. Practical implementation involves applying and assessing security technologies at a partner enterprise. Evaluation includes performance metrics analysis, vulnerability assessments, and employee awareness surveys to measure the impact of the implemented solutions.

As a result, the work analyzed the current threat landscape affecting enterprise computer networks, evaluated various security technologies including firewalls, intrusion detection and prevention systems (IDS/IPS), anti-malware solutions, encryption techniques, and network access control (NAC). Practical implementation of these technologies was conducted at a partner enterprise, Business-Tech, during an internship. Key actions included upgrading firewall systems, implementing IDS/IPS, conducting employee training programs, enhancing encryption protocols, and developing a comprehensive incident response plan. The evaluation revealed

significant improvements in network security, including reduced security incidents, enhanced data protection, improved employee awareness, and faster incident response.

Field of application. The developed approaches and findings can be used to enhance the security of computer networks in various enterprises, particularly those in the financial sector. The recommendations provide practical guidelines for implementing and maintaining robust network security measures.

Keywords: ENTERPRISE COMPUTER NETWORK, NETWORK SECURITY, CYBER THREATS, FIREWALLS, IDS/IPS, ANTIVIRUS SOFTWARE, ENCRYPTION, NETWORK ACCESS CONTROL, INCIDENT RESPONSE, EMPLOYEE TRAINING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
СУБД	Система управління базами даних
СУІБ	Система управління інформаційною безпекою
AI	Штучний Інтелект (Artificial Inteligence)
DDoS	Розподілена відмова в обслуговуванні (Distributed Denial of Service)
DoS	Відмова в обслуговуванні (Denial of Service)
DPI	Технологія перевірки мережевих пакетів (Deep Packet Inspection)
EPP	Захист кінцевих точок (Endpoint Protection Platform)
IDS	Система виявлення вторгнень (Intrusion Detection System)
IPS	Система запобігання вторгнень (Intrusion Prevention System)
ISO	Міжнародна організація зі стандартизації (International Standards Organisation)
MFA	Багато факторна автентифікація (Multi-Factor Authentication)
ML	Машинне навчання (Machine Learning)
NAC	Контроль доступу до мережі (Network Access Control)
VPN	Віртуальна приватна мережа (Virtual Private Network)

ВСТУП

Актуальність теми. У сучасну цифрову епоху безпека комп'ютерних мереж має першорядне значення для підприємств. Кіберзагрози стають все більш витонченими, націленими як на уряди, корпорації, так і на приватних осіб. Стрімкий розвиток IT-сектору призводить до зростання інформаційних ризиків та вразливостей. Забезпечення надійної мережевої безпеки має вирішальне значення для захисту конфіденційних даних і підтримки операційної цілісності. Крім того, фінансові наслідки та репутаційні збитки від кібератак підкреслюють необхідність використання передових технологій безпеки. Це дослідження спрямоване на нагальну потребу в ефективних заходах безпеки в корпоративних комп'ютерних мережах, що робить його важливим науковим дослідженням.

Мета роботи полягає у розробці та оцінці ефективних технологій безпеки для захисту комп'ютерних мереж підприємств від сучасних кіберзагроз.

Об’єкт дослідження – процес захисту комп'ютерних мереж підприємств, що охоплює різні технології та стратегії мінімізації кіберзагроз.

Предмет дослідження – технології та методи захисту, що використовуються для підвищення безпеки корпоративних комп'ютерних мереж.

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

1. Аналізувати сучасний ландшафт загроз, що впливають на корпоративні комп'ютерні мережі.

2. Оцінити різні технології безпеки, включаючи брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), рішення для захисту від шкідливого програмного забезпечення, методи шифрування та контроль доступу до мережі (NAC).

3. Впровадити ці технології на підприємстві-партнері.

4. Оцінити ефективність впроваджених рішень за допомогою аналізу показників ефективності, оцінки вразливостей та опитування співробітників.

5. На основі отриманих результатів розробити практичні рекомендації щодо посилення мережевої безпеки.

Методи дослідження. Для вирішення вищезазначеного наукового завдання були використані методи огляду літератури, аналізу конкретних ситуацій, практичного впровадження та оцінки. Огляд літератури містить огляд сучасних загроз та технологій безпеки. Тематичні дослідження ілюструють реальні застосування та ефективність різних заходів безпеки. Практичне впровадження включає застосування та оцінку технологій безпеки на підприємстві-партнері. Оцінка включає аналіз показників ефективності, оцінку вразливостей та опитування працівників для вимірювання впливу впроваджених рішень.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу обґрунтовано обирати методи та засоби захисту комп'ютерних мереж підприємства. Це необхідно для узгодження з бізнес-цілями, можливостями та ресурсами підприємства, що сприятиме підвищенню загальної безпеки мережі. Практичні рекомендації, отримані в результаті дослідження, можуть бути застосовані для підвищення мережевої безпеки на різних підприємствах, зокрема у фінансовому секторі, забезпечуючи надійний захист від кіберзагроз.

Розділ 1. ОГЛЯД ЛІТЕРАТУРИ ТА ТЕОРЕТИЧНІ ОСНОВИ

1.1 Загальний огляд мережевої безпеки

Кібербезпека покликана підтримувати більшість основних складових сучасного бізнесу: цілісність, конфіденційність і доступність даних за допомогою складних, взаємопов'язаних систем, які підтримують одна одну. У сучасному бізнесі згадка про надійні заходи мережевої безпеки стала вимогою часу, оскільки залежність від цифрової інфраструктури зросла. Розглянемо історію, ключові компоненти і, найголовніше, основи мережевої безпеки в застосуванні до сучасного підприємства. Дослідження ґрунтуватиметься на конкретних даних, підтверджених актуальними, сучасними дослідженнями та цитатами експертів.

1.1.1 Історія та виникнення мережевої безпеки

Історію мережевої безпеки можна простежити з самого її зародження в кінці 1960-х - на початку 1970-х років, коли основна увага була зосереджена на найпростіших типах контролю доступу та деяких заходах фізичної безпеки. У 1980-х роках, з розробкою перших базових брандмауерів і антивірусних програм, почалася перша розробка систем для протидії більш складним загрозам, але найбільш значущий переломний момент настане з масовою появою Інтернету в 1990-х роках, призведе до експоненціального зростання кількості підключень до мережі. Це палиця з двома кінцями: вона може бути як можливістю для надзвичайного зростання, так і джерелом великої небезпеки від кіберзагроз.

Згідно з історичним дослідженням Cisco (2019), більш досконалі версії протоколів безпеки почали з'являтися на початку 90-х років. Першими з'явилися брандмауери - технології, які працювали з фільтрацією пакетів та перевіркою стану пакетів. Приблизно в цей же час були створені перші технології шифрування, які додали суттєвий рівень захисту до передачі даних.

«Історія мережевої безпеки є свідченням постійної гонки озброєнь між захисниками і зловмисниками, коли кожне вдосконалення технології безпеки зустрічають все більш витончені загрози» [24].

1.1.2 Принципи та концепції

Загальні типи мережевої безпеки базуються на наступних принципах, які стосуються різних аспектів захисту даних і систем:

1. Конфіденційність: Це гарантує, що доступ до даних мають лише уповноважені особи. Деякі методи, що використовуються для збереження конфіденційності, включають шифрування, SSL і VPN.
2. Цілісність: Гарантує, що інформація є правильною і не була підроблена. Для цього використовуються контрольні суми, хеш-функції та цифрові підписи, зазвичай для забезпечення цілісності даних під час передачі та зберігання.
3. Доступність: Мережеві сервіси та дані доступні, коли це необхідно для доступу автентифікованих користувачів. Сюди входять превентивні заходи проти стратегії обходу відмов і DoS-атак.

Рис 1.1 Схематичне зображення тріади інформаційної безпеки.

Мережева безпека як така є найважливішим фактором успіху бізнесу в епоху цифрових технологій. Загрози кібербезпеці є сучасними та поширеними, вони здатні підірвати безперервність бізнесу, поставити під загрозу фінансову

цілісність організацій та дискредитувати репутацію бізнесу. Нещодавно компанія IBM (2023) повідомила, що середня вартість витоку даних становить $4,45 млн, підкресливши фінансові наслідки слабкої мережевої безпеки [26].

«Сьогодні хороша мережева безпека - це не варіант, а необхідність. Це не просто питання вартості. Йдеться про здатність організації успішно працювати, впевнено керувати своєю мережею, бути повністю захищеною і відповідати жорсткому регуляторному середовищу, яке постійно розширюється» [39].

1.1.3 Ключові компоненти мережевої безпеки

Мережева безпека - це сукупність усіх спеціалізованих технологій і практик, що використовуються для захисту цифрового простору організації.

Брандмауери визначаються як периметр між довіреною внутрішньою мережею та ненадійними зовнішніми мережами. Вони фільтрують вхідний і вихідний трафік на основі попередньо визначених правил безпеки. Новими функціями брандмауерів є перевірка наступного покоління, яка включає глибоку перевірку пакетів (DPI) і системи запобігання вторгненням (IPS).

Системи виявлення вторгнень проти систем запобігання вторгненням: Якщо IDS є нав'язливою або іншими словами проштовхується через мережеву систему моніторингу для глибокого спостереження, то IPS, з іншого боку, є пасивною за своєю природою, активно блокуючи загрози безпеці централізовано. Ці типи систем є критично важливими для виявлення та пом'якшення наслідків атак на безпеку в режимі реального часу.

Антивірусне програмне забезпечення - це захисні програми, призначені для запобігання шкідливому програмному забезпеченню, найчастіше призначеному для пошкодження, порушення роботи або отримання несанкціонованого доступу до комп'ютерних систем. Воно повинно оновлювати свою базу даних для захисту від нових загроз.

VPN: Віртуальні приватні мережі забезпечують безпечні та зашифровані з'єднання через менш захищені мережі, такі як Інтернет, щоб забезпечити

передачу даних між віддаленими користувачами та їхніми організаціями.

Шифрування - це процес кодування інформації в код або переклад, який можна прочитати, лише якщо його успішно розшифрувати. Конфіденційна інформація повинна передаватися і зберігатися безпечно.

Мережева безпека, розроблена за допомогою моделювання та архітектури

Моделі та архітектури - Багато моделей та архітектур забезпечують основу для практичної реалізації мережевої безпеки:

1. Модель нульової довіри: Модель безпеки, заснована на принципі «ніколи не довіряй, завжди перевіряй». Вона перевіряє особу всіх людей і пристроїв, які намагаються отримати доступ до ресурсів всередині або за межами периметра мережі. Найбільш ефективна в середовищах з підвищеним рівнем віддаленого доступу.

2. Принцип найменших привілеїв: Це правило стверджує, що користувачам слід надавати найменший обсяг доступу, необхідний їм для виконання своєї роботи, а також найменший обсяг привілеїв доступу, щоб обмежити вплив атаки невеликою областю.

1.1.4 Сучасні загрози мережевій безпеці

У сучасному динамічному та різноманітному середовищі загроз деякі з найбільш значущих загроз включають

Шкідливе програмне забезпечення: Шкідливе програмне забезпечення, навмисно розроблене для отримання несанкціонованого доступу, пошкодження або порушення роботи комп'ютерів або мереж. Різні типи шкідливих програм включають віруси, хробаки, троянські програми та програми-вимагачі.

Фішинг: шахрайські електронні листи, які або перенаправляють користувача на шахрайський веб-сайт, або виманюють у нього конфіденційну інформацію, таку як імена користувачів, паролі або навіть дані кредитних карток.

DDoS-атаки: зловмисники насичують мережу великими обсягами інтернет-трафіку, роблячи її непридатною для використання потенційними

користувачами. Це може порушити бізнес-операції і вважається значною фінансовою втратою.

APT - це просунута і наполеглива форма кібератаки, призначена для проникнення в мережу, щоб залишатися непоміченою протягом тривалого часу. Зазвичай її метою є викрадення даних, а не заподіяння негайної шкоди. У 2019 році опитування Ponemon Institute показало, що 68% організацій зазнали щонайменше однієї фішингової атаки за останній рік.

Зі збільшенням кількості та витонченості кіберзагроз вдосконалюються тактики та інструменти, які зловмисники використовують щодня. Все це змушує організації застосовувати багаторівневі підходи до безпеки для ефективного захисту своїх мереж.

1.1.5 Людський фактор у мережевій безпеці

Людський фактор відіграє важливу роль у визначенні ступеня дотримання заходів безпеки в мережі. Безпекові аспекти людського фактору - це обізнаність і навчання співробітників, які є важливими в будь-якій організації. Згідно зі звітом Verizon 2021, 85% витоків даних мали людський аспект - фішинг, неправомірне використання даних або загальне порушення правил безпеки. Це зробить працівників більш підготовленими та поінформованими про останні загрози безпеці та найкращі практики, оскільки компанії можуть інвестувати в часті навчальні програми. Це також може допомогти запобігти ризикам або зменшити вплив людських помилок завдяки ретельним заходам контролю доступу та регулярному оновленню протоколів безпеки.

1.2 Поточне середовище загроз

Сучасне середовище загроз стало дуже динамічним, складним і змінюється завдяки широкому спектру нових кіберзагроз з точки зору їхньої витонченості та масштабу.

1.2.1 Типи кіберзагроз

Шкідливе програмне забезпечення - це будь-яке програмне забезпечення, призначене для проникнення, виведення з ладу або знищення комп'ютерної системи. До поширених типів шкідливих програм належать віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Зараження шкідливим програмним забезпеченням часто відбувається через вкладення в електронні листи, завантаження або використання іншого програмного забезпечення.

Лише у 2021 році компанія McAfee (2021) відзначила 62% зростання кількості атак програм-вимагачів, які шифрують дані жертви, а потім вимагають гроші за програмний ключ, який розшифровує ці дані.

Вимагачі продовжують залишатися одним з найактивніших і найвпливовіших видів кіберзлочинності, зважаючи на зростаючі вимоги зловмисників та постійні інновації в атаках [25].

Фішинг: однією зі стратегій, що використовуються для отримання доступу до різних даних, є фішингові атаки. Зазвичай кіберзлочинці маніпулюють електронною поштою та веб-комунікаціями, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як облікові дані для входу в систему та фінансову інформацію, для зловмисного використання. Здебільшого вони приходять під виглядом повідомлень від надійних джерел, яким довіряють.

Ця потенційна загроза добре задокументована. Це підтверджується звітом Робочої групи з боротьби з фішингом, яка зафіксувала понад 220 000 унікальних повідомлень про фішинг у першому кварталі 2021 року.

