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: “ МЕТОДИ УПРАВЛІННЯ БЕЗПЕКОЮ ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ”

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

_____ Владислав Комірний
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Владислав КОМІРНИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Діана ПРИМАЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

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
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Комірному Владиславу Валерійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи управління безпекою віддаленого доступу до корпоративних інформаційних систем”,
керівник кваліфікаційної роботи ПРИМАЧЕНКО Діана.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “29” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *методи управління безпекою,корпоративні інформаційні системи, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1 Дослідити теоретичні основи організації та забезпечення безпеки віддаленого доступу.
   4.2 Проаналізувати існуючі механізми та стан безпеки віддаленого доступу.
   4.3. Розробити та впровадити методи підвищення безпеки віддаленого доступу.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних основ організації та забезпечення безпеки віддаленого доступу	08.04.2026	
4.	Аналіз існуючих механізмів та стану безпеки віддаленого доступу	15.04.2026	
5.	Розробка та впровадження методів підвищення безпеки віддаленого доступу	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	05.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Владислав КОМІРНИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(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 Комірний В.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи управління безпекою віддаленого доступу до корпоративних інформаційних систем"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КОМІРНИЙ Владислав у кваліфікаційній роботі дослідив теоретичні основи організації та забезпечення безпеки віддаленого доступу, проаналізував існуючі механізми та стан безпеки віддаленого доступу, розробив та впровадив методи підвищення безпеки віддаленого доступу, розробив практичні рекомендації за темою дослідження.

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

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

Керівник кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Комірний В.В. 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 Комірного Владислава
на тему “Методи управління безпекою віддаленого доступу до корпоративних інформаційних систем”

Актуальність. Однією з найважливіших складових забезпечення інформаційної безпеки сучасних організацій є захист віддаленого доступу до корпоративних інформаційних систем. Активне впровадження дистанційної роботи, хмарних сервісів та мобільних технологій значно розширило можливості доступу користувачів до корпоративних ресурсів, водночас підвищивши рівень кіберзагроз та ризиків несанкціонованого доступу.

Віддалений доступ є одним із найбільш вразливих елементів корпоративної IT-інфраструктури, оскільки може стати об'єктом атак зловмисників, спрямованих на компрометацію облікових записів, перехоплення даних, поширення шкідливого програмного забезпечення та порушення конфіденційності інформації. У зв’язку з цим особливої актуальності набуває розроблення та впровадження ефективних методів управління безпекою віддаленого доступу, які забезпечують надійну автентифікацію користувачів, контроль доступу до інформаційних ресурсів, моніторинг подій безпеки та своєчасне реагування на інциденти.

Позитивні сторони.

1. У роботі досліджено теоретичні основи забезпечення безпеки віддаленого доступу до корпоративних інформаційних систем та визначено основні загрози, вразливості й механізми їх нейтралізації.
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, сформульовано обґрунтовані висновки. Основні положення роботи представлено у вигляді таблиць і рисунків.
3. Автор опрацював значну кількість наукових джерел, зокрема сучасні зарубіжні публікації та матеріали з питань інформаційної безпеки, управління ризиками й впливу людського фактору.
4. За результатами дослідження запропоновано рекомендації щодо підвищення рівня безпеки віддаленого доступу шляхом удосконалення механізмів автентифікації, контролю доступу, моніторингу мережевої активності та управління ризиками інформаційної безпеки.

Недоліки.

Доцільно було б приділити більше уваги практичному аналізу сучасних програмних та апаратних засобів забезпечення безпеки віддаленого доступу, а також порівнянню ефективності різних методів автентифікації та контролю доступу в корпоративних інформаційних системах.

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

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

Рецензент:

_____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню впливу людського фактору на ефективність системи управління інформаційною безпекою. Робота складається зі вступу, трьох розділів, що містять 8 рисунків, 9 таблиць, висновків і списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 82 аркуші, з яких 5 аркушів займають список використаних джерел.

Метою роботи є дослідження методів управління безпекою віддаленого доступу до корпоративних інформаційних систем та розроблення рекомендацій щодо підвищення рівня захисту інформаційних ресурсів від несанкціонованого доступу і кіберзагроз.

Об'єктом дослідження є процес забезпечення безпеки віддаленого доступу до корпоративних інформаційних систем.

Предмет дослідження – методи, механізми та засоби управління безпекою віддаленого доступу, зокрема технології автентифікації, контролю доступу, моніторингу подій безпеки та управління ризиками в корпоративних інформаційних системах.

Методи дослідження. Для вирішення означеного наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, оцінювання ризиків, експертної оцінки, а також системний підхід до управління інформаційною безпекою.

Як результат у роботі досліджено теоретичні основи організації та забезпечення безпеки віддаленого доступу, проаналізовано існуючі механізми та стан безпеки віддаленого доступу, розроблено та впроваджено методи підвищення безпеки віддаленого доступу, розроблено практичні рекомендації за темою дослідження.

Галузь застосування. Отримані результати можуть бути використані для підвищення рівня безпеки віддаленого доступу до корпоративних інформаційних систем, удосконалення механізмів автентифікації та контролю доступу, впровадження сучасних засобів захисту інформації, а також для

розроблення заходів щодо мінімізації ризиків несанкціонованого доступу до корпоративних ресурсів.

Ключові слова: БЕЗПЕКА ВІДДАЛЕНОГО ДОСТУПУ, КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ, КІБЕРБЕЗПЕКА, VPN, ZERO TRUST, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ (MFA), КОНТРОЛЬ ДОСТУПУ, МОНІТОРИНГ БЕЗПЕКИ, УПРАВЛІННЯ РИЗИКАМИ, ЗАХИСТ ДАНИХ.

ABSTRACT

The qualification work is devoted to the study of the impact of the human factor on the effectiveness of the information security management system. The work consists of an introduction, three chapters containing 8 figures, 9 tables, conclusions and the list of references containing 44 items. The total volume of the work is 82 pages, of which 5 pages is occupied by the list of references.

The purpose of the study is to investigate methods for managing the security of remote access to corporate information systems and to develop recommendations for enhancing the protection of information resources against unauthorised access and cyber threats.

The object the study is the process of ensuring the security of remote access to corporate information systems.

The subject of the study is the methods, mechanisms and means of managing remote access security, in particular technologies for authentication, access control, security event monitoring and risk management in corporate information systems.

Research methods. In order to solve the above-mentioned scientific task, this study employs methods of analysis and synthesis, comparison, classification, risk assessment, expert evaluation, as well as a systematic approach to information security management.

As a result, this paper investigates the theoretical foundations of organising and ensuring remote access security, analyses existing mechanisms and the current state of remote access security, develops and implements methods to enhance remote access security, and formulates practical recommendations on the research topic.

Field of application. The results obtained can be used to enhance the security of remote access to corporate information systems, improve authentication and access control mechanisms, implement modern information security measures, and develop strategies to minimise the risks of unauthorised access to corporate resources.

Keywords: REMOTE ACCESS SECURITY, CORPORATE INFORMATION SYSTEMS, CYBERSECURITY, VPN, ZERO TRUST, MULTIFACTOR

AUTHENTICATION (MFA), ACCESS CONTROL, SECURITY MONITORING, RISK MANAGEMENT, DATA PROTECTION.

ЗМІСТ

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційних технологій, поширення дистанційної роботи, хмарних сервісів та мобільних пристроїв зумовлюють постійне зростання потреби у безпечному віддаленому доступі до корпоративних інформаційних систем. Водночас розширення можливостей віддаленої взаємодії створює додаткові ризики несанкціонованого доступу, витоку конфіденційної інформації, компрометації облікових записів та реалізації інших кіберзагроз. Сучасні корпоративні інформаційні системи потребують впровадження ефективних методів управління безпекою віддаленого доступу, які забезпечують надійну автентифікацію користувачів, контроль їхніх прав доступу, захист каналів передавання даних та своєчасне виявлення підозрілої активності. Незважаючи на постійне вдосконалення засобів захисту, кіберзлочинці активно використовують нові методи атак, що вимагає регулярного вдосконалення механізмів безпеки.

У зв’язку з цим особливої актуальності набуває дослідження методів управління безпекою віддаленого доступу до корпоративних інформаційних систем, аналіз сучасних загроз та розроблення рекомендацій щодо підвищення рівня захищеності корпоративних інформаційних ресурсів.

Мета роботи полягає у аналізі сучасних методів управління безпекою віддаленого доступу до корпоративних інформаційних систем, оцінюванні їх ефективності та розробленні рекомендацій щодо підвищення рівня захищеності корпоративних інформаційних ресурсів.

Об’єкт дослідження **–** корпоративні інформаційні системи, що забезпечують віддалений доступ користувачів до інформаційних ресурсів підприємства.

Предмет дослідження – організаційні та технічні методи управління безпекою віддаленого доступу до корпоративних інформаційних систем.

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

1. Дослідити теоретичні основи організації та забезпечення безпеки

віддаленого доступу.

4.2 Проаналізувати існуючі механізми та стан безпеки віддаленого доступу.

4.3. Розробити та впровадити методи підвищення безпеки віддаленого доступу.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі використано методи аналізу та синтезу для дослідження сучасних підходів до забезпечення безпеки віддаленого доступу, методи порівняння та класифікації для оцінювання існуючих технологій і засобів захисту, методи оцінювання ризиків для визначення рівня загроз інформаційній безпеці, а також системний підхід до управління безпекою віддаленого доступу в корпоративних інформаційних системах. Також, застосовано методи узагальнення та експертного оцінювання для формування рекомендацій щодо підвищення рівня захищеності корпоративних інформаційних ресурсів.

Практичне значення одержаних результатів. Практичне значення роботи полягає в можливості використання отриманих результатів для вдосконалення процесів управління безпекою віддаленого доступу до корпоративних інформаційних систем. Запропоновані рекомендації можуть бути використані для підвищення рівня захисту інформаційних ресурсів, удосконалення механізмів автентифікації та контролю доступу, зменшення ризиків несанкціонованого доступу, а також підвищення ефективності функціонування корпоративної системи інформаційної безпеки в умовах сучасних кіберзагроз.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІДДАЛЕНОГО ДОСТУПУ

1.1 Поняття віддаленого доступу та його роль у сучасних корпоративних інформаційних системах

Віддалений доступ став невід'ємним елементом функціонування сучасних корпоративних інформаційних систем. Трансформація бізнес-процесів, поширення хмарних сервісів, збільшення кількості розподілених команд, а також потреба у забезпеченні безперервності діяльності підприємств сприяли суттєвому зростанню ролі механізмів дистанційного доступу до інформаційних ресурсів. Сучасні організації дедалі частіше функціонують у середовищі, де працівники, партнери та клієнти взаємодіють із корпоративними системами незалежно від географічного розташування, використовуючи глобальні мережі передачі даних. У зв'язку з цим питання організації та забезпечення безпеки віддаленого доступу набуває особливого значення, оскільки саме через віддалені канали взаємодії реалізується значна частина операцій з обробки, передавання та зберігання інформації [1].

Поняття віддаленого доступу розглядається як сукупність програмно-технічних засобів, протоколів і механізмів, що забезпечують можливість користувачу отримувати доступ до інформаційних ресурсів, програмного забезпечення, серверів, баз даних та інших компонентів інформаційної системи без фізичної присутності у локальній мережі організації. Основною характеристикою віддаленого доступу є використання мережевих технологій для встановлення зв'язку між віддаленим користувачем і корпоративною інфраструктурою. Такий доступ може здійснюватися через мережу Інтернет, приватні мережі, мобільні канали зв'язку або спеціалізовані телекомунікаційні системи.

Віддалений доступ охоплює не лише підключення до окремого комп'ютера або сервера, а й повноцінну інтеграцію користувача у корпоративне

інформаційне середовище. Це передбачає можливість роботи з внутрішніми сервісами організації, електронним документообігом, системами управління ресурсами підприємства, корпоративними базами даних, аналітичними платформами та іншими критично важливими інформаційними ресурсами. Віддалений доступ перетворився з допоміжного інструменту на стратегічний компонент цифрової інфраструктури підприємства.

Розвиток концепції віддаленого доступу безпосередньо пов’язаний із еволюцією комп’ютерних мереж та інформаційних технологій. На ранніх етапах розвитку обчислювальних систем віддалена взаємодія реалізовувалася через термінальний доступ до центральних обчислювальних машин. Користувачі підключалися до серверів за допомогою телефонних ліній та модемів, використовуючи текстові інтерфейси та базові протоколи передавання даних. З розвитком локальних мереж та Інтернету можливості дистанційної роботи значно розширилися, а поява технологій VPN, хмарних обчислень, веборієнтованих сервісів і мобільних платформ забезпечила формування сучасних моделей віддаленої взаємодії [2].

Суттєвий вплив на розвиток віддаленого доступу мала концепція цифрової трансформації бізнесу. Сучасні підприємства орієнтуються на забезпечення мобільності персоналу, оперативного доступу до корпоративних ресурсів та оптимізації бізнес-процесів. У результаті організації впроваджують розподілені інформаційні системи, які дозволяють працівникам виконувати професійні обов’язки незалежно від місця перебування. Особливої актуальності ця тенденція набула після глобального поширення дистанційних форм роботи, що стало каталізатором масового впровадження засобів віддаленого доступу.

У корпоративних інформаційних системах віддалений доступ виконує низку важливих функцій. Насамперед він забезпечує безперервність діяльності організації, дозволяючи співробітникам підтримувати робочі процеси навіть за відсутності фізичного доступу до офісної інфраструктури. Це особливо важливо для міжнародних компаній, організацій із розгалуженою структурою, а також

підприємств, діяльність яких потребує цілодобового доступу до інформаційних ресурсів.

Рис.1.1 Основні компоненти системи віддаленого доступу в корпоративній інформаційній системі

Віддалений доступ сприяє підвищенню ефективності управління підприємством. Керівники та спеціалісти отримують можливість оперативно взаємодіяти з корпоративними системами, аналізувати дані, здійснювати контроль за виконанням завдань та приймати управлінські рішення в режимі реального часу. Завдяки цьому підвищується швидкість обробки інформації та скорочується час реагування на зміни зовнішнього середовища [3].

Важливим аспектом використання віддаленого доступу є підтримка гнучких моделей організації праці. Сучасні концепції управління персоналом передбачають активне використання дистанційної та гібридної роботи, що дозволяє оптимізувати витрати підприємства, розширити можливості залучення висококваліфікованих спеціалістів та підвищити рівень задоволеності працівників. У цьому сенсі засоби віддаленого доступу стають основою реалізації концепції цифрового робочого місця.

Не менш важливою є роль віддаленого доступу у забезпеченні взаємодії між структурними підрозділами організації та зовнішніми контрагентами. Корпоративні інформаційні системи дедалі частіше функціонують як інтегровані платформи, що об’єднують різні бізнес-процеси та забезпечують обмін інформацією між учасниками економічної діяльності. Віддалений доступ дозволяє організувати безпечну взаємодію між філіями підприємства, постачальниками, клієнтами та партнерами, забезпечуючи оперативність і надійність інформаційного обміну.

Сучасні технології віддаленого доступу базуються на використанні різноманітних мережевих протоколів та архітектурних рішень. Одним із найбільш поширених механізмів є використання віртуальних приватних мереж, які забезпечують створення захищених каналів зв’язку через загальнодоступні мережі. Технологія VPN дозволяє шифрувати передані дані та забезпечувати конфіденційність інформації під час взаємодії віддалених користувачів із корпоративною мережею.

Іншим важливим напрямом розвитку віддаленого доступу є використання хмарних технологій. Хмарні сервіси дозволяють організаціям надавати доступ до інформаційних ресурсів через вебінтерфейси та спеціалізовані платформи, що функціонують у середовищі Інтернет. Такий підхід забезпечує масштабованість, гнучкість та зниження витрат на підтримку локальної інфраструктури. Одночасно з цим зростає значення механізмів автентифікації, контролю доступу та захисту даних у хмарному середовищі.

Поширення мобільних пристроїв також суттєво вплинуло на розвиток систем віддаленого доступу. Смартфони, планшети та портативні комп’ютери стали повноцінними інструментами роботи з корпоративними ресурсами. Це призвело до формування концепції BYOD, відповідно до якої працівники використовують власні пристрої для доступу до інформаційних систем підприємства. З одного боку, така модель підвищує мобільність та зручність роботи, а з іншого — створює додаткові ризики інформаційній безпеці [4].

