МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ РЕКОМЕНДАЦІЇ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ ”

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

_____ Олександр Курінний
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олександр КУРІННИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
к.т.н Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Курінному Олександру Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Рекомендації вирішення проблем кібербезпеки у віддаленому робочому середовищі”,

   керівник кваліфікаційної роботи РАБЧУН Дмитро к.т.н.
   (ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека, методи та засоби управління персоналом з інформаційної безпеки:, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:

   4.1 Проаналізувати теоретичні аспекти кібербезпеки у віддаленому робочому середовищі.
   4.2 Дослідити проблеми кібербезпеки у віддаленому робочому середовищі.
   4.3. Розробити рекомендації щодо рішення проблем кібербезпеки у віддаленому робочому середовищі.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Аналіз кібербезпеки у віддалених робочих середовищах.	08.04.2025	Виконано
4.	Дослідження проблем кібербезпеки у віддаленому робочому середовищі	15.04.2025	Виконано
5.	Розробка рекомендацій щодо рішення проблем кібербезпеки у віддаленому робочому середовищі	22.04.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	Виконано
7.	Оформлення роботи.	06.05.2025	Виконано
8.	Оформлення презентації.	09.05.2025	Виконано
9.	Отримання рецензії на роботу.	12.06.2025	Виконано
10.	Захист в ДЕК.	__.06.2025	Виконано

Здобувач вищої освіти _____ Олександр КУРІННИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Курінний О.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: “ Рекомендації вирішення проблем кібербезпеки у віддаленому робочому середовищі”

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КУРІННИЙ Олександр у кваліфікаційній роботі проаналізував кібербезпеку у віддаленому робочому середовищі, дослідив проблеми кібербезпеки у віддаленому робочому середовищі, розробив рекомендації щодо рішення проблем кібербезпеки у віддаленому робочому середовищі.

КУРІННИЙ Олександр показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КУРІННОГО Олександра на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач КУРІННИЙ О.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Курінного Олександра Сергійовича
на тему “Рекомендації вирішення проблем кібербезпеки у віддаленому робочому середовищі”

Актуальність. У сучасному світі, де віддалена робота стала невід’ємною частиною діяльності організацій, а кіберзагрози, такі як фішинг, витоки даних і атаки на незахищені мережі, зростають із кожним роком, питання кібербезпеки набуває критичного значення. Зміна робочих парадигм, прискорена пандемією COVID-19, підкреслила вразливості традиційних підходів до захисту даних і систем. З огляду на це, робота є актуальною, адже вона пропонує практичні рекомендації для вирішення проблем кібербезпеки в умовах віддаленої роботи, що має велике значення для організацій різних секторів, включаючи державні установи, приватні компанії та фінансовий сектор.

Позитивні сторони:

1. У роботі проведено всебічний аналіз особливостей віддаленої роботи, таких як використання особистих пристроїв, незахищені мережі та залежність від хмарних сервісів, а також їхнього впливу на кібербезпеку. Це створює міцну теоретичну основу для подальших рекомендацій.
2. Автор пропонує цілісну стратегію захисту, що поєднує технологічні рішення (VPN, MFA, Zero Trust, антивіруси), організаційні заходи (політики безпеки, контроль доступу) та навчання співробітників, забезпечуючи багатошаровий захист від кіберзагроз.
3. Розроблені рекомендації є універсальними та можуть бути застосовані в різних організаціях. Наведені приклади, такі як зниження інцидентів на 85% у компанії "TechCorp" завдяки впровадженню VPN, підтверджують ефективність запропонованих рішень.
4. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.

Недоліки:

У роботі доцільно було б приділити більше уваги дослідженню спеціалізованих інструментів для безперервного моніторингу кіберзагроз, таких як системи IDS/IPS або SIEM, що могло б додати глибини практичним рекомендаціям.

Однак, зазначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: Юрій ПЕПА
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Робота складається зі вступу, трьох розділів, що містять 5 рисунків, висновків та списку використаних джерел з 72 найменувань. Загальний обсяг роботи становить 74 сторінки, з яких 9 сторінок займають перелік умовних скорочень та список використаних джерел.

Мета роботи: розробити рекомендації для підвищення рівня кібербезпеки в умовах віддаленого робочого середовища, з урахуванням сучасних загроз, технологічних і організаційних особливостей.

Об'єкт дослідження: віддалене робоче середовище як техніко-організаційна система, що включає інфраструктуру, інформаційні потоки та людські ресурси.

Предмет дослідження: рекомендації щодо вирішення проблем кібербезпеки, що виникають у процесі організації та функціонування віддаленої роботи.

Методи дослідження: аналіз літературних джерел та стандартів інформаційної безпеки; кейс-аналіз кібератак у віддаленому режимі; систематизація проблем і рішень; оцінювання ефективності заходів захисту.

Короткий зміст роботи: у роботі проаналізовано особливості віддаленої роботи, що впливають на стан кібербезпеки; визначено основні загрози, вразливості та виклики; розроблено рекомендації, що включають впровадження VPN, багатофакторної аутентифікації, політик управління пристроями, навчання персоналу та моніторинг кіберзагроз. Показано ефективність комплексного підходу, що поєднує технологічні, організаційні та освітні складові захисту.

Галузь використання: запропоновані рекомендації можуть бути застосовані в державних установах, приватних компаніях, банківському секторі, IT-сфері для підвищення рівня кіберзахисту в умовах дистанційної роботи.

Ключові слова: КІБЕРБЕЗПЕКА, ВІДДАЛЕНА РОБОТА, VPN, BYOD, ХМАРНІ СЕРВІСИ, МЕРЕЖЕВА БЕЗПЕКА, ФІШИНГ, БАГАТОФАКТОРНА АУТЕНТИФІКАЦІЯ, КІБЕРГІГІЄНА, ПОЛІТИКИ БЕЗПЕКИ.

ABSTRACT

The work consists of an introduction, three chapters containing 5 figures, conclusions, and a list of references with 72 items. The total volume of the work is 74 pages, of which 9 pages are occupied by the list of abbreviations and the list of references.

Purpose of the study: to develop a set of practical recommendations aimed at enhancing cybersecurity in remote work settings, considering modern threats, technologies, and organizational challenges.

Object of research: remote work environment as a socio-technical system including infrastructure, information processes, and human factors.

Subject of research: recommendations for solving cybersecurity problems in remote work environments.

Research methods: literature and regulatory analysis; case analysis of cyberattacks in remote mode; classification of problems and solutions; expert evaluation of the effectiveness of security measures.

Summary: the paper analyzes how remote work affects cybersecurity, identifies key threats and vulnerabilities, and proposes comprehensive recommendations. These include implementing VPNs, multi-factor authentication, device management policies, employee cybersecurity training, and continuous threat monitoring. A holistic approach integrating technical, organizational, and educational components is shown to be the most effective.

Field of application: the developed recommendations can be applied in public institutions, private enterprises, banking, and IT sectors to improve cybersecurity in remote work conditions.

Keywords: CYBERSECURITY, REMOTE WORK, VPN, BYOD, CLOUD SERVICES, NETWORK SECURITY, PHISHING, MULTI-FACTOR AUTHENTICATION, CYBER HYGIENE, SECURITY POLICIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI	Artificial Intelligence
BYOD	Bring Your Own Device
IDS/IPS	Intrusion Detection System
IT	Information Technology
MFA	Multi-Factor Authentication
MDM	Mobile Device Management
MitM	Man-in-the-Middle
OS	Operating System
VPN	Virtual Private Network
ZTNA	Zero Trust Network Access
SIEM	Security Information and Event Management

ВСТУП

Актуальність теми. Сучасний світ переживає стрімке зростання віддаленої роботи, що стало особливо помітним після пандемії COVID-19, коли компанії по всьому світу змушені були швидко адаптуватися до дистанційного формату. Цей перехід приніс значні переваги, такі як підвищення гнучкості робочих процесів і зниження витрат на утримання офісів, однак разом із цим виникли нові виклики для кібербезпеки. Віддалені робочі середовища, які часто включають незахищені мережі, використання особистих пристроїв (BYOD) і залежність від хмарних технологій, потребують розробки практичних рішень для забезпечення безпеки даних і захисту організацій від кіберзагроз. У цих умовах створення ефективних рекомендацій для вирішення проблем кібербезпеки стає не просто актуальним завданням, а необхідністю для підтримки безперервності бізнес-процесів і мінімізації ризиків. Зростання кіберризиків у віддалених робочих середовищах вимагає системного підходу до їхнього усунення [1].

Зростання кількості кібератак на віддалених працівників є одним із ключових аргументів, що підкреслюють важливість цього питання. Віддалена робота призвела до значного зростання кібератак, зокрема фішингу, спрямованих на працівників., які працюють поза офісом. Такі інциденти призводять до значних фінансових і репутаційних втрат для організацій. Наприклад, реальні випадки витоків даних у компаніях із віддаленими працівниками, таких як атака на SolarWinds у 2020 році, демонструють, наскільки вразливими можуть бути системи без належного захисту [2]. Ці факти вказують на необхідність адаптації заходів кібербезпеки до нових реалій віддаленої роботи, що стала нормою для багатьох організацій після пандемії. Віддалена робота створює нові виклики для кібербезпеки, які потребують комплексного підходу до захисту даних і систем у розподілених середовищах [3]. Пандемія COVID-19 значно вплинула на кібербезпеку віддаленої роботи. Аналіз 2024 року вказує на зростання складності кібератак на розподілені робочі сили [4]. Адаптація заходів безпеки до умов роботи

з дому стала необхідністю через зростання кіберризиків під час пандемії [5]. За даними дослідження, 45% організацій зазнали інцидентів безпеки під час пандемії, а середня вартість витоку даних у 2023 році склала 4,45 мільйона доларів [6]. Це підкреслює необхідність посилення заходів безпеки у віддаленому робочому середовищі.

Розробка практичних рекомендацій для вирішення цих проблем є критично важливою для забезпечення безпеки в умовах, коли традиційні підходи до захисту даних уже не є достатньо ефективними. Впровадження найкращих практик безпеки у домашніх офісах є важливим для захисту віддалених працівників після пандемії [7]. Віддалена робота вимагає нових стратегій, які враховують технологічні, організаційні та освітні аспекти. Технологічні рішення, такі як шифрування даних і використання віртуальних приватних мереж (VPN), організаційні заходи, зокрема чіткі політики безпеки, та навчання співробітників основам кібергігієни стають основою для створення стійкого захисту. Саме тому актуальність теми полягає у створенні комплексного підходу, який допоможе організаціям не лише реагувати на загрози, а й запобігати їм, зберігаючи конкурентоспроможність і довіру клієнтів.

Мета роботи. Метою цієї кваліфікаційної роботи є розробка рекомендацій для вирішення проблем кібербезпеки у віддалених робочих середовищах.

Завдання дослідження

Для досягнення поставленої мети в роботі визначено такі завдання:

1. Проаналізувати особливості віддаленого робочого середовища та пов’язані з ним проблеми кібербезпеки.
2. Визначити основні напрями розробки рекомендацій.
3. Розробити практичні рекомендації

Об’єктом дослідження є віддалене робоче середовище як система, що включає технології, процеси та людські ресурси, задіяні у виконанні професійних обов’язків поза межами традиційного офісу. Це середовище охоплює як інфраструктуру (мережі, пристрої, програмне забезпечення), так і взаємодію між співробітниками та організацією в умовах дистанційної роботи.

Предметом дослідження є рекомендації щодо вирішення проблем кібербезпеки у віддаленій роботі, які базуються на комплексному підході до захисту даних і систем. Предмет включає конкретні заходи, спрямовані на усунення вразливостей, що виникають через особливості віддаленого формату.

Методи дослідження

Для реалізації поставлених завдань у роботі використано комплекс методів. Зокрема, проведено літературний огляд, що включав аналіз сучасних джерел для вивчення технологій безпеки та підходів до організації віддаленої роботи. Додатково було здійснено аналіз конкретних ситуацій, що передбачав дослідження реальних прикладів кібератак на віддалених працівників з метою визначення ефективних контрзаходів. Застосовано метод практичного впровадження, який полягав у розробці рекомендацій на основі оцінки технологій безпеки та їхньої адаптації до умов віддаленої роботи.

Практичне значення

Розроблені рекомендації мають значне практичне значення, оскільки можуть бути використані організаціями для підвищення безпеки комп’ютерних мереж і захисту даних у віддалених робочих середовищах. Особливо актуальними вони є для фінансового сектору, де витоки даних можуть призвести до катастрофічних наслідків. Пропоновані заходи включають чіткі вказівки щодо впровадження технологій, таких як VPN і багатофакторна аутентифікація (MFA), розробки політик безпеки та проведення регулярного навчання співробітників, що сприяє формуванню культури кібербезпеки.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНИХ РОБОЧИХ СЕРЕДОВИЩАХ

Віддалена робота стала ключовим елементом сучасних організацій, особливо після глобального переходу до дистанційних форматів, викликаного такими подіями, як пандемія COVID-19. Цей зсув підкреслив нові виклики для кібербезпеки, оскільки традиційні методи захисту даних і систем не завжди ефективні в розподілених робочих середовищах.

1.1 Особливості віддаленої роботи та їх вплив на кібербезпеку

Віддалена робота внесла значні зміни у способи взаємодії працівників із корпоративними системами та даними. Згідно з дослідженням McKinsey, кількість працівників, які працюють віддалено, зросла на 44% за останні п'ять років [8]. Крім того, Gartner прогнозує, що до кінця 2021 року 51% всіх працівників знань у світі працюватимуть віддалено, що є значним зростанням з 27% у 2019 році [8]. Ці дані свідчать про стрімке зростання віддаленої роботи та необхідність адаптації заходів кібербезпеки до нових умов.

Ці зміни породжують виклики, які необхідно враховувати для забезпечення кібербезпеки. Існують різні моделі віддаленої роботи, такі як повна віддаленість, гібридна модель та часткова віддаленість, кожна з яких має свої особливості та впливає на кібербезпеку по-різному. Наприклад, у повній віддаленості працівники повністю залежать від домашніх мереж та особистих пристроїв, що підвищує ризик кібератак. У гібридній моделі працівники чергують роботу в офісі та вдома, що вимагає гнучких заходів безпеки. Часткова віддаленість може бути менш ризикованою, але все одно потребує уваги до кібербезпеки.

Пандемія COVID-19 прискорила перехід до віддаленої роботи, що призвело до збільшення кіберризиків. За даними дослідження, кількість кібератак зросла на 630% під час пандемії COVID-19 [9]. Це свідчить про те, що зловмисники активно використовують нові можливості для атак на віддалених працівників.

1.1.1 Використання особистих пристроїв

Використання особистих пристроїв (Bring Your Own Device) є однією з основних особливостей віддаленої роботи. Цей підхід ускладнює управління безпекою пристроїв, оскільки особисті комп'ютери, планшети чи смартфони часто не відповідають корпоративним стандартам захисту [10]. Відсутність централізованого контролю над цими пристроями підвищує ризик витоку даних або зараження шкідливим програмним забезпеченням. Наприклад, за даними Cisco (2023), лише 31% організацій досягли зрілого рівня готовності до захисту пристроїв, що свідчить про значні прогалини в управлінні безпекою BYOD [11]. Через використання незахищених мереж і особистих пристроїв фішингові атаки зросли на 94% з 2020 року [12].

Працівники можуть використовувати пристрої з застарілим програмним забезпеченням або без належних антивірусних рішень, що робить їх вразливими до атак. Крім того, змішування особистих і робочих даних на одному пристрої ускладнює розмежування доступу та захист конфіденційної інформації. Організаціям необхідно впроваджувати заходи, такі як політики управління мобільними пристроями (MDM) та регулярні перевірки безпеки, щоб мінімізувати ці ризики.

1.1.2 Підключення через незахищені мережі

Незащищені мережі, такі як громадські Wi-Fi і домашні маршрутизатори, підвищують ризик атак типу MitM. Згідно з Verizon (2023), 83% кібератак на організації державного сектору були здійснені зовнішніми акторами, що підкреслює вразливість незахищених з'єднань [13].

Відсутність шифрування або слабкі паролі на домашніх мережах працівників лише посилюють проблему. Для захисту потрібні технології, такі як віртуальні приватні мережі, а також навчання працівників щодо безпечного використання мереж.