«Фішингові атаки стають все більш витонченими і все частіше використовують соціальну інженерію - змушують людей робити щось без їхнього відома - замість того, щоб атакувати технологічні недоліки» [40].

Програма, що стоїть за такою DDoS-атакою (DDOS розшифровується як «розподілена відмова в обслуговуванні», коли мережа або веб-сайт атакується величезною масою інтернет-трафіку, що унеможливлює його перегляд інтернет-

користувачами. Як наслідок, бізнес-операції в організації порушуються, що наражає її на ймовірні фінансові та репутаційні втрати.

У 2020 році у світі буде здійснено майже 10 мільйонів DDoS-атак, що майже на 20% більше, ніж у попередньому році. Крім того, збільшується середній розмір атаки, оскільки компанія Blumberg повідомляє, що їй вдалося виявити атаки обсягом понад 1 ТБ.

«Розмір і частота DDoS-атак продовжує зростати, створюючи зростаючу загрозу для функціонування та відмовостійкості корпоративних мереж» [34].

1.2.2 Інсайдерські загрози

Зловживання доступом до інформаційних систем в організації з боку критично важливих співробітників може створити внутрішню загрозу. Це може бути навмисним, у випадку крадіжки даних, або ненавмисним, у випадку ненавмисного залишення даних у вразливому середовищі.

Як зазначає Ponemon Institute у 2020 році [35], «опитані компанії повідомили, що витоки даних були результатом зловмисних або недбалих дій співробітників, а середня загальна вартість одного такого випадку становила $11,45 млн».

«Внутрішні загрози залишаються головною проблемою для організацій, оскільки вони легко обходять традиційні засоби контролю безпеки, призначені для запобігання зловмисним атакам ззовні. » [35].

1.2.3 Останні тенденції та статистика

Організація Об'єднаних Націй визнає повернення кіберзлочинності під час пандемії COVID-19. Під впливом пандемії COVID-19 ситуація з кіберзагрозами зазнала вирішальних змін. З'явилися нові вразливості та зросли рівні кібератак, оскільки організації поспішили запровадити віддалену роботу. IC3 повідомила про 300% зростання кіберзлочинності з початку пандемії у 2020 році[13].

Зростання кількості програм-вимагачів: тенденція «програм-вимагачів як послуги» значною мірою демократизувала використання інструментів до такої міри, що навіть кіберзлочинці з меншими технічними навичками могли розпочати атаку. У цій схемі розробники продавали свої інструменти або здавали їх в оренду партнерам, а останні здійснювали атаки і ділилися прибутком.

Лише у 2020 році середня сума викупу зросла на 82%, що свідчить про прибутковість програм-вимагачів та їхню екзистенційну загрозу для бізнесу.

Використання вразливостей нульового дня: це недолік, який зловмисник може використати до того, як його виявить і виправить розробник. Це стає величезним ризиком, коли зловмисники можуть здійснити атаку без будь-якого попереднього попередження.

У 2021 році організації виявили рекордні 1 073 вразливості нульового дня, що на 40% більше, ніж у попередньому році - ще одна цифра, яка свідчить про важливість управління вразливостями та своєчасного встановлення патчів.

«Саме експлуатація вразливостей “нульового дня” є найстрашнішою проблемою для мережевої безпеки, оскільки вона обходить всі інші засоби захисту і сіє хаос» [42].

1.2.4 Виняткові приклади реальних кібератак

Атака на SolarWinds - хакери зламали ланцюжок постачання програмного забезпечення SolarWinds, великої IT-компанії, в результаті того, що було описано як найскладніша кібератака на сьогоднішній день. Шкідливий код був доданий до програмного забезпечення компанії Orion, після чого шкідливе програмне забезпечення було розіслано тисячам клієнтів, в тому числі державним установам і компаніям зі списку Fortune 500.

У спільному повідомленні ФБР, CISA та АНБ підтвердили, що атака була спрямована на понад 18 000 організацій, що ілюструє масштаб впливу та охоплення атак на ланцюги поставок.

«Інцидент з SolarWinds є суворим нагадуванням про вразливості, вбудовані в нашу цифрову екосистему, і про те, чому комплексний захист є настільки важливим для захисту ланцюга поставок» [31].

Атака хробака-вимагача на Колоніальний трубопровід - у травні 2021 року американський оператор паливних трубопроводів, компанія Colonial Pipeline, була виведена з ладу на кілька днів програмним забезпеченням-вимагачем. Цей інцидент викликав шокові хвилі на Східному узбережжі США, що мали каскадний вплив на економічну активність. Як повідомляється, компанія заплатила зловмисникам 4,4 мільйона доларів, що є яскравим прикладом руйнівних наслідків програм-вимагачів і серйозною організаційною дилемою.

«Атака на нафтопровід Colonial Pipeline підкреслює необхідність захисту критично важливої інфраструктури за допомогою промислових систем управління, а також те, як критичні кібератаки можуть мати серйозний вплив на інфраструктуру» 2021[31].

1.3 Методи забезпечення мережевої безпеки

Щоб відповісти на виклик боротьби з різноманітними високотехнологічними кіберзагрозами, з якими стикаються підприємства, підхід до забезпечення безпеки мережі перетворився на складну систему мережевої безпеки.

Розглянемо різні варіанти і методи, що використовуються для захисту цілісності та конфіденційності, а також доступності мережі. Також наведені цитати, дослідницькі факти та конкретні цифри, які допоможуть сформувати ефективні превентивні, детективні та коригувальні заходи.

1.3.1 Брандмауери

Брандмауери є критично важливими для нашої безпеки в мережі, оскільки вони відокремлюють наші довірені внутрішні мережі від ненадійних зовнішніх

мереж. Фактично, вони просіюють вхідний і вихідний трафік відповідно до попередньо встановлених політик безпеки.

За оцінками MarketsandMarkets, світовий ринок брандмауерів зросте з 3 мільярдів доларів США у 2020 році до 12,5 мільярдів доларів США до 2026 року, при середньорічному темпі зростання (CAGR) 32% протягом прогнозованого періоду [37].

«Брандмауери продовжують залишатися основним елементом мережевої безпеки, пропонуючи суттєві гарантії захисту від несанкціонованого доступу та потенційних загроз [37].

1.3.2 Шифрування

Коли ми шифруємо дані, це просто означає, що ми перетворюємо їх у формат, який може прочитати лише той, хто має ключ для розшифрування. Щоб уникнути злому, ми забезпечуємо шифрування даних і безпеку їх зберігання.

Наприклад, дослідження глобальних тенденцій шифрування, проведене Ponemon Institute (2021), виявило, що 50% організацій мають стратегію шифрування, що свідчить про те, що шифрування є найкращою практикою, яка набирає все більшої популярності.

«Шифрування має вирішальне значення для захисту приватної інформації, особливо в умовах, коли кіберзагрози стають все більш витонченими, а правила захисту даних - все більш суворими» [35].

1.3.3 Контроль доступу

Механізми контролю доступу обмежують доступ до мережевих ресурсів за допомогою ролей і дозволів користувачів. Це принцип найменших привілеїв, який обмежує шкоду від скомпрометованих акаунтів.

Згідно з дослідженням Інституту управління ідентифікацією (Identity Management Institute), проведеним у 2020 році, ефективні політики контролю

доступу можуть знизити ймовірність витоку даних на цілих 70%.

«Належний контроль доступу має вирішальне значення для зменшення ризиків безпеки, дозволяючи лише авторизованим користувачам отримувати доступ до конфіденційних даних. Інститут управління ідентифікацією, 2020.

1.3.4 Заходи виявлення інцидентів

Ці заходи спрямовані на виявлення інцидентів безпеки шляхом моніторингу мережі.

IDS/IPS (системи виявлення вторгнень і системи запобігання вторгненням)

Коли справа доходить до кваліфікації підозрілих дій, вам потрібні IDS/IPS. IDS пасивно відстежує мережевий трафік на предмет підозрілої активності, в той час як IPS про активно намагається зменшити загрози.

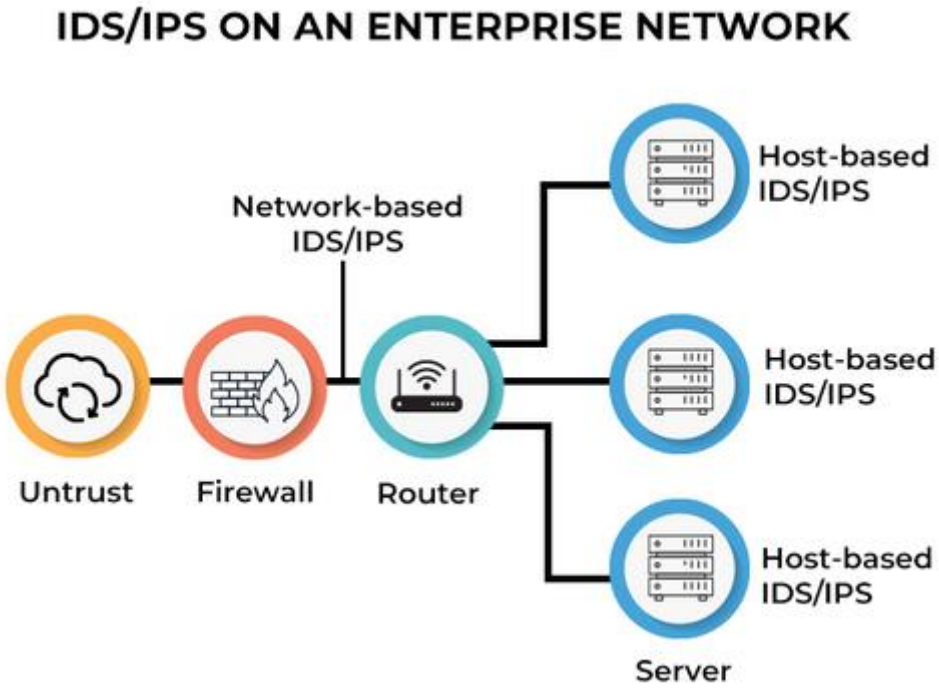

Рис 1.2 Робота IPS/IDS в корпоративній мережі.

Очікується, що до 2025 року світовий ринок IDS та IPS зросте до $8,6 млрд, що свідчить про зростання попиту на виявлення та запобігання загрозам у режимі реального часу (Grand View Research, 2021).

«IDS та IPS є важливими елементами повноцінної системи безпеки, яка може

забезпечити миттєве розуміння та реагування на кіберзагрози». [42]

1.3.5. Системи SIEM

Системи SIEM також збирають журнали з різних мережевих пристроїв і порівнюють їх, щоб виявити інциденти безпеки, які могли залишитися непоміченими через існуючі технічні обмеження. Єдина скляна панель для моніторингу та реагування на загрози мережевій безпеці.

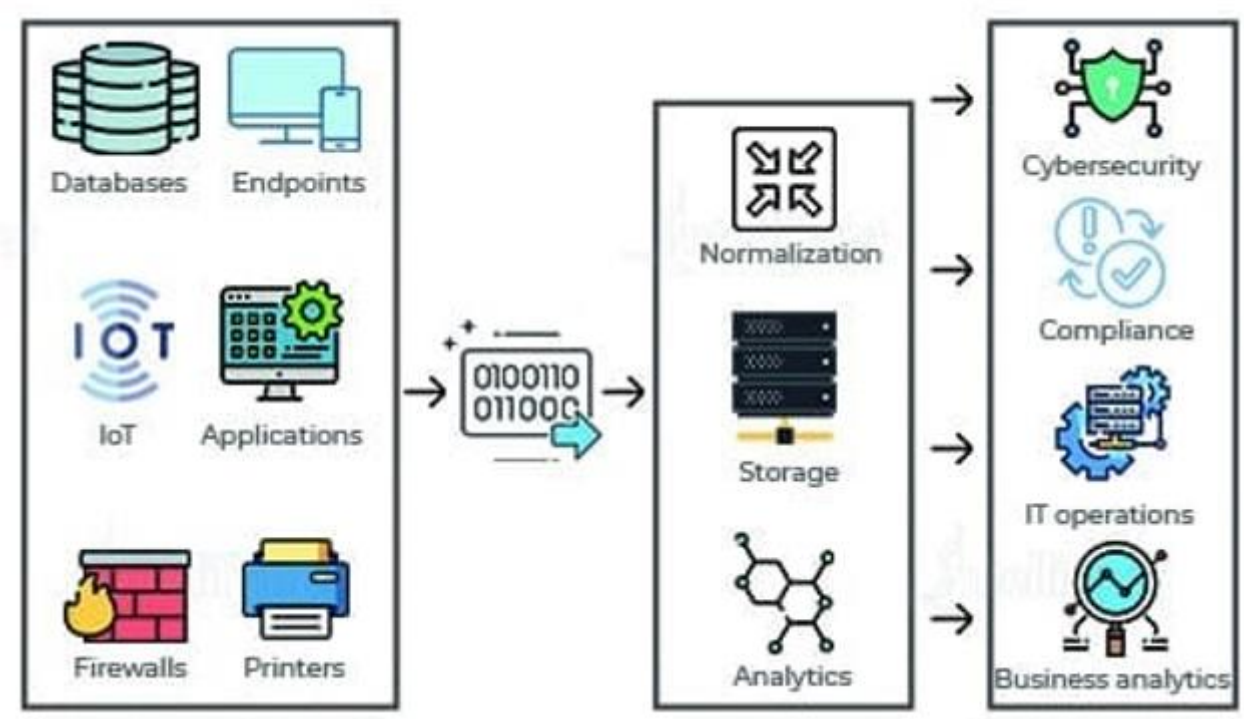

Рис 1.3 Архітектура роботи SIEM системи.

Згідно зі звітом Gartner (2020), світовий ринок SIEM досягне $5,5 млрд до 2025 року, що зумовлено зростанням попиту на просунуте виявлення загроз і управління відповідністю нормативним вимогам.

«Системи SIEM є критично важливими інструментами для підтримки мережевої безпеки в актуальному стані і забезпечують повну видимість і аналітичні можливості для пошуку і усунення загроз». [43]

1.3.6 Моніторинг та аналітика мережі в режимі реального часу

За допомогою постійного моніторингу та аналітики мережі можна виявити аномалії, які можуть виявитися сигналом про порушення безпеки. Машинне навчання, яке використовується для розуміння закономірностей і прогнозування можливих загроз, можливе в інструментах АТ завдяки використанню передової аналітики.

Згідно зі звітом Cisco (2021), 63% організацій використовують інструменти мережевого моніторингу для посилення своєї безпеки, що свідчить про нагальну потребу в безперервному моніторингу.