Таблиця 1.1

Порівняльна характеристика основних технологій віддаленого доступу

ТЕХНОЛОГІЯ	ОСНОВНИЙ ПРИНЦИП РОБОТИ	ПЕРЕВАГИ	НЕДОЛІКИ	РІВЕНЬ БЕЗПЕКИ
VPN	Створення захищеного тунелю через мережу Інтернет	Високий рівень захисту, підтримка корпоративних мереж	Потребує налаштування та адміністрування	Високий
RDP	Віддалене підключення до робочого столу комп'ютера	Повний доступ до робочого середовища	Вразливість до атак при неправильному налаштуванні	Середній
Хмарні сервіси	Доступ до ресурсів через вебінтерфейс або хмарну платформу	Масштабованість, мобільність, зручність	Залежність від Інтернет-з'єднання	Високий
SSH	Захищений доступ до серверів через командний інтерфейс	Надійне шифрування та адміністрування систем	Обмеженість графічного інтерфейсу	Високий
VDI	Віртуалізація робочих місць користувачів	Централізоване управління та контроль даних	Високі вимоги до ресурсів інфраструктури	Високий

Забезпечення безпеки віддаленого доступу є одним із ключових завдань сучасних корпоративних інформаційних систем. Віддалене підключення створює потенційні точки входу для несанкціонованого доступу, кібератак та витоку інформації. У зв'язку з цим організації змушені впроваджувати комплексні механізми захисту, що включають автентифікацію користувачів, шифрування даних, моніторинг мережевої активності, сегментацію мереж та використання систем виявлення вторгнень.

Одним із найважливіших елементів безпечного віддаленого доступу є процедура автентифікації користувачів. Традиційне використання логіна та пароля вже не забезпечує достатнього рівня захисту, тому сучасні системи дедалі частіше впроваджують багатофакторну автентифікацію. Такий підхід передбачає використання декількох незалежних факторів підтвердження особи

користувача, що значно ускладнює можливість несанкціонованого доступу до корпоративних ресурсів.

Не менш важливим аспектом є забезпечення конфіденційності та цілісності інформації під час її передавання через мережу. Для цього використовуються криптографічні методи захисту, які дозволяють запобігти перехопленню або модифікації даних. Сучасні протоколи шифрування забезпечують високий рівень захисту інформаційного обміну навіть у випадку використання незахищених каналів зв’язку.

У корпоративному середовищі також широко застосовуються системи контролю та управління доступом. Такі системи дозволяють визначати права користувачів відповідно до їх функціональних обов’язків, обмежувати доступ до критично важливих ресурсів та здійснювати аудит дій користувачів. Реалізація принципу мінімальних привілеїв сприяє зниженню ризику внутрішніх загроз та мінімізації наслідків можливих інцидентів інформаційної безпеки.

Важливу роль у забезпеченні безпеки віддаленого доступу відіграє моніторинг та аналіз мережевої активності. Сучасні системи інформаційної безпеки використовують засоби автоматизованого виявлення аномалій, аналізу поведінки користувачів та реагування на інциденти. Це дозволяє своєчасно виявляти спроби несанкціонованого доступу, шкідливу активність та інші загрози безпеці корпоративної інфраструктури [5].

Слід зазначити, що розвиток технологій віддаленого доступу супроводжується постійним ускладненням кіберзагроз. Зловмисники активно використовують фішингові атаки, шкідливе програмне забезпечення, експлуатацію вразливостей мережевих сервісів та соціальну інженерію для отримання доступу до корпоративних систем. Особливо небезпечними є атаки, спрямовані на компрометацію облікових записів користувачів або викрадення автентифікаційних даних.

У зв’язку з цим сучасні організації змушені впроваджувати комплексний підхід до забезпечення безпеки віддаленого доступу. Такий підхід передбачає поєднання технічних, організаційних та адміністративних заходів захисту. До

технічних заходів належать використання міжмережевих екранів, антивірусного програмного забезпечення, систем виявлення вторгнень та засобів криптографічного захисту інформації. Організаційні заходи включають розроблення політик інформаційної безпеки, регламентів доступу та процедур реагування на інциденти. Адміністративні заходи передбачають проведення навчання персоналу, контроль дотримання вимог безпеки та аудит інформаційної інфраструктури.

Одним із сучасних напрямів розвитку безпечного віддаленого доступу є концепція Zero Trust. Відповідно до цієї моделі жоден користувач або пристрій не вважається довіреним за замовчуванням, незалежно від місця перебування у мережі. Кожна спроба доступу до інформаційних ресурсів проходить перевірку автентичності, авторизації та відповідності політикам безпеки. Такий підхід дозволяє значно підвищити рівень захисту корпоративних інформаційних систем в умовах зростання кількості розподілених користувачів та хмарних сервісів.

Особливого значення питання віддаленого доступу набувають у сфері критичної інформаційної інфраструктури. Банківські установи, державні органи, енергетичні компанії, медичні заклади та інші організації, діяльність яких пов’язана з обробкою конфіденційної інформації, потребують впровадження підвищених вимог до захисту дистанційного доступу [6]. Порушення безпеки у таких системах може призвести до значних фінансових втрат, порушення функціонування критичних сервісів або витоку персональних даних.

Водночас використання віддаленого доступу створює низку організаційних та технічних викликів. Одним із них є забезпечення сумісності різних програмних платформ та пристроїв. Корпоративні інформаційні системи повинні підтримувати роботу з різними операційними системами, мобільними платформами та мережевими середовищами. Це ускладнює процес адміністрування та потребує впровадження уніфікованих механізмів управління доступом.

Іншим важливим викликом є забезпечення стабільності та продуктивності мережевої інфраструктури. Зростання кількості віддалених користувачів

призводить до збільшення навантаження на сервери, канали зв’язку та системи безпеки. Для підтримки ефективної роботи організації необхідно забезпечити високу пропускну здатність мережі, резервування каналів зв’язку та балансування навантаження.

Необхідно також враховувати людський фактор як одну з основних причин виникнення інцидентів інформаційної безпеки. Недостатній рівень обізнаності користувачів щодо правил безпечної роботи з корпоративними ресурсами може призвести до компрометації облікових записів або зараження інформаційної системи шкідливим програмним забезпеченням. Саме тому важливим елементом забезпечення безпеки віддаленого доступу є проведення регулярного навчання персоналу та формування культури інформаційної безпеки.

Отже, віддалений доступ є невід’ємним компонентом сучасних корпоративних інформаційних систем та одним із ключових факторів забезпечення ефективності діяльності організацій у цифровому середовищі. Його використання дозволяє реалізувати концепції мобільної та дистанційної роботи, забезпечити оперативний доступ до інформаційних ресурсів і підтримувати безперервність бізнес-процесів. Водночас розширення можливостей дистанційної взаємодії супроводжується зростанням кіберзагроз та необхідністю впровадження комплексних механізмів захисту інформації [7].

Теперішній етап розвитку корпоративних інформаційних систем характеризується переходом до інтегрованих моделей безпечного доступу, що поєднують використання хмарних технологій, криптографічних засобів захисту, багатофакторної автентифікації та інтелектуальних систем моніторингу безпеки. У перспективі роль віддаленого доступу буде лише зростати, оскільки цифрова трансформація економіки, розвиток глобальних інформаційних мереж та поширення гібридних форм організації праці формують нові вимоги до функціонування корпоративної інформаційної інфраструктури.

1.2 Основні загрози та ризики безпеки при віддаленому підключенні

Віддалений доступ став невід'ємною складовою сучасної інформаційної інфраструктури підприємств, державних установ та приватних користувачів. Активне впровадження хмарних сервісів, мобільних технологій, розподілених корпоративних мереж і моделей дистанційної роботи призвело до суттєвого зростання кількості підключень до інформаційних ресурсів поза межами локального середовища. Одночасно з підвищенням рівня доступності інформаційних систем значно зросла кількість кіберзагроз, пов'язаних із віддаленим підключенням. Віддалений доступ формує додаткову площину атаки, оскільки передбачає передачу даних через зовнішні канали зв'язку, використання публічних мереж та взаємодію між пристроями з різним рівнем захищеності. Саме тому питання аналізу загроз та ризиків безпеки при організації віддаленого доступу набуває особливої актуальності в умовах цифрової трансформації суспільства.

Основною особливістю віддаленого підключення є відсутність фізичного контролю над середовищем, у якому здійснюється доступ до корпоративних ресурсів. Якщо у межах локальної мережі адміністратори мають можливість контролювати обладнання, мережеві вузли та канали передачі даних, то при віддаленому підключенні значна частина інфраструктури стає потенційно вразливою до зовнішніх впливів. Користувачі можуть використовувати незахищені домашні мережі, публічні точки доступу Wi-Fi, особисті пристрої або застаріле програмне забезпечення, що створює сприятливі умови для реалізації кіберзагроз [8].

Однією з найбільш поширених загроз є несанкціонований доступ до інформаційних ресурсів. Такий доступ може бути реалізований шляхом компрометації облікових записів користувачів, перехоплення автентифікаційних даних або використання слабких механізмів ідентифікації. Зловмисники активно застосовують методи підбору паролів, атаки типу brute force, credential stuffing, а також фішингові кампанії для отримання конфіденційних даних користувачів.

Особливу небезпеку становить повторне використання паролів, оскільки компрометація одного сервісу може призвести до отримання доступу до корпоративної інфраструктури.

Важливим фактором ризику є недостатній рівень автентифікації користувачів. Використання лише пароля як єдиного механізму підтвердження особи вже не забезпечує належного рівня захисту. Сучасні кіберзагрози характеризуються високою швидкістю автоматизації та використанням спеціалізованих програмних засобів для перехоплення або підбору облікових даних. У зв'язку з цим значного поширення набувають багатофакторні механізми автентифікації, що передбачають додаткове підтвердження особи користувача за допомогою одноразових кодів, мобільних додатків, апаратних токенів або біометричних характеристик.

Суттєву небезпеку становлять атаки, пов'язані з перехопленням мережевого трафіку. У процесі віддаленого підключення інформація передається через канали зв'язку, які можуть бути недостатньо захищеними. За відсутності належного шифрування зловмисник може здійснювати аналіз або модифікацію переданих даних. Одним із найбільш небезпечних видів таких атак є атака «людина посередині» (Man-in-the-Middle), при якій атакуючий перехоплює обмін інформацією між користувачем та сервером. У результаті можливе викрадення конфіденційної інформації, зміна даних або перенаправлення користувача на фальшиві ресурси [9].

Окремою категорією загроз є вразливості програмного забезпечення, що використовується для організації віддаленого доступу. VPN-сервери, системи віддаленого адміністрування, шлюзи безпеки та інші компоненти мережевої інфраструктури можуть містити помилки або критичні вразливості. Несвоєчасне оновлення програмного забезпечення створює можливість для експлуатації відомих уразливостей та отримання несанкціонованого доступу до системи. Практика свідчить, що значна кількість успішних кібератак пов'язана саме з використанням застарілих версій програмних продуктів, для яких вже існують публічно доступні експлойти.

Особливу увагу необхідно приділяти ризикам, пов’язаним із використанням віддалених робочих станцій. У багатьох випадках співробітники використовують особисті пристрої для підключення до корпоративних ресурсів. Такі пристрої часто не відповідають вимогам інформаційної безпеки, не мають актуального антивірусного захисту або містять небезпечне програмне забезпечення. У разі зараження робочої станції шкідливим кодом виникає ризик проникнення атакуючого у корпоративну мережу. Найбільш поширеними типами шкідливого програмного забезпечення є троянські програми, кейлогери, програми-шифрувальники та бекдори, які дозволяють здійснювати прихований контроль над пристроєм користувача.

Однією з найбільш небезпечних тенденцій останніх років є поширення ransomware-атак. Програми-шифрувальники здатні блокувати доступ до корпоративних даних та вимагати викуп за їх відновлення. Віддалений доступ значно розширює можливості для проникнення такого шкідливого програмного забезпечення у внутрішню інфраструктуру організації. У багатьох випадках початковою точкою компрометації стають саме скомпрометовані облікові записи віддалених користувачів або незахищені VPN-з’єднання.

Суттєвий ризик для інформаційної безпеки становить людський фактор. Помилки користувачів залишаються однією з основних причин інцидентів інформаційної безпеки. Працівники можуть відкривати шкідливі вкладення електронної пошти, переходити за фальшивими посиланнями, використовувати ненадійні паролі або нехтувати вимогами політики безпеки. Соціальна інженерія є одним із найбільш ефективних інструментів атакуючих, оскільки дозволяє обійти технічні механізми захисту шляхом психологічного впливу на користувача. Найбільш поширеними формами соціальної інженерії є фішинг, spear phishing, vishing та smishing [10].

Значні ризики виникають унаслідок недостатньої сегментації мережі. Якщо віддалений користувач отримує надмірні привілеї доступу до корпоративної інфраструктури, компрометація його облікового запису може призвести до масштабного порушення безпеки всієї системи. У сучасних умовах

особливої актуальності набуває концепція Zero Trust, відповідно до якої жоден користувач або пристрій не повинен автоматично вважатися довіреним незалежно від місця підключення. Такий підхід передбачає постійну перевірку автентичності, контроль доступу та мінімізацію привілеїв користувачів.

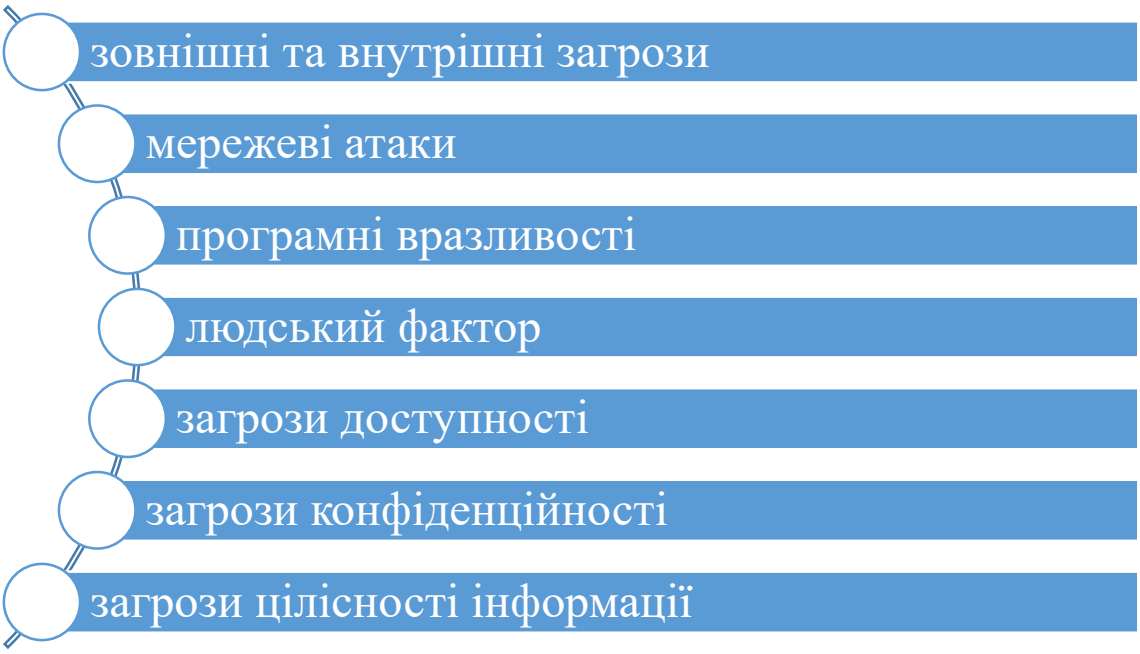

Рис. 1.2 Класифікація загроз безпеки при віддаленому доступі

Важливим аспектом безпеки віддаленого доступу є забезпечення конфіденційності, цілісності та доступності інформації. Порушення конфіденційності може призвести до витоку персональних даних, комерційної таємниці або службової інформації. Порушення цілісності полягає у несанкціонованій зміні інформації, що може мати критичні наслідки для функціонування організації. Втрата доступності інформаційних ресурсів може спричинити зупинку бізнес-процесів, фінансові втрати та репутаційні ризики.

Одним із суттєвих викликів є забезпечення безпеки хмарних сервісів, які активно використовуються для організації віддаленої роботи. Хмарна інфраструктура передбачає передачу частини функцій управління та зберігання даних сторонньому провайдеру. У результаті виникають ризики, пов’язані з неналежним налаштуванням сервісів, компрометацією облікових записів, помилками конфігурації або порушенням політики доступу. Неправильне

налаштування хмарних ресурсів може призвести до відкриття конфіденційної інформації у публічному доступі.