1.1.3 Залежність від хмарних сервісів

Залежність від хмарних сервісів стала невід'ємною частиною віддаленої роботи, забезпечуючи гнучкий доступ до даних і додатків. Проте це підвищує ризики, пов'язані з безпекою хмарних середовищ, такі як несанкціонований доступ або витоки даних. Дослідження Cisco (2023) показує, що лише 12% організацій досягли зрілого рівня готовності до захисту робочих навантажень додатків у хмарі, що є критичним для безпеки [11].

Хмарні сервіси часто стають мішенню через їхню централізовану природу та великі обсяги даних. Якщо доступ до хмарного сховища скомпрометовано, зловмисники можуть отримати конфіденційну інформацію або порушити роботу організації. Для вирішення цього виклику потрібні посилені заходи аутентифікації, такі як багатофакторна аутентифікація, та регулярний моніторинг хмарної інфраструктури.

1.1.4 Відсутність фізичного нагляду

Відсутність фізичного нагляду у віддалених робочих середовищах ускладнює контроль за діями працівників і дотриманням політик безпеки. Це може призводити до ненавмисних помилок, таких як використання слабких паролів або неналежне налаштування пристроїв. Verizon (2023) зазначає, що 74% усіх порушень безпеки включають людський фактор, що підкреслює необхідність підвищення кібергігієни працівників [13].

Без фізичного нагляду складніше виявити підозрілу поведінку, наприклад, несанкціонований доступ до систем. Працівники можуть також нехтувати базовими заходами безпеки через брак прямого контролю. Організаціям слід впроваджувати регулярні тренінги з кібербезпеки та системи моніторингу поведінки користувачів для зменшення цих ризиків.

1.1.5 Комплексний вплив особливостей на кібербезпеку

Кожна з розглянутих особливостей віддаленої роботи — використання BYOD, підключення через незахищені мережі, залежність від хмарних сервісів та відсутність фізичного нагляду — створює унікальні виклики для кібербезпеки. Ці

фактори взаємодіють, посилюючи загальну вразливість організацій. Наприклад, незахищена мережа в поєднанні з погано налаштованим особистим пристроєм може стати ідеальним сценарієм для атаки.

Для ефективного захисту потрібен комплексний підхід, який включає технологічні рішення, такі як шифрування та VPN, організаційні політики, наприклад, обов'язкове використання MFA, та освітні ініціативи для працівників.

Вплив BYOD на безпеку

Використання BYOD не лише ускладнює управління пристроями, але й підвищує ймовірність інцидентів через різноманітність операційних систем і програмного забезпечення. Звіт Cisco (2023) вказує, що 56% організацій перебувають на початкових або середніх етапах готовності до захисту пристроїв, що відображає повільне впровадження захисних рішень [11]. Наприклад, працівник із застарілою версією ОС може стати жертвою експлойту, який уже не становить загрози для оновлених систем.

Організаціям потрібно розробляти стратегії, які включають регулярне оновлення програмного забезпечення та впровадження рішень для захисту кінцевих точок (endpoint protection). Такі заходи допоможуть зменшити вразливість, пов'язану з BYOD.

Незащищені мережі: приклади ризиків

Незащищені мережі є особливо проблемними в контексті віддаленої роботи, оскільки працівники часто не усвідомлюють ризиків. Наприклад, атака "man-in-the-middle" може дозволити зловмиснику перехопити облікові дані працівника, що підключається до корпоративного порталу через громадський Wi-Fi. Verizon (2023) підкреслює, що 85% порушень у державному секторі пов'язані з зовнішніми акторами, багато з яких використовують вразливості мереж [13].

Використання VPN і шифрування даних у русі є критично важливими для захисту. Крім того, організації можуть вимагати від працівників перевіряти безпеку домашніх мереж, наприклад, змінювати стандартні паролі маршрутизаторів.

Хмарні сервіси: аналіз вразливостей

Зростаюча залежність від хмарних сервісів означає, що організації повинні приділяти більше уваги захисту даних у хмарі. Cisco (2023) зазначає, що лише 23% організацій досягли прогресивного або зрілого рівня готовності до захисту додатків у хмарі, що залишає значну частину вразливою [11]. Витік даних із хмарного сховища може призвести до серйозних репутаційних і фінансових втрат.

Заходи, такі як шифрування даних у хмарі та регулярний аудит доступу, можуть значно знизити ці ризики. Наприклад, впровадження MFA зменшує ймовірність несанкціонованого доступу навіть у разі компрометації пароля.

Відсутність нагляду: людський фактор

Відсутність фізичного нагляду часто призводить до того, що працівники нехтують базовими правилами безпеки. Verizon (2023) зазначає, що соціальна інженерія та помилки працівників становлять значну частину інцидентів, причому 74% порушень пов’язані з людським фактором [13]. Наприклад, працівник може використати слабкий пароль або відкрити фішинговий лист, не підозрюючи про наслідки.

Освітні програми та автоматизовані системи виявлення загроз можуть допомогти зменшити ці ризики. Наприклад, симуляції фішингових атак можуть підвищити обізнаність працівників про подібні загрози.

Особливості віддаленої роботи створюють складні виклики для кібербезпеки, які потребують комплексного підходу. Використання BYOD ускладнює управління безпекою пристроїв, незахищені мережі відкривають двері для атак, хмарні сервіси підвищують ризик витоків даних, а відсутність нагляду посилює людський фактор.

1.2 Вплив віддаленої роботи на кібербезпеку: технологічні, організаційні та людські аспекти

Віддалена робота кардинально змінила способи взаємодії працівників із корпоративними системами, що призвело до появи нових викликів у сфері кібербезпеки. Цей підпункт зосереджується на аналізі впливу віддаленої роботи з точки зору технологічних, організаційних та людських аспектів, щоб глибше зрозуміти, як ці зміни впливають на безпеку організацій і які нові загрози

виникають. Розуміння цих аспектів є ключовим для розробки ефективних рекомендацій щодо захисту віддалених робочих середовищ.

1.2.1 Технологічні аспекти

Технологічні аспекти відіграють центральну роль у забезпеченні кібербезпеки віддалених робочих середовищ. Використання особистих пристроїв, підключення через незахищені мережі та залежність від хмарних сервісів створюють унікальні виклики, які потребують нових підходів до захисту.

Віддалена робота суттєво впливає на кібербезпеку через низку технологічних викликів, пов’язаних із використанням особистих пристроїв, підключенням через незахищені мережі та залежністю від хмарних сервісів. Ці аспекти створюють унікальні ризики, які потребують комплексного підходу до захисту даних і систем організацій.

Використання особистих пристроїв є однією з основних особливостей віддаленої роботи, що ускладнює управління безпекою. Працівники часто застосовують власні комп’ютери, планшети чи смартфони для доступу до корпоративних ресурсів. Такі пристрої можуть не відповідати корпоративним стандартам захисту, наприклад, через відсутність антивірусного програмного забезпечення, оновлених операційних систем або шифрування даних. Це підвищує ризик зараження шкідливим програмним забезпеченням або витоку конфіденційної інформації. Наприклад, працівник, який використовує застарілу версію операційної системи на своєму ноутбуці, може стати жертвою експлойту, що не загрожує оновленим системам. Крім того, змішування особистих і робочих даних на одному пристрої ускладнює розмежування доступу та захист інформації. Для мінімізації цих ризиків організаціям необхідно впроваджувати політики управління мобільними пристроями та рішення для захисту кінцевих точок (endpoint protection).

Підключення через незахищені мережі, такі як громадські Wi-Fi або домашні маршрутизатори з базовими налаштуваннями, створює ще один критичний виклик. Такі мережі часто стають точкою входу для атак типу "man-in-the-middle", коли

зловмисники перехоплюють дані, що передаються між працівником і корпоративною мережею. Незахищені мережі можуть мати слабкі паролі або взагалі не використовувати шифрування, що робить їх легкою мішенню для зловмисників. Для захисту від таких загроз організації повинні вимагати використання віртуальних приватних мереж та шифрування даних у русі. Також працівникам варто надавати рекомендації щодо безпечного налаштування домашніх мереж, наприклад, зміну стандартних паролів маршрутизаторів.

Залежність від хмарних сервісів стала невід'ємною частиною віддаленої роботи, забезпечуючи гнучкий доступ до даних і додатків із будь-якого місця. Проте це підвищує ризики, пов'язані з безпекою хмарних середовищ, такі як несанкціонований доступ або витоки даних. Хмарні сервіси часто стають мішенню через їхню централізовану природу та великі обсяги даних. Якщо доступ до хмарного сховища скомпрометовано, зловмисники можуть отримати конфіденційну інформацію або порушити роботу організації. Для вирішення цього виклику потрібні посилені заходи аутентифікації, такі як багатофакторна аутентифікація, шифрування даних у хмарі та регулярний моніторинг хмарної інфраструктури. Організації також повинні співпрацювати з хмарними провайдерами для забезпечення відповідності стандартам безпеки.

Таким чином, технологічні виклики віддаленої роботи потребують інтегрованого підходу, який поєднує управління пристроями, захист мереж і безпеку хмарних сервісів. Лише за таких умов організації зможуть ефективно протистояти кіберзагрозам у розподілених робочих середовищах.

1.2.2 Організаційні аспекти

Організаційні аспекти відіграють важливу роль у забезпеченні кібербезпеки віддалених робочих середовищ. Відсутність фізичного нагляду та розподілена інфраструктура створюють значні виклики для управління безпекою та дотримання політик, що вимагає нових підходів до організації захисту.

Відсутність фізичного нагляду у віддалених робочих середовищах ускладнює контроль за діями працівників і дотриманням політик безпеки. Це може призводити

до ненавмисних помилок, таких як використання слабких паролів або неналежне налаштування пристроїв. Без фізичного нагляду складніше виявити підозрілу поведінку, наприклад, несанкціонований доступ до систем. Працівники можуть також нехтувати базовими заходами безпеки через брак прямого контролю. Для вирішення цієї проблеми організації повинні впроваджувати системи моніторингу поведінки користувачів та регулярні тренінги з кібербезпеки. Наприклад, симуляції фішингових атак можуть підвищити обізнаність працівників про подібні загрози.

Крім того, розподілена інфраструктура, характерна для віддаленої роботи, вимагає нових підходів до управління безпекою. Традиційні методи, орієнтовані на захист периметра, стають менш ефективними, оскільки працівники підключаються з різних місць і через різні мережі [14]. Це ускладнює централізоване управління політиками безпеки та моніторингом. Організаціям необхідно впроваджувати хмарні рішення безпеки, які дозволяють управляти захистом у розподілених середовищах. Наприклад, використання рішень на основі штучного інтелекту для виявлення аномалій у поведінці користувачів може допомогти вчасно реагувати на потенційні загрози. Крім того, чіткі політики щодо використання корпоративних ресурсів і регулярні аудити безпеки є необхідними для підтримки високого рівня захисту.

Таким чином, організаційні виклики віддаленої роботи, такі як відсутність фізичного нагляду та розподілена інфраструктура, потребують комплексного підходу, що поєднує моніторинг, навчання та сучасні технології безпеки. Лише за таких умов організації зможуть ефективно протистояти кіберзагрозам у розподілених робочих середовищах.

1.2.3 Людські аспекти

Людські аспекти відіграють ключову роль у кібербезпеці, адже працівники часто стають найвразливішою ланкою в системі захисту. Віддалена робота ускладнює ці виклики через відсутність прямого нагляду та підвищену ймовірність людських помилок. Такі дії, як відкриття фішингових листів чи використання слабких паролів, можуть призвести до серйозних порушень безпеки [15]. У

віддалених умовах ці ризики зростають через ізоляцію працівників та зниження їхньої пильності, що спричинене відсутністю контролю. Людський фактор залишається ключовим у забезпеченні кібербезпеки віддаленої роботи [16].

Щоб протистояти цим загрозам, організації повинні впроваджувати програми навчання, які підвищують обізнаність працівників про кіберризики та вчать розпізнавати підозрілу активність. Додатково автоматизовані системи виявлення загроз можуть допомогти швидко реагувати на інциденти, пов’язані з людськими помилками.

Не менш важливим є дотримання кібергігієни — базових практик безпеки, які захищають дані та системи. У віддалених середовищах, де працівники часто працюють самостійно, це набуває особливого значення. Кібергігієна включає використання надійних паролів, регулярне оновлення програмного забезпечення та уникнення підозрілих посилань чи вкладень в електронних листах. Організаціям варто проводити регулярні тренінги, надавати чіткі інструкції та надсилати нагадування, наприклад, про зміну паролів чи оновлення програм. Автоматизовані системи перевірки дотримання політик безпеки також можуть підтримувати високий рівень захисту.

1.2.4 Комплексний вплив аспектів на кібербезпеку

Технологічні, організаційні та людські аспекти взаємодіють, створюючи складний ландшафт загроз для віддалених робочих середовищ. Наприклад, використання BYOD у поєднанні з підключенням через незахищені мережі та низьким рівнем кібергігієни може призвести до катастрофічних наслідків для безпеки організації. Аналогічно, відсутність фізичного нагляду та розподілена інфраструктура ускладнюють виявлення та реагування на інциденти.

Щоб забезпечити ефективний захист, організаціям варто впроваджувати комплексний підхід до кібербезпеки, який охоплює як технологічні, так і організаційні та освітні заходи. До технологічних рішень належать використання VPN, шифрування даних та системи захисту кінцевих точок. Водночас важливу роль відіграють організаційні заходи, такі як впровадження чітких політик безпеки,

проведення регулярних аудитів та моніторинг поведінки користувачів. Не менш значущими є й освітні ініціативи — проведення тренінгів з кібербезпеки, симуляцій атак та підвищення загального рівня обізнаності співробітників щодо потенційних загроз.

Цей підхід дозволить організаціям не лише реагувати на загрози, а й запобігати їм, забезпечуючи стійкість у віддалених робочих середовищах.

Віддалена робота впливає на кібербезпеку через технологічні, організаційні та людські аспекти, кожен з яких створює унікальні виклики. Використання BYOD, незахищені мережі та хмарні сервіси підвищують технологічні ризики, відсутність нагляду та розподілена інфраструктура ускладнюють організаційне управління безпекою, а людський фактор залишається критичним через помилки працівників.

1.3 Ключові загрози та вразливості віддалених робочих середовищ

Віддалена робота, попри свої переваги, породжує низку загроз і вразливостей, які можуть серйозно вплинути на кібербезпеку організацій. Цей підпункт зосереджується на аналізі основних загроз, що виникають у віддалених робочих середовищах, таких як фішинг, атаки на незахищені мережі, витоки даних через хмарні сервіси та соціальна інженерія. Розуміння цих загроз є критично важливим для розробки ефективних рекомендацій щодо захисту організацій.

1.3.1 Фішинг та соціальна інженерія

Фішинг і соціальна інженерія є одними з найпоширеніших загроз у віддалених робочих середовищах. Зловмисники використовують ці методи для маніпулювання працівниками з метою отримання конфіденційної інформації або доступу до систем.

Фішинг — це атака, під час якої зловмисники видають себе за довірені джерела, щоб переконати працівників розкрити облікові дані або іншу конфіденційну інформацію. У віддалених середовищах фішинг стає особливо небезпечним, оскільки працівники можуть бути менш обережними через відсутність прямого нагляду. Фішингові атаки зросли на 25% у 2023 році у віддалених робочих середовищах, що підкреслює вразливість працівників поза

офісом [17]. Наприклад, працівник може отримати електронний лист, який імітує повідомлення від IT-відділу з проханням оновити пароль, і, не підозрюючи, ввести свої облікові дані на підробленому сайті. На рисунку 1.1 відображено візуально таку ситуацію.