У звіті зазначається: «Безперервний моніторинг мережі та розширена аналітика є ключем до проактивного виявлення та пом'якшення загроз». Щорічний звіт Cisco з кібербезпеки за 2021 рік. [24]

1.3.7 Плани реагування на інциденти

Тепер введіть плани того, що слід робити під час порушення безпеки... плани реагування на інциденти. Ці плани забезпечать належне та своєчасне реагування на інциденти, зменшуючи їхній вплив.

Згідно з дослідженням Інституту SANS за 2020 рік, організації, які мають офіційні плани реагування на інциденти, можуть знизити вартість витоку даних на 50 відсотків.

«IT-лідери повинні створювати ретельні плани реагування на інциденти, щоб мінімізувати потенційні наслідки порушень і забезпечити швидке відновлення». [18]

1.3.8 Управління виправленнями

Управління виправленнями - це постійне оновлення програмного забезпечення та систем для вирішення проблем безпеки, які в іншому випадку можуть бути використані для отримання несанкціонованого доступу до цих

цифрових ресурсів. Оперативне встановлення виправлень також допомагає запобігти використанню зловмисниками відомих вразливостей.

Звіт компанії Flexera (2021) показав, що 60% витоків даних у 2020 році були пов'язані з вразливостями, для яких вже були доступні, але не застосовані патчі, що ще раз підкреслює зростаючу потребу в ефективному управлінні патчами.

«Управління виправленнями - один з основних принципів мережевої безпеки: усунення дірок у безпеці, створених відомими вразливостями в програмному забезпеченні.» [44].

1.3.9 Резервне копіювання та відновлення

Регулярне створення резервних копій даних, з яких можна відновити критичні дані у разі їх втрати через видалення або пошкодження. Щоб зберегти цілісність даних і вирішити проблему в міру її виникнення, бути більш продуктивними, необхідно мати правильну стратегію резервного копіювання та відновлення.

Згідно з опитуванням, проведеним Veeam (2021), 95% організацій стикалися з незапланованими відключеннями та резервним копіюванням, і стратегії відновлення відіграли величезну роль у зменшенні впливу.

«Доступність даних підвищується, а стійкість до кіберзагроз покращується завдяки надійним рішенням для резервного копіювання та відновлення» [32].

1.3.10 Поглиблені моделі безпеки

Вирішення проблеми складності мережевої безпеки: мережева безпека ще більше ускладнюється безліччю технологій та інструментів, доступних для захисту інфраструктури, тому багато організацій впровадили цілісні системи безпеки, які включають превентивні, детекторні та коригувальні засоби контролю безпеки, щоб допомогти впоратися з цією складністю.

1.3.11 NIST Cybersecurity Framework

NIST Cybersecurity Framework пропонує керівні принципи безпеки для управління ризиками безпеки. Вони включають 5 основних функцій: Ідентифікація, Захист, Виявлення, Реагування та Відновлення.

1.3.12 ISO 27001

ISO 27001 (офіційно відомий як ISO 27001:2005) - це специфікація для системи управління інформаційною безпекою (СУІБ). Він описує її як основу для управління, зберігання та захисту конфіденційної інформації компанії.

За даними Міжнародної організації зі стандартизації (ISO) (2021), кількість сертифікатів ISO 27001 зросла на 20%, що свідчить про його більшу прийнятність.

«ISO 27001 визначає еталон управління інформаційною безпекою, що дозволяє організаціям захищати свої дані» [11].

1.3.13 Штучний інтелект і машинне навчання

Штучний інтелект, автоматизація та машинне навчання вносять кардинальні зміни в мережеву безпеку і надають можливості для вдосконалення механізмів виявлення загроз і реагування на них. Ці проблеми вирішуються за допомогою потокових і пакетних технологій, які можуть аналізувати великі масиви даних для виявлення закономірностей і прогнозування загроз.

Згідно зі звітом Accenture (2023), використання штучного інтелекту в кібербезпеці зростатиме на 23% у середньорічному обчисленні до 2026 року через підвищений попит на кращі можливості виявлення загроз.

«AI+ML - це зміна, яка відбувається в кібербезпеці, що дає зловмисникам все, що їм потрібно, аж до можливості випереджати нас зі своїми загрозами» [23].

1.3.14 Технології блокчейн

Не менш важливо, що блокчейн також має застосування в мережевій безпеці, для перевірки даних в мережі, перевірка знову ж таки управляється повністю незалежно від решти системи. Завдяки своїй децентралізованості та захищеності від несанкціонованого втручання, він є актуальним для захисту транзакцій та ідентифікації особи.

«Вважається, що технології блокчейн підвищують безпеку мережі завдяки захищеному від несанкціонованого доступу управлінню даними, а також додає прозорості, а отже, як наслідок, довіри» [30].

1.3.15 Квантова криптографія

Квантова криптографія вражає тим, що вона використовує принципи квантової механіки для пошуку способів безпечної комунікації. Вважається, що вона захищена від атак, які можуть зламати традиційні схеми шифрування

Майбутні можливості для захисту чутливої комунікації були підтверджені Агентством Європейського Союзу з кібербезпеки (ENISA) (2020), підкріплюючи аргумент, що квантова криптографія може стати ключем до більш захищеного майбутнього, оскільки технологія її застосування буде продовжувати розвиватися в найближчі роки.

Квантова криптографія - це майбутнє захищених комунікацій, що перевершує всі наявні на сьогоднішній день методи боротьби з кіберзагрозами.

Висновки до розділу 1

Дослідження підкреслює важливість мережевої безпеки для підприємств у

цифрову епоху. Зростання складності та кількості кіберзагроз підкреслює критичну важливість захисту операцій для збереження ваших цінних даних, а також забезпечення безперебійної роботи вашого бізнесу. Такі інциденти, як атаки на SolarWinds та Colonial Pipeline, продемонстрували високу плату за недотримання правил технологічної безпеки підприємства.

Мережева безпека - це не лише захист даних, але й, що не менш важливо, збереження довіри та підтримка безперервної роботи підприємства. Неспроможність захистити ці мережеві ресурси може призвести до серйозних фінансових збитків, юридичної відповідальності, шкоди репутації тощо. Таким чином, високий рівень мережевої безпеки є обов'язковим для будь-якого бізнесу в 21 столітті, який прагне захистити свої активи і зберегти довіру клієнтів.

Середовище загроз швидко розвивається і постійно змінюється, тому дуже важливо бути в курсі останніх виявлених загроз. Зростаюче поширення програм-вимагачів (RaaS), монетизація вразливостей «нульового дня» і більш досконалі фішингові схеми свідчать про зростаючу майстерність кіберзлочинців і нові способи, які вони розробляють, щоб залишатися непоміченими під час впровадження зловмисного коду. Це вимагає тристороннього підходу до мережевої безпеки, що означає поєднання трьох способів захисту, виявлення та реагування.

Організації повинні бути в курсі нових загроз і постійно оновлювати свої методики з захисту, щоб запобігти появі нових вразливостей. Для цього потрібно йти в ногу з часом та новітніми технологіями та інформувати всіх співробітників про правила кібергігієни, засновані на найкращих практиках безпеки. Освітні курси та інформаційні кампанії можуть допомогти зменшити кількість людських помилок. Людські помилки - це найслабший зв'язок і, як наслідок, наш найбільший ризик.

Для забезпечення ефективного захисту мережі необхідний комплекс превентивних, детективних і коригувальних заходів. Ці механізми - брандмауери, шифрування даних і контроль доступу - призначені для запобігання несанкціонованим вторгненням і захисту конфіденційних даних.

Засоби виявлення, які складаються з систем IDS, IPS та SIEM, що дозволяють відстежувати мережевий трафік на предмет підозрілої активності та сигналізувати про неї в режимі реального часу.

Існує широкий спектр методів, що використовуються для забезпечення мережевої безпеки, і всі вони постійно розвиваються разом з прогресуючим характером кіберзагроз. Щоб захистити свої цифрові активи, підприємства повинні дотримуватися наскрізних превентивних механізмів - від перевірених часом традиційних методів, таких як брандмауери та шифрування, до найсучасніших технологій, таких як штучний інтелект, блокчейн, квантова криптографія.

Оскільки кіберзагрози з часом змінюються і розширюються, постійне ознайомлення з новими технологіями і передовим досвідом матиме вирішальне значення для збереження конкурентоспроможності в сфері кібербезпеки.

Знання основ історії та принципів мережевої безпеки допоможе вам побудувати своє навчання таким чином, щоб пояснити, як можна і потрібно керувати мережею на високому рівні, використовуючи будь-який з тисяч існуючих інструментів і методологій. Поєднуючи ці різні підходи та правила безпеки відповідно до постійно змінюваного середовища загроз, організації можуть досягти успіху та краще захистити свої ключові активи від атак.

РОЗДІЛ 2 ОСНОВНІ ХАРАКТЕРИСТИКИ ТЕХНОЛОГІЙ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ ПЕРСОНАЛУ

2.1 Управління ризиками

Кіберзагрози можуть спіткати компанію будь-якої миті, і, відверто кажучи, бізнесу потрібне технологічне рішення для захисту мережі, оскільки загрози постійно змінюються. Інтегровані разом, ці інструменти створюють правильні пари для моніторингу та автоматизованого попередження, виявлення та реагування на широкий спектр інцидентів безпеки. Ключові технологічні інструменти, що використовуються в мережевій безпеці (опис, підкріплений даними, цитатами експертів, результатами досліджень). Тут також висвітлено, як ці інструменти використовуються на підприємствах, а також кращі практики та потенційні виклики.

2.1.1 Брандмауери

Для початку брандмауери створюють кам'яну стіну над мережею. Брандмауери фільтрують і пропускають пакети на основі правил політики безпеки, які визначають дозволену і заборонену поведінку пакета. Апаратні або програмні, або обидва Зашифровані VPN. Очікується, що світовий ринок брандмауерів досягне $12,5 млрд до 2025 року, згідно з даними MarketsandMarkets (2020), зі зростаючим попитом на рішення для мережевої безпеки в усіх галузях.

Реалізація: До поширених типів брандмауерів належать брандмауери з фільтрацією пакетів, брандмауери з перевіркою стану та брандмауери наступного покоління (NGFW). Брандмауери нового покоління надають додаткові можливості, такі як DPI, інформування про додатки та інтегроване запобігання вторгненням.

Рекомендація: Оновлюйте правила брандмауера, наприклад, у разі появи

нових загроз або змін в організації. Слідкуйте за підозрілими журналами брандмауера. Сегментація мережі для зменшення потенційного впливу порушень. Виконуйте регулярний аудит брандмауера, щоб забезпечити дотримання політик безпеки.

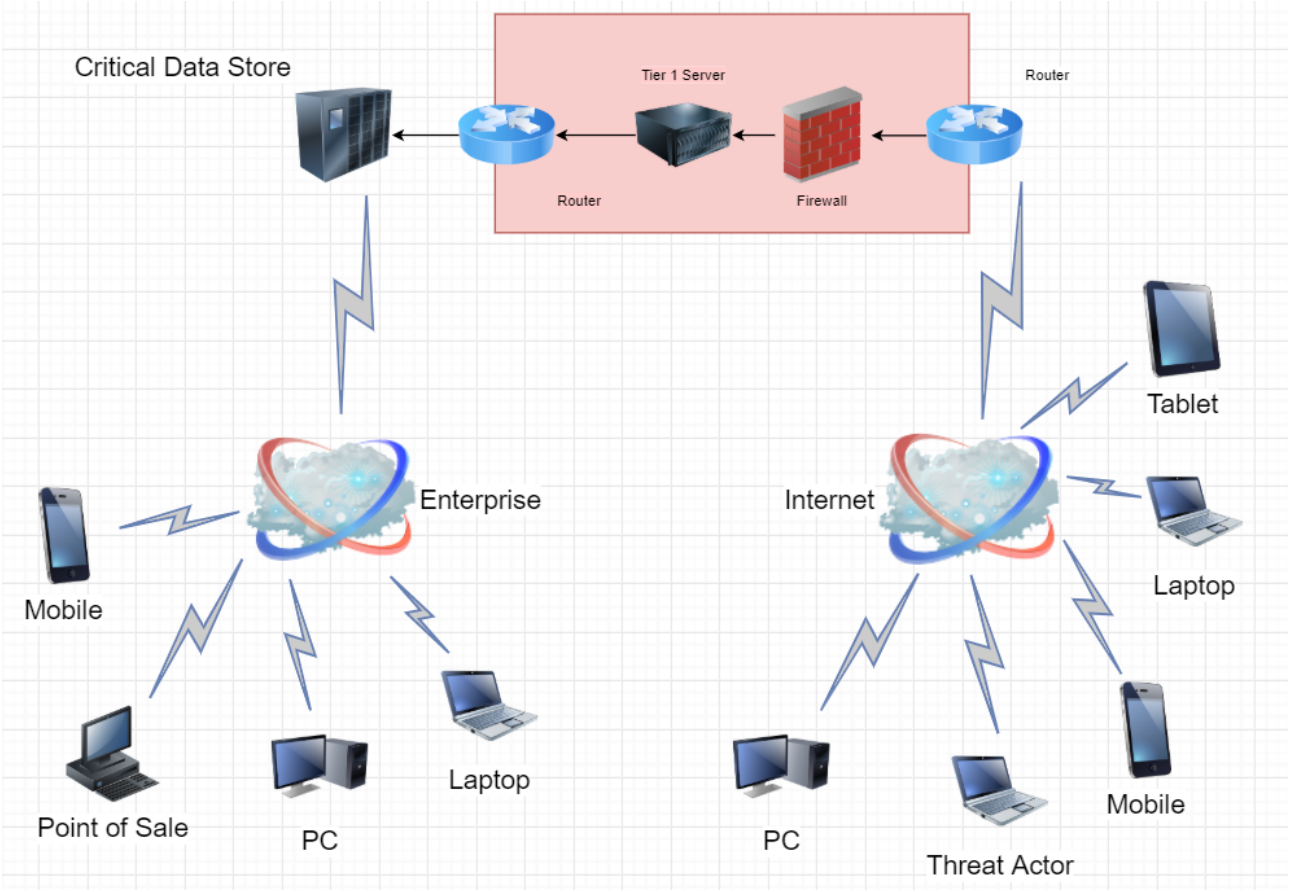

Рис 2.1 Схема роботи брандмауера у комп'ютерній мережі.

Кроки для впровадження:

Оцінка: Визначте, які брандмауери найкраще підходять для мережевої архітектури. Це має визначатися такими факторами, як розмір мережі, обсяг трафіку і навіть потреби в безпеці.