Значну небезпеку становлять DDoS-атаки, спрямовані на порушення доступності систем віддаленого доступу. Перевантаження VPN-шлюзів, серверів автентифікації або мережевої інфраструктури може унеможливити підключення користувачів до корпоративних ресурсів. Особливо критичними такі атаки є для організацій, діяльність яких повністю залежить від дистанційного доступу до інформаційних систем [11].

Таблиця 1.2

Основні загрози безпеці при віддаленому підключенні та їх наслідки

ЗАГРОЗА	СПОСІБ РЕАЛІЗАЦІЇ	МОЖЛИВІ НАСЛІДКИ
Несанкціонований доступ	Компрометація паролів, brute force	Викрадення даних, порушення конфіденційності
Фішингові атаки	Підроблені листи та вебресурси	Отримання облікових даних
Man-in-the-Middle	Перехоплення мережевого трафіку	Модифікація або викрадення інформації
Шкідливе ПЗ	Зараження віддалених пристроїв	Втрата контролю над системою
Ransomware	Шифрування даних	Блокування роботи організації
DDoS-атаки	Перевантаження серверів	Втрата доступності сервісів
Внутрішні загрози	Дії співробітників	Витік або знищення інформації

Не менш важливою проблемою є недостатній рівень моніторингу та аудиту подій безпеки. Відсутність централізованого журналювання дій користувачів, аналізу мережевого трафіку та систем виявлення вторгнень значно ускладнює своєчасне виявлення інцидентів безпеки. У сучасних умовах ефективна система моніторингу повинна забезпечувати безперервний аналіз подій, автоматичне виявлення аномальної активності та оперативне реагування на потенційні загрози.

Суттєвим ризиком є також використання незахищених протоколів віддаленого доступу. Протоколи, які не підтримують сучасні алгоритми шифрування або передають дані у відкритому вигляді, створюють можливість

для перехоплення конфіденційної інформації. Саме тому використання застарілих технологій дистанційного доступу є неприпустимим у сучасних інформаційних системах.

Окрему категорію загроз становлять внутрішні порушники. Працівники організації, які мають легітимний доступ до інформаційних ресурсів, можуть навмисно або ненавмисно здійснювати дії, що призводять до порушення безпеки. Внутрішні загрози є особливо небезпечними через наявність у працівників доступу до корпоративних ресурсів та розуміння внутрішньої структури інформаційної системи. У таких випадках важливе значення мають політики контролю доступу, аудит дій користувачів та розмежування повноважень.

Отже, організація безпечного віддаленого доступу потребує комплексного підходу, що включає використання сучасних криптографічних засобів захисту, багатофакторної автентифікації, систем моніторингу безпеки, сегментації мережі та постійного оновлення програмного забезпечення. Аналіз сучасних загроз свідчить про те, що віддалений доступ є однією з найбільш вразливих складових інформаційної інфраструктури, а ефективне управління ризиками безпеки повинно базуватися на принципах безперервного контролю, мінімізації привілеїв та проактивного виявлення потенційних загроз.

1.3 Методи та технології захисту віддаленого доступу

Забезпечення безпеки віддаленого доступу є одним із ключових напрямів сучасної системи інформаційної безпеки, оскільки саме дистанційне підключення створює додаткові канали взаємодії між користувачем та корпоративною інформаційною інфраструктурою. У процесі розвитку цифрових технологій, хмарних сервісів та моделей дистанційної роботи питання захисту віддаленого доступу набуло стратегічного значення для підприємств, державних установ та організацій різного рівня. Ефективний захист віддалених підключень повинен забезпечувати конфіденційність, цілісність та доступність інформації, а

також запобігати несанкціонованому доступу до ресурсів інформаційної системи.

Система захисту віддаленого доступу базується на комплексному підході, який передбачає використання організаційних, програмних, технічних та криптографічних засобів безпеки. Основною метою таких заходів є мінімізація ризиків, пов’язаних із передачею даних через відкриті канали зв’язку, використанням зовнішніх мереж та підключенням віддалених користувачів до корпоративної інфраструктури. Важливою особливістю сучасних систем захисту є багаторівневий принцип побудови безпеки, при якому порушення одного механізму захисту не призводить до компрометації всієї системи.

Одним із найважливіших методів забезпечення безпеки віддаленого доступу є використання технологій криптографічного захисту інформації. Шифрування даних дозволяє унеможливити перехоплення або несанкціоноване ознайомлення з інформацією під час її передачі мережею. Найбільш поширеним рішенням у сфері захисту віддалених підключень є використання VPN-технологій. Virtual Private Network забезпечує створення захищеного тунелю між користувачем та корпоративною мережею, у межах якого інформація передається у зашифрованому вигляді. VPN-технології дозволяють приховувати мережевий трафік від сторонніх осіб та забезпечують безпечне підключення навіть через публічні мережі Інтернет [12].

Сучасні VPN-рішення використовують різні протоколи захисту інформації, серед яких найбільш поширеними є IPSec, SSL/TLS та WireGuard. Протокол IPSec забезпечує захист мережевого трафіку на мережевому рівні та широко використовується у корпоративних системах. SSL VPN функціонує на транспортному рівні та забезпечує захищений доступ через веббраузер або спеціалізований клієнт. Технологія WireGuard є сучасним високопродуктивним VPN-протоколом, який характеризується спрощеною архітектурою, високою швидкістю роботи та використанням сучасних криптографічних алгоритмів.

Важливим елементом системи захисту є автентифікація користувачів. Автентифікація забезпечує перевірку особи користувача перед наданням

доступу до інформаційних ресурсів. Традиційне використання лише паролів вже не відповідає сучасним вимогам інформаційної безпеки, оскільки паролі можуть бути скомпрометовані шляхом фішингових атак, підбору або перехоплення. У зв’язку з цим значного поширення набули багатофакторні методи автентифікації, які передбачають використання декількох незалежних факторів підтвердження особи.

Багатофакторна автентифікація базується на поєднанні різних категорій факторів: знання, володіння та біометричних характеристик. До факторів знання належать паролі або PIN-коди, до факторів володіння — мобільні пристрої, токени або смарткарти, а до біометричних факторів — відбитки пальців, розпізнавання обличчя чи голосу. Використання багатофакторної автентифікації суттєво знижує ризик несанкціонованого доступу навіть у випадку компрометації одного з факторів захисту.

Однією з ключових технологій захисту віддаленого доступу є система управління доступом. Контроль доступу передбачає обмеження прав користувачів відповідно до їх функціональних обов’язків та рівня повноважень. Найбільш поширеним принципом є принцип мінімальних привілеїв, відповідно до якого користувач отримує лише ті права доступу, які необхідні для виконання службових завдань. Такий підхід дозволяє мінімізувати можливі наслідки компрометації облікового запису або помилкових дій користувача [13].

Сучасні системи безпеки активно використовують концепцію Zero Trust, яка передбачає відмову від автоматичної довіри до будь-якого користувача або пристрою незалежно від місця підключення. У межах цієї концепції кожна спроба доступу підлягає перевірці, а доступ до ресурсів надається лише після підтвердження автентичності користувача та оцінки рівня безпеки пристрою. Zero Trust передбачає постійний моніторинг активності користувачів, аналіз поведінкових характеристик та використання механізмів адаптивного контролю доступу.

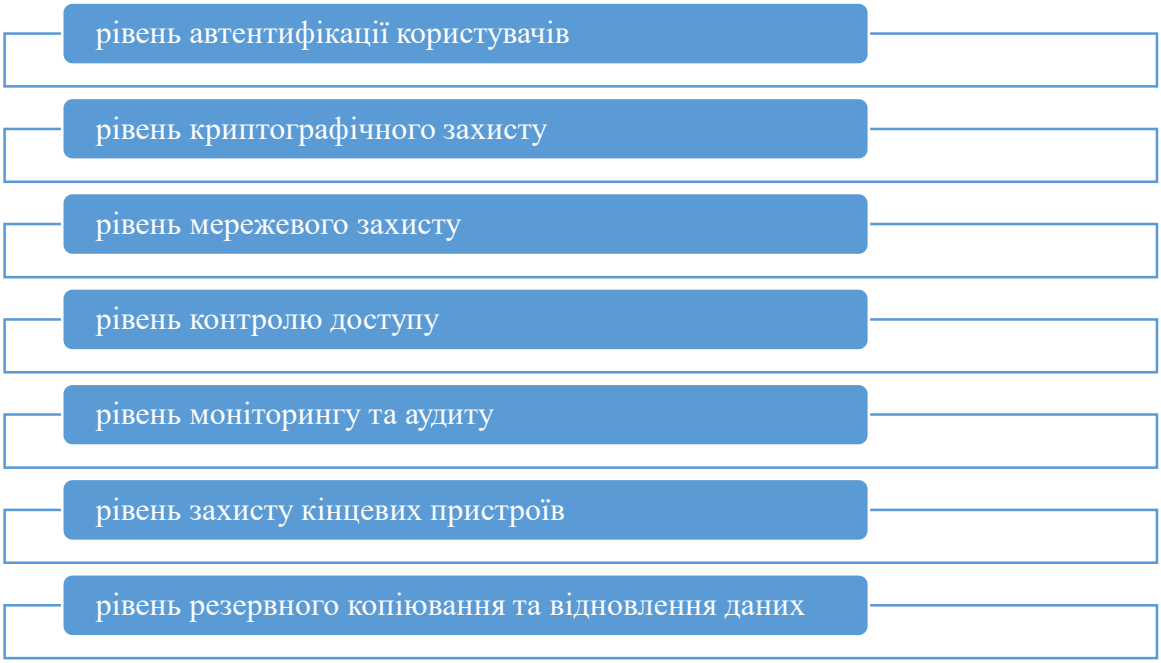

Рис. 1.3 Багаторівнева система захисту віддаленого доступу

Важливу роль у забезпеченні безпеки віддаленого доступу відіграють міжмережеві екрани. Firewall є засобом контролю мережевого трафіку та забезпечує фільтрацію вхідних і вихідних з'єднань відповідно до встановлених правил безпеки. Міжмережеві екрани дозволяють блокувати небажані мережеві підключення, обмежувати доступ до окремих сервісів та виявляти підозрілу активність. Сучасні міжмережеві екрани нового покоління підтримують функції аналізу прикладного трафіку, виявлення вторгнень та інтеграції із системами моніторингу безпеки.

Суттєве значення мають системи виявлення та запобігання вторгненням. IDS та IPS забезпечують автоматичний аналіз мережевого трафіку та виявлення аномальної активності або ознак кібератак. Системи IDS здійснюють моніторинг подій та формують повідомлення про потенційні загрози, тоді як IPS мають можливість автоматично блокувати небезпечні дії. Використання таких систем дозволяє оперативно реагувати на спроби несанкціонованого доступу, мережеві атаки або розповсюдження шкідливого програмного забезпечення [14].

Таблиця 1.3

Основні технології захисту віддаленого доступу

ТЕХНОЛОГІЯ	ПРИЗНАЧЕННЯ	ОСНОВНІ ФУНКЦІЇ
VPN	Захищене підключення користувачів	Шифрування трафіку, створення захищеного тунелю
MFA	Підтвердження особи користувача	Багатофакторна автентифікація
Firewall	Контроль мережевого трафіку	Фільтрація з'єднань, блокування атак
IDS/IPS	Виявлення та блокування атак	Аналіз трафіку, запобігання вторгненням
EDR	Захист кінцевих пристроїв	Моніторинг та реагування на загрози
SIEM	Моніторинг подій безпеки	Аналіз журналів та кореляція подій
MDM	Управління мобільними пристроями	Контроль безпеки та конфігурації

Не менш важливим елементом захисту є антивірусне програмне забезпечення та системи Endpoint Detection and Response. Традиційні антивірусні засоби забезпечують виявлення відомих типів шкідливого програмного забезпечення на основі сигнатурного аналізу. Проте сучасні кіберзагрози характеризуються використанням складних механізмів маскування та модифікації шкідливого коду, що потребує застосування більш ефективних технологій захисту. Системи EDR дозволяють здійснювати поведінковий аналіз процесів, виявляти підозрілу активність на кінцевих пристроях та автоматично реагувати на інциденти безпеки.

Увагу необхідно приділяти захисту кінцевих пристроїв користувачів. Безпечне віддалене підключення неможливе без належного рівня захищеності робочих станцій, ноутбуків або мобільних пристроїв. Для цього використовуються засоби централізованого управління пристроями, політики безпеки, контроль встановлення програмного забезпечення та шифрування локальних носіїв інформації. У багатьох організаціях застосовується концепція BYOD, яка дозволяє працівникам використовувати власні пристрої для роботи. У такому випадку особливо важливим є використання систем Mobile Device

Management, що забезпечують контроль безпеки мобільних пристроїв та централізоване управління ними.

Одним із важливих напрямів захисту є забезпечення безпеки мережевої інфраструктури. Для цього використовуються технології сегментації мережі, які дозволяють розділити інформаційну систему на окремі ізольовані сегменти. У разі компрометації одного сегмента це ускладнює подальше поширення атаки всередині корпоративної мережі. Сегментація також дозволяє реалізувати диференційований контроль доступу до різних категорій інформаційних ресурсів.

Важливим методом забезпечення безпеки є постійне оновлення програмного забезпечення та управління вразливостями. Розробники програмних продуктів регулярно випускають оновлення безпеки, спрямовані на усунення виявлених уразливостей. Несвоєчасне встановлення таких оновлень створює ризик експлуатації відомих вразливостей зловмисниками. Системи управління вразливостями дозволяють автоматизувати процес сканування інформаційної інфраструктури, виявлення потенційних слабких місць та контролю встановлення оновлень.

Суттєву роль у системі захисту віддаленого доступу відіграє моніторинг подій безпеки та аудит дій користувачів. Централізовані системи журналювання забезпечують збір, аналіз та зберігання інформації про події в інформаційній системі. Використання SIEM-систем дозволяє автоматизувати процес кореляції подій, виявлення аномальної активності та реагування на інциденти безпеки. Аналіз журналів подій забезпечує можливість оперативного виявлення спроб несанкціонованого доступу, підозрілих дій користувачів або ознак компрометації системи.

Необхідним елементом системи захисту є резервне копіювання інформації. Наявність резервних копій дозволяє забезпечити відновлення даних у випадку кібератак, технічних збоїв або пошкодження інформації. Особливого значення резервне копіювання набуває у контексті протидії ransomware-атакам, оскільки

дозволяє відновити працездатність інформаційної системи без сплати викупу зловмисникам.

Важливим складником забезпечення безпеки є організаційні заходи. До них належать розробка політик інформаційної безпеки, регламентів використання віддаленого доступу, навчання персоналу та контроль дотримання вимог безпеки. Практика свідчить, що навіть найсучасніші технічні засоби захисту не забезпечують належного рівня безпеки без відповідного рівня обізнаності користувачів. Регулярне проведення тренінгів, інструктажів та тестування працівників дозволяє знизити ризики, пов’язані з людським фактором.

Особливу увагу необхідно приділяти криптографічному захисту даних. Сучасні алгоритми шифрування забезпечують високий рівень захисту інформації від несанкціонованого доступу. Для захисту віддалених з’єднань використовуються симетричні та асиметричні криптографічні алгоритми, цифрові сертифікати та інфраструктура відкритих ключів. Використання сертифікатів дозволяє підтверджувати автентичність серверів та забезпечувати захищений обмін ключами шифрування.

Перспективним напрямом розвитку систем захисту є використання технологій штучного інтелекту та машинного навчання. Такі системи здатні аналізувати великі обсяги даних, виявляти аномалії поведінки користувачів та прогнозувати потенційні загрози безпеці. Використання інтелектуальних механізмів аналізу дозволяє підвищити ефективність виявлення складних та цільових кібератак.

Отже, сучасні методи та технології захисту віддаленого доступу формують комплексну багаторівневу систему забезпечення інформаційної безпеки. Ефективний захист дистанційних підключень передбачає поєднання криптографічних засобів, багатофакторної автентифікації, контролю доступу, систем моніторингу безпеки та організаційних заходів. У сучасних умовах постійного зростання кількості кіберзагроз забезпечення безпечного віддаленого доступу є необхідною умовою стабільного функціонування інформаційних

систем та захисту корпоративних ресурсів від несанкціонованого доступу і кібератак.