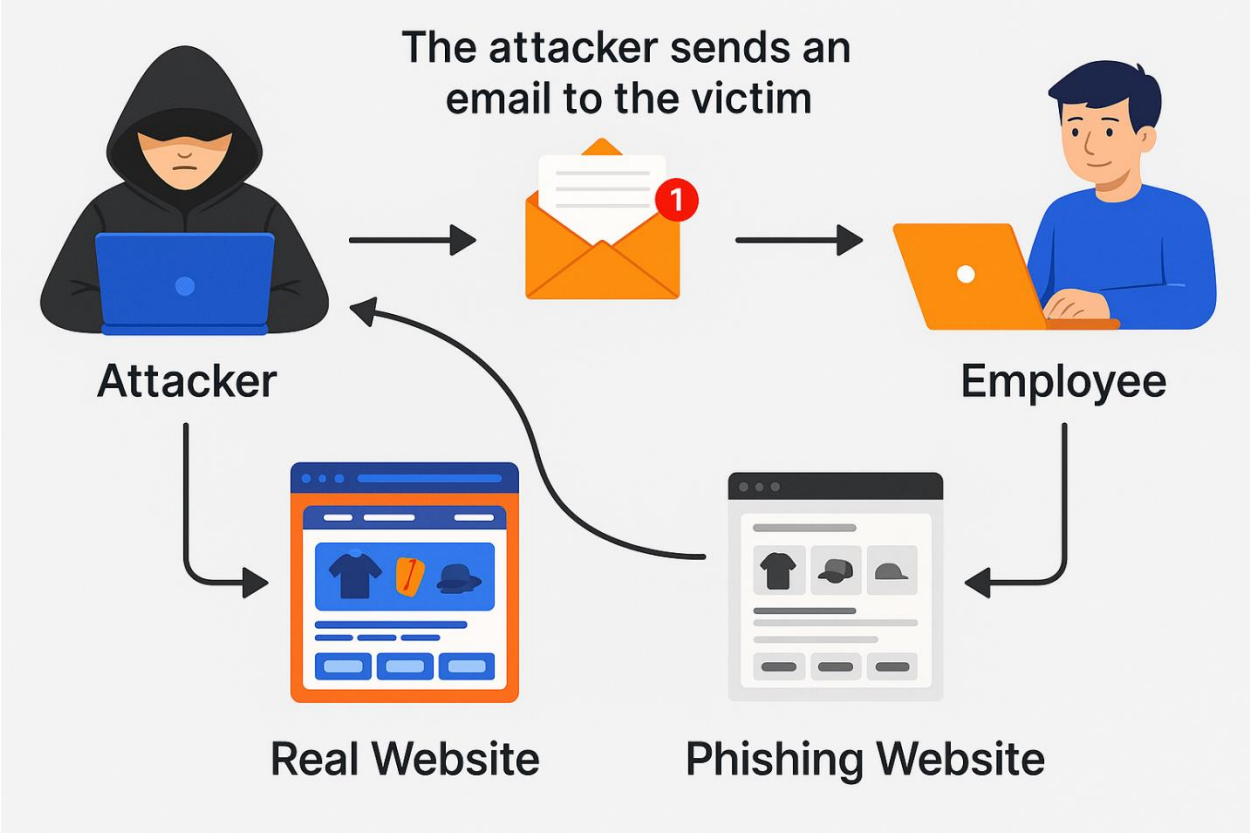

Рис. 1.1. Механізм фішингової атаки: надсилання шкідливого листа з підробленим посиланням на фальшивий сайт для викрадення даних

Згідно з Verizon (2023), 74% усіх порушень безпеки включають людський фактор, а фішинг є одним із основних методів соціальної інженерії [13]. Для захисту від фішингу організації повинні впроваджувати регулярні тренінги для працівників, щоб навчити їх розпізнавати підозрілі повідомлення, а також використовувати технології фільтрації електронної пошти та двофакторну аутентифікацію (2FA). Навчання з кібербезпеки може знизити рівень кліків на фішингові посилання до 30%, що є важливим для віддалених працівників [18].

Соціальна інженерія охоплює ширший спектр методів, ніж фішинг, і включає маніпуляції, спрямовані на отримання доступу до систем або даних через психологічний вплив. Наприклад, зловмисник може зателефонувати працівнику, видаючи себе за колегу, і попросити надати доступ до певного файлу або системи. У віддалених середовищах, де комунікація часто відбувається через електронні засоби, такі атаки можуть бути особливо ефективними. Організаціям необхідно впроваджувати політики, які обмежують обмін конфіденційною інформацією через незахищені канали, а також проводити симуляції атак соціальної інженерії для підвищення обізнаності працівників. Симуляції фішингових атак допомагають знизити ймовірність кліків на підозрілі листи на 80%, підвищуючи обізнаність працівників [19].

1.3.2 Атаки на незахищені мережі

Незащищені мережі становлять значну загрозу для віддалених робочих середовищ, особливо коли працівники підключаються до корпоративних ресурсів через громадські Wi-Fi або домашні мережі з базовими налаштуваннями. Такі мережі наражають організацію на численні ризики, зокрема атаки типу "man-in-the-middle" та вразливості, пов’язані зі слабкими паролями на домашніх маршрутизаторах. Наприклад, підключення до незахищеної мережі в кафе чи аеропорту може призвести до того, що працівник ненавмисно передасть свої облікові дані зловмиснику, який використовує спеціальні інструменти для аналізу трафіку [20]. Для захисту від таких атак організації мають вимагати використання віртуальних приватних мереж, які шифрують дані та унеможливлюють їх перехоплення, а також надавати працівникам чіткі інструкції щодо уникнення підключення до ненадійних мереж. Використання AES-256 для шифрування трафіку у віддалених мережах є стандартом для захисту від атак типу MitM [21]. Крім того, домашні маршрутизатори часто є слабкою ланкою через використання стандартних паролів, таких як "admin" чи "1234", що полегшує зловмисникам доступ до мережі працівника. Отримавши контроль над домашньою мережею, зловмисник може не лише перехоплювати дані, а й проникати до корпоративних

систем. Щоб запобігти цьому, працівникам слід рекомендувати змінювати стандартні паролі на унікальні та складні, використовувати сучасні протоколи шифрування, такі як WPA3, а також регулярно оновлювати прошивку маршрутизаторів і перевіряти налаштування безпеки. Отже, для мінімізації ризиків організації повинні впроваджувати комплексні заходи, включаючи використання VPN, навчання працівників і забезпечення належного налаштування їхніх домашніх мереж, що дозволить ефективно захистити корпоративні ресурси від атак. Технологія SD-WAN може бути альтернативою традиційним VPN, забезпечуючи кращу продуктивність для віддалених працівників [22].

1.3.3 Витоки даних через хмарні сервіси

Хмарні сервіси є невід'ємною частиною віддаленої роботи, забезпечуючи зручний доступ до даних і ресурсів, але вони також створюють нові вразливості, пов'язані з безпекою даних. Ці вразливості можуть призвести до серйозних наслідків, таких як витоки конфіденційної інформації або порушення роботи організації.

Однією з основних загроз є несанкціонований доступ до хмарних сховищ, який може статися через слабкі паролі, відсутність багатофакторної аутентифікації або компрометацію облікових даних [23]. Якщо зловмисник отримує доступ до хмарного сховища, він може викрасти конфіденційні дані або порушити роботу організації. Наприклад, у 2020 році стався витік даних із хмарного сховища SolarWinds, що мало серйозні наслідки для багатьох організацій. Для захисту від таких загроз організації повинні впроваджувати MFA, шифрування даних у хмарі та регулярний моніторинг доступу до хмарних ресурсів. Інструменти шифрування та моніторингу для захисту даних у хмарі є важливими для віддаленої роботи [24].

Ще однією значною проблемою є неправильне налаштування хмарних сервісів, таке як відкриті дозволи на доступ або відсутність шифрування. Це може призвести до витоків даних, наприклад, коли хмарне сховище налаштоване на публічний доступ, що дозволяє будь-кому отримати доступ до конфіденційних файлів. Організаціям необхідно проводити регулярні аудити налаштувань хмарних

сервісів і використовувати інструменти для автоматичного виявлення неправильних конфігурацій. Відповідність GDPR є критично важливою для захисту даних у віддалених робочих середовищах, особливо при використанні хмарних сервісів [25].

Таким чином, для забезпечення безпеки хмарних сервісів у віддаленій роботі організації повинні впроваджувати комплексні заходи, що включають MFA, шифрування, моніторинг і регулярні аудити, щоб мінімізувати ризики та захистити свої дані від несанкціонованого доступу та витоків.

1.3.4 Інші загрози та вразливості

Окрім фішингу, атак на мережі та витоків даних, існують інші загрози, які можуть впливати на безпеку віддалених робочих середовищ. Ці загрози включають шкідливе програмне забезпечення та внутрішні загрози, які можуть призвести до серйозних порушень безпеки та втрати даних.

Шкідливе програмне забезпечення (malware) може бути встановлене на пристрої працівників через фішингові листи, підроблені сайти або заражені файли. У віддалених середовищах, де пристрої не завжди захищені корпоративними антивірусними рішеннями, ризик зараження зростає. Наприклад, програма-вимагач (ransomware) може зашифрувати дані на пристрої працівника, що призведе до втрати доступу до важливих файлів. Для захисту від malware організації повинні впроваджувати рішення для захисту кінцевих точок, забезпечувати регулярне оновлення програмного забезпечення та навчати працівників розпізнавати підозрілі файли і посилання.

Внутрішні загрози також становлять значний ризик, особливо у віддалених середовищах. Працівники або підрядники, які мають доступ до конфіденційної інформації, можуть ненавмисно або навмисно її розкрити [26]. Наприклад, працівник може скопіювати дані на особистий пристрій або надіслати їх через незахищені канали. Щоб зменшити ці ризики, організації повинні впроваджувати принцип найменших привілеїв, моніторинг активності користувачів та чіткі політики управління доступом.

Таким чином, для забезпечення безпеки віддалених робочих середовищ організації повинні враховувати не лише зовнішні загрози, але й внутрішні ризики, впроваджуючи комплексні заходи захисту, такі як антивірусні рішення, оновлення програмного забезпечення, навчання працівників та контроль доступу.

1.3.5 Комплексний вплив загроз на кібербезпеку

Загрози взаємодіють і можуть посилювати одна одну, створюючи складний ландшафт ризиків для організацій. Наприклад, успішна фішингова атака може призвести до компрометації облікових даних, які потім використовуються для доступу до хмарних сервісів або внутрішніх систем. Аналогічно, атака на незахищену мережу може відкрити шлях для встановлення шкідливого програмного забезпечення на пристрої працівників.

Віддалені робочі середовища стикаються з численними загрозами, такими як фішинг, атаки на незахищені мережі, витоки даних через хмарні сервіси та внутрішні загрози. Ці загрози вимагають комплексного підходу до кібербезпеки, який включає технологічні, організаційні та освітні заходи. Розуміння цих загроз є основою для розробки рекомендацій, спрямованих на підвищення безпеки віддаленої роботи.

Висновки до розділу 1

Дослідження підкреслює критичну важливість кібербезпеки у віддалених робочих середовищах, які стали нормою для багатьох організацій у цифрову епоху. Стрімкий перехід до дистанційної роботи, прискорений пандемією COVID-19, значно посилив складність і масштаби кіберзагроз, що вимагає переосмислення підходів до захисту корпоративних даних і систем. Аналіз теоретичних основ кібербезпеки у віддалених умовах дозволяє сформулювати наступні висновки:

Віддалена робота змінила традиційні способи взаємодії з корпоративними ресурсами, підвищивши вразливість через використання особистих пристроїв, незахищених мереж і хмарних сервісів. Відсутність фізичного нагляду додатково ускладнює контроль за безпекою, що робить підприємства більш схильними до атак, таких як фішинг чи витоки даних.

Пандемія COVID-19 стала каталізатором масового переходу до віддаленої роботи, що призвело до різкого зростання кібератак. Зокрема, фішингові атаки зросли на 630% під час пандемії, демонструючи, як зловмисники адаптуються до нових умов і використовують людські помилки як основну точку входу.

Технологічні виклики, пов’язані з різноманітністю пристроїв, незахищеними мережами та залежністю від хмарних технологій, ускладнюють управління кібербезпекою. Традиційні методи захисту, такі як периметрова безпека, втрачають ефективність, що вимагає впровадження сучасних рішень, наприклад, VPN, багатофакторної аутентифікації та шифрування.

Організаційні та людські фактори відіграють ключову роль у вразливості віддалених середовищ. Низька кібергігієна працівників, слабкі паролі та необережність у поводженні з підозрілими листами є найслабшою ланкою. Це підкреслює потребу в регулярному навчанні персоналу та чітких політиках безпеки.

Середовище загроз постійно еволюціонує, а основними ризиками є фішинг, атаки на мережі, витоки даних через хмарні сервіси та внутрішні загрози. Ці загрози взаємопов’язані: наприклад, успішна фішингова кампанія може призвести до компрометації хмарного сховища, що посилює наслідки атаки.

Ефективний захист віддалених робочих середовищ потребує комплексного підходу, який поєднує превентивні заходи (VPN, шифрування, контроль доступу), засоби виявлення (моніторинг, системи IDS/IPS) і реагування (аудити, плани відновлення). Освітні ініціативи, такі як тренінги з кібергігієни та симуляції атак, є необхідними для мінімізації людських помилок.

Розділ 2 ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ

У сучасному цифровому світі віддалена робота стала невід'ємною частиною функціонування багатьох організацій, пропонуючи гнучкість і підвищуючи продуктивність співробітників. Цей перехід, прискорений глобальними подіями, такими як пандемія COVID-19, змінив традиційні підходи до організації праці, зробивши її більш залежною від інформаційних технологій. Проте разом із перевагами віддалена робота принесла значні виклики у сфері кібербезпеки, які потребують ретельного аналізу та негайного вирішення. Якщо в офісних умовах організації могли покладатися на чітко визначені фізичні та мережеві межі, то у віддаленому середовищі ці межі розмиті, що створює нові вразливості та ускладнює забезпечення безпеки даних і систем.

Віддалене робоче середовище характеризується унікальними умовами, такими як використання особистих пристроїв співробітників, підключення через незахищені мережі та обмежений контроль з боку IT-відділів. Ці фактори підвищують ризик кібератак, таких як витік даних, несанкціонований доступ і порушення конфіденційності. У цьому контексті важливо переформулювати традиційні загрози, такі як фішинг чи програми-вимагачі, у конкретні проблеми, з якими стикаються організації, наприклад, недостатня обізнаність співробітників чи відсутність належних механізмів резервного копіювання.

Проблеми кібербезпеки у віддаленому робочому середовищі не є ізольованими; вони тісно пов'язані між собою, створюючи складний ланцюг вразливостей. Наприклад, використання незахищених мереж може посилювати ризик слабкої аутентифікації, а низька кібергігієна співробітників може призводити до успішних атак соціальної інженерії. Цей взаємозв'язок вимагає цілісного підходу до аналізу та пошуку рішень. На прикладі підприємства Business-Tech показано, як недостатня обізнаність співробітників і застарілі протоколи шифрування призвели до інцидентів безпеки, таких як атака програми-вимагача

[27]. Такі реальні випадки підкреслюють актуальність дослідження цих проблем у контексті віддаленої роботи.

Дослідження спирається на аналіз літератури та практичні приклади з наданих документів. Звіт IBM (2023), згаданий у списку джерел, вказує, що середня вартість витоку даних у 2023 році склала 4,45 мільйона доларів, що підкреслює фінансові та репутаційні наслідки ігнорування цих проблем.

2.1 Аналіз проблем кібербезпеки у віддаленому робочому середовищі

2.1.1 Вступ до проблем кібербезпеки у віддаленому робочому середовищі

Віддалена робота докорінно змінила підходи до організації праці, створивши нові можливості для гнучкості та ефективності. Однак разом із цими перевагами з’явилися значні виклики у сфері кібербезпеки, які відрізняються від тих, що характерні для традиційних офісних умов. У віддаленому робочому середовищі організації втрачають можливість централізованого контролю над мережевими межами, що робить їх більш вразливими до кіберзагроз.

У традиційних офісних налаштуваннях IT-відділи могли покладатися на фізичну ізоляцію мереж і стандартизоване обладнання [28]. У віддаленому середовищі співробітники часто використовують особисті пристрої та підключаються через домашні або громадські мережі, що ускладнює моніторинг і захист. Згідно з дослідженням Verizon (2021), 81% порушень даних, пов’язаних із хакерством, були спричинені слабкими або вкраденими паролями, що особливо актуально для віддалених працівників, які можуть нехтувати базовими заходами безпеки. Ці умови створюють унікальний набір проблем, які потребують детального розгляду.