Обробка конкретних запитів: Налаштуйте правила брандмауера відповідно до політики безпеки організації; налаштуйте правила вхідного і вихідного трафіку, списки ACL і зони/інтерфейси.

Розгортання: Стратегічно розгортайте брандмауер по всій мережі, по

периметру, всередині центру обробки даних і між внутрішніми сегментами. Переконайтеся, що у вас є можливості резервування та обходу відмови.

Відстежуйте старіння: Постійно відстежуйте активність, журнали та продуктивність брандмауерів; виправляйте та оновлюйте як прошивку, так і правила брандмауера, щоб усунути нові загрози. Здійснюйте регулярний моніторинг і налаштування, щоб підтримувати їх у найкращому стані.

2.1.2 IDS та IPS

IDS та IPS дуже важливі для виявлення та запобігання зловмисній діяльності всередині мережі. У той час як IDS спостерігає за мережевим трафіком на предмет підозрілої активності, IPS робить крок далі, блокуючи виявлені загрози. За даними Grand View Research (2021), очікується, що до 2025 року світовий ринок IDS та IPS досягне 8,6 мільярда, що зумовлено зростаючою потребою в передових рішеннях для виявлення та запобігання загрозам.

«IDS/IPS є важливими частинами системи безпеки, додаючи вбудований рівень захисту з можливістю моніторингу та реагування в режимі реального часу для кращого виявлення та захисту від загроз». - Grand View Research, 2021.

Впровадження:

Розміщення: IDS/IPS повинні бути розміщені в мережі для моніторингу критично важливих точок трафіку в мережі, таких як периметр мережі, центри обробки даних і чутливі внутрішні сегменти.

Конфігурація: Оновлюйте сигнатури IDS/IPS, щоб виявляти найновіші загрози. Дозвольте системам знаходити баланс між виявленням реальних загроз та уникненням надмірної кількості хибних спрацьовувань. Поєднання методів, заснованих на сигнатурах та аномаліях, для досягнення кращих результатів.

Інтеграція: Переконайтеся, що IDS/IPS інтегровані з іншими інструментами безпеки, такими як SIEM-системи, щоб забезпечити кращу кореляцію та можливості реагування.

Кроки для впровадження:

Оцінка потреб: Визначте ключові активи і потоки даних в мережі, вирішіть, де найбільш корисно розгорнути IDS/IPS, щоб виявити будь-яку потенційну проблему.

Вибір IDS/IPS: Залежно від вимог, виберіть між мережевими IDS/IPS (NIDS/NIPS) або IDS/IPS на основі хостів (HIDS/HIPS). NIDS/NIPS контролюють мережевий трафік, тоді як HIDS/HIPS контролюють кожний окремий пристрій.

Розгортання: Правильно налаштуйте правила виявлення та порогові значення, щоб зменшити кількість хибних спрацьовувань і виявити якомога більше загроз.

Обслуговування: Постійно оновлюйте сигнатури IDS/IPS. Регулярно переглядайте та коригуйте правила та політики виявлення. Моніторинг продуктивності та ефективності IDS/IPS в режимі реального часу.

2.1.3 Системи SIEM

SIEM-системи збирають і аналізують дані журналів з численних мережевих пристроїв і виявляють інциденти безпеки. Таким чином, вони є центральним управлінням мережевою безпекою і допомагають у реагуванні на інциденти, об'єднуючи інформацію з інших точок.

SIEM-системи стали обов'язковим елементом сучасної мережевої безпеки, забезпечуючи потужну видимість і аналітику для виявлення та пом'якшення загроз.

Впровадження:

Інтеграція: Інтегруйте SIEM з іншими інструментами безпеки, такими як брандмауери, IDS/IPS і платформи захисту кінцевих точок, щоб збирати дані з усіх джерел.

Проте, правила та оповіщення SIEM можуть бути адаптовані до індивідуальних вимог та ландшафту загроз підприємства. Визначте варіанти використання та інформаційні панелі, щоб показати пріоритети безпеки організації

Обслуговування: Переконайтеся, що ви часто оновлюєте програмне забезпечення SIEM і правила, щоб відповідати новим загрозам і вразливостям. Систематично переглядайте та налаштовуйте конфігурацію SIEM, щоб підвищити точність виявлення та зменшити кількість хибних спрацьовувань.

Кроки для впровадження:

Планові роботи: Визначення обсягу та цілей впровадження SIEM. Визначення важливих джерел даних, мережевих пристроїв, серверів і додатків, які будуть інтегровані в SIEM.

Зображення для після інсталяційного періоду: Розгортання платформи SIEM. Розгортання збирача даних і агентів для збору даних журналів з усіх джерел. Безпечний вхід та ефективне накопичення журналів.

Проектування: Налаштуйте та створіть кастомізовані правила SIEM, політики кореляції та оповіщення відповідно до потреб організації в безпеці. Створіть інформаційні панелі та звіти для відстеження в реальному часі.

Оперативні завдання: Регулярно оновлювати правила SIEM та політики кореляції. Проводити регулярні перевірки роботи та ефективності SIEM. Проводити безперервне навчання для аналітиків безпеки, щоб забезпечити точне наповнення SIEM.

2.1.4 Технології шифрування

Зашифровані дані (використовуються при надсиланні/отриманні та зберіганні) - перетворюють звичайні текстові дані в зашифровані таким чином, що тільки одержувач, який має ключ шифрування, може їх прочитати. Це життєво важливо для захисту конфіденційних даних від будь-якого несанкціонованого доступу.

Шифрування є важливим аспектом захисту конфіденційних даних, оскільки кіберзагрози стають дедалі складнішими, а закони про конфіденційність даних розширюють свою сферу дії.

Впровадження:

Data-at-REST: Конфіденційні дані, що зберігаються на серверах, у базах даних і на резервних носіях, повинні бути зашифровані. При всіх методах шифрування зашифровані дані повинні бути зашифровані за алгоритмом AES-256 або вище.

Дані в дорозі: Захистіть передачу даних, використовуючи протоколи шифрування SSL/TLS для таких мереж, як електронна пошта, передача файлів і веб-комунікації.

Захистіть керування ключами та забезпечте їх зберігання та ротацію. Використовуйте апаратні модулі безпеки (HSM) для забезпечення відповідності ключів.

Кроки для впровадження:

Оцінка: Визначте, які дані є чутливими, а які потрібно зашифрувати. Сюди також входять дані в стані спокою/дані в русі та дані, що використовуються.

Виберіть інструменти шифрування: Виберіть правильні інструменти та протоколи шифрування для організації; деякі з прикладів - шифрування всього диска (наприклад, LUKS або BitLocker), шифрування на рівні файлів (наприклад, GPG або Enchive) і безпека на транспортному рівні (TLS) для комунікації.

Керування ключами: створіть та впровадьте протокол керування ключами, який повинен включати генерацію ключів, розподіл ключів, зберігання ключів, ротацію ключів та відкликання ключів. Безпечні рішення для управління ключами, наприклад, HSM.

Розгортання: Розгортайте інструменти шифрування в точках передачі даних. Зробіть інтеграцію з поточними системами та робочими процесами якомога простішою.

Моніторинг та підтримка: Постійно переглядайте та оновлюйте політики та практики шифрування. Відстежуйте ефективність рішень для шифрування та усувайте будь-які вразливості або невідповідності нормативним вимогам.

2.1.5 Платформи захисту кінцевих точок

Платформи EPP захищають окремі інструменти, підключені до мережі, включаючи настільні комп'ютери, ноутбуки та мобільні пристрої. Серед інших інтегрованих функцій безпеки, які допомагають захистити кінцеву точку від кіберзагроз, - антивірус та антивірусне програмне забезпечення. Згідно з дослідженням IDC (2021), до 2026 року ринок безпеки кінцевих точок зросте до 20,8 мільярда доларів США завдяки більшому поширенню та складності кіберзагроз, а також більш потужним кінцевим точкам.

«Ера сучасного підприємства вимагає захисту кінцевих точок, коли пристрої підключаються до мережевих ресурсів, незалежно від того, де вони використовуються кінцевими користувачами» [45].

Впровадження:

Розгортання програмного забезпечення: Переконайтеся, що розгорнуте програмне забезпечення (ПЗ для захисту кінцевих точок) оновлюється на всіх кінцевих точках. Використовуйте інструменти виявлення та реагування на кінцевих точках (EDR) для пошуку та усунення загроз.

Впровадження політик: Впроваджуйте політики безпеки, що передбачають необхідність оновлення, сканування та дотримання найкращих практик безпеки. Використовуйте рішення для керування пристроями для моніторингу та забезпечення дотримання вимог.

Виявлення: Виявлення підозрілих загроз у режимі реального часу та негайне реагування на них. Негайне виявлення та реагування на загрози. Розгортання за допомогою централізованої консолі керування, щоб бути впевненими, що всі кінцеві точки організації перебувають під контролем.

Етапи впровадження:

Оцінка потреб: Визначте кінцеві пристрої, що використовуються в організації, та оцініть ризики безпеки, пов'язані з цими пристроями. Проектування рішення EPP.

Вибір правильного рішення EPP: Обирайте рішення EPP, яке пропонує комплексний захист - антивірус, захист від шкідливого програмного

забезпечення, брандмауер та EDR.

Розгортання: Розгорніть рішення EPP на BCIX кінцевих точках. Безпечна конфігурація для забезпечення дотримання політик і налаштувань.

Управління та моніторинг: Централізовано реагуйте на загрози, автоматично розгортайте оновлення та контролюйте безпеку кінцевих точок за допомогою централізованих інструментів управління. Інвестуйте в безперервний моніторинг і розвідку загроз, щоб ефективно протистояти новим загрозам.

Навчання для користувачів: Розкажіть співробітникам про важливість захисту кінцевих точок і про те, як підтримувати безпеку кінцевих точок. Навчіть співробітників виявляти загрози та реагувати на них.

2.1.6 VPN

VPN забезпечують безпечне з'єднання через Інтернет і дозволяють віддаленому користувачеві передавати зашифровані дані в корпоративну мережу. Знову ж таки, це ключовий фактор для компаній з розподіленою робочою силою. За даними Global Market Insights (2022), очікується, що до 2026 року ринок VPN перевищить 70 мільярдів доларів, оскільки компанії все частіше шукають безпечні рішення для віддаленого доступу.

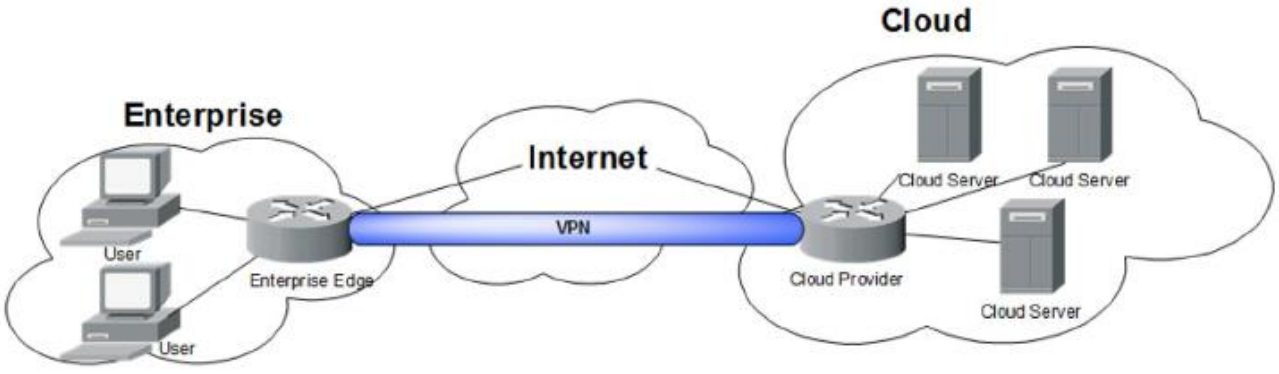

Рис 2.2 Схематичне зображення роботи VPN у корпоративній мережі.

«VPN є життєво важливими для захисту віддаленого доступу, особливо у світі віддаленої роботи та хмарних підключень» [46].

Впровадження:

Типи VPN: Вибирайте з різних типів VPN, включаючи VPN між сайтами

для захищених з'єднань між кількома офісними сайтами та VPN для віддаленого доступу для користувачів.

Шифрування протоколу: Коли мова йде про методи тунелювання, завжди шукайте шифрування найвищого стандарту, наприклад, IPsec або SSL/TLS, при підключенні за допомогою VPN.

Автентифікація користувачів: додайте додатковий рівень безпеки, запровадивши MFA для доступу до VPN.

Кроки для впровадження:

Оцінка потреб: Визначте специфікації VPN, наприклад, налаштування VPN відповідно до потреб організації у віддаленому доступі та типу даних. Визначте, скільки користувачів і які пристрої використовують VPN.

Вибір рішення VPN: Виберіть рішення VPN, яке підходить для вашої організації. Часто враховують простоту використання, масштабованість, сумісність з існуючими середовищами та підтримку високоякісних протоколів шифрування.

Встановіть конфігурацію: На цьому етапі налаштовується програмне забезпечення сервера і клієнта VPN. Встановіть протоколи шифрування та автентифікації. Тут ви визначаєте політики доступу, щоб визначити віддалені ресурси, до яких можуть отримати доступ віддалені користувачі.

Розгортання: клієнтське програмне забезпечення VPN встановлюється на пристрої користувачів. Надайте працівникам чудові інструкції з налаштування та використання VPN.

Моніторинг та підтримка: Постійно слідкуйте за використанням та продуктивністю VPN. Клієнт VPN має вразливості (виправляйте програмне забезпечення). Регулярно переглядайте політики доступу до VPN, а також активність користувачів.

2.1.7 Комплексне планування

Перш ніж впроваджувати інструмент мережевої безпеки, проведіть детальну оцінку вимог організації, поточної інфраструктури та потенційних вразливостей. Створіть ретельний план впровадження, який визначає цілі, графік і потреби в ресурсах.

Етапи планування:

Оцінка ризиків: Визначте ризики та вразливості, які загрожують безпеці вашої програми/мережі. Оцініть наслідки та ймовірність різних атак.

Оцінка вимог: Визначте вимоги до безпеки організації. Сюди входить визначення критично важливих активів, вимог до відповідності та бізнес-цілей.

Розподіл ресурсів: Складіть бюджет і розподіліть ресурси, необхідні для процесу впровадження інструментів безпеки. Переконайтеся, що є достатньо персоналу і технологічних ресурсів для підтримки розгортання.

Розробка часової шкали: Встановіть реалістичний графік процесу впровадження, включаючи важливі етапи та терміни.