Висновки до розділу 1

У розділі було розглянуто теоретичні основи організації та забезпечення безпеки віддаленого доступу в сучасних корпоративних інформаційних системах. Проведений аналіз дозволив встановити, що розвиток цифрових технологій, поширення дистанційної роботи, використання хмарних сервісів та глобальних мережевих інфраструктур сприяли суттєвому зростанню ролі віддаленого доступу у функціонуванні підприємств і організацій. Віддалений доступ забезпечує оперативну взаємодію користувачів з корпоративними ресурсами незалежно від їх географічного розташування, підвищує гнучкість бізнес-процесів та ефективність управління інформаційними ресурсами.

У ході дослідження було визначено сутність поняття віддаленого доступу, його основні принципи функціонування та значення для сучасних інформаційних систем. Встановлено, що віддалений доступ є важливим елементом корпоративної IT-інфраструктури, який забезпечує можливість безпечної взаємодії користувачів із серверами, базами даних, корпоративними мережами та програмними ресурсами через зовнішні канали зв’язку. Разом із перевагами дистанційної взаємодії віддалений доступ створює додаткові ризики інформаційній безпеці, оскільки розширює площину потенційних кібератак та ускладнює контроль за середовищем підключення користувачів.

Аналіз основних загроз та ризиків безпеки при віддаленому підключенні показав, що найбільш небезпечними є несанкціонований доступ до інформаційних ресурсів, фішингові атаки, перехоплення мережевого трафіку, використання шкідливого програмного забезпечення, експлуатація вразливостей програмних засобів, DDoS-атаки та внутрішні загрози. Особливу небезпеку становить людський фактор, оскільки помилки користувачів та методи соціальної інженерії залишаються одними з основних причин компрометації

інформаційних систем. Встановлено, що сучасні кіберзагрози характеризуються високим рівнем автоматизації, складністю реалізації та постійною еволюцією методів атак, що потребує застосування комплексних підходів до забезпечення інформаційної безпеки.

У результаті дослідження методів та технологій захисту віддаленого доступу було визначено, що ефективна система безпеки повинна базуватися на принципах багаторівневого захисту та поєднувати організаційні, програмні й технічні засоби безпеки. До основних технологій захисту належать VPN-з'єднання, багатофакторна автентифікація, міжмережеві екрани, системи виявлення та запобігання вторгненням, засоби криптографічного захисту, системи моніторингу подій безпеки та технології захисту кінцевих пристроїв. Важливе значення має також реалізація концепції Zero Trust, яка передбачає постійний контроль автентичності користувачів та мінімізацію привілеїв доступу.

Проведений аналіз дозволяє зробити висновок, що забезпечення безпеки віддаленого доступу є складним комплексним процесом, який потребує постійного вдосконалення механізмів захисту відповідно до розвитку сучасних кіберзагроз. Ефективне функціонування корпоративних інформаційних систем можливе лише за умови впровадження сучасних технологій захисту, систематичного моніторингу подій безпеки, оновлення програмного забезпечення та підвищення рівня обізнаності користувачів у сфері кібербезпеки. Отже, організація безпечного віддаленого доступу є необхідною умовою забезпечення стабільності, надійності та захищеності сучасних інформаційних систем.

Розділ 2 АНАЛІЗ ІСНУЮЧИХ МЕХАНІЗМІВ ТА СТАНУ БЕЗПЕКИ ВІДДАЛЕНОГО ДОСТУПУ

2.1 Аналіз архітектури корпоративної інформаційної системи та каналів віддаленого доступу

Корпоративні інформаційні системи є складними багаторівневими структурами, що об’єднують програмні, технічні та мережеві компоненти з метою забезпечення ефективного функціонування бізнес-процесів, управління даними та підтримки комунікації між користувачами. Розвиток цифрових технологій, поширення хмарних сервісів та впровадження моделей дистанційної роботи сприяли суттєвому розширенню можливостей віддаленого доступу до корпоративних ресурсів. У зв’язку з цим аналіз архітектури корпоративної інформаційної системи та каналів віддаленого доступу є важливим етапом оцінювання рівня інформаційної безпеки та визначення потенційних вразливостей інфраструктури.

Архітектура корпоративної інформаційної системи являє собою сукупність взаємопов’язаних компонентів, що забезпечують обробку, зберігання, передачу та захист інформації. До основних елементів такої системи належать серверна інфраструктура, мережеве обладнання, системи зберігання даних, програмні сервіси, робочі станції користувачів та засоби захисту інформації. Залежно від масштабів організації та специфіки її діяльності архітектура інформаційної системи може включати локальні сервери, хмарні платформи, віртуалізовані середовища та гібридні інфраструктури [15].

У корпоративних мережах значного поширення набуває багаторівнева архітектура, яка передбачає поділ системи на окремі функціональні рівні. Найчастіше використовуються трирівневі моделі, що включають рівень представлення, прикладний рівень та рівень баз даних. Рівень представлення забезпечує взаємодію користувача з інформаційною системою через

вебінтерфейси або клієнтські додатки. Прикладний рівень виконує обробку бізнес-логіки та забезпечує взаємодію між сервісами. Рівень баз даних відповідає за зберігання, обробку та управління інформаційними ресурсами. Такий підхід дозволяє підвищити масштабованість системи, спростити адміністрування та забезпечити розмежування функціональних компонентів.

Рис. 2.1 Архітектура корпоративної інформаційної системи з віддаленим доступом

Особливе значення в архітектурі корпоративної інформаційної системи мають канали віддаленого доступу, через які користувачі здійснюють підключення до інформаційних ресурсів організації. Віддалений доступ може реалізовуватися за допомогою VPN-з’єднань, вебінтерфейсів, систем віддаленого адміністрування, хмарних платформ або спеціалізованих корпоративних сервісів. Кожен із таких каналів має власні особливості функціонування та рівень захищеності, що безпосередньо впливає на загальний стан інформаційної безпеки.

Таблиця 2.1

Основні канали віддаленого доступу в корпоративних інформаційних системах

КАНАЛ ДОСТУПУ	ПРИЗНАЧЕННЯ	ОСНОВНІ РИЗИКИ
VPN	Захищене підключення до корпоративної мережі	Компрометація облікових даних
Вебінтерфейс	Доступ через браузер	Фішинг, атаки на вебдодатки
Хмарні сервіси	Віддалена робота з даними	Витік інформації, помилки конфігурації
RDP	Віддалене адміністрування	Brute force, несанкціонований доступ
Мобільні додатки	Доступ із мобільних пристроїв	Втрата пристрою, шкідливе ПЗ

Найбільш поширеним механізмом організації захищеного віддаленого доступу є використання VPN-технологій. Virtual Private Network дозволяє створювати захищений канал зв’язку між користувачем та корпоративною мережею через публічні мережі передачі даних. У межах VPN-з’єднання інформація передається у зашифрованому вигляді, що ускладнює можливість її перехоплення або модифікації сторонніми особами. Залежно від особливостей архітектури підприємства можуть використовуватися VPN-рішення на основі IPSec, SSL/TLS або WireGuard [16].

Аналіз каналів віддаленого доступу свідчить про те, що значна кількість корпоративних систем використовує веборієнтовані сервіси для забезпечення дистанційної роботи користувачів. Хмарні платформи, системи електронного документообігу, CRM-системи та корпоративні портали забезпечують доступ до ресурсів через браузер або мобільні додатки. Такий підхід суттєво спрощує організацію дистанційної роботи, однак створює додаткові ризики, пов’язані з безпекою вебдодатків, захистом сеансів автентифікації та контролем доступу до інформації.

Важливим елементом корпоративної архітектури є мережеве обладнання, яке забезпечує маршрутизацію та фільтрацію трафіку між сегментами мережі. До таких засобів належать маршрутизатори, комутатори, міжмережеві екрани, шлюзи безпеки та системи балансування навантаження. Саме через мережеву інфраструктуру реалізується контроль доступу користувачів до внутрішніх

ресурсів організації. Наявність помилок конфігурації або використання застарілого обладнання може створювати додаткові вразливості для кібератак.

Корпоративні інформаційні системи часто функціонують у гібридному середовищі, що поєднує локальні та хмарні ресурси. Гібридна архітектура дозволяє організаціям оптимізувати витрати на IT-інфраструктуру, забезпечити масштабованість сервісів та підвищити доступність інформаційних ресурсів. Водночас використання хмарних технологій ускладнює процес забезпечення безпеки, оскільки частина інфраструктури перебуває під управлінням зовнішнього провайдера. У такому випадку особливого значення набуває захист каналів зв’язку між локальною мережею підприємства та хмарними сервісами.

Одним із ключових аспектів аналізу архітектури корпоративної системи є оцінювання механізмів автентифікації та авторизації користувачів. У більшості сучасних систем використовуються централізовані служби управління обліковими записами, такі як Active Directory або LDAP. Вони забезпечують єдину систему ідентифікації користувачів та контроль доступу до ресурсів. Використання централізованої автентифікації дозволяє спростити адміністрування облікових записів та забезпечити контроль дій користувачів у межах корпоративної мережі.

Значна увага приділяється аналізу механізмів сегментації мережі. Сегментація передбачає розподіл корпоративної мережі на окремі логічні або фізичні сегменти, що дозволяє обмежити доступ користувачів до критичних ресурсів та знизити ризик поширення атаки всередині системи. У багатьох організаціях застосовується модель DMZ, у межах якої зовнішні сервіси розміщуються в окремому сегменті мережі, ізольованому від внутрішньої інфраструктури підприємства [17].

Аналіз існуючих каналів віддаленого доступу свідчить про те, що однією з найбільш поширених проблем є недостатній рівень захисту кінцевих пристроїв користувачів. Працівники часто використовують домашні комп’ютери, мобільні телефони або незахищені мережі Wi-Fi для підключення до корпоративних ресурсів. Такі пристрої можуть містити вразливості, шкідливе програмне

забезпечення або застарілі версії операційних систем. У результаті компрометація кінцевого пристрою може стати початковою точкою проникнення зловмисника до корпоративної мережі.

Суттєву роль у забезпеченні безпеки відіграють системи моніторингу та журналювання подій. Корпоративні інформаційні системи повинні забезпечувати централізований збір журналів подій, аналіз мережевого трафіку та контроль активності користувачів. Використання SIEM-систем дозволяє здійснювати кореляцію подій безпеки, виявляти аномальну активність та оперативно реагувати на інциденти. Аналіз журналів доступу є важливим елементом аудиту безпеки та дозволяє виявляти спроби несанкціонованого підключення або підозрілу поведінку користувачів.

Важливим напрямом аналізу є оцінювання рівня захищеності каналів передачі даних. У корпоративних системах використовуються криптографічні механізми захисту інформації, зокрема протоколи TLS та IPSec [18]. Шифрування мережевого трафіку дозволяє забезпечити конфіденційність інформації та унеможливлює її перехоплення під час передачі через відкриті мережі. Разом із тим ефективність криптографічного захисту залежить від правильності налаштування алгоритмів шифрування, управління ключами та використання актуальних сертифікатів безпеки.

Окрему увагу необхідно приділяти оцінюванню політик безпеки та процедур управління доступом. У багатьох організаціях спостерігається проблема надмірних привілеїв користувачів, що підвищує ризик компрометації критичних ресурсів. Ефективна система безпеки повинна базуватися на принципі мінімальних привілеїв та передбачати регулярний аудит прав доступу користувачів. Крім того, важливе значення має використання багатофакторної автентифікації для захисту облікових записів від несанкціонованого доступу.

Результати аналізу сучасних корпоративних інформаційних систем свідчать про те, що основними вразливостями каналів віддаленого доступу є недостатній рівень захисту кінцевих пристроїв, використання застарілих протоколів зв’язку, слабкі механізми автентифікації, помилки конфігурації

мережевого обладнання та відсутність належного моніторингу подій безпеки. Значна частина успішних кібератак пов’язана саме з компрометацією віддалених облікових записів або експлуатацією вразливостей мережевої інфраструктури.

Аналіз архітектури корпоративної інформаційної системи та каналів віддаленого доступу дозволяє визначити основні компоненти інформаційної інфраструктури, оцінити рівень їх захищеності та виявити потенційні ризики інформаційній безпеці. Сучасні корпоративні системи характеризуються складною багаторівневою структурою та активним використанням віддалених каналів зв’язку, що потребує впровадження комплексних механізмів захисту, постійного моніторингу подій безпеки та вдосконалення політик контролю доступу.

2.2 Оцінка вразливостей і потенційних каналів несанкціонованого доступу

Оцінювання вразливостей і потенційних каналів несанкціонованого доступу у контексті віддаленого доступу потребує системного підходу, який охоплює технічні, організаційні та процесні аспекти. Центральним завданням є ідентифікація точок атаки на рівнях мережевої взаємодії, транспорту, застосунків, облікових записів і керування даними, а також визначення ймовірності реалізації загроз із урахуванням типового профілю зловмисника, наявності засобів експлуатації й ступеня впливу на конфіденційність, цілісність і доступність. Вразливості систем віддаленого доступу, зокрема VPN-рішень, шлюзів Zero Trust Network Access (ZTNA), серверів віддаленого робочого столу (RDP), протоколів SSH, а також хмарних брокерів доступу до застосунків, часто мають спільні корені: помилки конфігурування, застарілі або незапатчені компоненти, слабкі механізми автентифікації, відсутність сегментації та моніторингу, а також людський чинник у процесах адміністрування і користування.

На мережевому рівні найпоширенішими є вразливості, пов’язані з відкритими інтерфейсами керування та надмірною експозицією портів. Публічний експорт RDP, SSH чи адміністративних веб-інтерфейсів VPN-шлюзів у мережу Інтернет створює передумови для брутфорсу та автоматизованого підбору облікових даних, експлуатації відомих уразливостей служб та здійснення розвідки інфраструктури [19]. Відсутність або некоректне застосування списків контролю доступу й геофільтрації дозволяє атакувальникам із глобального простору адрес під’єднуватися до точок входу без суттєвих перешкод. До цього додається ризик використання застарілих криптографічних наборів і протоколів: TLS зі слабкими шифрами, старі версії SSH або IKEv1/агресивний режим у IPsec, що спрощують проведення атак типу зниження рівня шифрування та перехоплення сесій за наявності проміжних вузлів.

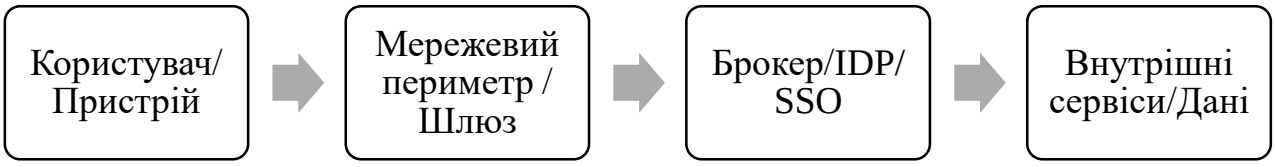

Рис. 2.2 Ланцюг потенційних каналів несанкціонованого доступу у віддаленому доступі

На транспортному рівні критичними є вади у впровадженні TLS/DTLS, механізмах встановлення ключів і обміну сертифікатами. Неправильна валідація сертифікатів, прийняття самопідписаних або прострочених сертифікатів без

додаткового контролю, відсутність перевірки відкликання чи застосування HSTS у веб-порталах доступу доходять до категорії системних помилок, що відкривають шлях до атак «людина посередині». Деґрадація безпеки можлива також через повторне використання ключів, недостатню ентропію під час генерації, або слабкі параметри обміну (наприклад, статичні ключі замість еліптичних дифі-гелманівських епімерів). На рівні каналів тунелювання у VPN важливо враховувати уразливості до роз'єднання тунелю (split tunneling) без належних правил маршрутизації, що може призводити до витоку трафіку в неконтрольовані сегменти, а також недоліки механізмів захисту від витоку DNS під час активної сесії [20].

На рівні застосунків віддаленого доступу джерелами ризику є як власні уразливості серверних компонентів (веб-портали VPN, брокери доступу, RDP-шлюзи), так і інтеграційні вузли: SSO-провайдери, проксі, агенти на кінцевих точках. Типові помилки включають ін'єкційні атаки в параметрах автентифікації або самих порталів, відкриті редіректи, неправильне керування сесіями (довготривалі токени без прив'язки до пристрою чи контексту), відсутність привілейованого розмежування в доступі до бекенд-сервісів, а також логічні вади в реалізації MFA. Окремої уваги заслуговують токени доступу у федеративних схемах (SAML, OIDC): підміна аудиторії, перепризначення редіректів, підпис некоректними алгоритмами, повторне використання токенів унаслідок відсутності прив'язки до клієнтської платформи або помилок у валідації nonce/атрибутів.