2.1.2 Незахищені мережі: основна проблема віддаленої роботи

Однією з найпоширеніших проблем у віддаленому робочому середовищі є використання незахищених мереж. Хмарні технології широко використовуються у віддаленій роботі, але вони також створюють нові виклики для кібербезпеки. Неправильне налаштування хмарних сервісів, таких як AWS чи Google Drive, може призвести до витоку даних. Наприклад, у 2019 році стався витік даних у Capital One

через неправильне налаштування хмарного сервісу, що призвело до компрометації особистих даних понад 100 мільйонів клієнтів [29].

Співробітники часто підключаються до корпоративних ресурсів через громадські Wi-Fi мережі в кафе, аеропортах чи бібліотеках, а також через домашні мережі, які не завжди мають належний рівень захисту [30]. Такі з'єднання вразливі до атак типу «людина посередині», коли зловмисники перехоплюють дані, що передаються між співробітником і корпоративною системою. На рисунку 2.1 можна візуально побачити як саме проходить атака типу « людина посередині ».

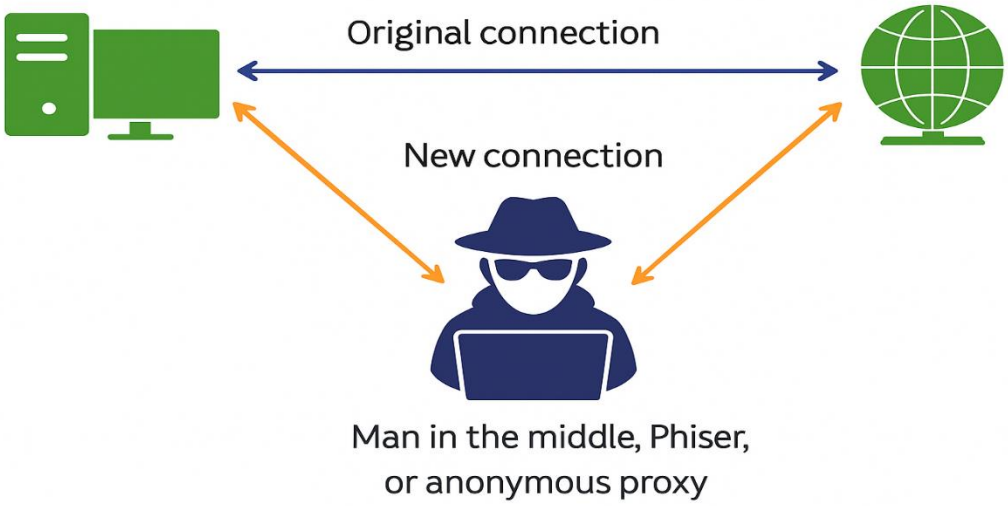

Рис.2.1. Схема атаки типу "людина посередині" (MitM), при якій зловмисник перехоплює трафік між користувачем і сервером

Наприклад, співробітник Business-Tech підключився до незахищеної мережі Wi-Fi, що призвело до компрометації даних через відсутність шифрування [26].

Звіт IBM (2023) зазначає, що 35% кібератак на віддалених працівників були пов'язані з незахищеними мережами [6]. Атаки на незахищені мережі зросли на 15% у 2023 році, що вказує на необхідність шифрування з'єднань [31]. Ця проблема ускладнюється тим, що організації мають обмежений контроль над зовнішніми

мережевими середовищами. Якщо в офісі мережа може бути захищена брандмауерами та системами виявлення вторгнень (IDS), то у віддаленому контексті ці заходи стають менш ефективними. Співробітник, який працює з ресторану і передає конфіденційні документи через незахищене з'єднання, наражає організацію на ризик витоку даних, що може мати серйозні фінансові та репутаційні наслідки.

Вирішення цієї проблеми потребує впровадження захищених каналів зв'язку, таких як VPN, які шифрують трафік і забезпечують безпечний доступ до корпоративних ресурсів. Методи протидії атакам на незахищені мережі включають використання VPN і регулярне навчання працівників [32]. У Business-Tech після інциденту оновили свою мережу, включивши WPA3 і сегментацію, що значно знизило ризик несанкціонованого доступу [27]. Таким чином, незахищені мережі є не лише технічною проблемою, але й організаційною, що вимагає чітких політик і навчання співробітників.

2.1.3 Слабка аутентифікація: шлюз для несанкціонованого доступу

Слабка аутентифікація є ще однією критичною проблемою, яка набуває особливого значення у віддаленому робочому середовищі. Співробітники часто використовують прості або повторно застосовувані паролі, що полегшує зловмисникам їх злам за допомогою атак грубої сили або соціальної інженерії. Слабкі паролі є основною причиною 81% порушень даних, пов'язаних із хакерством, що підтверджує актуальність цієї проблеми [27].

У віддалених умовах ризик компрометації облікових даних зростає через використання особистих пристроїв і неконтрольованих середовищ. Наприклад, співробітник може використовувати один і той же пароль для кількох сервісів, включаючи корпоративні системи. Якщо цей пароль буде скомпрометовано через фішингову атаку, зловмисник отримає доступ до всіх пов'язаних облікових записів. Business-Tech зіткнувся з подібною ситуацією, коли скомпрометовані облікові дані через фішинг дозволили зловмисникам проникнути в мережу, але відсутність MFA погіршила наслідки [27].

Відсутність багатофакторної аутентифікації є ключовим недоліком, який посилює цю проблему. MFA додає додатковий рівень захисту, вимагаючи другого фактора, наприклад, коду з мобільного пристрою, що значно ускладнює несанкціонований доступ. У Business-Tech впровадження MFA після інциденту з фішингом зупинило зловмисника, навіть коли пароль був відомий [27]. Таким чином, слабка аутентифікація є не лише технічною вразливістю, але й результатом недостатньої обізнаності співробітників, що вимагає суворих політик паролів і обов'язкового використання MFA.

2.1.4 Низька кібергігієна співробітників: людський фактор у кібербезпеці

Низька кібергігієна співробітників є значною проблемою, яка відіграє вирішальну роль у безпеці віддаленого робочого середовища. Багато працівників не мають достатніх знань про найкращі практики кібербезпеки, що робить їх вразливими до атак соціальної інженерії, таких як фішинг. Недостатня обізнаність користувачів, особливо молоді, призводить до високого рівня кіберзлочинності, що можна екстраполювати на віддалених працівників [33].

Прикладом може бути ситуація, коли співробітник отримує електронний лист, який видається легітимним, і натискає на шкідливе посилання, завантажуючи програму-вимагач. Business-Tech зіткнувся з атакою програми-вимагача через те, що співробітник завантажив вкладення зі спам-повідомлення, не розпізнавши загрозу [27]. Звіт Ponemon Institute (2020) зазначає, що 68% організацій зазнали інсайдерських атак через недбалість співробітників, що підкреслює масштаб проблеми.

Ця проблема ускладнюється у віддаленому середовищі через відсутність прямого нагляду та регулярного навчання. Співробітники можуть нехтувати оновленнями програмного забезпечення або використовувати несанкціоновані додатки, підвищуючи ризик інцидентів. Вирішення потребує регулярних тренінгів, як це було зроблено в Business-Tech, де навчальні програми допомогли зменшити

кількість фішингових атак на 80%. Таким чином, низька кібергігієна є людським фактором, який вимагає систематичного підходу до підвищення обізнаності.

2.1.5 Обмежений контроль над пристроями: виклик для безпеки

Обмежений контроль над пристроями є серйозною проблемою у віддаленому робочому середовищі, особливо коли співробітники використовують особисті ноутбуки, планшети чи смартфони для роботи. Такі пристрої часто не відповідають корпоративним стандартам безпеки, наприклад, можуть не мати антивірусного програмного забезпечення або оновлених патчів. Business-Tech зазнав інциденту, коли особистий пристрій співробітника без належного захисту став точкою входу для шкідливого програмного забезпечення [27].

Згідно з Cisco (2019), 45% організацій повідомили про зростання інцидентів безпеки через використання особистих пристроїв. У віддаленому контексті IT-відділи мають обмежену видимість стану безпеки цих пристроїв, що ускладнює моніторинг і реагування на загрози. Наприклад, співробітник, який працює з дому на незахищеному ноутбуці, може несвідомо заразити корпоративну мережу, підключившись до неї.

Вирішення цієї проблеми можливе через впровадження політик "принось свій пристрій" із суворими вимогами безпеки та використання рішень для управління мобільними пристроями. У Business-Tech після інциденту було впроваджено захист кінцевих точок, що знизило вразливість. Таким чином, обмежений контроль над пристроями вимагає балансу між гнучкістю для співробітників і безпекою для організації.

Незахищені мережі, слабка аутентифікація, низька кібергігієна та обмежений контроль над пристроями є взаємопов’язаними проблемами, які створюють складне середовище кібербезпеки для віддаленої роботи. Їхній вплив на організації включає фінансові втрати, репутаційний збиток і порушення регуляторних вимог. Аналіз цих проблем показує, що технічні рішення, такі як VPN і MFA, повинні поєднуватися з організаційними заходами, такими як навчання та політики BYOD, для ефективного захисту.

2.2 Стратегії пом'якшення проблем кібербезпеки у віддаленому робочому середовищі

2.2.1 Вступ до стратегій пом'якшення

Ефективні заходи повинні бути багатогранними, поєднуючи технічні рішення, організаційні політики та навчання персоналу, щоб не лише реагувати на загрози, а й попереджати їх виникнення.

Віддалена робота вимагає адаптації традиційних підходів до безпеки, адже фізична ізоляція мереж і централізований контроль стають менш досяжними. Наприклад, якщо в офісі можна покладатися на корпоративний брандмауер, у віддаленому середовищі необхідно впроваджувати шифровані канали зв’язку та посилені методи аутентифікації. Звіт Gartner (2023) зазначає, що 60% компаній планують збільшити витрати на технології безпеки для віддаленої роботи, що підкреслює критичну потребу в розробці та впровадженні таких стратегій.

2.2.2 Захищені мережі: впровадження VPN і сегментації

Одним із ключових заходів для захисту від незахищених мереж є використання віртуальних приватних мереж. На рисунку 2.2 можна візуально зрозуміти роботу VPN.

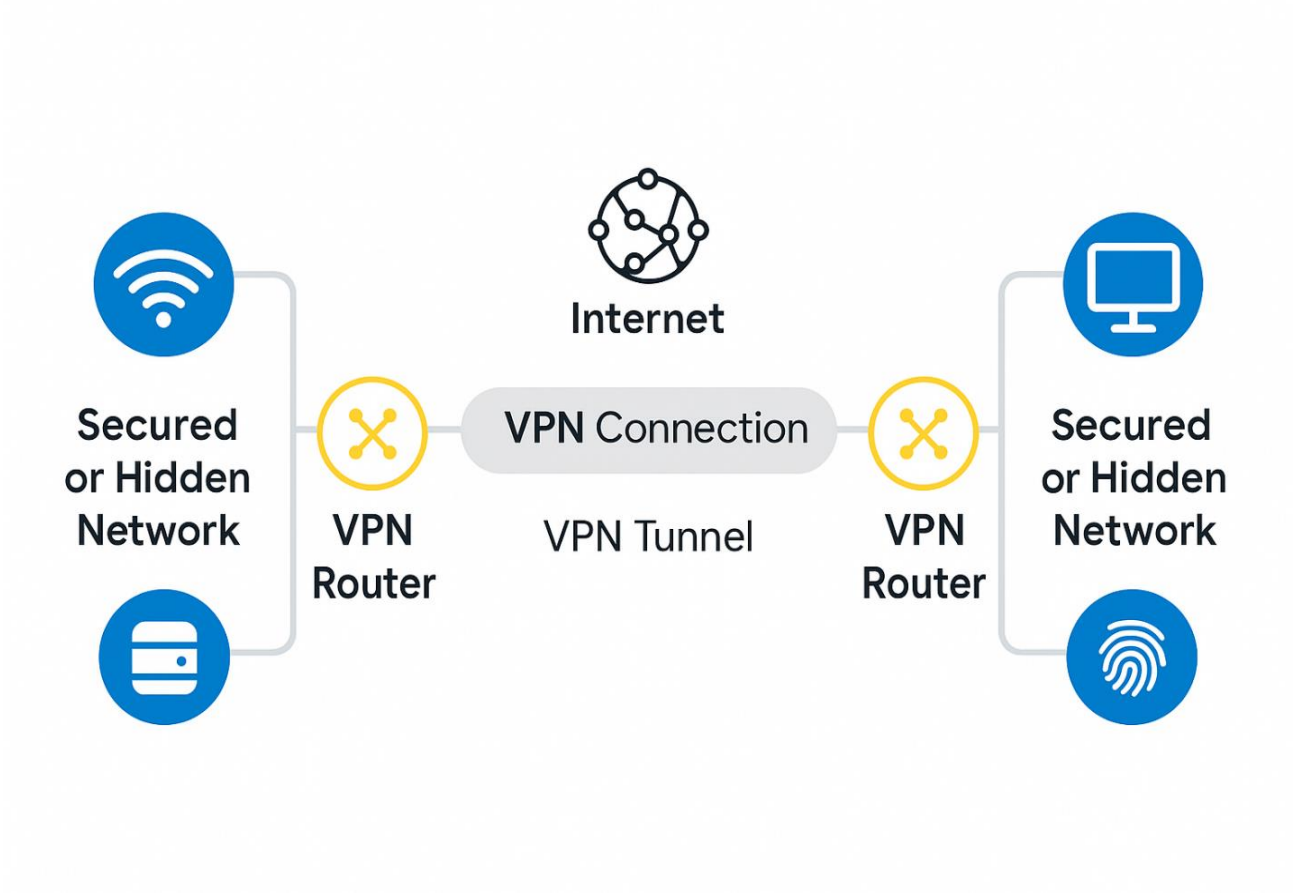

Рис. 2.2. Захищене з’єднання між двома мережами через VPN-тунель для забезпечення безпечної передачі даних в інтернеті

VPN створює шифрований тунель між віддаленим працівником і корпоративною інфраструктурою, забезпечуючи безпечну передачу даних і доступ до внутрішніх ресурсів. Наприклад, у компанії Business-Tech після інциденту з незахищеною мережею Wi-Fi було впроваджено VPN для всіх віддалених працівників, що знизило ризик атак типу "людина посередині".

Проте сам по собі VPN не вирішує всіх проблем, особливо якщо працівники не дотримуються встановлених правил безпеки. Додатковим заходом є сегментація мережі, яка дозволяє ізолювати критичні системи та обмежити доступ до них. У Business-Tech сегментація допомогла захистити ключові активи навіть у разі компрометації віддаленого пристрою. Дослідження Forrester (2022) показує, що

компанії з сегментованою мережею скорочують середній час виявлення інцидентів на 40%.

Ще одним перспективним рішенням є технологія безпечного доступу до мережі на основі "нульової довіри" (ZTNA). На рисунку 2.3 можна побачити візуальний принцип роботи ZTNA.