Регулярні оновлення та виправлення

Переконайтеся, що всі інструменти безпеки оновлені найновішими патчами та підписами. Це дуже важливо для захисту від будь-яких нових загроз або вразливостей. Створіть процес управління виправленнями, щоб полегшити автоматизацію та адміністрування оновлень.

Кроки для регулярних оновлень:

Політика управління виправленнями: Ми готуємо політику для визначення, тестування та встановлення виправлень.

Автоматизовані інструменти керування виправленнями: Легко встановлюйте патчі та оновлення за допомогою автоматизованих інструментів управління патчами.

Тестування: Встановіть тестовий патч у контрольованому середовищі та перевірте, чи працює система без помилок.

Безперервний моніторинг нових патчів і вразливостей: Підпишіться на повідомлення від постачальників і служби безпеки.

2.1.8 Складність і вартість

Якщо ви збираєтесь захищати систему за допомогою безлічі інструментів безпеки, це може стати складним і дорогим завданням. Для того, щоб боротися з цим, компаніям потрібно оцінити свої потреби в безпеці та інвестувати в рішення, які можуть рости разом з ними, забезпечуючи максимальну віддачу для їхніх інвестицій.

Рішення:

Ранжування: Впроваджуйте інструмент безпеки, який отримав найвищий рейтинг за результатами оцінки ризиків та пріоритетів безпеки.

Масштабування: Обирайте масштабовані рішення, які можуть бути адаптовані до кожного розширення компанії та відповідати динамічним потребам у сфері безпеки.

Проведіть аналіз витрат і вигод: Проведіть аналіз витрат і вигод, щоб зрозуміти можливу рентабельність інвестицій (ROI) для різних інструментів безпеки і визначити найбільш вигідні для використання.

Рішення:

Налаштування та калібрування: Інструменти безпеки слід регулярно налаштовувати і калібрувати, щоб підвищити їхню точність і зменшити кількість хибних спрацьовувань і негативних результатів.

Поведінкова аналітика: Використовуйте поведінкову аналітику, щоб покращити традиційні методи виявлення та отримати уявлення про те, як може діяти типова загроза.

Цикли зворотного зв'язку: Налаштуйте цикли зворотного зв'язку, щоб постійно вдосконалювати алгоритми виявлення, використовуючи досвід, отриманий з реальних даних та інцидентів.

2.2 Політики Інформаційної Безпеки

Існують різні доступні міжнародні формати політик, які можна взяти за приклад при розробці документу про політику інформаційної безпеки вашої організації.

Ці шаблони, по суті, універсальні і не обов'язково пов'язані з компанією. Тому їх потрібно розробляти за участі керівництва, щоб отримати унікальний документ, який відповідатиме потребам підприємства.

2.2.1 ISO 27000

ISO - це серія стандартів, яка надає організаціям комплексну структуру для політик і стандартів інформаційної безпеки.

Він корисний для кожної організації, якій необхідно захистити свої інформаційні активи, включаючи фінансові звіти, інформацію про співробітників, інтелектуальну власність або дані про клієнтів. Почнемо з ISO 27001:2013, який встановлює вимоги до сімейства стандартів інформаційної безпеки.

Система управління інформаційною безпекою. Другий документ серії ISO 27000, що походить від початкової версії ISO 27000, ISO 27002:2013, містить кодекс практик, які забезпечують безпеку. Ці три документи підпадають під сімейство третього документа серії ISO.

Впроваджені стандарти для підтримки вимог ISO 27000- 27003:2010 - цей стандарт спеціально створений для підтримки на етапі впровадження системи управління безпекою. Четвертим у цій серії є ISO 27004:2009, який включає в себе вимірювання того, що необхідно для системи інформаційної безпеки.

ISO 27001:2013 визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. Його розроблено для використання організаціями будь-якого типу, будь-якого розміру та сфери діяльності. Таким чином, це великий і загальний документ, і вибір щодо його прийняття та впровадження повинен бути стратегічним. Процес

адаптації стандарту повинен відповідати потребам організації, а також адаптуватися для узгодження з бізнес-перспективою. Ініціювання нової політики залишатиметься прерогативою правління та виконавчого керівництва, виходячи зі стану безпеки, в той час як правління також залишає за собою право включати додаткові розширені набори контролів.

Всебічний аналіз ризиків інформаційної безпеки організації має важливе значення для вибору відповідних засобів контролю.

ISO 27002:2013 - це, по суті, свого роду Настанова, в якій згадуються всі види безпеки, навіть якщо вона не обмежується лише безпекою IT-систем (ISO 27002:2013). Він забезпечує основу для керівних принципів найкращих практик, а також набір рекомендацій, які вказують, що слід робити, а не як це робити, щоб допомогти організаціям керувати процесами інформаційної безпеки. Як кодекс керівних принципів, специфікація не вимагає, щоб організації приймали її як стандарт; організації можуть вільно обирати ті керівні принципи, які застосовуються до їхньої організації. Цей стандарт вважається невід'ємною частиною будь-якої організації, яка залежить від своїх даних.

Він був сформульований як керівництво з впровадження для організацій, які вирішили впровадити стандарти ISO 27000. Він забезпечує керівництво на початковому етапі розробки СУІБ, зокрема, на етапах специфікації та проектування. Він надає підтримку організаціям на етапі оцінювання СУІБ з використанням ISO 27004, який є стандартом для вимірювання систем управління інформаційною безпекою. Організація, яка впровадила СУІБ, повинна періодично проводити оцінку, щоб переконатися, що вимоги безпеки були виконані. Стандарт також визначає метрики та вимірювання, необхідні для перевірки компетентності СУІБ, а також моделі аналізу для підвищення їхньої ефективності. Результати вимірювань підтримують зрілість інформаційної безпеки, а також підтримують бізнес- та інженерні рішення.

Сімейство стандартів ISO 27000 забезпечує структуру, в рамках якої можуть бути розроблені процеси управління. Організація не зобов'язана приймати всі політики, включені в це сімейство стандартів. Суть питання

полягає в тому, щоб зрозуміти застосовні сфери, в яких організація хоче працювати, а потім налаштувати засоби контролю на етапах розробки та впровадження. Завжди пам'ятайте, що політики повинні залишатися допоміжним засобом, а не перешкодою для організації в досягненні її бачення! На закінчення, остаточний успіх проекту інформаційної безпеки базуватиметься на прихильності керівництва, що є поєднанням розуміння цілей організації та потреб безпеки керівником проекту.

2.2.2 NIST

Національний інститут стандартів і технологій США (NIST) відомий створенням дуже детальних і всеосяжних стандартів. У складі NIST є Відділ комп'ютерної безпеки (CSD), завданням якого є розробка стандартів і технологій для захисту інформаційних систем від загроз конфіденційності, цілісності та доступності інформації та послуг.

Відділ зайняв освітню позицію щодо вразливостей та ризиків, пов'язаних з IT-організаціями. Він також досліджує та публікує рекомендації щодо низьковитратних методів забезпечення безпеки. У свою чергу, NIST створює засоби контролю, стандарти, політики та програми перевірки, які допомагають забезпечити безпеку споживачів, а також мінімальні вимоги до безпеки. NIST опублікував понад 300 документів, пов'язаних з безпекою. Одним з таких документів є всебічні дослідження та документація, проведені інститутом, такі як Спеціальна публікація (SP) серії 800. Розробляючи настанови, публікації та довідкові матеріали з технічної безпеки інформації, NIST виконує свою місію сприяння інноваціям і промисловій конкурентоспроможності США шляхом розвитку вимірювальної науки, стандартів і технологій для посилення економічної та громадської безпеки.

2.2.3 ITIL

Бібліотека інфраструктури інформаційних технологій (ITIL) - це набір найкращих практик для організації IT-послуг.

Мета: Забезпечити врахування стратегічних міркувань безпеки на операційному рівні. Інформаційна безпека розглядається як життєвий цикл, який необхідно регулювати, планувати, проектувати, тестувати та управляти. ITIL визначає складові інформаційної безпеки як політики, процеси, процедури та робочі інструкції. Використовуючи ITIL як сходинку, організації можуть розробити надійну і добре узгоджену структуру безпеки, яка базується на найкращих практиках. Вона також підлягає постійному перегляду, що гарантує організації можливість оцінити, наскільки ефективними є її стратегії безпеки. Це допомагає впровадити структуровану структуру безпеки, тим самим уникаючи безсистемного виконання та поспішних рішень. ITIL, за замовчуванням, запитує всю відповідну звітність, тримаючи виконавче керівництво в межах поточного стану безпеки, щоб рішення були актуальними. Ролі та обов'язки повинні бути чітко визначені разом з процедурами дій у випадку інциденту.

2.2.4 COBIT

COBIT - це система управління, розроблена ISACA, яка гарантує, що інформація підприємства не буде розкрита неавторизованим суб'єктам (конфіденційність), інформація не буде дублюватися або маніпулюватися неавторизованими суб'єктами для досягнення бажаного результату (цілісність), а інформація, ресурси та процеси будуть доступні для використання уповноваженими суб'єктами (доступність) COBIT 5 в частині безпеки збалансовує структуру для досягнення переваг при одночасному збереженні оптимальних рівнів ризиків і ресурсів, що використовуються в сфері безпеки. Це фактично допомагає забезпечити кращу гнучку лінію для розмежування керівництва та менеджменту, оскільки саме обов'язки керівництва контрастують з обов'язками менеджменту. Практика COBIT підтверджує це, не тільки

залучаючи всі зацікавлені сторони та третіх осіб до побудови системи інформаційної безпеки організації, але й окреслюючи їхні обов'язки.
COBIT 5 для інформаційної безпеки має структуру, яка включає принципи та засоби.

Якщо добре придивитися, то принципи забезпечують ефективний контроль і управління, а засоби дозволяють належним чином використовувати ресурси заради створення цінності для організації та зацікавлених сторін.

Висновки до розділу 2

Дослідження методів та інструментів, що використовуються для забезпечення безпеки, показало важливість цілісного та всебічного підходу до безпеки корпоративних мереж. Належні методи дослідження (якісні або кількісні) додають міцного підґрунтя для аналізу потреб у безпеці та її реалізації. Детальне вивчення технологічних засобів, таких як антивіруси, VPN, брандмауери і системи виявлення вторгнень, підкреслює, як кожен з них виконує свою індивідуальну функцію, що підвищує необхідність багаторівневої стратегії захисту. Відповідність визнаним стандартам (наприклад, ISO 27001) не тільки задовольнить законодавчі вимоги, але й забезпечить вищий рівень захисту (спонукаючи до постійного вдосконалення стандартів безпеки шляхом запровадження систематичного управління ризиками).

Порівняльна оцінка різних інструментів і технологій підкреслює необхідність кастомізації рішень безпеки на основі власного сценарію. Наприклад, автоматизовані рішення для управління комплаєнсом і розширена аналітика допомагають контролювати і підтримувати комплаєнс, впливаючи на економію ручних зусиль і підвищуючи точність. Більше того, поєднання цих технологій як складової ширших організаційних стратегій допомагає перестати розглядати засоби контролю безпеки як пожежогасіння, а як крок у єдиному процесі забезпечення безпеки, що веде боротьбу з загрозою ще до того, як вона матеріалізується.

Задоволення вимог відповідності є складним завданням, але компанії можуть впоратися з ним завдяки постійній оцінці ризиків, навчанню співробітників виявляти загрози та використанню технологій для забезпечення більш високого рівня прозорості мережі. Цей успішний приклад демонструє, як стратегічні ініціативи з комплаєнсу та безпеки, такі як централізоване управління даними та широкі навчальні програми, сприяють значному підвищенню ефективності комплаєнсу та безпеки.

Для забезпечення найкращої комплаєнс-підтримки та стійкості підприємства в галузі, організації можуть швидко реагувати на зміни регуляторного ландшафту або появу нових технологій. Штучний інтелект і машинне навчання відіграватимуть важливу роль у забезпеченні мережевої безпеки і працюватимуть у співпраці з людським розумом для більш плавного оповіщення і реагування на загрози в майбутньому. Однак організації, які приймають ці зміни і більш повно інтегрують комплаєнс як аспект своїх основних бізнес-процесів, будуть краще підготовлені до захисту своїх мереж і структурування своїх майбутніх операцій для досягнення успіху.

РОЗДІЛ 3 ТЕМАТИЧНІ ДОСЛІДЖЕННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1. Огляд середовища мережевої безпеки підприємства

3.1.1 Типова топологія корпоративної мережі

Корпоративна мережа, що використовується в Business-Tech, є складною і містить багато взаємопов'язаних елементів, призначених для забезпечення безперервності зв'язку, обміну даними та управління ресурсами. Мережева інфраструктура включає локальну мережу (LAN), що використовується всіма комп'ютерами, які знаходяться в приміщенні компанії, та центральний сервер, який контролює інформацію та дані серверів, доступних у цій локальній мережі.

Архітектура мережі інтегрує дротове та бездротове з'єднання, щоб забезпечити співробітникам гнучкість та мобільність спільної роботи. Стабільний та високошвидкісний доступ до Інтернету для дротових підключень та бездротовий доступ для мобільних пристроїв, таких як ноутбуки, планшети та смартфони, є важливими компонентами мережі. Мережа розділена, щоб спростити управління мережевим трафіком і підвищити безпеку шляхом відокремлення критично важливих розділів від розділів загального доступу.

Брандмауер відстежує весь вхідний і вихідний мережевий трафік і вирішує, чи блокувати або дозволяти певний трафік відповідно до визначеного набору правил безпеки, щоб запобігти зовнішнім загрозам. VPN допомагають забезпечити безпеку віддалених працівників, а мережеві комутатори та маршрутизатори керують передачею та маршрутизацією даних між різними точками мережі.

Пристрої безпеки, такі як системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), використовуються для моніторингу трафіку, що проходить через мережу, на предмет підозрілої активності та вжиття коригувальних заходів для запобігання порушень безпеки. На всіх пристроях встановлюються рішення для захисту кінцевих точок, які можуть включати

антивірусні та анти шпигунські програми для захисту критично важливих ресурсів і даних від шкідливого програмного забезпечення та сучасних загроз безпеки. Завдяки резервному копіюванню дані завжди будуть доступні у випадку збою системи або атаки.