Ідентифікація і автентифікація користувачів формують один із найчутливіших сегментів. Слабкі паролі, відсутність або формальне застосування багатофакторної автентифікації, використання одноразових кодів через небезпечні канали (SMS без додаткових обмежень), а також схильність користувачів до фішингу призводять до захоплення акаунтів. Багато сучасних атак використовують проксі для перехоплення MFA-сесій, фармінг-сторінки, що ретранслюють трафік до легітимних порталів, крадіжку сесійних cookies та токенів через ін'єкції у браузері або на кінцевій точці. Додатковий ризик створює

відсутність політик умовного доступу, коли підвищений ризик аутентифікації (невідомий пристрій, нетипова геолокація, аномальна година) не спричиняє вимогу додаткових факторів чи блокування доступу. Небезпечна практика повторного використання облікових даних між корпоративними та особистими ресурсами прискорює атаки credential stuffing після витоків з третіх сторін [21].

Контроль доступу і авторизація часто страждають від макрорівневих помилок моделювання. Рольові моделі з надмірними дозволами, відсутність принципу найменших привілеїв і недостатня сегментація призводять до того, що компрометація одного облікового запису відкриває широкі горизонти латерального переміщення. Застосункові шлюзи без контекстної перевірки стану пристрою (постура) і без мікросегментації дозволяють доступ до широких мережевих діапазонів або цілих внутрішніх порталів, замість публікації окремих сервісів з дрібнозернистою авторизацією. В екосистемах з привілейованими доступами (адміністративні консолі, системи керування мережею, сховища секретів) ризик множиться у разі відсутності розмежування обов’язків, затвердження змін і контролю сесій. Типова вада — відсутність Just-in-Time видання привілеїв і механізмів запису/реплею сесій для подальшого розслідування.

Кінцеві точки користувачів — це критична площина атак, оскільки компрометація клієнтського пристрою надає атакувальнику легітимні канали до корпоративних ресурсів. Недостатній контроль цілісності й відповідності (відсутність EDR/антимальварного захисту, застарілі ОС, відсутність шифрування диска, вимкнені брандмауери), відсутність контейнеризації робочих профілів на BYOD-пристроях і слабкі політики оновлень створюють умови для крадіжки облікових даних, підміни конфігурацій VPN/агентів ZTNA, ін’єкції в браузер і ексфільтрації даних [22]. Додатковий ризик становить відсутність контролю периферії (USB-носії, друк), що може конвертуватися у швидкі канали витоку за наявності віддаленого доступу. Важливими є також ризики локального кешування корпоративних даних у незахищених профілях і синхронізації з особистими хмарами.

Інфраструктурні компоненти віддаленого доступу — VPN-шлюзи, контролери і брокери — часто стають цілями атак через відомі уразливості у прошивках і веб-компонентах, неправильні публічні конфігурації або недоліки у процедурі оновлення. Проблеми ключового керування включають зберігання приватних ключів і сертифікатів на пристроях без апаратної ізоляції, спільне використання облікових записів адміністрування та відсутність ротації секретів. Резервні канали доступу, створені для аварійного відновлення, нерідко залишаються недостатньо задокументованими і контролюються слабше, ніж основні, що перетворює їх на приховані вектори проникнення [23]. У середовищах з мультіхмарною або гібридною архітектурою помилки маршрутизації й відсутність узгоджених політик мережевої сегментації між майданчиками створюють «містки довіри», якими атакувальник може скористатися після компрометації одного сегмента.

Ланцюг постачання та залежності в системах віддаленого доступу формують окрему категорію ризиків. Агенти доступу, бібліотеки криптографії, модулі аутентифікації, плагіни для керування сесіями та інтеграції з SIEM/IDP можуть містити уразливості або бути вектором цілеспрямованого втручання. Відсутність процедур верифікації цілісності пакунків, контролю підписів, порушення принципів мінімізації (встановлення надлишкових модулів), а також несвоєчасне оновлення до виправлених версій підвищують імовірність експлуатації. У сценаріях розширення довіри до партнерів і підрядників помилки в договорах рівня доступу та технічному контролі з боку третьої сторони здатні відкрити обхідні шляхи авторизації, особливо коли зовнішні ідентичності мапуються на внутрішні ролі без додаткових атестацій.

Людський чинник і соціальна інженерія традиційно залишаються дієвими каналами несанкціонованого доступу. Фішингові кампанії націлені на користувачів віддаленого доступу через імітацію порталів входу, повідомлення про блокування облікового запису чи терміновість проходження «повторної верифікації». В умовах розподіленої праці користувачі частіше взаємодіють поза захищеним периметром і застосовують особисті пристрої, що збільшує площину

ризику. Комплексні атаки поєднують фішинг із телефонним супроводом (vishing), підробленими push-запитами MFA (MFA fatigue) і шкідливими вкладеннями для розгортання бекдорів на кінцевій точці. Недостатня обізнаність співробітників щодо ознак підроблених доменів, сертифікатів і незвичних поведінкових ознак сесій призводить до запізнілої реакції, коли компрометація вже відбулася [24].

Моніторинг і виявлення інцидентів у системах віддаленого доступу часто ускладнюються фрагментацією журналів і відсутністю єдиної кореляції подій. Логі з VPN, брокерів, ідентифікаційних провайдерів, кінцевих точок і хмарних сервісів зберігаються в різних сховищах, мають неоднорідні формати та різні періоди ретенції. Цим користуються зловмисники, які намагаються залишатися «під радаром», варіюючи годину, інтервали активності та географію IP для уникнення простих правил виявлення. Відсутність детальної телеметрії (наприклад, інформації про пристрій, версію клієнта, стан захисту, параметри мережі) знижує якість верифікації постури і не дозволяє впроваджувати поведінкові моделі для оцінки ризику сесії. Додатковою проблемою є нечіткі процедури реагування: якщо процес відкликання токенів, примусової переавтентифікації, ізоляції пристрою та блокування маршрутизації не автоматизований, вікно можливостей для атакувальника подовжується.

Особливу увагу слід приділити витокам метаданих і побічним каналам. Навіть за наявності криптографічного захисту вмісту трафіку, часові характеристики, розміри пакетів і патерни взаємодії можуть розкривати структуру сервісів, типи застосунків і приблизний обсяг оброблюваних даних. Неправильна конфігурація DNS, відсутність ізоляції запитів або використання публічних резолверів без шифрування створюють додаткові можливості для спостереження і спрямованих атак. У контексті мобільних клієнтів важливими є ризики перехоплення на рівні операторських мереж та використання незахищених точок Wi-Fi, де підміна шлюзів і captive-порталів може ініціювати атаки на сесію або на сам клієнтський стек [25].

Управління вразливостями вимагає формалізованої процедури інвентаризації активів і точок доступу, реєстру залежностей, регулярного сканування та пріоритезації виправлень із урахуванням експлуатабельності. Системи віддаленого доступу повинні мати короткі цикли оновлень, планові вікна для застосування патчів на шлюзах і брокерах, а також механізми тестування оновлень у стейджинговому середовищі. Важливо забезпечити криптографічну гігієну: ротацію ключів і сертифікатів, контроль термінів дії, застосування сучасних наборів шифрів, заборону застарілих протоколів та активне використання сертифікатів з апаратним захистом ключів. З огляду на поширення хмарних ідентичностей, необхідно узгодити політики між локальними та хмарними провайдерами, уніфікувати вимоги до MFA, умовного доступу, перевірок пристрою, а також централізувати збір журналів та аналітику.

Моделі загроз для віддаленого доступу мають враховувати різні класи супротивника: від опортуністичних кіберзлочинців, що покладаються на масові сканування та відомі експлойти, до цілеспрямованих груп з розширеними можливостями, які застосовують ланцюгові атаки через постачальників, фішинг-проксі, експлуатацію нульового дня в інфраструктурних компонентах і приховані канали керування. Оцінка ризику повинна включати сценарії компрометації одного елемента довіри і подальшої ескалації: захоплення акаунта з базовою роллю з використанням слабкої MFA, латеральний рух через слабку сегментацію до середовищ з підвищеними правами, експлуатація службавтоматизації для розгортання бекдорів і подальший ексфільт даних через легітимні тунелі. Критично важливо моделювати атаки на доступність: DDoS на портали автентифікації, виснаження пулів сесій VPN, блокування каталогів ідентичностей або шифрування конфігураційних сховищ.

Відповідні компенсуючі заходи повинні базуватися на принципах «нульової довіри»: верифікація кожної сесії та кожної дії, сегментація доступу до рівня окремого застосунку, постійна оцінка контексту ризику та мінімізація привілеїв. На практичному рівні це означає обмеження публічної експозиції інтерфейсів, впровадження брокерів, що термінують TLS на периметрі та

виконують протокольне посередництво, примусове застосування фішингостійких факторів (апаратні ключі, платформи з прив’язкою до пристрою), захист токенів від повторного використання, короткоживучі сесії з повторною перевіркою ризику і пристрою, а також автоматизовані плейбуки реагування, які анулюють сесії, відкликають маркери доступу та ізолюють пристрої без участі людини [26]. Посилення спостережуваності через централизацію журналів, нормалізацію подій і застосування поведінкової аналітики знижує середній час виявлення, тоді як контроль конфігурацій і безперервні тести проникнення верифікують, що політики діють як задумано.

Потенційні канали несанкціонованого доступу можна класифікувати на прямі та опосередковані. До прямих належать компрометація облікових записів і токенів, експлуатація уразливостей у публічних інтерфейсах віддаленого доступу, маніпуляції з протоколами шифрування та перехоплення сесій на незахищених мережах. Опосередковані канали включають атаки через залежності постачальників і інтеграційні модулі, використання некоректно конфігурованих резервних доступів, зловживання довірою між середовищами (dev/test/prod), ін’єкцію шкідливого коду у клієнтські агенти, а також ексфільтрацію даних через синхронізовані користувацькі сервіси за межами корпоративного контролю. Для кожного каналу оцінка повинна визначати актив, що під загрозою, шлях атаки, засоби й індикатори компрометації, наявні контролі та їхню ефективність, а також пріоритетні заходи зниження ризику з урахуванням вартості і впливу на бізнес-процеси.

Таблиця 2.2

Канали несанкціонованого доступу, вплив і пріоритет зниження ризику

КАНАЛ АТАКИ	ТИПОВА ВРАЗЛИВІСТЬ/ ПОМИЛКА	ЙМОВІРНІСТЬ	ВПЛИВ	ОСНОВНІ ІНДИКАТОРИ КОМПРОМЕТАЦІЇ	ПРІОРИТЕТНІ ЗАХОДИ
Компрометація облікових записів	Слабкі паролі, відсутність фішингостійкої MFA	Висока	Високий	Нетипові геолокації, аномальна активність входів, зростання відмов MFA	Аппаратні ключі/FIDO2, умовний доступ, паролі з менеджером, моніторинг ризику
Перехоплення сесій (MITM/MFA-проксі)	Прийняття слабких сертифікатів, відсутність прив’язки токена	Середня-висока	Високий	Неспівпадіння атрибутів клієнта, часті перевидачі токенів	Валідація TLS, прив’язка токенів до пристрою, короткі сесії, детект проксі
Експлуатація публічних інтерфейсів	Незапатчені шлюзи, відкриті адмін-панелі	Середня	Високий	Сканування, спроби експлойтів, аномальні коди відповіді	Сегментація, ACL/геофільтр, швидкі патчі, WAF/штучні затримки
Латеральний рух після входу	Надмірні ролі, відсутність мікросегментації	Середня	Високий	Нові з’єднання до критичних сегментів, ескалація прав	Зменшення прав, мікросегментація, JIT-привілеї, запис сесій
Компрометація кінцевої точки	Відсутність EDR, застаріле ПЗ, BYOD без постури	Висока	Середній-високий	Алерти EDR, підозрілі модулі, зміни агентів	Обов’язкова постура, шифрування дисків, ізоляція, оновлення
Атаки через ланцюг постачання	Уразливі агенти/бібліотеки, слабкий контроль підписів	Середня	Високий	Нетипові оновлення, невідповідні підписи	Верифікація підписів, SBOM, контроль змін, тестування оновлень
Витоки через DNS/маршрути	Split tunneling без контролю, витік DNS	Середня	Середній	Запити до публічних резолверів, розбіжність маршрутів	Політика тунелювання, внутрішній DoH/DoT, контроль маршрутів
Виснаження доступності	DDoS на портали/шлюзи, виснаження сесій	Середня	Високий	Стрибок навантаження, падіння сесій	Захист від DDoS, autoscaling, rate-limit, резервні точки входу

З погляду зрілості процесів безпеки, вразливість часто корениться у відсутності інтегрованої моделі керування життєвим циклом доступу: від запиту прав і заснування ідентичності до їх періодичного перегляду, тимчасового підвищення та своєчасної деактивації. Неповні реєстри служб і винятків, ручні погодження без технічного відображення в системах контролю доступу, слабкі перевірки приналежності пристрою та стану безпеки призводять до ситуацій, коли формально обмежений доступ у практиці є значно ширшим [27]. Додатково, неузгодженість між політиками IT-експлуатації та інформаційної безпеки (наприклад, винятки для віддалених адміністраторів, тестових облікових записів, тимчасових тунелів для підрядників) створює «сіру зону», важкоконтрольовану моніторингом і аудитом.

Підсумовуючи, оцінка вразливостей і потенційних каналів несанкціонованого доступу у віддалених сценаріях повинна розглядатися як безперервний процес, що поєднує технічний аналіз, моделювання загроз, перевірку контролів та регулярне тестування на проникнення. Пріоритет надається усуненню помилок експозиції, впровадженню фішингостійкої автентифікації, мікросегментації доступу, підвищенню спостережуваності та автоматизації реагування. Взаємозв’язок між конфігураційною дисципліною, криптографічною гігієною, зрілістю керування ідентичностями і культурою безпеки персоналу визначає реальний рівень стійкості системи до сучасних атак на віддалений доступ.

2.3 Аналіз ефективності застосовуваних засобів автентифікації, авторизації та шифрування

Ефективність функціонування системи захисту віддаленого доступу безпосередньо залежить від надійності механізмів автентифікації, авторизації та шифрування інформації. Саме ці компоненти формують основу системи інформаційної безпеки корпоративної мережі та забезпечують контроль доступу користувачів до інформаційних ресурсів, захист конфіденційних даних і

запобігання несанкціонованому втручанню в роботу інформаційної системи. У сучасних умовах постійного зростання кількості кіберзагроз особливого значення набуває аналіз ефективності засобів захисту, які використовуються для забезпечення безпеки віддаленого доступу [28].

Автентифікація є процесом перевірки особи користувача перед наданням доступу до інформаційних ресурсів. Основним завданням механізмів автентифікації є підтвердження того, що користувач дійсно є тим, за кого себе видає. У більшості корпоративних інформаційних систем традиційно використовуються парольні механізми автентифікації, що базуються на введенні логіна та пароля. Незважаючи на простоту реалізації та широке поширення, парольна автентифікація має низку суттєвих недоліків, пов’язаних із ризиком компрометації облікових даних.

Практика свідчить, що значна кількість інцидентів інформаційної безпеки виникає саме через використання слабких або повторно застосованих паролів. Користувачі часто створюють прості паролі, які легко піддаються підбору, або використовують однакові комбінації для різних сервісів. У результаті компрометація одного облікового запису може призвести до отримання доступу до корпоративної інформаційної системи. Крім того, паролі можуть бути викрадені шляхом фішингових атак, використання шкідливого програмного забезпечення або перехоплення мережевого трафіку [29].

Для підвищення рівня безпеки сучасні корпоративні системи активно впроваджують багатофакторну автентифікацію. Multi-Factor Authentication передбачає використання декількох незалежних факторів підтвердження особи користувача. Найчастіше поєднуються пароль, одноразовий код підтвердження та мобільний пристрій або апаратний токен. Використання багатофакторної автентифікації значно підвищує ефективність захисту, оскільки навіть у випадку компрометації пароля зловмисник не може отримати доступ до системи без другого фактора підтвердження.