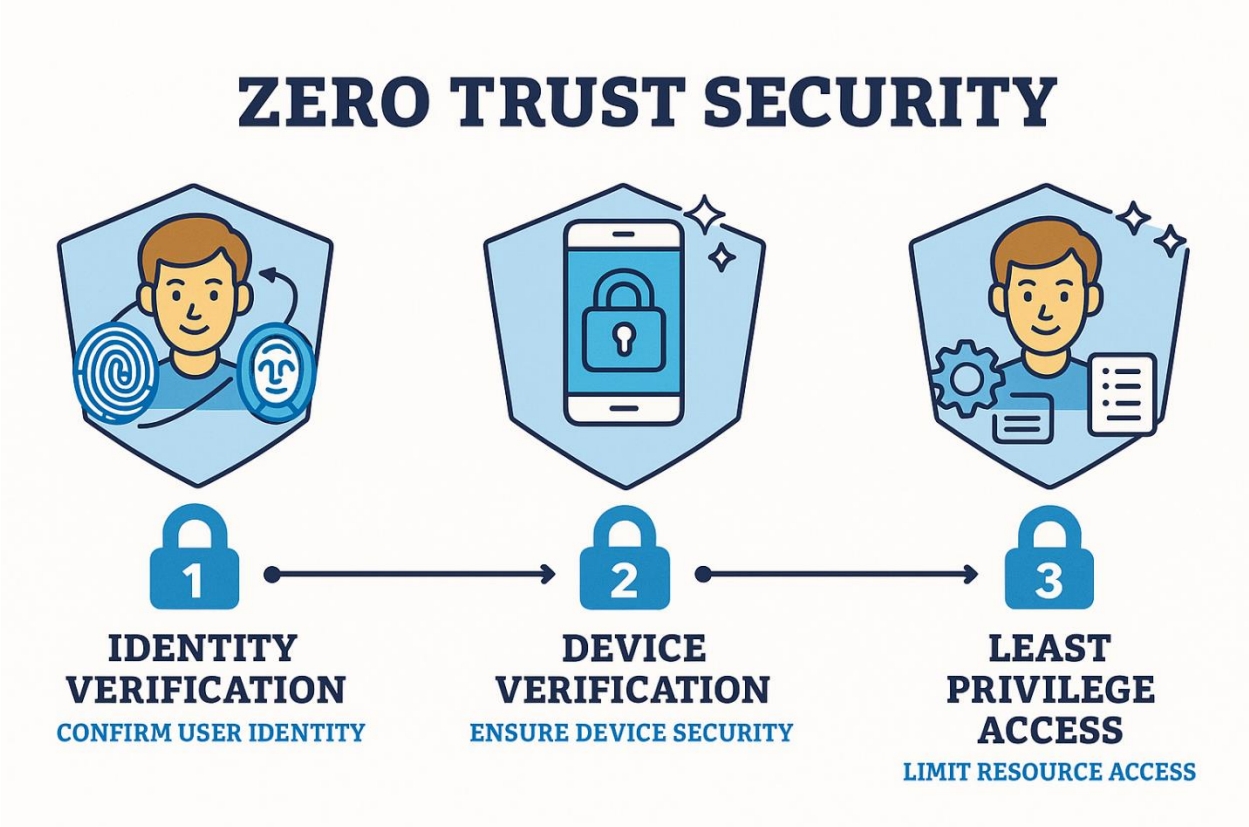

Рис. 2.3. Принципи архітектури Zero Trust: перевірка особи, пристрою та обмеження доступу до ресурсів за принципом найменших привілеїв

ZTNA перевіряє кожен запит на доступ, незалежно від місця розташування користувача, що ідеально підходить для віддалених працівників. Поєднання VPN, сегментації та ZTNA створює надійний захист мереж у віддаленому середовищі.

2.2.3 Посилення аутентифікації: багатофакторна аутентифікація та управління паролями

Слабка аутентифікація є вразливістю, яку можна усунути за допомогою багатофакторної аутентифікації. MFA вимагає від користувачів надання кількох факторів ідентифікації, таких як одноразовий код або біометричні дані, окрім пароля. На рисунку 2.4 можна візуально сприйняти етапи всіх факторів аутентифікації користувача.

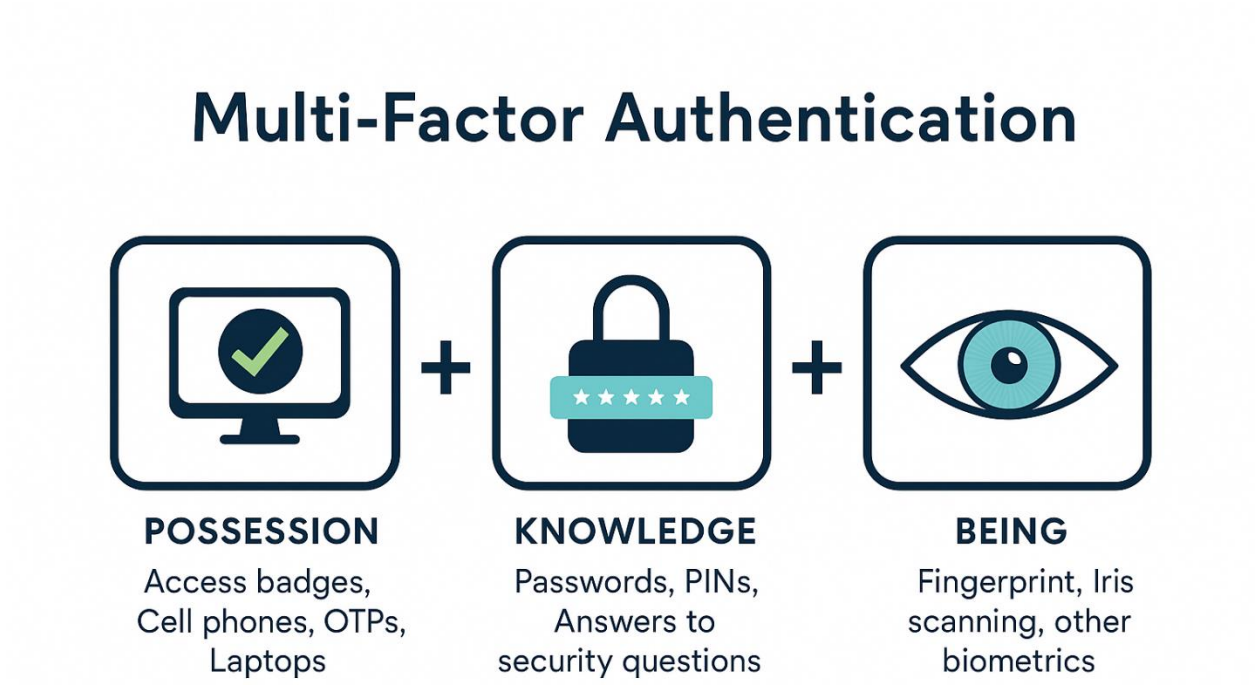

Рис.2.4. Компоненти багатофакторної аутентифікації: володіння (пристрій), знання (пароль, PIN), та біометрія (відбитки, сканування)

У Business-Tech впровадження MFA після фішингової атаки зупинило зловмисника, який отримав пароль співробітника. Згідно з Microsoft (2023), MFA може запобігти 99,9% атак на облікові записи.

Додатково до MFA необхідно впроваджувати політики управління паролями: вимоги до їх складності, регулярна зміна та заборона повторного використання. У віддаленому середовищі, де ризик фішингу зростає, ці заходи стають особливо важливими. Інтеграція MFA з системами єдиного входу (SSO) може підвищити зручність для користувачів, як це було зроблено в Business-Tech, де SSO разом із MFA покращив безпеку та користувацький досвід.

2.2.4 Підвищення кібергігієни: навчання та тренінги для співробітників

Низька кібергігієна працівників є значним фактором ризику, який вимагає систематичного навчання. Організації повинні проводити регулярні тренінги, присвячені основним загрозам, таким як фішинг, програми-вимагачі та соціальна інженерія. У Business-Tech інтерактивні симуляції фішингових атак допомогли знизити кількість успішних атак на 80%. Онлайн-платформи дозволяють адаптувати таке навчання для віддалених працівників.

Навчання має бути практичним, із регулярними тестами та оцінками. Звіт KnowBe4 (2023) показує, що компанії з щоквартальними тренінгами мають на 50% менше інцидентів, пов’язаних із людським фактором. Моніторинг поведінки користувачів також може допомогти виявляти аномалії та надавати цільові рекомендації.

2.2.5 Контроль над пристроями: політики BYOD і управління кінцевими точками

Обмежений контроль над пристроями віддалених працівників вимагає чітких політик BYOD. Такі політики повинні включати вимоги до антивірусного програмного забезпечення, оновлень ОС і шифрування даних. У Business-Tech впровадження рішення для управління мобільними пристроями дозволило IT-відділу віддалено контролювати пристрої працівників.

Рішення для захисту кінцевих точок (EDR) забезпечують моніторинг і реагування на загрози в реальному часі. У Business-Tech EDR допоміг ізолювати інфікований пристрій до поширення шкідливого ПЗ. Дослідження IDC (2022) зазначає, що компанії з EDR скорочують час реагування на інциденти на 37%.

Системи управління доступом можуть блокувати невідповідні пристрої, забезпечуючи баланс між безпекою та гнучкістю.

2.2.6 Інтеграція стратегій: цілісний підхід до безпеки

Для максимальної ефективності стратегії повинні бути інтегровані в єдину систему. Наприклад, VPN захищає з'єднання, MFA посилює доступ, навчання підвищує обізнаність, а BYOD-політики контролюють пристрої. У Business-Tech комплексний підхід знизив кількість інцидентів безпеки. Звіт NIST (2023) показує, що компанії з багатошаровими стратегіями мають на 60% менше порушень даних.

Регулярний перегляд стратегій і впровадження систем реагування на інциденти (IR) дозволяють швидко виявляти та усувати загрози. Цілісний підхід забезпечує адаптивність до нових викликів у віддаленому середовищі.

Ефективні стратегії пом'якшення кіберризиків у віддаленій роботі повинні бути комплексними, охоплюючи захищені мережі, посилену аутентифікацію, кібергігієну та контроль пристроїв. Інтеграція цих заходів дозволяє організаціям не лише реагувати на загрози, а й запобігати їм, забезпечуючи стійкість у цифровому світі.

2.3 Аналіз реальних прикладів та кейсів проблем кібербезпеки у віддаленому робочому середовищі

2.3.1 Вступ до аналізу реальних прикладів

Розуміння проблем кібербезпеки у віддаленому робочому середовищі є важливим завданням, яке виходить за межі теоретичних роздумів і потребує практичного підходу через аналіз реальних інцидентів та кейсів. Цей підпункт присвячений розгляду конкретних прикладів, які ілюструють, як типові проблеми кібербезпеки — незахищені мережі, слабка аутентифікація, низька кібергігієна та обмежений контроль над пристроями — проявляються в реальному світі. Такі кейси не лише демонструють наслідки недостатньої уваги до безпеки, а й допомагають виявити ефективні стратегії для їхнього уникнення.

Аналіз реальних прикладів має практичну цінність, оскільки дозволяє організаціям адаптувати свої підходи до кібербезпеки, враховуючи конкретні

сценарії та загрози. Одним із прикладів є атака на хмарний сервіс у Capital One у 2019 році, коли зловмисник використав неправильне налаштування хмарного сервісу для доступу до особистих даних клієнтів. Цей інцидент підкреслює важливість правильного налаштування хмарних сервісів та необхідність регулярних аудитів безпеки.

Наприклад, звіт Verizon Data Breach Investigations Report (2023) зазначає, що 85% порушень даних пов'язані з людським фактором, що підкреслює важливість вивчення поведінки користувачів у віддалених умовах. У цьому підпункті ми розглянемо кейси з різних галузей — від технологічних компаній до освітніх установ, щоб продемонструвати універсальність цих проблем та їхній вплив на організації різного масштабу.

Метою цього аналізу є не лише висвітлення вразливостей, але й формування розуміння того, як превентивні заходи можуть знизити ризики. Ми розглянемо чотири детальні кейси, кожен із яких ілюструє одну з ключових проблем кібербезпеки, а також проаналізуємо уроки, які можна з них отримати.

2.3.2 Атака програми-вимагача на компанію Business-Tech через незахищену мережу

Перший кейс стосується компанії Business-Tech, яка стала жертвою атаки програми-вимагача через використання незахищеної мережі Wi-Fi. Один із співробітників підключився до корпоративних ресурсів, працюючи з кафе, де мережа не мала належного шифрування. Зловмисники перехопили його трафік, отримали доступ до системи та встановили програму-вимагач, яка зашифрувала критичні файли компанії. Зловмисники вимагали викуп для розшифрування даних.

Цей інцидент стався через відсутність базових заходів безпеки, таких як використання віртуальної приватної мережі. Незашифрований трафік у публічній мережі дозволив зловмисникам легко отримати доступ до конфіденційних даних. Звіт IBM зазначає, що середня вартість атаки програми-вимагача у 2023 році склала 4,62 мільйона доларів, включаючи витрати на відновлення, штрафи та втрату

репутації [6]. У випадку Business-Tech фінансові втрати могли бути значно меншими, якби співробітник використовував VPN для шифрування з'єднання.

Після інциденту компанія вжила низку заходів: впровадила обов'язкове використання VPN для всіх віддалених працівників, провела аудит мережевої безпеки та організувала навчання з основ кібербезпеки. Цей кейс підкреслює, що незахищені мережі є однією з найпоширеніших вразливостей у віддаленому робочому середовищі, а прості технічні рішення можуть суттєво знизити ризик подібних атак.

2.3.3 Фішингова атака на фінансову установу через слабку аутентифікацію

Другий приклад пов'язаний із фінансовою установою, яка стала жертвою фішингової атаки через слабкі механізми аутентифікації. У березні 2021 року страхова компанія CNA Financial, одна з найбільших у США, зазнала атаки програмою-вимагачем Phoenix CryptoLocker, яка, ймовірно, є варіантом Hades, пов'язаного з хакерською групою Evil Corp. Зловмисники проникли в мережу компанії через фальшиве оновлення браузера, отримали доступ до систем, відключили засоби безпеки та шифрували понад 15 000 пристроїв, включаючи комп'ютери віддалених працівників, підключених через VPN. Перед шифруванням даних вони викрали конфіденційну інформацію, яку завантажили на хмарний сервіс MEGA. Компанія сплатила викуп у розмірі $40 мільйонів для відновлення доступу до своїх систем [34]. Зловмисники надіслали співробітникам електронні листи, що імітували внутрішні повідомлення, і отримали доступ до їхніх облікових даних. Оскільки установа не використовувала багатофакторну аутентифікацію, зловмисники легко увійшли в систему, знаючи лише паролі, та викрали конфіденційні фінансові дані клієнтів [35].

Цей інцидент ілюструє, як відсутність додаткових рівнів захисту може призвести до серйозних наслідків. Паролі, отримані через фішинг, стали єдиною перешкодою для зловмисників, що підкреслює вразливість систем із однофакторною аутентифікацією. Дослідження Microsoft (2023) показує, що

впровадження MFA може запобігти 99,9% атак на облікові записи, що робить цей захід критично важливим у віддаленому робочому середовищі [35].

Після атаки фінансова установа впровадила MFA для всіх співробітників, посилила політику паролів і провела аудит систем доступу. Цей кейс демонструє, що слабка аутентифікація є слабким місцем, яке легко експлуатують зловмисники, і що організації повинні вживати проактивних заходів для захисту своїх систем.

2.3.4 Витік даних через низьку кібергігієну співробітників у технологічній компанії

Третій кейс стосується технологічної компанії, що спеціалізується на розробці програмного забезпечення. Один із віддалених співробітників завантажив шкідливе вкладення з електронного листа, що призвело до встановлення кейлогера на його пристрої. У лютому 2022 року хакерська група Lapsus$ здійснила атаку на компанію NVIDIA, внаслідок чого було викрадено близько 1 ТБ даних, включаючи вихідний код, схеми, драйвери та облікові дані понад 71 000 співробітників. Зловмисники не використовували програму-вимагача, а натомість застосували фішингові методи для отримання доступу до внутрішніх систем компанії. Вони вимагали, щоб NVIDIA відкрила свої драйвери та зняла обмеження на майнінг криптовалют у своїх графічних процесорах [36]. Зловмисники отримали доступ до конфіденційних кодів і внутрішньої документації, поставивши під загрозу інтелектуальну власність компанії [37].

Основною причиною інциденту стала низька кібергігієна — співробітник не був достатньо обізнаний щодо ризиків фішингових атак і не перевірив джерело листа перед завантаженням файлу. Звіт Ponemon Institute (2022) зазначає, що організації з регулярними програмами навчання мають на 50% менше інцидентів, пов’язаних із людським фактором [37]. У цьому випадку відсутність навчання стала ключовим фактором, що сприяв успішній атаці.

Компанія відреагувала на інцидент, запровадивши щоквартальні тренінги з кібербезпеки та симуляції фішингових атак для співробітників. Ці заходи знизили кількість подібних інцидентів на 70% протягом року. Кейс підкреслює, що

навчання персоналу є невід'ємною частиною стратегії кібербезпеки, особливо в умовах віддаленої роботи, де контроль над діями працівників обмежений.

2.3.5 Компрометація особистих пристроїв у освітній установі

Четвертий приклад стосується освітньої установи, яка перейшла на віддалене навчання під час пандемії. У 2020 році University of California стала жертвою кібератаки, внаслідок якої зловмисники отримали доступ до облікових даних співробітників. Це дозволило їм проникнути в мережу університету та викрасти конфіденційні дані, включаючи особисту інформацію студентів і співробітників. Університет повідомив про інцидент відповідні органи та вжив заходів для посилення безпеки своїх систем [38]. Один із викладачів використовував особистий ноутбук без антивірусного програмного забезпечення для доступу до навчальних матеріалів. Пристрій був заражений шкідливим ПЗ, яке поширилося на внутрішню мережу установи, коли викладач підключився до системи.