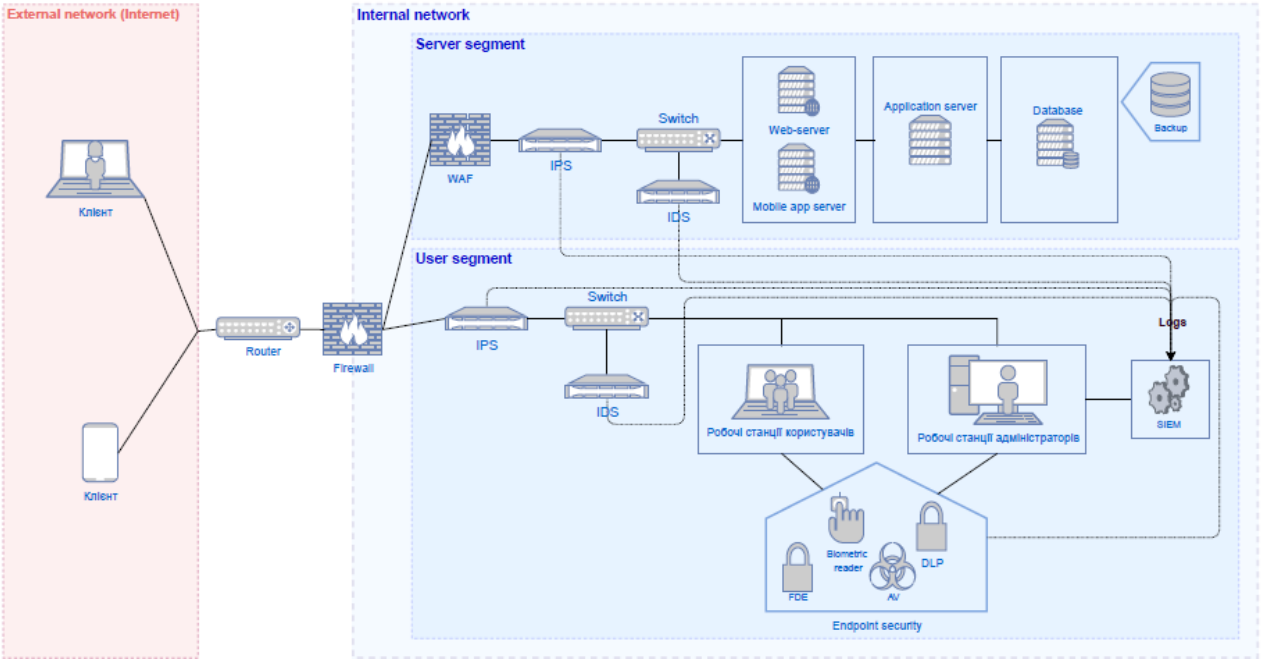

Рис 3.1 Схематичне зображння різних систем захисту у корпоративній мережі.

3.1.2 Поширені проблеми безпеки підприємств

Незважаючи на добре організовану мережу, організаціям доводиться стикатися з різними атаками на мережеву безпеку, які призводять до компрометації мережі та витоку даних. Зростання кількості кібератак та підвищення їх складності є однією з найважливіших проблем. Фішинг, програми-вимагачі та сучасні постійні загрози (APT) постійно змінюються, тому малому бізнесу може бути складно залишатися в курсі новітніх механізмів безпеки.

Ймовірно, найпоширенішою загрозою є фішингові атаки, в яких зловмисники намагаються обманом змусити співробітників поділитися конфіденційною інформацією за допомогою оманливих електронних листів або повідомлень. Такі атаки призводять до витоку даних і втрати грошей, якщо

працівники несвідомо надають облікові дані або переходять за шкідливими посиланнями. Атаки з вимогою викупу, різновид шкідливого програмного забезпечення, що шифрує дані і блокує доступ до них до моменту сплати викупу, можуть призвести до зриву бізнес-операцій і можуть бути дуже дорогими.

Іншою проблемою є інсайдерська загроза, незалежно від того, чи це зловмисний інсайдер, чи ненавмисна загроза. Атаки соціальної інженерії можуть бути використані для обману співробітників, які мають доступ до конфіденційної інформації, змушуючи їх несвідомо порушувати безпеку, що може призвести до вторгнення і нанесення шкоди. Важливою частиною вашої системи безпеки має бути навчання співробітників та дотримання ними найкращих практик безпеки.

Зростаюче використання мобільних пристроїв і збільшення кількості віддалених працівників ще більше ускладнюють ситуацію, оскільки периметр мережі поширюється на працівників, які працюють вдома. Ці віддалені, іноді мобільні, точки входу в мережу можуть не мати такого ж рівня безпеки, як пристрої, що знаходяться у фізичному приміщенні компанії, і можуть бути можливим способом проникнення в мережу. Проте ці кінцеві точки повинні бути безпечними, а мережа повинна бути захищеною, і безпечний віддалений доступ за допомогою VPN є обов'язковим.

Невеликі організації часто обмежені в коштах і не мають достатньої кількості персоналу для фінансування інфраструктури та безпеки, необхідних для захисту від зловмисників; це є значною проблемою. Ця ж нестача ресурсів IT-безпеки в поєднанні з неадекватним мережевим захистом і можливостями реагування на інциденти створює проблеми в захисті від подій безпеки і реагуванні на них.

3.1.3 Опис підприємства

Business-Tech - це невелика місцева компанія, яка спеціалізується на IT-рішеннях та консалтингу. У компанії працює близько 50 постійних співробітників, більшість з яких є IT-консультантами, інженерами-

програмістами, адміністративним персоналом та продавцями. Крім того, мережева інфраструктура допомагає здійснювати їхню діяльність, надаючи їхнім співробітникам чудовий рівень комунікації та співпраці.

Мережа Business-Tech складається з центрального сервера, на якому працюють ключові програми та бази даних, а також колекції дротових і бездротових пристроїв по всьому офісу. Робочі станції адміністративного персоналу знаходяться в адміністративній зоні, а середовище розробки для розробників програмного забезпечення - у виробничій зоні. Гостьові мережі обмежують доступ користувачів, резервуючи місця для відвідувачів і клієнтів, що є хорошим способом захисту від зовнішніх загроз.

Однак Business-Tech - мале підприємство - стикається з кількома проблемами безпеки. Фішинг є постійною загрозою, а співробітники постійно отримують оманливі електронні листи.

Компанія також стикається з проблемою забезпечення доступу фахівців до IT-систем, що є важливим для консультантів, які виконують багато роботи за межами офісу. Забезпечення безпечного та ефективного віддаленого доступу є неймовірно важливим для підтримки продуктивності працівників компанії в умовах, коли робочі практики стають дедалі гнучкішими.

Такий обмежений бюджет вимагає від компанії використання певної форми економічно ефективної мережевої безпеки.

На рисунку 3.1 показано схему мережі Business-Tech, яка показує різні задіяні компоненти і взаємозв'язки між ними.

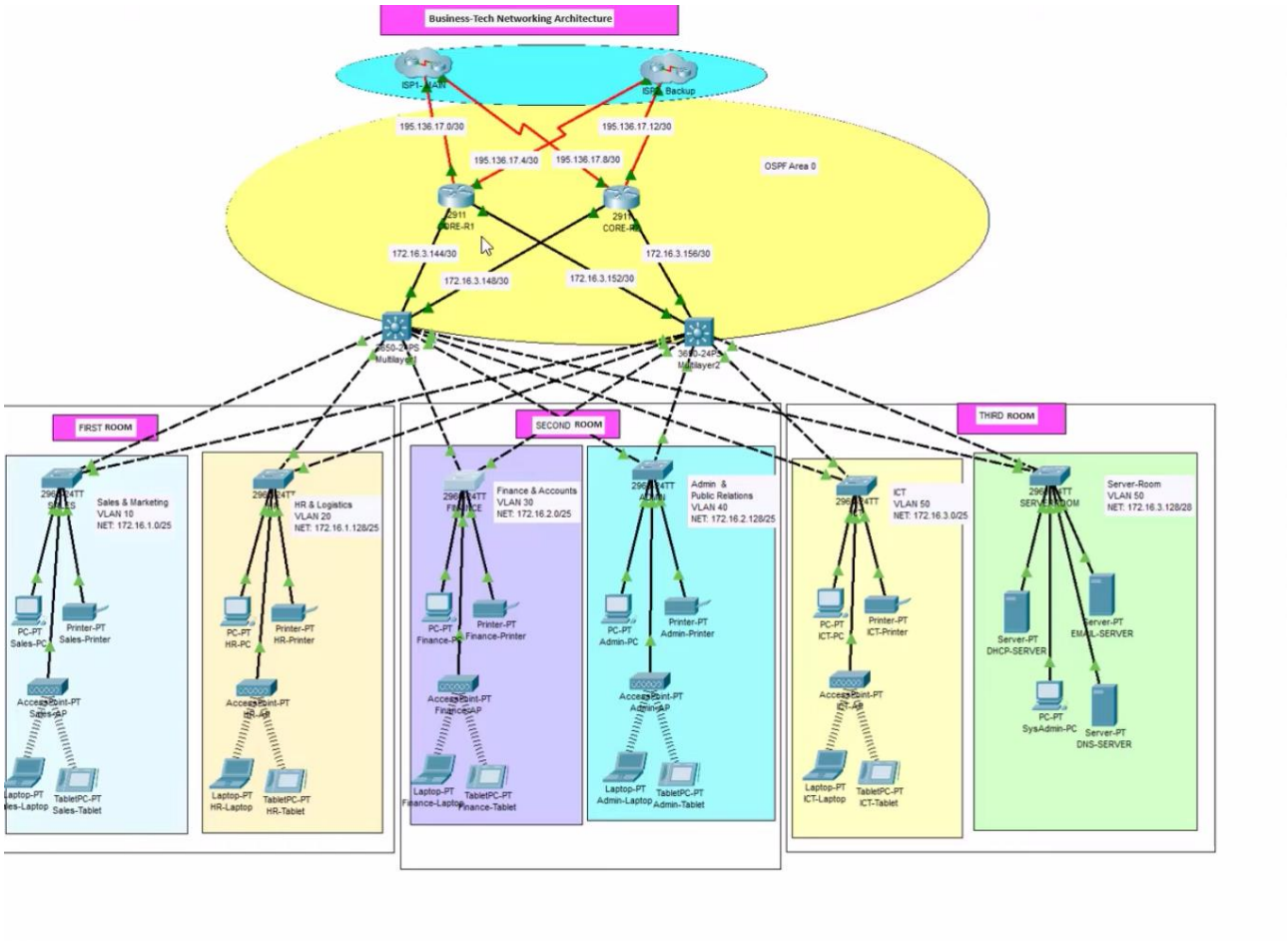

Рис 3.1 Мережева архітектура підприємства Business-Tech.

Таким чином, мережева безпека невеликого підприємства, такого як Business-Tech, вимагає уваги до різноманітних взаємопов'язаних пристроїв і систем.

3.1.4 Повсякденна діяльність

Мале підприємство Business-Tech, як і всі малі підприємства, стикається з багатьма загрозами безпеки та вразливими місцями для цілісності мережі та безпеки даних. Нижче наведено детальний аналіз конкретних експлойтів та інцидентів, що сталися в компанії. Компанія зазнала серйозного порушення безпеки, пов'язаного з фішинговою атакою. У цьому випадку кільком співробітникам були надіслані електронні листи від надійного партнера з проханням оновити дані для входу на автентичній веб-сторінці, яка виглядала як справжня. Однак деякі співробітники повелися на цю хитрість і надали свої

облікові дані, якими потім скористалися зловмисники.

Ця фішингова атака відкрила ці дані для сторонніх очей - дані, що включали інформацію про клієнтів та внутрішні комунікації. У цілеспрямованій фішинговій кампанії зловмисники використовували облікові дані для входу в систему електронної пошти компанії та перегляду приватних електронних листів і вкладених файлів. Цей злам створив ризик для довіри до конфіденційних даних і призвів до простою в роботі Business-Tech, поки IT-команда працювала над усуненням наслідків зловмисників, ліквідацією наслідків і перевстановленням системи безпеки.

3.1.5 Вразливість у бездротовій мережі

Однією з основних вразливостей, виявлених у Business-Tech, був брак безпеки в бездротовій мережі. Wi-Fi мережа компанії була налаштована із застарілими протоколами шифрування, що залишало її відкритою для всіх, крім найпростіших спроб злому (спочатку це був WEP, а не WPA2). Вперше ми виявили цю загрозу під час планового аудиту безпеки, який виявив ознаки несанкціонованого підключення до мережі, що могло призвести до прослуховування та перехоплення конфіденційних даних.

3.1.6 Атака вірусу-вимагача

Компанія також зазнала атаки вірусу-вимагача. Один із співробітників завантажив виконуване вкладення зі спам-повідомлення і через нього на його робочу станцію було встановлено програму-вимагач. Програма-здирник заблокувала конфіденційні файли і погрожувала опублікувати їх, якщо не буде отримано викуп. У Business-Tech були резервні копії, але їх створення та відновлення відбувалося повільно, що призводило до тимчасових простоїв.

3.1.7 Аналіз першопричини порушення безпеки

Проведено детальний аналіз, щоб зрозуміти першопричини цих порушень безпеки. Виявилося, що вони були майже повністю спричинені відсутністю обізнаності та навчання працівників з питань безпеки. Брандмауери були встановлені, але працівники не знали, як ідентифікувати фішингові електронні листи, а фішинг - це те, що дозволило програмі проникнути в систему в першу чергу. Скомпрометовані облікові дані самі по собі можуть бути небезпечними, але відсутність багатофакторної автентифікації (MFA) робила цей сценарій набагато гіршим, оскільки це, по суті, давало зловмисникам вільний доступ.

Найбільш значний ризик безпеки був пов'язаний з небезпечними застарілими налаштуваннями безпеки в бездротових мережах. Перша реалізація мережі Wi-Fi ніколи не переглядалася і не оновлювалася, щоб відповідати сучасним вимогам безпеки. Причиною такого недогляду була відсутність регулярних аудитів та оцінок безпеки. Нарешті, мережа не була належним чином сегментована, щоб запобігти несанкціонованому доступу неавторизованих пристроїв до найбільш важливих ділянок мережі.

Атака з вимогою викупу була результатом недостатнього рівня безпеки кінцевих точок і практик користувачів. Слабка фільтрація електронної пошти дозволила співробітнику отримати шкідливе повідомлення. Робоча станція не була обладнана сучасними засобами виявлення загроз, тому програма-вимагач залишилася невиявленою і змогла зашифрувати файли. Цей інцидент продемонстрував необхідність впровадження належних практик захисту кінцевих точок і регулярного оновлення визначень для виявлення вірусів.

3.1.8 Вжиті заходи для покращення безпеки

Після цих інцидентів компанія Business-Tech вжила низку заходів, щоб уникнути їх повторення в майбутньому:

1. Навчальні програми для співробітників: Розроблені для допомоги у

розпізнаванні фішингових загроз та дотриманні найкращих практик безпеки.