Ефективність багатофакторної автентифікації підтверджується практикою використання сучасних систем кіберзахисту. Застосування одноразових кодів,

push-повідомлень, біометричних методів або апаратних ключів безпеки дозволяє суттєво знизити ризик несанкціонованого доступу. Особливо ефективними вважаються апаратні токени та технології FIDO2, які забезпечують стійкість до фішингових атак та виключають передачу паролів через мережу [30].

Водночас навіть багатофакторна автентифікація не гарантує абсолютного захисту. Однією з актуальних проблем є використання методів соціальної інженерії, за допомогою яких зловмисники можуть отримати одноразові коди підтвердження або змусити користувача самостійно підтвердити авторизацію. Крім того, складність процедур автентифікації може негативно впливати на зручність роботи користувачів, що іноді призводить до нехтування вимогами безпеки.

Таблиця 2.3

Порівняльна характеристика засобів автентифікації та шифрування

ЗАСІБ ЗАХИСТУ	ПЕРЕВАГИ	НЕДОЛІКИ	РІВЕНЬ ЕФЕКТИВНОСТІ
Парольна автентифікація	Простота використання	Вразливість до фішингу та brute force	Середній
MFA	Високий рівень захисту	Складність для користувача	Високий
Біометрична автентифікація	Зручність та унікальність	Потреба спеціального обладнання	Високий
TLS/IPSec	Надійне шифрування трафіку	Вимоги до налаштування	Високий
VPN	Захищений канал зв’язку	Можливість компрометації VPN-облікових записів	Високий
Active Directory	Централізоване управління доступом	Критичність компрометації сервера	Високий

Важливим елементом системи захисту є авторизація користувачів. Авторизація визначає рівень доступу користувача до ресурсів інформаційної системи після успішного проходження автентифікації. Основною метою авторизації є забезпечення контролю над використанням інформаційних ресурсів відповідно до функціональних обов’язків працівників. Найбільш

поширеною моделлю є рольова модель управління доступом, у межах якої права користувачів визначаються відповідно до їх ролі в організації.

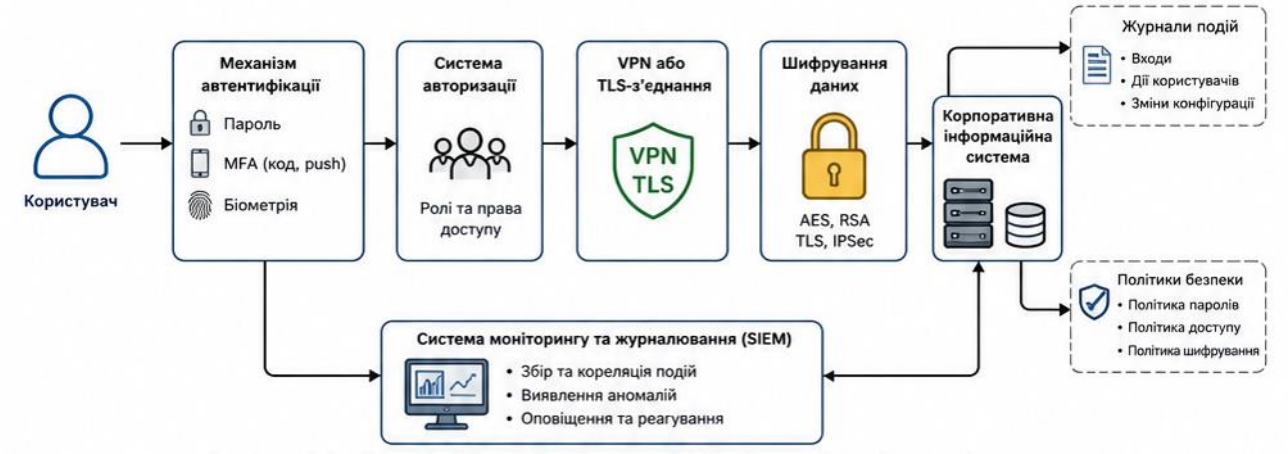

Рис. 2.3 Взаємодія механізмів автентифікації, авторизації та шифрування

Ефективність систем авторизації значною мірою залежить від правильності налаштування політик доступу та розмежування привілеїв користувачів. Надмірні права доступу є однією з найпоширеніших проблем корпоративних інформаційних систем. Якщо користувач отримує доступ до ресурсів, які не пов’язані з його професійними обов’язками, це створює додаткові ризики витоку інформації або несанкціонованих дій. У зв’язку з цим важливе значення має реалізація принципу мінімальних привілеїв, відповідно до якого користувач повинен мати лише ті права доступу, які необхідні для виконання службових функцій.

У корпоративних системах широко використовуються централізовані системи управління доступом, зокрема Active Directory та LDAP-служби. Такі системи забезпечують єдину політику автентифікації та авторизації, централізоване управління обліковими записами та контроль дій користувачів. Використання централізованих служб значно підвищує ефективність адміністрування та дозволяє оперативно реагувати на інциденти інформаційної безпеки [31].

Окрему увагу необхідно приділяти аналізу ефективності криптографічного захисту інформації. Шифрування є одним із ключових механізмів забезпечення конфіденційності даних під час їх передачі через мережу. У процесі організації

віддаленого доступу найчастіше використовуються протоколи TLS, SSL та IPSec, які забезпечують створення захищених каналів зв’язку між користувачем та корпоративною мережею.

Ефективність шифрування залежить від використаних криптографічних алгоритмів, довжини ключів та правильності реалізації механізмів управління сертифікатами. Сучасні системи безпеки використовують алгоритми AES, RSA та ECC, які забезпечують високий рівень криптографічної стійкості. Використання застарілих алгоритмів або протоколів, таких як SSL старих версій чи слабкі алгоритми хешування, створює ризик компрометації інформації та перехоплення мережевого трафіку.

Особливого значення набуває захист VPN-з’єднань, оскільки саме через VPN реалізується більшість віддалених підключень до корпоративної мережі. Аналіз сучасних VPN-рішень свідчить про те, що найбільш ефективними є протоколи IPSec та WireGuard, які використовують сучасні криптографічні алгоритми та забезпечують високий рівень продуктивності. У свою чергу використання застарілих протоколів PPTP або слабких методів шифрування значно знижує рівень інформаційної безпеки [32].

Важливим аспектом оцінювання ефективності засобів шифрування є управління криптографічними ключами. Надійність системи шифрування безпосередньо залежить від захищеності ключової інформації. У корпоративних інформаційних системах використовуються інфраструктури відкритих ключів, цифрові сертифікати та системи автоматизованого управління сертифікатами. Порушення процесу управління ключами може призвести до компрометації зашифрованих даних навіть при використанні сучасних алгоритмів шифрування.

Суттєвим фактором ефективності систем автентифікації та шифрування є рівень інтеграції засобів захисту з системами моніторингу безпеки. Сучасні системи SIEM дозволяють здійснювати аналіз спроб входу, виявляти аномальну активність користувачів та автоматично реагувати на потенційні загрози. Використання поведінкового аналізу дозволяє виявляти підозрілі спроби авторизації, нетипові місця входу або ознаки компрометації облікових записів.

Аналіз сучасних корпоративних інформаційних систем свідчить про те, що найбільш ефективними є комплексні механізми захисту, які поєднують багатофакторну автентифікацію, рольову модель доступу, сучасні криптографічні алгоритми та системи моніторингу подій безпеки. Поєднання декількох рівнів захисту дозволяє значно знизити ризик успішної реалізації кіберзагроз та забезпечити належний рівень безпеки віддаленого доступу.

Разом із тим ефективність засобів автентифікації, авторизації та шифрування значною мірою залежить від правильності їх налаштування та адміністрування. Наявність помилок конфігурації, використання застарілих протоколів, недостатній контроль доступу або відсутність регулярного оновлення програмного забезпечення можуть суттєво знизити рівень інформаційної безпеки. Саме тому забезпечення ефективного функціонування систем захисту потребує постійного аудиту безпеки, тестування вразливостей та вдосконалення політик контролю доступу [33].

Отже, аналіз ефективності застосовуваних засобів автентифікації, авторизації та шифрування показує, що сучасні корпоративні інформаційні системи потребують використання комплексних багаторівневих механізмів захисту. Найбільш ефективними є системи, які поєднують багатофакторну автентифікацію, централізоване управління доступом, сучасні криптографічні технології та автоматизований моніторинг подій безпеки. Впровадження таких механізмів дозволяє забезпечити захист корпоративних ресурсів від несанкціонованого доступу, мінімізувати ризики витоку інформації та підвищити загальний рівень кібербезпеки організації.

Висновки до розділу 2

У другому розділі було проведено аналіз існуючих механізмів та стану безпеки віддаленого доступу в корпоративних інформаційних системах. У результаті дослідження встановлено, що сучасна корпоративна інформаційна інфраструктура характеризується складною багаторівневою архітектурою, яка

включає серверні компоненти, мережеві сервіси, хмарні платформи, системи управління доступом та канали дистанційного підключення користувачів. Активне використання віддаленого доступу забезпечує гнучкість бізнес-процесів та підтримку дистанційної роботи, однак одночасно створює додаткові ризики інформаційній безпеці.

У ході аналізу архітектури корпоративної інформаційної системи та каналів віддаленого доступу було визначено основні компоненти мережевої інфраструктури, механізми взаємодії користувачів із корпоративними ресурсами та особливості функціонування VPN-з’єднань, вебсервісів і хмарних платформ. Встановлено, що найбільш уразливими елементами системи є канали передачі даних, віддалені облікові записи користувачів та кінцеві пристрої, через які здійснюється підключення до корпоративної мережі.

Оцінка вразливостей і потенційних каналів несанкціонованого доступу показала, що основними загрозами для корпоративної інформаційної системи є використання слабких механізмів автентифікації, недостатній рівень сегментації мережі, помилки конфігурації мережевого обладнання, експлуатація вразливостей програмного забезпечення та людський фактор. Значна частина ризиків пов’язана з фішинговими атаками, компрометацією облікових записів, використанням незахищених мережевих з’єднань і недостатнім контролем дій користувачів.

У результаті аналізу ефективності застосовуваних засобів автентифікації, авторизації та шифрування встановлено, що найбільш надійний рівень захисту забезпечується комплексним використанням багатофакторної автентифікації, сучасних криптографічних алгоритмів, VPN-технологій, централізованих систем управління доступом та систем моніторингу подій безпеки. Разом із тим ефективність засобів захисту значною мірою залежить від правильності їх налаштування, регулярного оновлення програмного забезпечення та дотримання політик інформаційної безпеки.

Результати проведеного аналізу свідчать про необхідність постійного вдосконалення механізмів захисту віддаленого доступу, впровадження сучасних

технологій кібербезпеки та комплексного підходу до управління ризиками інформаційної безпеки. Забезпечення надійного захисту корпоративної інформаційної системи можливе лише за умови поєднання технічних, програмних та організаційних засобів безпеки, а також постійного моніторингу стану захищеності інформаційної інфраструктури.

Розділ 3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ БЕЗПЕКИ ВІДДАЛЕНОГО ДОСТУПУ

3.1 Проєктування удосконаленої моделі безпечного віддаленого доступу

Проєктування удосконаленої моделі безпечного віддаленого доступу є одним із ключових етапів забезпечення інформаційної безпеки сучасних корпоративних інформаційних систем. У сучасних умовах цифровізації бізнес-процесів, активного використання хмарних сервісів та дистанційної роботи традиційні механізми захисту вже не забезпечують належного рівня безпеки. Постійне зростання кількості кіберзагроз, складність атак та розширення каналів віддаленого підключення вимагають створення комплексної багаторівневої моделі захисту, яка забезпечуватиме конфіденційність, цілісність і доступність інформаційних ресурсів.

Основною метою проєктування удосконаленої моделі безпечного віддаленого доступу є формування ефективної системи захисту, здатної мінімізувати ризики несанкціонованого доступу, витоку інформації, компрометації облікових записів та порушення функціонування корпоративної мережі. Така модель повинна враховувати сучасні принципи кібербезпеки, особливості функціонування корпоративної інформаційної системи, наявні загрози та вимоги до захисту інформації [34].

Процес проєктування моделі безпечного віддаленого доступу базується на принципах багаторівневого захисту, відповідно до яких система безпеки повинна складатися з декількох взаємопов’язаних рівнів контролю та захисту. Реалізація такого підходу дозволяє знизити ймовірність успішної реалізації кібератаки навіть у випадку компрометації одного з компонентів системи. Основними складовими удосконаленої моделі є механізми автентифікації та авторизації користувачів, криптографічний захист інформації, сегментація мережі,

моніторинг подій безпеки, контроль кінцевих пристроїв та системи реагування на інциденти.

Одним із ключових елементів запропонованої моделі є використання концепції Zero Trust. Даний підхід передбачає відсутність автоматичної довіри до будь-якого користувача або пристрою незалежно від місця підключення до мережі. У межах концепції Zero Trust кожна спроба доступу до інформаційних ресурсів повинна супроводжуватися перевіркою особи користувача, аналізом рівня безпеки пристрою та оцінюванням контексту підключення. Такий підхід дозволяє значно знизити ризики внутрішніх та зовнішніх загроз.

Важливою складовою удосконаленої моделі є система багатофакторної автентифікації користувачів. Запропонована модель передбачає використання щонайменше двох незалежних факторів підтвердження особи, що значно підвищує рівень захисту облікових записів. У якості факторів автентифікації можуть використовуватися паролі, одноразові коди підтвердження, мобільні додатки, біометричні параметри або апаратні ключі безпеки. Особливу ефективність забезпечує використання адаптивної автентифікації, яка враховує місце підключення користувача, тип пристрою, час входу та поведінкові характеристики [35].

Таблиця 3.1

Основні компоненти удосконаленої моделі безпечного віддаленого доступу

Компонент системи	**Призначення**	**Основні функції**
MFA	Захист облікових записів	Багатофакторна автентифікація
VPN/IPSec	Захищений канал зв’язку	Шифрування мережевого трафіку
IAM	Управління доступом	Контроль ролей та привілеїв
Firewall	Захист мережі	Фільтрація трафіку
SIEM	Моніторинг безпеки	Аналіз та кореляція подій
EDR	Захист кінцевих пристроїв	Виявлення шкідливої активності
Backup System	Відновлення даних	Резервне копіювання інформації

Удосконалена модель також передбачає централізоване управління доступом користувачів. Для цього використовуються служби каталогів та

системи Identity and Access Management, які забезпечують контроль прав доступу до корпоративних ресурсів. У межах моделі реалізується принцип мінімальних привілеїв, відповідно до якого користувач отримує лише ті права доступу, які необхідні для виконання його службових обов’язків. Такий підхід дозволяє мінімізувати ризики компрометації критичних ресурсів у випадку несанкціонованого доступу до облікового запису.

Особливу увагу у процесі проєктування приділено криптографічному захисту інформації. Для забезпечення конфіденційності даних у процесі передачі через зовнішні мережі пропонується використання VPN-з’єднань на основі сучасних криптографічних протоколів IPSec або WireGuard [36]. Передача даних здійснюється через захищені тунелі із використанням алгоритмів шифрування AES-256 та сучасних механізмів обміну криптографічними ключами. Використання надійних алгоритмів шифрування дозволяє унеможливити перехоплення або модифікацію інформації під час її передачі.

Важливим компонентом моделі є сегментація корпоративної мережі. Поділ інформаційної інфраструктури на окремі логічні сегменти дозволяє обмежити доступ користувачів до критичних ресурсів та мінімізувати ризик поширення атаки всередині мережі. У запропонованій моделі передбачається виділення окремих сегментів для серверів баз даних, систем адміністрування, користувацьких пристроїв та зовнішніх сервісів. Між сегментами реалізується контроль доступу за допомогою міжмережевих екранів та політик фільтрації мережевого трафіку.

Одним із пріоритетних напрямів удосконалення безпеки є забезпечення захисту кінцевих пристроїв користувачів. У запропонованій моделі передбачається використання систем Endpoint Detection and Response та Mobile Device Management, які забезпечують централізований контроль стану безпеки робочих станцій і мобільних пристроїв. Такі системи дозволяють виявляти шкідливу активність, контролювати встановлення програмного забезпечення, виконувати оновлення систем безпеки та блокувати скомпрометовані пристрої.

Суттєву роль у функціонуванні удосконаленої моделі відіграє система моніторингу та аналізу подій безпеки. Для забезпечення постійного контролю мережевої активності пропонується використання SIEM-систем, які забезпечують централізований збір журналів подій, кореляцію інформації та автоматичне виявлення підозрілої активності. Використання механізмів поведінкового аналізу дозволяє своєчасно виявляти аномалії, підозрілі спроби входу та ознаки компрометації облікових записів [37].