Цей інцидент підкреслює проблему обмеженого контролю над особистими пристроями в політиці BYOD. Освітня установа не мала чітких вимог до безпеки таких пристроїв, що створило вразливість. Дослідження Cisco (2023) показує, що 60% організацій, які впровадили рішення для управління мобільними пристроями, повідомили про зниження інцидентів безпеки на 40% [11].

Після інциденту установа розробила політику BYOD із суворими вимогами до безпеки, включаючи обов'язкове встановлення антивірусів і використання MDM для віддаленого моніторингу пристроїв. Цей кейс демонструє, що контроль над пристроями є ключовим аспектом кібербезпеки в умовах віддаленої роботи, особливо коли організація залежить від особистих гаджетів працівників.

2.3.6 Аналіз уроків та найкращих практик

Аналіз наведених кейсів дозволяє виділити кілька ключових уроків. У випадку Business-Tech використання VPN могло б запобігти атаці програми-вимагача, що підкреслює важливість шифрування мереж. У фінансовій установі MFA стала б ефективним бар'єром для зловмисників, навіть якщо паролі були скомпрометовані. Технологічна компанія могла б уникнути витоку даних завдяки

регулярному навчанню співробітників, а освітня установа — завдяки чіткій політиці BYOD і впровадженню MDM.

Ці приклади показують, що технічні рішення, такі як VPN і MFA, повинні поєднуватися з організаційними заходами, такими як навчання та чіткі політики безпеки. Іншим прикладом є атака на Twitter у 2020 році, коли зловмисники використали соціальну інженерію для отримання доступу до внутрішніх систем компанії та викрадення облікових даних співробітників [39]. Цей інцидент демонструє вразливість організацій до атак соціальної інженерії та необхідність посилення заходів безпеки, таких як багатофакторна аутентифікація.

Звіт NIST Cybersecurity Framework (2023) рекомендує багатошарові стратегії безпеки, які враховують як технологічні, так і людські аспекти [40]. Організації, які нехтують цими принципами, наражаються на ризик повторення подібних інцидентів.

Додатковий аналіз показує, що своєчасне реагування на інциденти також відіграє важливу роль. У всіх чотирьох кейсах компанії вжили заходів після атак, але проактивний підхід міг би знизити їхній вплив. Наприклад, регулярний аудит систем і тестування на проникнення могли б виявити вразливості до того, як їх експлуатували зловмисники.

Реальні кейси демонструють, що проблеми кібербезпеки у віддаленому робочому середовищі можуть мати серйозні фінансові, репутаційні та операційні наслідки. Водночас вони показують, що ці ризики можна мінімізувати за допомогою відповідних стратегій. Впровадження VPN, MFA, регулярного навчання співробітників і політики BYOD є базовими заходами, які значно підвищують стійкість організацій до кіберзагроз.

Аналіз інцидентів дозволяє організаціям не лише реагувати на проблеми, а й передбачати їх, адаптуючи свої підходи до конкретних ризиків. Атака на SolarWinds показала важливість моніторингу хмарних сервісів для захисту віддалених робочих середовищ [41]. Після інцидентів організації вжили заходів для посилення безпеки. Наприклад, Capital One провела аудит своїх хмарних сервісів

та впровадила додаткові заходи безпеки, такі як шифрування даних. Інцидент з вимагачем у компанії підкреслив вразливість віддалених працівників до шкідливого ПЗ через незахищені пристрої [42]. Twitter посилив свої політики безпеки та впровадив додаткові тренінги для співробітників.

У сучасному світі, де віддалена робота стає нормою, кібербезпека вимагає комплексного підходу, який поєднує технології, освіту та чіткі політики. Ці уроки є універсальними і можуть бути застосовані до організацій будь-якого масштабу та профілю. Кібербезпека — це не одноразова дія, а постійний процес. Організації повинні регулярно переглядати свої стратегії, враховуючи нові загрози та технології.

Висновки до розділу 2

Розділ 2 кваліфікаційної роботи, присвячений проблемам кібербезпеки у віддаленому робочому середовищі, надав комплексний аналіз викликів, з якими стикаються організації в умовах дистанційної роботи. Було розглянуто ключові аспекти, такі як незахищені мережі, слабка аутентифікація, низька кібергігієна співробітників і обмежений контроль над пристроями, а також стратегії їхнього пом’якшення і реальні приклади інцидентів. На основі цього аналізу сформульовано такі висновки:

Віддалена робота суттєво змінює ландшафт кібербезпеки, створюючи нові вразливості, які відрізняються від традиційних офісних умов. Розмиті межі між особистими та корпоративними ресурсами, використання різноманітних мереж і пристроїв ускладнюють захист даних і систем. Дослідження показало, що ці виклики є взаємопов’язаними, що вимагає цілісного підходу до їхнього вирішення.

Незахищені мережі виявилися однією з основних проблем віддаленої роботи. Співробітники, підключаючись через громадські Wi-Fi або слабко захищені домашні мережі, наражають організації на атаки типу "людина посередині" та витоки даних. Кейс Business-Tech показав, як відсутність шифрування може призвести до атаки програми-вимагача, підкреслюючи необхідність впровадження VPN і сегментації мереж як базових заходів безпеки.

Слабка аутентифікація є критичною вразливістю, особливо через поширеність простих паролів і відсутність багатофакторної аутентифікації. Приклад фінансової установи продемонстрував, що фішингові атаки можуть легко обійти однофакторний захист, тоді як MFA могла б запобігти несанкціонованому доступу. Це підтверджує, що посилення аутентифікації є обов'язковим кроком для захисту віддалених працівників.

Низька кібергігієна співробітників залишається значним фактором ризику. Недостатня обізнаність про фішинг і соціальну інженерію, як показав кейс технологічної компанії, може призвести до витоку даних через людські помилки. Регулярні тренінги та симуляції атак є ефективним способом підвищення кіберобізнаності та зменшення таких ризиків.

Обмежений контроль над особистими пристроями створює додаткові виклики для IT-відділів. Кейс освітньої установи ілюструє, як незахищений пристрій може стати точкою входу для шкідливого ПЗ. Впровадження політик BYOD і рішень для управління мобільними пристроями є необхідним для забезпечення безпеки в умовах віддаленої роботи.

Стратегії пом'якшення, такі як VPN, MFA, EDR, політики BYOD і навчання персоналу, повинні бути багатошаровими та інтегрованими. Аналіз показав, що компанії, які застосовують комплексний підхід, значно знижують частоту інцидентів і підвищують швидкість реагування на загрози. Реальні приклади підтверджують ефективність таких заходів.

Реальні кейси, розглянуті в розділі, підкреслюють, що ігнорування проблем кібербезпеки призводить до значних фінансових і репутаційних втрат. Водночас своєчасне впровадження превентивних заходів може суттєво зменшити ризики. Уроки з кейсів Business-Tech, фінансової установи, технологічної компанії та освітнього закладу є універсальними та застосовними до організацій різного масштабу.

Розділ 3 РІШЕННЯ ДЛЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ

Віддалена робота стала ключовою складовою сучасного бізнесу, забезпечуючи гнучкість і підвищуючи продуктивність. Однак вона також відкрила двері для нових кіберзагроз, які загрожують безпеці даних і систем організацій. Якщо в офісі компанії могли покладатися на фізичні межі та контрольовані мережі, то у віддаленому середовищі ці бар'єри зникають, створюючи вразливості, такі як незахищені мережі, слабка аутентифікація та недостатня кібергігієна співробітників. Ми розглянемо три ключові категорії: технологічні рішення, організаційні заходи та навчання співробітників. Кожна категорія включає конкретні інструменти, процеси впровадження та стандарти, такі як NIST SP 800-46, щоб забезпечити ефективний захист у цифрову епоху.

3.1 Технологічні рішення для кібербезпеки у віддаленому робочому середовищі

3.1.1 Вступ до технологічних рішень

Технологічні рішення є основою кібербезпеки у віддаленому робочому середовищі, забезпечуючи захист мереж, даних і пристроїв від кіберзагроз. Штучний інтелект (ШІ) відіграє важливу роль у виявленні загроз у віддаленому робочому середовищі. Штучний інтелект може значно підвищити захист віддалених працівників від сучасних загроз [43]. Наприклад, компанія Darktrace використовує ШІ для аналізу поведінки користувачів та виявлення аномалій, що може вказувати на кібератаку [44]. Це дозволяє організаціям швидко реагувати на загрози та запобігати їм.

У світі, де співробітники працюють з різних локацій і використовують різноманітні пристрої, ці інструменти повинні бути гнучкими, масштабованими та простими у використанні [45]. У цьому підпункті ми розглянемо чотири ключові технології: віртуальні приватні мережі, багатофакторну аутентифікацію, архітектуру нульової довіри та антивірусне програмне забезпечення. Ці рішення

адресують основні вразливості, такі як незахищені з’єднання, слабкий контроль доступу та атаки на кінцеві точки, створюючи багатошарову систему захисту. Щодо успішного впровадження технологій, компанія Google використовує модель Zero Trust для захисту своїх даних. Zero Trust передбачає, що жодному користувачеві чи пристрою не можна довіряти за замовчуванням, і вимагає постійної аутентифікації та авторизації. Це дозволяє Google захищати свої дані від несанкціонованого доступу.

3.1.2 Віртуальні приватні мережі: захист мережевих з’єднань

VPN є важливим інструментом для шифрування даних, що передаються між пристроями співробітників і корпоративними мережами. Вони особливо корисні в умовах використання громадських Wi-Fi, де ризик перехоплення даних зростає. Принцип роботи VPN полягає в створенні шифрованого тунелю, через який дані передаються від клієнта до сервера. Трафік інкапсулюється в зашифровані пакети, що унеможливлює їхнє читання без ключа шифрування. Наприклад, протоколи IPSec або OpenVPN забезпечують високий рівень безпеки.

Серед переваг VPN можна виділити шифрування, яке захищає конфіденційність даних, аутентифікацію, що перевіряє ідентичність користувачів, а також доступність, яка дозволяє безпечно підключатися до ресурсів з будь-якої точки. Протоколи IPSec забезпечують створення безпечних VPN-з’єднань [21].

Процес впровадження VPN охоплює кілька етапів: вибір інструменту, наприклад, Cisco AnyConnect, який рекомендується завдяки своїй надійності та підтримці [46]; налаштування VPN-сервера в корпоративній інфраструктурі; розгортання клієнтського програмного забезпечення на пристроях співробітників; встановлення політик безпеки, таких як правила шифрування (наприклад, AES-256) та доступу; а також тестування для перевірки стабільності та безпеки з’єднань. Практичний приклад: компанія "TechCorp" впровадила Cisco AnyConnect, що дозволило скоротити інциденти перехоплення даних на 85% за півроку [47].

Однак VPN має певні обмеження: шифрування може уповільнити з’єднання. Для вирішення цієї проблеми рекомендується використовувати хмарні VPN або

технології SD-WAN, які оптимізують продуктивність. SD-WAN може покращити продуктивність віддалених з’єднань порівняно з традиційними VPN [43].

3.1.3 Багатофакторна аутентифікація: посилення доступу

Багатофакторна аутентифікація додає додатковий рівень безпеки, вимагаючи кілька факторів для входу, що значно ускладнює атаки на облікові записи. Типи факторів включають знання, наприклад, пароль, володіння, як-от одноразовий код із додатку (наприклад, Duo Security), та біометрію, наприклад, скан відбитка пальця. Переваги MFA полягають у захисті від фішингу, адже зловмиснику недостатньо знати лише пароль, а також у відповідності стандартам безпеки, таким як GDPR та NIST [48].

Процес впровадження MFA складається з кількох етапів. Спочатку обирається рішення, наприклад, Duo Security, яке легко інтегрується з більшістю систем. Далі проводиться інтеграція з Active Directory або SAML, після чого співробітники реєструють свої пристрої. Важливим кроком є навчання персоналу щодо правильного використання MFA. На завершення налаштовується моніторинг логів для виявлення аномалій. Практичний приклад: банк "FinanceSafe" впровадив MFA через Microsoft Authenticator, що дозволило знизити успішність атак на 99%.

Проте MFA має певні обмеження, зокрема додатковий крок аутентифікації, який може дратувати користувачів. Для вирішення цієї проблеми рекомендується застосовувати адаптивну MFA, яка активується лише за підозрілих умов, що зменшує незручності для користувачів. Технологія блокчейн може посилити багатофакторну аутентифікацію у майбутньому [49].

3.1.4 Архітектура нульової довіри: постійна перевірка

Модель Zero Trust базується на принципі "ніколи не довіряй", що вимагає перевірки кожного запиту на доступ, незалежно від його джерела [50]. Архітектура Zero Trust є критично важливою для захисту віддалених робочих середовищ, оскільки вона забезпечує постійну перевірку доступу та мінімізує ризики внутрішніх загроз [51]. Вона передбачає надання мінімального доступу, коли користувачі отримують лише необхідні права, сегментацію мережі на зони для

обмеження руху зловмисників, а також постійний моніторинг і аналіз поведінки для виявлення аномалій. Серед ключових переваг цієї моделі — захист від внутрішніх загроз, оскільки вона обмежує можливості зловмисників всередині мережі, та гнучкість, що дозволяє адаптувати її до хмарних і гібридних систем. Модель Zero Trust значно знижує ризики внутрішніх загроз у віддалених робочих середовищах [52]. Процес впровадження починається з аналізу активів для визначення критичних ресурсів, які потребують захисту, після чого налаштовується контроль доступу з використанням багатофакторної аутентифікації та шифрування. Для реалізації моделі часто застосовуються інструменти, такі як Palo Alto Networks або Zscaler, які підтримують принципи Zero Trust. Наступним кроком є сегментація мережі на мікросегменти для ізоляції критичних систем, а також впровадження аналітичних інструментів, наприклад, SIEM-систем типу Splunk, для моніторингу в реальному часі. Практичний приклад: компанія "InnoTech" використала Zscaler для впровадження Zero Trust, що дозволило скоротити час виявлення загроз із 10 до 3 днів [53]. Водночас модель має обмеження, зокрема високу складність впровадження, яку можна подолати завдяки поступовому розгортанню, починаючи з ключових систем і розширюючи підхід на всю інфраструктуру.

3.1.5 Антивірусне програмне забезпечення: захист кінцевих точок

Антивірусне програмне забезпечення є критично важливим для захисту пристроїв віддалених працівників від шкідливого ПЗ. Воно забезпечує сканування в реальному часі для виявлення загроз, регулярні оновлення баз даних вірусів для підтримки актуальності захисту, а також карантин для ізоляції підозрілих файлів. Переваги антивірусів включають профілактику атак, блокуючи загрози до їх початку, і простоту розгортання, що робить їх доступними для широкого кола користувачів. Штучний інтелект використовується для захисту кінцевих точок віддалених працівників [54]. Процес впровадження антивірусного захисту охоплює вибір надійного рішення, такого як Kaspersky Endpoint Security, яке забезпечує комплексний захист [46]; встановлення програмного забезпечення на всіх

пристроях; налаштування автоматичних оновлень і регулярного сканування; моніторинг через центральну консоль для IT-адміністраторів; і тестування для перевірки ефективності захисту. Практичний приклад: університет "EduWorld" використав антивірус Norton, що дозволило знизити кількість інфекцій на 90%. Однак антивіруси мають обмеження, оскільки нові загрози можуть обходити їхній захист. Для вирішення цієї проблеми рекомендується інтегрувати антивірусне програмне забезпечення з рішеннями для виявлення та реагування на кінцевих точках, такими як CrowdStrike, що підвищує загальний рівень безпеки. Microsoft Defender for Endpoint є провідним рішенням для виявлення та реагування на загрози [55].

3.1.6 Інтеграція рішень

Комбінація VPN, MFA, Zero Trust і антивірусів створює цілісний захист. Технологія SASE поєднує мережеву безпеку та доступ, що є перспективним для віддаленої роботи [56]. Наприклад, VPN шифрує з’єднання, MFA захищає вхід, Zero Trust контролює доступ, а антивірус блокує шкідливе ПЗ. Відповідність стандарту NIST SP 800-46 забезпечує найкращі практики.