2. Багатофакторна автентифікація (MFA): Впроваджена для покращення захисту облікових даних.

3. Оновлення бездротової мережі: Перебудована для впровадження нових функцій безпеки (WPA3) та включена до регулярних аудитів безпеки.

4. Сегментація мережі: Покращена для відокремлення критичних зон від менш захищених ділянок.

5. Передові технології фільтрації електронної пошти: Впроваджені для виявлення та запобігання вкладенням, зараженим вірусом-вимагачем.

6. Покращення безпеки кінцевих точок: Включають виявлення загроз у реальному часі та заходи реагування.

7. Регулярне резервне копіювання: Покращене для забезпечення швидкого відновлення даних після атаки.

Ці інциденти та порушення виявили серйозні вразливості безпеки та недоліки в системі безпеки компанії. Після проведеного аналізу та впровадження вказаних заходів Business-Tech значно знизила ризик майбутніх загроз і покращила захист своєї мережі та даних. Забезпечення належного навчання співробітників, актуальності конфігурацій безпеки та належного захисту кінцевих точок є ключовими для підтримки високого рівня безпеки в компанії.

3.2 Спостереження за змінами та обслуговуванням

Компанія Business-Tech дуже серйозно ставиться до ризиків та інцидентів, пов'язаних з інформаційною безпекою. Це змусило її вдосконалити деякі захисні заходи, щоб впоратися з ризиками для мережевої безпеки та захистити конфіденційні дані.

3.2.1 Покращення програм навчання та підвищення обізнаності

Перш за все, компанія покращила програми навчання та підвищення

обізнаності співробітників. У минулому проводилися регулярні тренінги, де працівники отримували знання про фішинг, як розпізнавати небезпечні електронні листи, а також деякі прості рекомендації щодо покращення їхнього стану кібербезпеки. Ці тренінги включали імітацію фішингових вправ, де детально розглядалися типи фішингових атак, способи їх виявлення та повідомлення про них.

3.2.2 Зміна налаштувань Wi-Fi мережі

Щоб зменшити ризики в мережі Wi-Fi, Business-Tech змінила налаштування структури Wi-Fi. Це включало заміну застарілого шифрування WEP на WPA3, найновіший і найбезпечніший стандарт шифрування. Це значно зменшило кількість агентів загроз, які використовували мережу без належного дозволу. Крім того, компанія вирішила сегментувати свою мережу, створивши різні зони, такі як адміністративні операції, середовища розробки та гостьовий доступ. Така сегментація сприяла стримуванню потенційних порушень і обмежила доступ до чутливих частин мережі для несанкціонованих пристроїв.

Редизайн бездротової мережі виявився одним з найефективніших кроків. Використовуючи шифрування WPA3 та ізолюючи мережу на окремі зони, Business-Tech підвищила безпеку і збільшила мережевий трафік. Це ефективно запобігає доступу несанкціонованих пристроїв до чутливих частин мережі, що зменшує ймовірність витоку даних і покращує загальний стан безпеки.

3.2.3 Впровадження багатофакторної автентифікації (MFA)

Business-Tech впровадила багатофакторну автентифікацію (MFA). MFA забезпечує додатковий рівень захисту, вимагаючи другої форми перевірки разом з паролями, що ускладнює зловмисникам доступ навіть за наявності скомпрометованих облікових даних. Це особливо важливо для запобігання несанкціонованому доступу через фішингові атаки.

Розгортання багатофакторної автентифікації стало ще однією важливою перемогою. Це унеможливлює несанкціонований доступ навіть у випадку витоку облікових даних. Облікові дані співробітника були отримані за допомогою фішингової атаки, але зловмисник не зміг увійти в систему через вимогу MFA. Це стало ще одним нагадуванням про ефективність MFA у блокуванні несанкціонованого доступу та про необхідність багаторівневого захисту.

3.2.4 Безпека електронної пошти

Business-Tech значно зменшила кількість фішингових електронних листів, що надходять співробітникам, впровадивши більш просунуті рішення для фільтрації електронної пошти. Компанія також запустила алгоритми машинного навчання для деяких облікових записів користувачів, щоб визначити ті повідомлення, які повинні бути заблоковані. Це успішно блокувало багато спроб фішингу ще до того, як вони досягли цілей. В результаті кількість успішних фішингових атак всередині компанії була зведена практично до нуля.

3.3 Проблеми імплементації та їх вирішення

3.3.1 Спротив працівників

Найбільшою проблемою був спротив працівників до змін. Вони неохоче приймали нові протоколи та додаткові кроки для автентифікації. Щоб вирішити цю проблему, Business-Tech провела поглиблене навчання, пояснюючи необхідність цих заходів і як вони приносять користь компанії. Демонстрація наслідків порушень безпеки та прикладів, коли нові заходи можуть бути корисними, допомогла працівникам прийняти нові правила.

3.3.2 Технічні труднощі

Під час модернізації мережевої інфраструктури виникли технічні

труднощі. Перехід від шифрування WEP до WPA3 та розбивка мережі на частини вимагали ретельного планування. Business-Tech спланував оновлення в неробочий час і всебічно тестував зміни перед їх впровадженням. Компанія також звернулася за допомогою до зовнішніх експертів для швидшого впровадження змін.

3.3.3 Фінансові перешкоди

Фінансові обмеження вимагали ретельного обмірковування. Business-Tech зосередилася на найбільш важливих передових практиках безпеки та використовувала інструменти безпеки з відкритим вихідним кодом і хмарні сервіси для економії коштів. Крім того, компанія працювала з постачальниками, щоб отримати агресивні ціни та підтримку.

3.4 Організаційні стратегії та настанови

3.4.1 Розробка політики безпеки

Щоб зміцнити свою мережеву безпеку, Business-Tech почала розробляти чітко визначену політику безпеки, яка відповідає потребам організації в операційному середовищі, де вона функціонує. Важливою частиною цього процесу є проведення детальної оцінки ризиків, спрямованої на виявлення будь-яких потенційних загроз і вразливостей, притаманних лише цій організації. Це стало основою політики, яка вирішує питання захисту даних, контролю доступу, реагування на інциденти та прийнятного використання.

3.4.2 Політика захисту даних

Business-Tech розробила політику захисту даних, щоб контролювати, як захищати всю конфіденційну інформацію з моменту її створення до утилізації. Політика вимагає шифрування конфіденційних даних і передбачає процедури

управління, зберігання та знищення даних.

3.4.3 Реагування на інциденти

Життєвий цикл реагування на інциденти задокументовано за допомогою політик реагування на інциденти для створення контрольованого процесу управління та вирішення інцидентів безпеки в міру їх виникнення. Ці політики встановлюють процедури звітування про інциденти, проведення розслідувань та вжиття коригувальних заходів. Регулярно проводяться тренінги, щоб усі працівники були обізнані з цими політиками і знали, що робити у випадку порушення таких процедур.

3.4.4 Регулярний аудит безпеки

Business-Tech дотримується низки найкращих практик постійного управління безпекою, щоб зберегти інформацію компанії в безпеці. Регулярний аудит безпеки є одним з головних правил. Щоквартальний аудит проводиться для виявлення нових вразливостей, перевірки дотримання політик безпеки та підтвердження того, що всі впровадження безпеки працюють належним чином. Аудит надає результати, які дозволяють уточнити та оновити політики та процедури безпеки.

3.4.5 Моніторинг діяльності мережі

Business-Tech постійно контролює діяльність мережі шляхом розгортання передових систем SIEM (Security Information and Event Management - управління інформацією про безпеку та подіями). Це дозволяє команді безпеки аналізувати сповіщення, які надсилаються мережевими пристроями та додатками в режимі реального часу, щоб виявляти потенційні загрози та швидко реагувати на них.

3.4.6 Оновлення та управління виправленнями

Регулярне оновлення та управління виправленнями є важливою частиною постійного успішного управління безпекою. Це гарантує, що все програмне забезпечення та системи є актуальними та захищеними від відомих на даний момент вразливостей.

3.4.7 Процес управління змінами

Компанія Business-Tech застосовує суворий процес управління змінами, коли йдеться про внесення будь-яких змін до IT-інфраструктури. Цей процес включає всебічне тестування та затвердження, щоб зміни не призвели до появи нових вразливостей і не зруйнували існуючі засоби контролю безпеки. Плани резервного копіювання та аварійного відновлення регулярно перевіряються та тестуються під тиском, щоб гарантувати швидке відновлення після інцидентів з безпекою.

3.4.8 Вплив керівництва та менеджменту в забезпеченні мережевої безпеки

Керівництво Business-Tech має ключову роль у забезпеченні мережевої безпеки компанії. Беручи участь у розробці та впровадженні політик безпеки, керівництво демонструє свою прихильність до важливості мережевої безпеки. Це починається з самого верху, з чіткого акценту на безпеці з боку вищого керівництва та виділення необхідних ресурсів для розробки, впровадження та підтримки надійних заходів безпеки.

3.4.9 Дотримання нормативних стандартів

Керівництво також несе відповідальність за дотримання організацією нормативних і галузевих стандартів. Це передбачає постійну обізнаність про

регуляторні зміни та адаптацію політик і практик безпеки відповідно до них. Необхідна також перевірка з боку зовнішніх джерел, які оцінюють компанію на відповідність вимогам і пропонують вказівки щодо областей, які можна поліпшити.

Стратегія мережевої безпеки Business-Tech:

Розробка комплексної політики безпеки: Охоплює захист даних, контроль доступу, реагування на інциденти та прийнятне використання.

Впровадження безпеки в усій організації: Включає регулярні аудити безпеки, моніторинг діяльності мережі та управління виправленнями.

Дотримання практик безпеки після впровадження: Реалізація програм навчання та інформування співробітників, суворий процес управління змінами, перевірка планів резервного копіювання та аварійного відновлення.

Роль керівництва та менеджменту: Впровадження культури безпеки, інтеграція з бізнес-стратегією, дотримання нормативних стандартів.

Завдяки таким суворим стратегіям, тривалій пильності та вкоріненому мисленню, орієнтованому на безпеку, Business-Tech може гарантувати, що вона може захистити свої мережі та дані від нових загроз. Інвестиції в безпеку відображають відданість керівництва захисту активів компанії, а також забезпечують ресурси і фокус для досягнення місії та цілей фірми.

3.5 Оцінка та вплив заходів безпеки

Надійність засобів контролю безпеки, впроваджених у Business-Tech, була піддана ретельній перевірці за допомогою структурованої системи періодичних аудитів, оцінок вразливостей та моніторингу ефективності.

Оцінка показує, що інвестиції в загальнокорпоративні навчальні програми покращують загальну обізнаність працівників та їхні навички щодо виявлення фішингу та повідомлення про нього. Зокрема, впровадження багатофакторної автентифікації (MFA) успішно призвело до зменшення кількості випадків несанкціонованого доступу. Кількість успішних входів з використанням паролів,

отриманих внаслідок втрати облікових даних, помітно зменшилася.

Ефективні системи фільтрації електронної пошти, здатні зупиняти фішингові та спам-повідомлення, призвели до зменшення кількості загроз безпеці, що проникали в організацію.

Реконфігурація бездротової мережі на WPA3 і включення сегментації мережі дозволили стримати спроби несанкціонованого доступу та помістити критичні частини мережі в ізольовану зону, вільну від вторгнень.

Після впровадження посиленого захисту кінцевих точок і регулярного резервного копіювання даних кількість фішингових атак зменшилася на 80%, без жодної успішної атаки зловмисників з вимогою викупу.

Моніторинг у режимі реального часу та реагування на інциденти стали значно швидшими, що дозволило швидше виявляти та усувати загрози. Середній час виявлення та реагування на інциденти скоротився на 50%, зменшивши збитки та запобігши простою в роботі.

Регулярне резервне копіювання даних і дотримання стандартів шифрування забезпечили цілісність даних та їх доступність. Ефективність планів аварійного відновлення була доведена, оскільки компанія змогла швидко відновити роботу з мінімальною втратою даних під час змодельованих сценаріїв атаки.

Відгуки від працівників, IT-відділу, керівництва та решти організації були переважно позитивними. Співробітники повідомили, що відчувають себе більш впевнено з новими заходами безпеки, зазначивши, що навчальні програми допомогли їм покращити виявлення та уникнення загроз.

IT-персонал відзначив зручний дизайн і високу продуктивність вдосконалених систем фільтрації електронної пошти та моніторингу в режимі реального часу. Вони також зазначили, що нове обладнання, програмне забезпечення та процедури для кінцевих точок безпеки дають хороші результати без значних проблем з інтеграцією.

Керівництво усвідомлює вигоду для організації, коментує впровадження інших дорогих засобів захисту від проникнень та підтримку операційної

ефективності.

На основі отриманих відгуків, Business-Tech переглянула стратегію постійного вдосконалення. Завдяки постійному перегляду політики безпеки, безперервним навчальним програмам і впровадженню найсучасніших технологій безпеки, організація здатна протистояти новітнім загрозам і бути готовою реагувати на нові тенденції.

3.6 Майбутні напрямки технологічної безпеки для підприємства

Мережева безпека - це постійно змінна сфера, на яку впливають нові тенденції та технологічні досягнення. Нижче розглянемо деякі з найбільш значущих тенденцій, які формують майбутнє мережевої безпеки, та надамо рекомендації для Business-Tech щодо адаптації до цих змін.

Однією з найбільш значущих тенденцій є використання штучного інтелекту та машинного навчання для забезпечення безпеки. Ці технології дозволяють виявляти загрози та реагувати на них, аналізуючи великі обсяги даних у режимі реального часу. Вони можуть профілювати патерни, які свідчать про зловмисну активність, та швидко адаптуватися до нових загроз, забезпечуючи еволюційний захист від сучасних кіберзагроз.

Ще однією важливою тенденцією є архітектура нульової довіри. Ця концепція передбачає, що жодному суб'єкту всередині або поза мережею не слід автоматично довіряти. Кожен користувач або пристрій, який намагається отримати доступ до мережевих ресурсів, повинен бути перевірений. Це обмежує загрозу внутрішніх атак і переміщення через мережу, застосовуючи суворий контроль доступу на основі ідентифікації та стану пристрою.

Постійне інформування співробітників про нові загрози безпеки та найкращі практики є критично важливим. Навчальний контент повинен оновлюватися з появою нових технологій або змін у кіберпросторі.

Передові технології, такі як AI, ML і блокчейн, можуть бути дорогими. Business-Tech повинна розподіляти інвестиції відповідно до ступеня ризику та

серйозності. Партнерство з постачальниками технологій і хмарних рішень може допомогти в управлінні витратами.