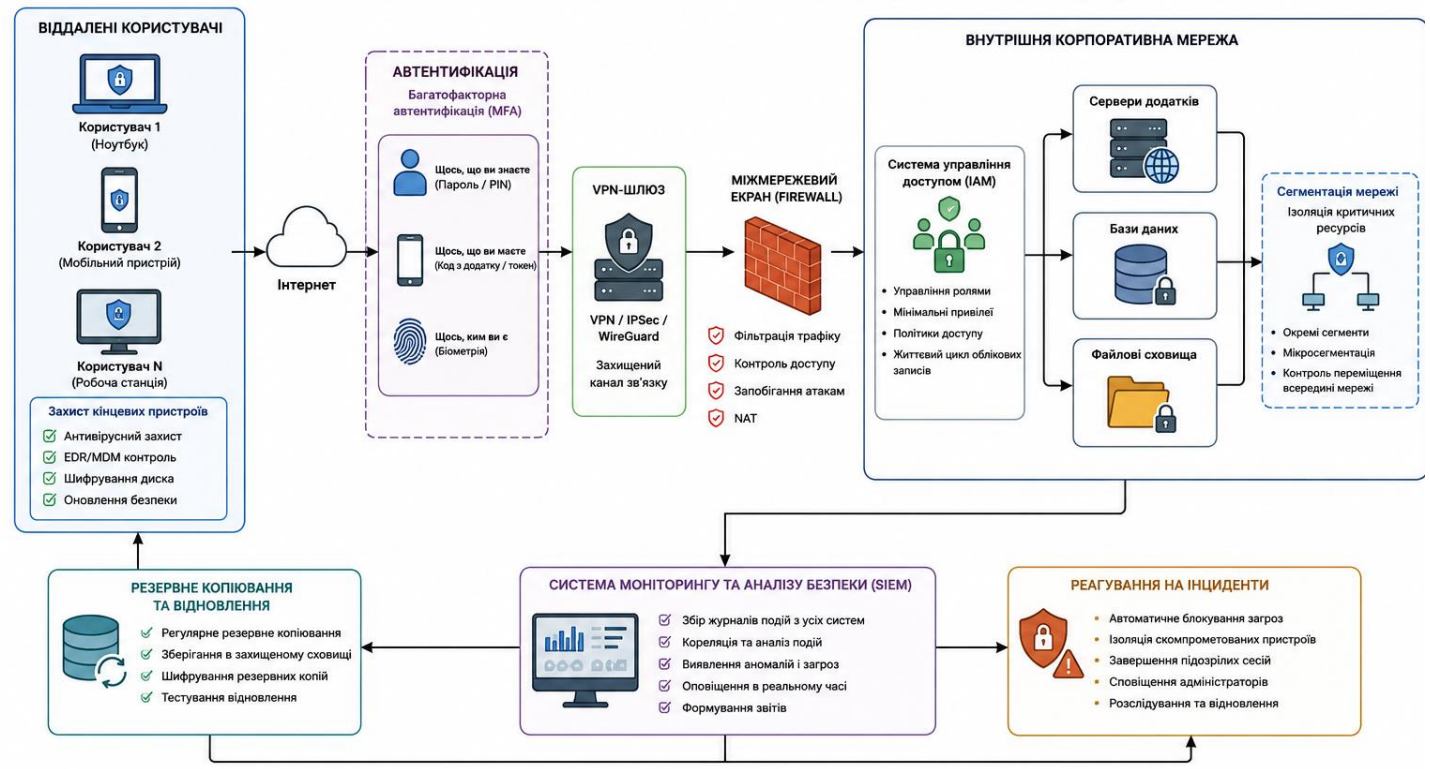

Рис. 3.1 Удосконалена модель безпечного віддаленого доступу

Важливою складовою моделі є система реагування на інциденти інформаційної безпеки. У межах проєктованої системи передбачається автоматизоване реагування на виявлені загрози, включаючи блокування підозрілих підключень, ізоляцію скомпрометованих пристроїв, примусове завершення сеансів користувачів та формування повідомлень для адміністраторів безпеки. Реалізація автоматизованих механізмів реагування дозволяє мінімізувати час між виявленням загрози та її нейтралізацією.

У процесі проєктування значна увага приділяється резервному копіюванню та відновленню інформації. Запропонована модель передбачає створення резервних копій критичних даних із використанням захищених

сховищ та регулярним тестуванням процедур відновлення. Це дозволяє забезпечити безперервність функціонування корпоративної інформаційної системи у випадку кібератак, технічних збоїв або пошкодження даних.

Ефективність функціонування удосконаленої моделі безпечного віддаленого доступу значною мірою залежить від організаційних заходів забезпечення інформаційної безпеки. У межах моделі передбачається впровадження політик безпеки, регламентів використання віддаленого доступу, процедур контролю дій користувачів та регулярного навчання персоналу. Особливе значення має підвищення рівня обізнаності працівників щодо сучасних кіберзагроз, методів соціальної інженерії та правил безпечної роботи з інформаційними ресурсами.

Запропонована модель також враховує можливість масштабування корпоративної інфраструктури та інтеграції із хмарними сервісами. У сучасних умовах значна частина організацій використовує гібридні середовища, які поєднують локальні та хмарні ресурси. Саме тому модель передбачає використання єдиної системи управління доступом, централізованого моніторингу та захищених каналів зв’язку між локальною мережею та хмарною інфраструктурою.

У результаті проєктування удосконаленої моделі безпечного віддаленого доступу формується комплексна багаторівнева система захисту, здатна забезпечити високий рівень інформаційної безпеки корпоративної мережі. Реалізація запропонованого підходу дозволяє мінімізувати ризики несанкціонованого доступу, підвищити ефективність виявлення загроз та забезпечити стабільне функціонування інформаційної інфраструктури підприємства в умовах постійного зростання кількості кіберзагроз.

3.2 Розробка практичних рекомендацій щодо впровадження сучасних засобів захисту

Розробка практичних рекомендацій щодо впровадження сучасних засобів захисту є важливим етапом удосконалення системи безпеки віддаленого доступу в корпоративних інформаційних системах. У сучасних умовах стрімкого розвитку цифрових технологій та постійного зростання кількості кіберзагроз організації потребують не лише використання окремих засобів захисту, а й формування комплексної стратегії кібербезпеки. Практичні рекомендації повинні враховувати особливості корпоративної інфраструктури, наявні ризики інформаційної безпеки, масштаби діяльності підприємства та сучасні вимоги до захисту інформаційних ресурсів.

Одним із ключових напрямів підвищення рівня безпеки є впровадження багатофакторної автентифікації для всіх користувачів, які здійснюють віддалене підключення до корпоративної мережі. Використання лише парольної автентифікації вже не забезпечує належного рівня захисту через високий ризик компрометації облікових даних. Практика свідчить, що впровадження MFA дозволяє суттєво знизити кількість успішних атак, пов’язаних із викраденням або підбором паролів [38]. Для корпоративних систем доцільним є використання мобільних додатків генерації одноразових кодів, push-підтверджень або апаратних токенів безпеки.

Важливим практичним заходом є використання сучасних VPN-рішень для організації захищених каналів зв’язку. У процесі впровадження системи віддаленого доступу рекомендується відмовитися від застарілих протоколів PPTP та L2TP без додаткового захисту на користь IPSec, SSL VPN або WireGuard. Сучасні VPN-рішення забезпечують високий рівень криптографічного захисту, підтримують сучасні алгоритми шифрування та дозволяють реалізувати централізоване управління віддаленими підключеннями [39].

Особливу увагу необхідно приділяти політикам управління доступом користувачів. Для мінімізації ризиків несанкціонованого доступу

рекомендується впровадження принципу мінімальних привілеїв. Кожен користувач повинен отримувати доступ лише до тих ресурсів, які необхідні для виконання його функціональних обов'язків. Регулярний аудит облікових записів, контроль активних сесій та своєчасне блокування невикористовуваних акаунтів дозволяють значно підвищити рівень інформаційної безпеки.

Практичні рекомендації також передбачають впровадження централізованих систем управління ідентифікацією та доступом. Використання IAM-рішень дозволяє автоматизувати процес управління обліковими записами, реалізувати єдину політику автентифікації та забезпечити контроль життєвого циклу користувачів. Централізоване управління доступом особливо важливе для великих корпоративних систем із розгалуженою структурою підрозділів та значною кількістю віддалених користувачів.

Таблиця 3.2

Практичні рекомендації щодо впровадження сучасних засобів захисту

НАПРЯМ ЗАХИСТУ	**РЕКОМЕНДОВАНИЙ ЗАСІБ**	**ОЧІКУВАНИЙ РЕЗУЛЬТАТ**
Автентифікація	MFA, FIDO2	Зниження ризику компрометації акаунтів
Захист каналів зв'язку	VPN IPSec/WireGuard	Захищена передача даних
Управління доступом	IAM, RBAC	Контроль прав користувачів
Захист пристроїв	EDR, MDM	Виявлення шкідливої активності
Моніторинг безпеки	SIEM	Виявлення інцидентів у реальному часі
Захист даних	AES-256, TLS	Захист конфіденційної інформації
Резервне копіювання	Backup System	Відновлення даних після інцидентів

Одним із найбільш важливих напрямів удосконалення системи захисту є забезпечення безпеки кінцевих пристроїв. Працівники, які використовують домашні комп'ютери або мобільні пристрої для роботи з корпоративними ресурсами, повинні дотримуватися встановлених вимог безпеки. Для цього рекомендується використовувати системи Endpoint Detection and Response,

антивірусне програмне забезпечення, засоби шифрування локальних носіїв інформації та системи централізованого оновлення програмного забезпечення. Додатково доцільно впроваджувати політики контролю пристроїв, які обмежують підключення незареєстрованого або небезпечного обладнання до корпоративної мережі [40].

Суттєве значення має впровадження систем моніторингу та аналізу подій безпеки. Використання SIEM-платформ дозволяє забезпечити централізований збір журналів подій, аналіз мережевої активності та автоматичне виявлення аномалій. У межах практичних рекомендацій доцільно передбачити налаштування автоматизованих механізмів реагування на інциденти безпеки, які забезпечують оперативне блокування підозрілих підключень або ізоляцію скомпрометованих пристроїв.

Важливим практичним заходом є регулярне оновлення програмного забезпечення та управління вразливостями. Значна кількість кібератак пов’язана з експлуатацією відомих вразливостей, для яких вже існують оновлення безпеки. Рекомендується впровадження централізованої системи управління оновленнями, яка забезпечуватиме автоматичне встановлення критичних патчів для операційних систем, серверів, мережевого обладнання та прикладного програмного забезпечення.

Для забезпечення стійкості інформаційної системи до кібератак доцільно впроваджувати сегментацію мережі. Поділ корпоративної інфраструктури на окремі сегменти дозволяє обмежити переміщення зловмисника у випадку компрометації одного з компонентів системи. Рекомендується виділення окремих сегментів для серверів баз даних, адміністративних систем, користувацьких пристроїв та зовнішніх сервісів. Контроль взаємодії між сегментами повинен здійснюватися за допомогою міжмережевих екранів та політик фільтрації трафіку [41].

Практичні рекомендації також передбачають використання сучасних криптографічних засобів захисту інформації. Передача даних через мережу повинна здійснюватися виключно із використанням захищених протоколів TLS

або IPSec. Для шифрування конфіденційної інформації рекомендується застосування алгоритмів AES-256 та сучасних механізмів управління криптографічними ключами. Окрему увагу необхідно приділяти захисту резервних копій та криптографічному захисту даних, що зберігаються на мобільних пристроях.

Важливим складником системи захисту є формування політики резервного копіювання та відновлення даних. Практика свідчить, що наявність актуальних резервних копій дозволяє мінімізувати наслідки ransomware-атак та інших інцидентів інформаційної безпеки. Рекомендується створення декількох копій критичних даних із їх зберіганням у захищених локальних або хмарних сховищах. Крім того, необхідно регулярно тестувати процедури відновлення інформації для перевірки працездатності систем резервного копіювання.

Одним із найважливіших напрямів забезпечення безпеки є підвищення рівня обізнаності персоналу у сфері кібербезпеки. Людський фактор залишається однією з основних причин успішної реалізації кібератак, тому працівники повинні регулярно проходити навчання щодо безпечного використання корпоративних ресурсів. Рекомендується проведення тренінгів із протидії фішинговим атакам, правил використання віддаленого доступу, захисту облікових записів та виявлення підозрілої активності.

Важливою рекомендацією є впровадження політик інформаційної безпеки та регламентів використання віддаленого доступу. Такі документи повинні визначати порядок підключення до корпоративної мережі, вимоги до паролів, правила використання особистих пристроїв, процедури реагування на інциденти та відповідальність користувачів за порушення вимог безпеки. Наявність чітких регламентів дозволяє стандартизувати процеси забезпечення безпеки та мінімізувати ризики, пов’язані з людським фактором.

Сучасні умови функціонування корпоративних інформаційних систем також вимагають використання концепції Zero Trust. Практичне впровадження даного підходу передбачає постійну перевірку користувачів та пристроїв, контроль кожної спроби доступу до ресурсів і використання адаптивних

механізмів автентифікації [42]. Реалізація концепції нульової довіри дозволяє суттєво підвищити рівень захисту корпоративної мережі від внутрішніх та зовнішніх загроз.

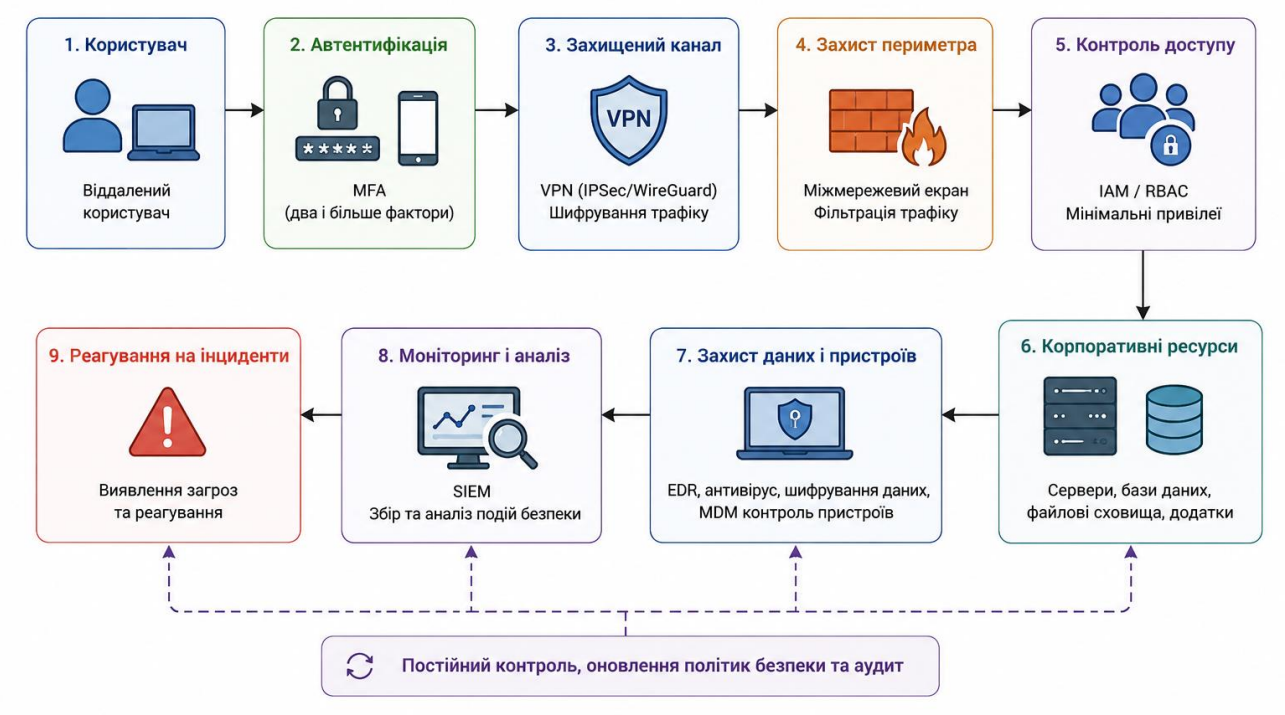

Рис. 3.2 Практична модель впровадження сучасних засобів захисту віддаленого доступу

Важливим елементом практичних рекомендацій є проведення регулярного аудиту інформаційної безпеки та тестування системи захисту. Періодичне виконання аналізу вразливостей, тестування на проникнення та оцінювання ефективності засобів захисту дозволяє своєчасно виявляти слабкі місця системи та вдосконалювати механізми безпеки. Крім того, аудит дозволяє перевірити відповідність корпоративної системи сучасним стандартам інформаційної безпеки.