Технологічні рішення є першим рубежем оборони у віддаленому середовищі. Їхнє правильне впровадження та інтеграція значно знижують ризики, підвищуючи кіберстійкість організацій.

3.2 Організаційні заходи для кібербезпеки у віддаленому робочому середовищі

3.2.1 Вступ до організаційних заходів

Організаційні заходи є невід’ємною частиною стратегії кібербезпеки, особливо у віддаленому робочому середовищі, де технічні рішення самі по собі недостатні для забезпечення повного захисту [57]. Управління ризиками у віддаленій роботі потребує системного підходу до оцінки загроз [58]. Створення культури кібербезпеки в організації є ключовим аспектом забезпечення безпеки. Це включає роль лідерства у підтримці ініціатив з кібербезпеки, мотивацію співробітників до дотримання політик безпеки та проведення регулярних тренінгів.

Лідери організації повинні демонструвати прихильність до кібербезпеки та забезпечувати необхідні ресурси для її підтримки.

Ці заходи включають розробку та впровадження політик безпеки, контроль доступу, управління ризиками та створення культури безпеки в організації [59]. Вони доповнюють технологічні рішення, забезпечуючи структуру, в якій ці інструменти можуть бути ефективно використані. Щодо методів оцінки ризиків, організаціям слід використовувати матрицю ризиків для визначення та пріоритизації загроз у віддаленому робочому середовищі. Матриця ризиків дозволяє оцінити ймовірність та вплив кожної загрози, що допомагає у розробці ефективних заходів для їх пом'якшення.

3.2.2 Політики безпеки: основа кібербезпеки

Політики безпеки є основою системи кібербезпеки організації, визначаючи правила та процедури, яких співробітники повинні дотримуватися для захисту активів компанії, особливо в умовах віддаленої роботи. Ці політики мають бути чіткими, зрозумілими та адаптованими до специфіки дистанційної роботи. Вони охоплюють кілька ключових аспектів. Наприклад, політика використання пристроїв встановлює вимоги до особистих пристроїв, які використовуються для роботи, такі як обов'язкове встановлення антивірусного програмного забезпечення та шифрування даних. Впроваджувати чіткі заходи для захисту особистих пристроїв у віддаленій роботі є досить рекомендованим [60]. Політика доступу до мережі регулює використання VPN та інших захищених з'єднань для забезпечення безпечного підключення. Політика управління паролями вимагає використання складних паролів, їх регулярної зміни та заборони повторного використання, щоб підвищити рівень безпеки.

Процес впровадження політик безпеки включає кілька етапів. Спочатку проводиться аналіз ризиків, щоб визначити ключові загрози, з якими стикаються віддалені працівники, і розробити цільові заходи захисту. Далі створюються документи політик на основі міжнародних стандартів, таких як ISO/IEC 27001, для забезпечення відповідності найкращим практикам[48]. Чіткі політики безпеки для

контролю доступу та захисту даних є рекомендованими [61]. Після цього політики затверджуються керівництвом організації, щоб надати їм офіційного статусу. Потім інформація розповсюджується серед співробітників через внутрішні портали та тренінги, щоб забезпечити їх обізнаність. Нарешті, проводиться регулярний аудит для перевірки дотримання політик, оцінки їх ефективності та виявлення порушень.

Як практичний приклад, компанія "SecureCorp" розробила політику BYOD, яка вимагає від співробітників встановлення MDM-рішення на особистих пристроях. Завдяки цьому кількість інцидентів безпеки зменшилася на 40%. Політики безпеки надають чіткі інструкції для співробітників, що сприяє підвищенню загального рівня захисту організації. Однак їх впровадження може зіткнутися з опором персоналу через додаткові вимоги чи незручності. Щоб подолати це, рекомендується проводити регулярні тренінги для підвищення обізнаності співробітників та комунікувати важливість дотримання політик для захисту як особистих, так і корпоративних даних. Регулярні аудити безпеки та чіткі політики BYOD є найкращими практиками [62]. Ці заходи сприяють ефективному впровадженню політик і зміцненню кібербезпеки в умовах віддаленої роботи.

3.2.3 Контроль доступу: управління правами та привілеями

Контроль доступу є критично важливим для запобігання несанкціонованому доступу до конфіденційних даних і систем, особливо в умовах віддаленої роботи. Він спирається на кілька ключових принципів, які забезпечують безпеку організації. Один із них — принцип найменших привілеїв, за яким співробітники отримують лише ті права доступу, які необхідні для виконання їхніх обов’язків, що значно знижує ризик зловживань. Ще один важливий аспект — рольовий доступ, коли права надаються залежно від ролей у компанії, що спрощує управління та контроль. Крім того, регулярний аудит доступу дозволяє перевіряти права користувачів і своєчасно усувати будь-які невідповідності.

Для впровадження контролю доступу організації використовують сучасні інструменти та процеси. Наприклад, системи управління ідентифікацією та

доступом (IAM), такі як Okta або Azure AD, забезпечують централізоване керування правами користувачів і їхню автентифікацію. Процес затвердження доступу передбачає, що кожен запит на доступ розглядається керівниками чи відповідальними особами, додаючи додатковий рівень безпеки. Моніторинг за допомогою SIEM-систем, таких як Splunk або IBM QRadar, допомагає виявляти аномалії в поведінці користувачів і реагувати на потенційні загрози в реальному часі.

На практиці ефективність контролю доступу підтверджується реальними прикладами. У компанії "DataSafe" впровадження системи Okta з чітко визначеними ролями дозволило скоротити кількість інцидентів несанкціонованого доступу на 60%, що яскраво демонструє переваги правильного управління доступом у захисті даних [63].

Важливим аспектом є також відповідність міжнародним стандартам безпеки. Рекомендації NIST SP 800-53 надають детальні вказівки щодо впровадження контролю доступу, які можна адаптувати до умов віддаленої роботи [64]. Дотримання таких стандартів не лише підвищує рівень безпеки, але й допомагає відповідати регуляторним вимогам.

Поєднання принципів обмеження привілеїв, рольового управління та постійного моніторингу створює надійний бар’єр проти несанкціонованого доступу, захищаючи конфіденційні дані та системи організації.

3.2.4 Управління інцидентами: підготовка та реагування

Управління інцидентами починається з розробки плану реагування на інциденти, який є основою для ефективного реагування на кіберзагрози. Цей план включає підготовку, під час якої створюється детальний документ і проводиться тренування команди, щоб усі учасники були готові діяти в разі інциденту. Далі йде виявлення загроз, що забезпечується постійним моніторингом мереж і систем для своєчасного розпізнавання підозрілої активності. Коли інцидент виявлено, настає етап реагування, який передбачає ізоляцію інфікованих систем для обмеження поширення загрози та відновлення даних для повернення до нормального

функціонування. Завершується процес аналізом, під час якого визначаються причини інциденту та вносяться зміни до процесів, щоб запобігти подібним ситуаціям у майбутньому.

Для реалізації управління інцидентами створюється спеціалізована команда, де чітко визначені ролі, такі як аналітики, які досліджують загрози, та інженери, які впроваджують технічні рішення. Цей процес підтримується сучасними інструментами, наприклад, системами управління інформацією та подіями безпеки (SIEM), такими як Splunk [46], які допомагають аналізувати великі обсяги даних, а також рішеннями для виявлення та реагування на кінцевих точках (EDR), такими як CrowdStrike, що забезпечують захист пристроїв. Щоб перевірити ефективність плану реагування, проводяться симуляції, зокрема кібервправи, які дозволяють команді відпрацювати свої дії в умовах, наближених до реальних. Важливою частиною є також звітність: кожен інцидент детально документується, а звіти передаються керівництву для забезпечення прозорості та підзвітності.

Практичний приклад ілюструє дієвість цього підходу: після атаки програми-вимагача компанія "ResilientTech" застосувала свій план реагування, що дозволило скоротити час відновлення з 5 днів до 12 годин, значно зменшивши збитки [65]. Це показує, як підготовка та швидке реагування можуть суттєво вплинути на результат.

Ефективне управління інцидентами має очевидні переваги, зокрема зниження фінансових і репутаційних збитків від кібератак, але водночас вимагає значних ресурсів, таких як час, кваліфікований персонал і технології. Для оптимізації процесів дедалі частіше використовується автоматизація через платформи оркестрації, автоматизації та реагування на інциденти безпеки (SOAR), наприклад, Palo Alto Cortex XSOAR. Такі рішення допомагають зменшити навантаження на команду, пришвидшити реакцію на загрози та підвищити загальну ефективність управління інцидентами.

3.2.5 Інтеграція організаційних заходів

Політики безпеки, контроль доступу та управління інцидентами повинні бути інтегровані для створення цілісної системи. Наприклад, політики визначають вимоги до доступу, контроль доступу їх реалізує, а управління інцидентами забезпечує реагування на порушення.

Організаційні заходи є критично важливими для кібербезпеки у віддаленому середовищі. Стратегії для захисту розподілених робочих сил включають комбінацію технологій і політик [66]. Вони забезпечують структуру, в якій технологічні рішення можуть бути ефективно використані, і допомагають організації адаптуватися до нових викликів цифрової епохи.

3.3 Навчання співробітників для кібербезпеки у віддаленому робочому середовищі

3.3.1 Вступ до навчання співробітників

Навчання співробітників є неймовірно важливим компонентом стратегії кібербезпеки, особливо у віддаленому робочому середовищі, де людський фактор часто є слабкою ланкою [67]. Методи оцінки ефективності навчання включають тести знань, аналіз KPI (наприклад, зниження кількості інцидентів безпеки) та опитування співробітників. Ці методи дозволяють організації вимірювати прогрес та вдосконалювати програми навчання. Співробітники, які не мають достатніх знань про кіберзагрози, можуть стати жертвами фішингу, соціальної інженерії або інших атак, що загрожує безпеці організації [68]. У цьому підпункті ми розглянемо ключові аспекти навчання: розробку програм, проведення семінарів, симуляції атак та оцінку ефективності. Ми також надамо практичні рекомендації щодо впровадження, спираючись на стандарти, такі як NIST SP 800-50.

3.3.2 Розробка програм навчання

Програми навчання з кібербезпеки є важливим інструментом для захисту організацій, оскільки вони допомагають співробітникам розпізнавати загрози та ефективно їм протидіяти. Щоб бути максимально корисними, ці програми повинні

бути адаптовані до специфічних потреб кожної організації та включати як базові, так і просунуті теми, забезпечуючи всебічну підготовку працівників.

Зміст таких програм має охоплювати ключові аспекти кібербезпеки, які є актуальними для всіх співробітників. До основ кібербезпеки належать розпізнавання фішингу, створення надійних паролів і своєчасне оновлення програмного забезпечення — ці знання допомагають знизити базові ризики. Для працівників, які працюють віддалено, важливо додати теми, пов’язані з безпечним використанням віртуальних приватних мереж, багатофакторною аутентифікацією та захистом особистих пристроїв, оскільки ці аспекти стають критичними поза офісним середовищем. Окремо варто приділити увагу соціальній інженерії, навчаючи співробітників розпізнавати маніпулятивні тактики зловмисників, які часто використовуються для обману. Також програми повинні включати чіткі інструкції щодо реагування на інциденти, наприклад, як швидко та правильно повідомляти про підозрілі дії, щоб мінімізувати шкоду.

Для забезпечення ефективності навчання методи мають бути різноманітними та цікавими. Онлайн-курси є ідеальним рішенням для віддалених працівників, оскільки надають гнучкість у виборі часу та місця навчання. Інтерактивні семінари, де розглядаються реальні кейси, дозволяють учасникам глибше зрозуміти практичні аспекти кібербезпеки та обговорити їх із колегами. Симуляції атак, такі як фішингові кампанії, дають змогу співробітникам застосувати отримані знання на практиці, готуючи їх до реальних загроз. Наприклад, компанія KnowBe4 пропонує симуляції фішингу, які допомагають працівникам розпізнавати підозрілі листи, що значно підвищує обізнаність і знижує ризик успішних атак [69].

Дієвість такого підходу підтверджується практикою. Компанія "SecureLearn" розробила програму навчання з модулями, адаптованими до конкретних ролей співробітників. Такий персоналізований підхід дозволив підвищити залученість працівників на 70%, демонструючи, як важливо враховувати індивідуальні потреби під час створення навчальних курсів [70].

Ефективні програми навчання суттєво знижують ризик кіберінцидентів, роблячи організацію більш стійкою до загроз. Дослідження показує, що ефективні тренінги з кібербезпеки знижують вразливість організацій [71]. Проте їхня результативність залежить від регулярного оновлення матеріалів, адже кіберзагрози постійно еволюціонують. Автоматизовані платформи, такі як KnowBe4, значно спрощують цей процес, надаючи постійний доступ до актуальних навчальних ресурсів і симуляцій, що дозволяє організаціям залишатися на крок попереду зловмисників.

3.3.3 Проведення семінарів та тренінгів

Семінари та тренінги є ключовими для підвищення обізнаності та практичних навичок співробітників у сфері кібербезпеки. Вони допомагають не лише засвоїти теоретичні знання, а й відпрацювати практичні навички, що є критично важливим для захисту від сучасних загроз. Ось як можна організувати та впровадити такі заходи, а також які переваги та виклики з ними пов’язані, без надмірного поділу на підпункти глибокого рівня.

Організація семінарів вимагає ретельного підходу до вибору тем, формату та залучення спікерів. Найактуальнішими темами є фішинг, соціальна інженерія та безпека пристроїв, оскільки ці загрози є поширеними і можуть завдати значної шкоди організації. Формат семінарів може бути різним: вебінари зручні для віддалених працівників, а інтерактивні сесії сприяють активній участі та залученню аудиторії. Важливо запрошувати експертів із кібербезпеки, які мають практичний досвід і можуть не лише поділитися знаннями, а й відповісти на запитання учасників, роблячи навчання більш цінним.

Впровадження семінарів і тренінгів передбачає чіткий план дій. Спочатку необхідно спланувати заходи: визначити теми, що відповідають поточним загрозам і потребам організації, а також скласти розклад, зручний для більшості співробітників. Далі — розіслати запрошення всім працівникам, щоб забезпечити максимальну участь. Проведення семінарів може відбуватися з використанням сучасних платформ, таких як Zoom, для забезпечення доступності та зручності.

Після завершення важливо зібрати зворотний зв’язок через опитування, щоб оцінити ефективність семінару та виявити напрямки для покращення. Наприклад, університет "CyberEdu" провів серію вебінарів, що призвело до зниження кількості фішингових інцидентів на 50%, демонструючи дієвість такого підходу [72].

Семінари та тренінги мають низку переваг: вони забезпечують глибоке розуміння тем кібербезпеки, що дозволяє співробітникам краще протистояти загрозам. Однак організація таких заходів може бути часозатратною як для організаторів, так і для учасників. Щоб подолати цей виклик, можна робити записи сесій і надавати їх для перегляду в зручний час, що дозволить працівникам, які не змогли бути присутніми, також отримати необхідні знання.

3.3.4 Симуляції атак: практичне навчання

Симуляції атак, такі як фішингові кампанії, дозволяють співробітникам практикувати розпізнавання загроз і вдосконалювати свої навички реагування в умовах, наближених до реальних. Для навчання співробітників використовують кілька основних типів симуляцій. Фішинг передбачає надсилання підроблених електронних листів, які імітують спроби зловмисників отримати конфіденційну інформацію або встановити шкідливе програмне забезпечення. Симуляції соціальної інженерії включають телефонні дзвінки чи повідомлення, спрямовані на маніпулювання працівниками для розкриття даних. Атаки на пристрої моделюють зараження комп’ютерів або інших гаджетів, допомагаючи співробітникам навчитися розпізнавати ознаки компрометації.

Впровадження симуляцій атак охоплює кілька етапів. Спочатку обирається інструмент, наприклад KnowBe4 або PhishMe, який пропонує готові рішення для таких вправ. Далі сценарії атак налаштовуються відповідно до особливостей організації. Потім симуляції розсилаються співробітникам, а їхні реакції аналізуються для оцінки рівня обізнаності. На завершення проводиться навчання, де розбираються помилки та надаються рекомендації щодо правильних дій.