Впровадження нових технологій може вимагати спеціалізованих навичок, яких може не бути у нинішньої робочої сили. Програми навчання та розвитку для IT-персоналу можуть допомогти подолати цю проблему. Співпраця з зовнішніми професіоналами та консалтинговими фірмами з питань безпеки також може бути корисною.

Впровадження нових технологій в існуючі системи може бути складним і може порушити існуючі операції. Застосування поетапного підходу до впровадження, починаючи з пілотних проектів, може знизити цей ризик. Належне тестування та валідація забезпечать безперешкодну інтеграцію без зупинки операцій.

Business-Tech повинні бути в курсі змін у нормативних актах і підтверджувати, що нові заходи безпеки відповідають чинним стандартам. Це означає звернення за порадами до юристів і фахівців з комплаєнсу та забезпечення дотримання юридичних зобов'язань.

Працівники можуть чинити опір новим протоколам безпеки. Залучення працівників до процесу змін, інформування про нові заходи безпеки, їхні переваги та надання необхідного навчання і підтримки допоможуть подолати цей опір.

Висновки до розділу 3

Фахівці з кібербезпеки Business-Tech провели довгий і ретельний аналіз конкретних порушень і недоліків, щоб підсумувати найбільш слабкі місця, такі як застарілі методи шифрування, недостатній захист кінцевих точок. Компанія зробила кілька кроків, щоб усунути ці прогалини в безпеці, впровадивши суворі навчальні програми, вдосконалені методи фільтрації електронної пошти,

багатофакторну автентифікацію (MFA) та нові рішення для захисту кінцевих точок.

Ці заходи також позитивно вплинули на навчальні програми для співробітників. Кількість фішингових інцидентів зменшилася на 80%, а співробітники стали краще виявляти спроби фішингу та повідомляти про них. Впровадження MFA значно зменшило кількість інцидентів несанкціонованого доступу, ускладнюючи зловмисникам використання скомпрометованих облікових даних. Вдосконалені системи фільтрації електронної пошти зменшили кількість фішингових листів і спаму, що потрапляють до співробітників, зупиняючи багато загроз безпеці ще до того, як вони стали проблемою. Редизайн бездротової мережі з використанням шифрування WPA3 та сегментація мережі забезпечили чітке відокремлення критично важливих сегментів мережі від потенційних вторгнень.

Все це разом підвищило рівень безпеки Business-Tech. Кількісні показники свідчать про значне зменшення кількості інцидентів та порушень. Середній час реагування на інциденти безпеки значно зменшився, що доводить ефективність безперервного моніторингу та ефективності протоколів реагування на інциденти. Компанія змогла зберегти критичні дані неушкодженими та доступними завдяки змодельованим сценаріям атак, де відновлення даних було успішним, підтверджуючи надійність їхніх планів резервного копіювання та аварійного відновлення.

Business-Tech повинна адаптуватися до нових тенденцій і технологій мережевої безпеки, щоб захищатися від нових загроз. Інвестуючи в AI і ML, впроваджуючи архітектуру нульової довіри, посилюючи безпеку периферійних пристроїв та досліджуючи можливості блокчейну, компанія може значно покращити свій стан безпеки. Проактивне вирішення питань за допомогою належного планування, інвестування ресурсів та залучення співробітників дозволить Business-Tech ефективно впроваджувати ці зміни, захищаючи активи та діяльність від постійно мінливих загроз кіберзлочинності.

ВИСНОВКИ

1. Досліджено різні типи кібератак

Виконуючи дослідження було розібрано та досліджено сучасні кіберзагрози як для підприємств так і для фізичних осіб. Дана інформація дала позитивні результати для досягнення поставлених цілей цієї наукової роботи.

2. Оглянуто літературу та інформації

Огляд літератури та зібрана інформація свідчать про те, що кожна організація повинна створити адекватний простір для політики і практики управління інформаційною безпекою, управління ризиками, спостереження і підтримки, а також для повсякденної діяльності та довгострокових заходів, спрямованих на вирішення технічних і нетехнічних аспектів СУІБ.

3. Досліджено стан мережевої безпеки підприємства.

Поточний стан характеризується зростаючою складністю та кількісною частотою кіберзагроз, таких як фішинг, програми вимагачі та атаки відмови в обслуговувані. Ця оцінка чітко підкреслює необхідність для значної кількості підприємств впроваджувати комплексні, багато рівневі системи захисту та використовувати новітні технології для ефективного захисту своїх мереж.

4. Проведено аналіз інцидентів та вразливостей безпеки

Підприємство зіткнулося з декількома серйозними проблемами безпеки. Детальний аналіз показав критичні недоліки, такі як застарілі протоколи шифрування інформації та недостатній захист кінцевих точок.

5. Впроваджено програми навчання співробітників

Було впроваджено комплексні навчальні програмні заходи для вирішення проблем з недостатньої обізнаності працівників щодо фішингових загроз. Заходи значно підвищили обізнаність працівників розпізнавати спроби фішингових атак

та як реагувати та продіяти їм. В результаті це привело до зменшення кількості інцидентів.

6. Впроваджено багатофакторні автентифікації

Це стало вирішальним кроком для зменшення кількості інцидентів несанкціонованого доступу. Додаткові етапи перевірки показали що лише скомпроментованих облікових даних працівників буде недостатньо для доступу до мережі, знову ж таки підвищуючи загальний рівень безпеки.

7. Розгорнуто вдосконалені системи фільтрації електронних пошт

Впроваджено складні системи фільтрації електронних пошт для виявлення та блокування фішингових і спам повідомлень. Це впровадження суттєво зменшило появу загрозо-вмісних повідомлень, які потрапляли на корпоративні пошти співробітників.

8. Усунуто вразливості бездротової мережі

Реконфігурація бездротової мережі з шифрувальною технологією WPA3 та сегментаціє мережі, успішно усунули вразливості щодо проникнення в локальні персональні ПК та інші прилади підприємства для ін’єкціювання, тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аніловська Г. Я., Марушко Н. С., Стоколоса Т. М. Інформаційні системи і технології у фінансах : навч. посіб. Львів : Магнолія 2006, 2015. 312 с.

2. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII. Голос України. 2017. 27 верес. (№ 178-179). С. 10–22.

3. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід правил щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). [Чинний від 2017-01-01]. Вид. офіц.. К. : ДП «УкрНДНЦ», 2016. 149с.

4. Біленчук П., Обіход Т. Небезпеки ядерної злочинності: аналіз вітчизняного і міжнародного законодавства. Юридичний вісник України. 2017. 20-26 жовт. (№ 42). С. 14–15.

5. Barney N., Shacklett M. E., Rosencrance L. What is Authentication? | Definition from TechTarget. Security. URL: http://searchsecurity.techtarget.com/definition/authentication(дата звернення: 20.04.2024).

6. Cao X. L. Research on Method of Information System Information Security Risk Management. Advanced Materials Research. 2014. Т. 926-930. С. 4105–4109. URL: https://doi.org/10.4028/www.scientific.net/amr.926-930.4105(дата звернення: 20.04.2024).

7. Current challenges in information security risk management / S. Fenz та ін. Information Management & Computer Security. 2014. Т. 22, № 5. С. 410–430. URL: https://doi.org/10.1108/imcs-07-2013-0053(дата звернення: 20.04.2024).

8. Cyber and Infrastructure Security Centre Website. Cyber and Infrastructure Security Centre Website. URL: http://www.tisn.gov.au/Documents/ITSEAG+IT+Security+Governance+paper+(Word).doc(дата звернення: 20.04.2024).

9. Different Forms of Decentralization. Center for International Earth Science Information Network.

URL: https://www.ciesin.org/decentralization/English/General/Different_forms.html(дата звернення: 20.04.2024).

10. Gauvain T. 1 Information Security Risk Management for Systems Engineers. INCOSE International Symposium. 1999. Т. 9, № 1. С. 780–785. URL: https://doi.org/10.1002/j.2334-5837.1999.tb00238.x(дата звернення: 20.04.2024).

11. Governance I. T. Information Security Risk Management for ISO 27001/ISO 27002. IT Governance Ltd, 2019. (дата звернення: 20.04.2024).

12. Greene S. Security Program and Policies: Principles and Practices. Pearson Technology Group, 2014. 648 с. (дата звернення: 20.04.2024).

13. Home. HHS.gov. URL: https://www.hhs.gov/ocr/privacy/(дата звернення: 20.04.2024).

14. IT security governance: Boards must act. ZDNET. URL: http://www.zdnet.com/article/it-security-governance-boards-must-act(дата звернення: 20.04.2024).

15. MindfulSecurity.com. 2009. Why is Information Security Important?. URL: http://mindfulsecurity.com/2009/07/01/why-is-information-security-important(дата звернення: 20.04.2024).

16. National Institute National Institute of Standards & Technology. Information Security Continuous Monitoring for Federal Information Systems and Organizations: Nist Sp 800-137. Independently Published, 2019. (дата звернення: 20.04.2024).

17. Networking Solutions: Discover Cloud Services. Networking Solutions: Discover Cloud Services | Extreme Networks. URL: https://www.extremenetworks.com/(дата звернення: 20.04.2024).

18. Security Best Practices for IT Project Managers | SANS Institute. Cyber Security Training | SANS Courses, Certifications & Research. URL: http://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257(дата звернення: 20.04.2024).

19. Understanding the Importance of and Implementing Internal Security Measures | SANS Institute. Cyber Security Training | SANS Courses, Certifications & Research.

URL: https://www.sans.org/reading-room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures-1901(дата звернення: 20.04.2024).

20. Security policy. Window SecuritzURL: https://www.windowsecurity.com/pages/security-policy.pdf(дата звернення: 22.05.2024).

21. Подкасти. Один з найбільших трубопроводів США, що транспортує паливо, призупинив роботу через кібератаку. Голос Америки Українською. URL: https://www.holosameryky.com/a/Truboprovid-kibernapad/5883228.html (дата звернення: 20.04.2024).

22. 85% of breaches involve the human element - Help Net Security. Help Net Security. URL: https://www.helpnetsecurity.com/2021/05/17/breaches-high-human-element/ (дата звернення: 20.04.2024).

23. Accenture's state of cybersecurity resilience 2023 report. Newsroom | Accenture. URL: https://newsroom.accenture.com/news/2023/aligning-cybersecurity-to-business-objectives-helps-drive-revenue-growth-and-lower-costs-of-breaches-accenture-report-finds (дата звернення: 20.04.2024).

24. Annual report 2023. Cisco. URL: https://www.cisco.com (дата звернення: 20.04.2024).

25. Report mcafee. Business Wire URL: https://www.businesswire.com/news/home/20190827005835/en/McAfee-Report-Uncovers-Ransomware-Resurgence (дата звернення: 20.04.2024).

26. Cost of a data breach 2023 | IBM. IBM in Deutschland, Österreich und der Schweiz. URL: https://www.ibm.com/reports/data-breach (дата звернення: 20.04.2024).

29. Cybersecurity threats in 2022 – Here's what you need to know. Veeam Software Official Blog. URL: https://www.veeam.com/blog/cyber-security-threats.html (дата звернення: 20.04.2024).

30. Deloitte's 2021 global blockchain survey. Deloitte Insights. URL: https://www.deloitte.com/global/en/our-

thinking/insights/multimedia/podcasts/global-blockchain-survey-2021.html (дата звернення: 20.04.2024).

31. Document: joint intelligence community statement on the solarwinds orion cyber incident. Law Fare Media. URL: https://www.lawfaremedia.org/article/document-joint-intelligence-community-statement-solarwinds-orion-cyber-incident (дата звернення: 20.04.2024).

32. Enterprise data protection best practices. Veeam Software Official Blog. URL: https://www.veeam.com/blog/enterprise-data-protection.html (дата звернення: 20.04.2024).

33. Intrusion detection / prevention system market - industry report 2025. Global Market Insights Inc. URL: https://www.gminsights.com/industry-analysis/intrusion-detection-prevention-system-ids-ips-market (дата звернення: 20.04.2024).

34. NETSCOUT threat intelligence report. Latest Cyber Threat Intelligence Report. URL: https://www.netscout.com/threatreport (дата звернення: 20.04.2024).

35. Ponemon institute reveals 68% of organizations were victims of successful endpoint attacks in 2019. markets.businessinsider.com. URL: https://markets.businessinsider.com/news/stocks/ponemon-institute-reveals-68-of-organizations-were-victims-of-successful-endpoint-attacks-in-2019-1028855557 (дата звернення: 20.04.2024).

36. Risks of unpatched vulnerabilities | prowriters insurance. ProWriters. URL: https://prowritersins.com/cyber-insurance-blog/unpatched-vulnerability-risks/ (дата звернення: 20.04.2024).

37. Security information and event management market growth drivers & opportunities. MarketsandMarkets.
URL: https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html (дата звернення: 20.04.2024).

38. The attack on colonial pipeline: what we've learned & what we've done over the past two years. Cybersecurity and Infrastructure Security Agency CISA. URL: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (дата звернення: 20.04.2024).

39. The threat landscape in 2021. Symantec Enterprise Blogs. URL: https://symantec-enterprise-blogs.security.com/threat-intelligence/threat-landscape-2021 (дата звернення: 20.04.2024).

40. Trends report q1 2021. APWG. URL: https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf (дата звернення: 20.04.2024).

41. Explanatory and overview on iso. ISO ORG. URL: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0.Explanatory_note_and_overview_on_ISO_Survey_2021_results.pdf?nodeid=22272345&vernum=-2 (дата звернення: 20.04.2024).

42. Intrusion detection and prevention systems market size, 2031. *Business Research Insights | Global Market Research Report & Consulting*. URL: https://www.businessresearchinsights.com/market-reports/intrusion-detection-and-prevention-systems-market-106715 (дата звернення: 20.04.2024).

43. Gartner forecasts global security and risk management spending. *Gartner*. URL: https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024.html (дата звернення: 20.04.2024).

44. Flexera releases 2021 state of the cloud report press release. *IT and Cloud Management, Optimization and Solutions | Flexera*. URL: https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report (дата звернення: 20.04.2024).

45. An unusual demand marks the global endpoint security market for endpoint solutions. *GRC Viewpoint*. URL: https://grcviewpoint.com/an-unusual-demand-marks-the-global-endpoint-security-market-for-endpoint-solutions/ (дата звернення: 20.04.2024).

46. Virtual private network (VPN) market size, analysis report 2032. *Global Market Insights Inc.* URL: https://www.gminsights.com/industry-analysis/virtual-private-network-vpn-market (дата звернення: 20.04.2024).