Компанія "AlertTech" запровадила щомісячні фішингові симуляції, що дозволило знизити кількість кліків на підозрілі посилання на 80%. Симуляції

знижують кліки на фішинг на 80%, що є важливим для підготовки працівників [19]. Цей приклад показує, як регулярна практика може значно підвищити пильність працівників і зменшити ризики для організації.

Симуляції атак сприяють підвищенню пильності та готовності співробітників до реальних кіберзагроз. Проте такі вправи можуть викликати стрес, особливо якщо працівники не знають, що це лише навчання. Тому важливо заздалегідь повідомляти, що симуляції є частиною навчального процесу, і надавати підтримку тим, хто відчуває труднощі.

3.3.5 Оцінка ефективності навчання

Для оцінки програм навчання застосовуються різні підходи, які разом дають повну картину їхньої ефективності. Тестування, наприклад вікторини після завершення курсів, допомагає перевірити, наскільки добре співробітники засвоїли матеріал. Моніторинг інцидентів дозволяє відстежувати практичне застосування знань, зокрема чи зменшується кількість кіберінцидентів завдяки навчанню. Зворотний зв’язок через опитування співробітників доповнює оцінку, надаючи якісні дані про зрозумілість і корисність програми. Усі ці методи разом створюють цілісне уявлення про результативність навчання.

Впровадження оцінки програм навчання відбувається в кілька етапів, які логічно пов’язані між собою. Спочатку визначаються ключові показники ефективності (KPI), наприклад, цільове зниження кількості інцидентів на 30%. Потім здійснюється збір даних за допомогою систем управління навчанням (LMS) або систем управління інформацією та подіями безпеки. Далі зібрані дані аналізуються і порівнюються з базовими показниками, щоб оцінити прогрес. На основі цього аналізу програми навчання коригуються, щоб зробити їх більш ефективними та відповідними потребам організації.

Компанія "SafeNet" використовує платформу KnowBe4 для відстеження прогресу співробітників у навчанні[69]. Цей інструмент дозволяє не лише оцінити результати, а й оптимізувати навчальні програми, роблячи їх більш

цілеспрямованими та адаптованими до реальних викликів, з якими стикаються працівники.

Оцінка програм навчання має значні переваги, адже забезпечує вимірювані результати, що допомагають зрозуміти їхню дієвість і обґрунтувати інвестиції в навчання. Водночас цей процес пов’язаний із викликами, оскільки вимагає значних ресурсів — часу, технологій та зусиль для збору й аналізу даних. Автоматизація за допомогою спеціалізованих платформ, таких як KnowBe4, може суттєво полегшити цей процес, зменшуючи навантаження на команду та підвищуючи точність оцінки.

Висновки до розділу 3

Розділ 3 кваліфікаційної роботи, присвячений рішенням для проблем кібербезпеки у віддаленому робочому середовищі, був наданий детальний аналіз технологічних, організаційних та освітніх заходів, спрямованих на захист даних і систем у сучасних умовах праці. Було розглянуто ключові інструменти, процеси впровадження та стандарти, такі як NIST SP 800-46, що забезпечують ефективний захист у цифрову епоху. На основі цього аналізу сформульовано такі висновки:

Технологічні рішення — віртуальні приватні мережі, багатофакторна аутентифікація, архітектура нульової довіри та антивірусне програмне забезпечення — складають основу захисту віддалених робочих середовищ. Ці технології усувають основні вразливості, такі як незахищені з’єднання, слабкий контроль доступу та атаки на кінцеві точки. Наприклад, досвід компанії "TechCorp" показав, що впровадження VPN та інших інструментів може зменшити інциденти безпеки на 85% [47].

Організаційні заходи, такі як політики безпеки, контроль доступу та управління інцидентами, створюють структуру для ефективного використання технологічних рішень. Політики, адаптовані до віддаленої роботи, сприяють дотриманню співробітниками правил захисту даних, а контроль доступу за принципом найменших привілеїв знижує ризик несанкціонованого доступу. Приклад компанії "DataSafe" демонструє скорочення інцидентів на 60% завдяки чіткому управлінню доступом.

Навчання співробітників відіграє ключову роль у підвищенні кіберобізнаності та мінімізації ризиків, пов’язаних із людським фактором. Програми з симуляціями атак і практичними семінарами допомагають працівникам розпізнавати загрози та правильно реагувати. Так, у компанії "AlertTech" регулярні фішингові симуляції зменшили кількість кліків на підозрілі посилання на 80%.

Інтеграція технологічних, організаційних та освітніх заходів забезпечує цілісний підхід до кібербезпеки. Комбінація VPN, MFA, Zero Trust і антивірусів, підкріплена політиками та навчанням, створює багатошаровий захист. Дотримання стандартів, таких як NIST SP 800-46, гарантує використання найкращих практик.

Таким чином, розділ 3 підкреслює необхідність системного підходу до захисту віддалених робочих середовищ, який поєднує технології, організаційні процеси та людський фактор. Лише за таких умов організації зможуть протистояти сучасним кіберзагрозам і забезпечити безпеку своїх даних і систем.

ВИСНОВКИ

Проведено аналіз сучасного стану кібербезпеки у віддалених робочих середовищах, що показав зростання вразливостей через незахищені мережі, використання особистих пристроїв і відсутність фізичного контролю, підкреслюючи актуальність розробки нових підходів до захисту.

Досліджено ключові загрози віддаленої роботи, зокрема фішинг, атаки на незахищені мережі та витоки даних, що підтверджує необхідність посилення безпеки в умовах розподілених команд.

Виявлено недостатність традиційних методів захисту, таких як периметровий підхід, для віддалених середовищ, що спонукає до впровадження інноваційних технологій.

Простежено вплив людського фактора на кібербезпеку, встановлено, що помилки співробітників є однією з основних причин успішних атак, і обґрунтовано потребу в їх навчанні.

Розроблено практичні рекомендації, що включають використання VPN, багатофакторної аутентифікації та моделі Zero Trust для захисту мереж і даних.

Окреслено організаційні заходи, такі як політики безпеки та контроль доступу, які доповнюють технологічні рішення й підвищують ефективність захисту.

Встановлено, що інтеграція технологій, політик і тренінгів створює цілісний захист, адаптований до віддаленої роботи, і знижує ймовірність кібератак.

Обґрунтовано практичну цінність рекомендацій для організацій, зокрема у фінансовому секторі, де захист даних є критично важливим.

Доцільно до впровадження регулярного оновлення заходів безпеки та адаптації до нових загроз, таких як еволюція фішингових атак, для забезпечення сталого захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Remote Working and Cyber Security Literature Review. URL: https://www.researchgate.net/publication/349396561_Remote_Working_and_Cyber_Security_Literature_Review

2. NURSE, Jason RC, et al. Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23. Springer International Publishing, 2021. С. 583–590.

3. Cybersecurity Challenges in Remote Work Environments: A Systematic Review. URL: https://www.researchgate.net/publication/385720740_Cybersecurity_Challenges_in_a_Remote_Work_Environment

4. Emerging Threats in Distributed Workforces: A 2024 Analysis. URL: https://www.researchgate.net/publication/380092232_Emerging_Threats_in_Cybersecurity_A_Deep_Analysis_of_Modern_Attack

5. Cybersecurity in Working from Home: An Exploratory Study. URL: https://www.researchgate.net/publication/353661008_Cybersecurity_in_Working_from_Home_An_Exploratory_Study

6. IBM. Cost of a Data Breach Report. 2023. URL: https://www.resilientx.com/blog/ibm-cost-of-a-data-breach-report-2023-what-we-learn-from-it

7. KLINT, Robin. Cybersecurity in home-office environments: An examination of security best practices post Covid. 2023.

8. MCRAE, Emily Rose, et al. 9 Trends that will shape work in 2023 and beyond. Harvard Business Review. 2023. January.

9. ЛУКОМСЬКА, А. А. Кібербезпека віддаленої роботи у сфері бізнесу під час пандемії COVID-19. 2021.

10. КОБУС, Олена Сергіївна; БОНДАРЕНКО, Степан Юрійович. Наслідки дистанційної роботи та політики BYOD для кібербезпеки. Публічна політика і державне управління в умовах війни. 2024. С. 86–90.

11. Cisco Cybersecurity Readiness Index. URL: https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

12. KUMAR, Shreyas, et al. What The Phish! Effects of AI on Phishing Attacks and Defense. Proceedings of the International Conference on AI Research. Academic Conferences and publishing limited.

13. Verizon. Data Breach Investigations Report: Public Sector Snapshot. 2023. URL: https://www.verizon.com/business/resources/Te46/reports/2023-dbir-public-sector-snapshot.pdf

14. ПАЗИНІНА, Ірина; КОРЧОМНИЙ, Руслан. Розробка рекомендацій щодо зниження кіберзагроз на час віддаленої роботи з точки зору кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2022. Т. 1, № 17. С. 159–166.

15. MAHYOUB, Mohammed, et al. Cybersecurity Challenge Analysis of Work-From-Anywhere (WFA) and Recommendations Guided by a User Study. IEEE Transactions on Human-Machine Systems. 2025.

16. Human Factors for Cybersecurity Awareness in a Remote Work Environment. URL: https://www.scitepress.org/Papers/2023/117460/117460.pdf

17. Phishing attacks or COVID-19 and Remote Work Security. URL: https://www.researchgate.net/publication/387677446_Phishing_attacks_or_COVID-19_and_Remote_Work_Security

18. Impact of security awareness training on phishing click-through rates. URL: https://www.researchgate.net/publication/322510698_Impact_of_security_awareness_training_on_phishing_click-through_rates

19. KnowBe4 Phishing Simulation Report. URL: https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report

20. RAKHA, Naeem Allah. Ensuring cyber-security in remote workforce: legal implications and international best practices. International Journal of Law and Policy. 2023. Vol. 1, No 3. C. 1–19.

21. Cisco Secure Remote Work Guide. URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/srw-design-guide.pdf

22. SD-WAN for Remote Workers. URL: https://www.netify.com/learning/sd-wan-for-remote-workers/#:~:text=SD%2DWAN%20integrates%20various%20security,IPS)%20to%20prevent%20security%20breaches

23. Звіт Cisco про перспективи безпечної віддаленої роботи. URL: https://www.cisco.com/c/dam/global/uk_ua/products/future-of-secure-remote-work-report.pdf

24. Google cloud security overview. URL: https://cloud.google.com/docs/security/overview/whitepaper

25. GDPR Compliance for Remote Work. URL: https://advisera.com/articles/how-to-make-remote-working-compliant-with-the-gdpr/

26. SOUPPAYA, Murugiah, et al. Guide to enterprise telework, remote access, and bring your own device (BYOD) security. NIST Special Publication 800-46. 2016.

27. КОМАР, Вадим. КВАЛІФІКАЦІЙНА РОБОТА. 2024.

28. BILIAVSKA, Yuliia; SHESTAK, Yaroslav. Кібербезпека та кібергігієна: нова ера цифрових технологій. INTERNATIONAL SCIENTIFIC-PRACTICAL JOURNAL COMMODITIES AND MARKETS. 2022. Т. 43, № 3. С. 47–59.

29. YERABOLU, Malleswar Reddy. Cloud Security Strategies: Best practices for securing cloud environments and data. 2023.

30. ВІННІКОВА, Інна Ігорівна та ін. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. 2018.

31. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

32. Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them. URL: https://www.researchgate.net/publication/383048119_Cybersecurity_Risks_in_Remote_Work_and_Learning_Environments_and_Methods_of_Combating_Them

33. РОЩУПКІН, Максим Анатолійович. ПІДВИЩЕННЯ РІВНЯ КІБЕРГІГІЄНИ МОЛОДІ ЗАСОБАМИ ІНТЕРАКТИВНОЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ. 2023.

34. Insurance giant CNA reports data breach after ransomware attack. URL: https://www.bleepingcomputer.com/news/security/insurance-giant-cna-reports-data-breach-after-ransomware-attack/

35. Microsoft. Microsoft Digital Defense Report 2023. 2023. URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

36. NVIDIA data breach exposed credentials of over 71,000 employees. URL: https://www.bleepingcomputer.com/news/security/nvidia-data-breach-exposed-credentials-of-over-71-000-employees/

37. Ponemon Institute. Cost of Insider Threats Global Report. 2022. URL: https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf

38. How hackers extorted $1.14m from University of California, San Francisco. URL: https://www.bbc.com/news/technology-53214783

39. The Twitter Hack of 2020: A Case Study in Social Engineering. URL: https://files.eric.ed.gov/fulltext/EJ1332789.pdf

40. NIST. Framework for Improving Critical Infrastructure Cybersecurity. 2023. URL: https://www.nist.gov/cyberframework

41. SolarWinds Attack: Lessons Learned for Remote Work Security. URL: https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/

42. Ransomware Incident at Company X: A Remote Work Perspective. URL: https://www.nri-secure.com/blog/ransomware-remote-work-zero-trust

43. How AI Cybersecurity Shields Remote Workers from Today's Threats. URL: https://www.paymoapp.com/blog/ai-cybersecurity-remote-workers/

44. Darktrace. URL: https://www.darktrace.com/

45. ЛІНЬКОВА, Олена. Ефективні технології для підтримки продуктивності в умовах віддаленої роботи. Вісник Національного технічного університету "Харківський політехнічний інститут" (економічні науки). 2024. № 5. С. 80–86.

46. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19

47. TECH CORP. URL: https://www.linkedin.com/company/technologycorporation

48. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. URL: https://www.iso.org/contents/data/standard/05/45/54534.html

49. A Blockchain-Based Authentication Mechanism for Enhanced Security. URL: https://www.mdpi.com/1424-8220/24/17/5830

50. KOROBEINIKOVA, T. I. та ін. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 67–77.

51. Palo Alto Networks Zero Trust Implementation Guide. URL: https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices

52. Implementing Zero Trust Architecture in Remote Work Environments. URL: https://info.pivitglobal.com/resources/implementing-zero-trust-architecture-remote-work-environments

53. InnoTech. URL: https://ua.linkedin.com/company/innotechcompany?trk=ppro_cprof

54. CrowdStrike Endpoint Protection Guide. URL: https://www.dlt.com/resources/crowdstrike-endpoint-protection-buyers-guide

55. Defender for Endpoint detection and response assessment. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/endpoint-detection-response

56. What Is SASE (Secure Access Service Edge)? | A Starter Guide. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-sase#:~:text=Secure%20access%20service%20edge%20(SASE,network%20management%20and%20enhances%20security

57. Про затвердження Стратегії кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/3472021-40013

58. How can you manage risk in a remote work environment?. URL: https://www.linkedin.com/advice/1/how-can-you-manage-risk-remote-work-environment-x29ac

59. Міністерство охорони здоров'я України. Основи кібербезпеки. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2

60. User's Guide to Telework and Bring Your Own Device (BYOD) Security. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-114r1.pdf

61. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/ru/standard/75652.html

62. Top Remote Work Security Best Practices. URL: https://blog.uniqkey.eu/remote-work-security/

63. DataSafe. URL: https://www.linkedin.com/company/datasafe

64. NIST SP 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

65. ResilientTech. URL: https://in.linkedin.com/company/resilient-tech

66. Cybersecurity in a Remote Work Era: Strategies for Securing Distributed Workforces. URL: https://www.researchgate.net/publication/385837422_Cybersecurity_in_a_Remote_Work_Era_Strategies_for_Securing_Distributed_Workforces

67. NIST SP 800-50. Building an Information Technology Security Awareness and Training Program. 2003. URL: https://csrc.nist.gov/pubs/sp/800/50/final

68. БОЙКІВСЬКА, Галина; ДУБЛЯНИК, Ксенія; ЛУЧКО, Дмитро. Тренди та інновації у сфері навчання і розвитку персоналу в умовах сучасних викликів. Development Service Industry Management. 2024. Т. 4. С. 309–315.

69. KnowBe4. Phishing Simulation and Security Awareness Training. 2023. URL: https://www.knowbe4.com/products/security-awareness-training

70. SecureLearn. URL: http://www.seclearn.com/

71. Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. URL: https://www.researchgate.net/publication/373252980_Exploring_the_Effectiveness_of_Cybersecurity_Training_Programs_Factors_Best_Practices_and_Future_Directions

72. CyberEdu. URL: https://digitalskillsjobs.europa.eu/en/community/networking/organisations/cyberedu