Отже, розроблені практичні рекомендації щодо впровадження сучасних засобів захисту спрямовані на формування комплексної системи безпеки віддаленого доступу, яка поєднує сучасні технічні рішення, організаційні заходи та механізми контролю інформаційної безпеки. Реалізація запропонованих рекомендацій дозволить підвищити рівень захищеності корпоративної інформаційної системи, мінімізувати ризики несанкціонованого доступу та

забезпечити стабільне функціонування інформаційної інфраструктури в умовах сучасних кіберзагроз.

3.3 Оцінка ефективності запропонованих заходів та їх вплив на рівень інформаційної безпеки

Оцінка ефективності запропонованих заходів щодо підвищення безпеки віддаленого доступу є важливим етапом визначення результативності впроваджених механізмів захисту та їх впливу на загальний рівень інформаційної безпеки корпоративної інформаційної системи. У сучасних умовах постійного зростання кількості кіберзагроз організації потребують не лише впровадження сучасних технологій захисту, а й систематичного аналізу ефективності функціонування засобів безпеки. Такий підхід дозволяє своєчасно виявляти недоліки системи захисту, оцінювати рівень ризиків та визначати напрями подальшого вдосконалення інформаційної інфраструктури.

Ефективність запропонованих заходів визначається рівнем зниження ймовірності реалізації кіберзагроз, скороченням кількості інцидентів інформаційної безпеки та підвищенням стійкості корпоративної мережі до зовнішніх і внутрішніх атак. Основними критеріями оцінювання є надійність механізмів автентифікації, ефективність контролю доступу, рівень захищеності каналів передачі даних, швидкість виявлення інцидентів та здатність системи забезпечувати безперервність функціонування інформаційних ресурсів.

Одним із найбільш результативних заходів є впровадження багатофакторної автентифікації. Використання MFA дозволяє суттєво знизити ризик несанкціонованого доступу до корпоративної мережі навіть у випадку компрометації пароля користувача. Аналіз сучасних систем кібербезпеки свідчить про те, що багатофакторна автентифікація значно ускладнює реалізацію фішингових атак, атак типу brute force та спроб використання викрадених облікових даних. Крім того, використання адаптивної автентифікації дозволяє

підвищити рівень контролю підозрілої активності та оперативно реагувати на спроби несанкціонованого входу.

Суттєвий вплив на підвищення рівня інформаційної безпеки має використання сучасних VPN-технологій та криптографічного захисту даних. Застосування VPN-з'єднань на основі IPSec або WireGuard забезпечує конфіденційність мережевого трафіку та захист інформації від перехоплення під час передачі через відкриті мережі. Використання сучасних алгоритмів шифрування дозволяє мінімізувати ризики компрометації інформації та забезпечити захист корпоративних ресурсів навіть у випадку використання незахищених каналів зв'язку.

Ефективність запропонованої моделі значною мірою забезпечується впровадженням централізованого управління доступом користувачів. Використання IAM-систем дозволяє автоматизувати процес адміністрування облікових записів, контролювати життєвий цикл користувачів та реалізувати принцип мінімальних привілеїв [43]. У результаті суттєво знижується ризик несанкціонованого доступу до критичних ресурсів та мінімізуються наслідки компрометації окремих облікових записів.

Важливим результатом реалізації запропонованих заходів є підвищення рівня захисту кінцевих пристроїв користувачів. Використання систем Endpoint Detection and Response, антивірусного програмного забезпечення та централізованого управління мобільними пристроями дозволяє своєчасно виявляти шкідливу активність, блокувати потенційно небезпечні процеси та контролювати відповідність пристроїв вимогам інформаційної безпеки. Це суттєво знижує ризик проникнення шкідливого програмного забезпечення до корпоративної мережі через віддалені робочі станції користувачів.

Суттєвий позитивний вплив на рівень інформаційної безпеки має впровадження систем моніторингу та аналізу подій безпеки. Використання SIEM-рішень забезпечує централізований збір журналів подій, автоматичне виявлення аномальної активності та оперативне реагування на інциденти безпеки. Завдяки кореляції подій система здатна виявляти складні атаки, які

неможливо визначити під час аналізу окремих подій. Крім того, використання автоматизованих механізмів реагування дозволяє мінімізувати час між виявленням загрози та її локалізацією.

Таблиця 3.3

Оцінка ефективності запропонованих заходів безпеки

Захід безпеки	Вплив на безпеку	Результат впровадження
MFA	Захист облікових записів	Зменшення ризику компрометації
VPN IPSec/WireGuard	Захист каналів передачі	Захищений обмін даними
IAM/RBAC	Контроль доступу	Мінімізація надмірних привілеїв
SIEM	Моніторинг інцидентів	Швидке виявлення загроз
EDR/MDM	Захист кінцевих пристроїв	Виявлення шкідливого ПЗ
Сегментація мережі	Локалізація атак	Обмеження поширення загроз
Backup System	Відновлення інформації	Забезпечення безперервності роботи

Ефективність запропонованих заходів також проявляється у підвищенні стійкості корпоративної мережі до внутрішніх загроз. Реалізація принципу Zero Trust забезпечує постійний контроль дій користувачів та перевірку кожного запиту на доступ до інформаційних ресурсів. Такий підхід дозволяє мінімізувати ризики, пов’язані з компрометацією облікових записів або несанкціонованими діями внутрішніх користувачів.

Значний вплив на загальний рівень безпеки має сегментація мережевої інфраструктури. Поділ корпоративної мережі на окремі логічні сегменти дозволяє локалізувати потенційні інциденти безпеки та обмежити поширення атаки всередині системи. У результаті навіть у випадку компрометації одного із сегментів ризик доступу до критичних ресурсів залишається мінімальним.

Важливим показником ефективності системи захисту є здатність забезпечувати безперервність функціонування інформаційної системи. Запропоновані заходи резервного копіювання та відновлення даних дозволяють мінімізувати наслідки кібератак, технічних збоїв або втрати інформації. Наявність актуальних резервних копій забезпечує можливість швидкого

відновлення працездатності корпоративної мережі та знижує ризик тривалого простою інформаційної системи.

Практичне впровадження запропонованих заходів також позитивно впливає на рівень керованості інформаційної інфраструктури. Централізовані системи моніторингу, управління доступом та контролю безпеки дозволяють адміністраторам оперативно отримувати інформацію про стан захищеності системи, виявляти слабкі місця та своєчасно реагувати на потенційні загрози. Це підвищує ефективність управління інформаційною безпекою та дозволяє забезпечити відповідність корпоративної інфраструктури сучасним вимогам кіберзахисту.

Суттєве значення для оцінювання ефективності має аналіз економічної доцільності впровадження сучасних засобів захисту. Незважаючи на необхідність фінансових витрат на впровадження систем MFA, VPN, SIEM або EDR, використання таких технологій дозволяє значно знизити потенційні збитки від витоку інформації, порушення функціонування бізнес-процесів або реалізації кібератак [44]. У довгостроковій перспективі інвестиції у засоби інформаційної безпеки забезпечують підвищення надійності корпоративної інфраструктури та стабільності функціонування організації.

Важливим аспектом оцінювання є також підвищення рівня обізнаності персоналу у сфері кібербезпеки. Регулярне проведення навчань, тестування працівників та впровадження політик інформаційної безпеки дозволяє знизити ризики, пов’язані з людським фактором. Працівники починають більш відповідально ставитися до захисту облікових записів, правил використання корпоративних ресурсів та виявлення потенційних загроз.

Разом із тим оцінка ефективності запропонованих заходів показує, що жодна система захисту не може гарантувати абсолютну безпеку інформаційної інфраструктури. Постійний розвиток кіберзагроз, поява нових методів атак та ускладнення технологій вимагають безперервного вдосконалення системи захисту. Саме тому важливим елементом забезпечення інформаційної безпеки є

регулярний аудит системи, аналіз вразливостей та адаптація політик безпеки до сучасних умов функціонування корпоративної мережі.

Отже, оцінка ефективності запропонованих заходів свідчить про доцільність впровадження комплексної багаторівневої системи захисту віддаленого доступу. Використання сучасних механізмів автентифікації, криптографічного захисту, моніторингу подій безпеки та контролю доступу дозволяє суттєво підвищити рівень інформаційної безпеки корпоративної інформаційної системи, мінімізувати ризики несанкціонованого доступу та забезпечити стабільне функціонування інформаційної інфраструктури в умовах сучасних кіберзагроз.

Висновки до розділу 3

У третьому розділі було розроблено та обґрунтовано методи підвищення безпеки віддаленого доступу до корпоративних інформаційних систем. У результаті дослідження сформовано удосконалену модель безпечного віддаленого доступу, яка базується на принципах багаторівневого захисту, концепції Zero Trust та комплексному використанні сучасних засобів інформаційної безпеки.

У межах розділу було запропоновано практичні рекомендації щодо впровадження багатофакторної автентифікації, VPN-технологій, систем централізованого управління доступом, моніторингу подій безпеки, захисту кінцевих пристроїв та резервного копіювання інформації. Визначено, що використання комплексного підходу до організації захисту дозволяє мінімізувати ризики несанкціонованого доступу, підвищити рівень контролю інформаційної інфраструктури та забезпечити стабільне функціонування корпоративної мережі.

Проведена оцінка ефективності запропонованих заходів підтвердила, що їх впровадження сприяє суттєвому підвищенню рівня інформаційної безпеки, зменшенню ймовірності реалізації кіберзагроз, покращенню захищеності каналів

віддаленого доступу та підвищенню стійкості корпоративної інформаційної системи до сучасних кібератак. Таким чином, запропоновані рішення можуть бути ефективно використані для вдосконалення системи управління безпекою віддаленого доступу в сучасних корпоративних інформаційних системах.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено методи управління безпекою віддаленого доступу до корпоративних інформаційних систем, проаналізовано сучасний стан захищеності віддалених підключень, визначено основні загрози інформаційній безпеці та розроблено комплекс заходів щодо підвищення рівня захисту корпоративної мережевої інфраструктури. Актуальність теми дослідження обумовлена стрімким розвитком цифрових технологій, активним використанням дистанційної роботи, хмарних сервісів та розширенням кількості користувачів, які здійснюють доступ до корпоративних ресурсів через зовнішні канали зв’язку.

У першому розділі роботи було розглянуто теоретичні основи організації та забезпечення безпеки віддаленого доступу. У процесі дослідження визначено сутність поняття віддаленого доступу та його роль у сучасних корпоративних інформаційних системах. Встановлено, що віддалений доступ є важливим компонентом сучасної інформаційної інфраструктури, який забезпечує гнучкість бізнес-процесів, мобільність працівників та ефективну взаємодію користувачів із корпоративними ресурсами незалежно від їх місцезнаходження. Разом із тим використання дистанційних каналів зв’язку створює додаткові ризики інформаційній безпеці та потребує впровадження комплексних механізмів захисту.

У ході аналізу основних загроз і ризиків безпеки при віддаленому підключенні було встановлено, що найбільшу небезпеку становлять несанкціонований доступ до інформаційних ресурсів, фішингові атаки, шкідливе програмне забезпечення, перехоплення мережевого трафіку, експлуатація вразливостей програмного забезпечення та людський фактор. Доведено, що сучасні кіберзагрози характеризуються високим рівнем автоматизації та складністю реалізації, що вимагає використання сучасних технологій захисту інформації.

Також у першому розділі було проаналізовано основні методи та технології забезпечення безпеки віддаленого доступу. Визначено, що ефективний захист корпоративної інформаційної системи повинен базуватися на комплексному використанні криптографічного захисту інформації, багатофакторної автентифікації, систем контролю доступу, міжмережевих екранів, засобів моніторингу безпеки та технологій захисту кінцевих пристроїв. Особливу увагу приділено концепції Zero Trust, яка передбачає постійний контроль кожного запиту на доступ до інформаційних ресурсів незалежно від місця підключення користувача.

У другому розділі роботи проведено аналіз існуючих механізмів та стану безпеки віддаленого доступу в корпоративних інформаційних системах. У результаті дослідження архітектури корпоративної інформаційної системи та каналів віддаленого доступу визначено основні компоненти мережевої інфраструктури, особливості функціонування VPN-з’єднань, вебсервісів та хмарних платформ. Встановлено, що найбільш уразливими елементами системи є канали передачі даних, кінцеві пристрої користувачів та механізми автентифікації.

Оцінка вразливостей і потенційних каналів несанкціонованого доступу дозволила виявити основні проблеми забезпечення інформаційної безпеки корпоративної мережі. Серед них визначено використання слабких паролів, недостатній рівень сегментації мережі, помилки конфігурації мережевого обладнання, відсутність постійного моніторингу подій безпеки та використання застарілих протоколів зв’язку. Доведено, що значна кількість інцидентів інформаційної безпеки виникає через людський фактор та недостатній рівень контролю доступу користувачів.

У межах аналізу ефективності застосовуваних засобів автентифікації, авторизації та шифрування встановлено, що найбільш ефективними є багаторівневі механізми захисту, які поєднують багатофакторну автентифікацію, сучасні криптографічні алгоритми, централізоване управління доступом та автоматизовані системи моніторингу безпеки. Разом із тим визначено, що

ефективність систем захисту значною мірою залежить від правильності їх налаштування, регулярного оновлення та дотримання політик інформаційної безпеки.

У третьому розділі роботи було розроблено та обґрунтовано методи підвищення безпеки віддаленого доступу до корпоративних інформаційних систем. У процесі проєктування удосконаленої моделі безпечного віддаленого доступу сформовано комплексну багаторівневу систему захисту, яка включає механізми багатофакторної автентифікації, VPN-захист, сегментацію мережі, системи моніторингу та аналізу подій безпеки, централізоване управління доступом і засоби захисту кінцевих пристроїв. Запропонована модель базується на принципах Zero Trust та забезпечує постійний контроль доступу до корпоративних ресурсів.

У межах розробки практичних рекомендацій щодо впровадження сучасних засобів захисту запропоновано використання MFA, VPN IPSec/WireGuard, SIEM-систем, EDR-рішень, IAM-платформ та систем резервного копіювання даних. Розроблені рекомендації спрямовані на мінімізацію ризиків несанкціонованого доступу, підвищення ефективності виявлення кіберзагроз та забезпечення безперервності функціонування корпоративної інформаційної системи.

Оцінка ефективності запропонованих заходів показала, що їх впровадження дозволяє суттєво підвищити рівень інформаційної безпеки корпоративної мережі, знизити ймовірність реалізації кібератак, забезпечити захист конфіденційної інформації та мінімізувати наслідки потенційних інцидентів безпеки. Доведено, що використання комплексного підходу до захисту віддаленого доступу забезпечує підвищення стійкості інформаційної системи до сучасних кіберзагроз та сприяє ефективному управлінню ризиками інформаційної безпеки.

Отже, поставлену мету кваліфікаційної роботи досягнуто, а визначені завдання виконано у повному обсязі. Результати проведеного дослідження підтверджують необхідність впровадження сучасних багаторівневих механізмів захисту віддаленого доступу та постійного вдосконалення систем управління

інформаційною безпекою відповідно до сучасних умов розвитку корпоративних інформаційних технологій і кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994 р. URL: zakon.rada.gov.ua/laws/show/80/94-вр

2. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. URL: zakon.rada.gov.ua/laws/show/2163-19

3. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023.

4. ДСТУ ISO/IEC 27002:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи інформаційної безпеки. Київ : ДП «УкрНДНЦ», 2024.

5. Stallings W. Cryptography and Network Security : Principles and Practice. 8th ed. Hoboken : Pearson, 2023. 880 p. URL: pearson.com/cryptography-and-network-security

6. Stallings W. Network Security Essentials : Applications and Standards. 7th ed. Hoboken : Pearson, 2021. 784 p. URL: pearson.com/network-security-essentials

7. Schneier B. Applied Cryptography : Protocols, Algorithms, and Source Code in C. Indianapolis : Wiley, 2015. 784 p. URL: wiley.com/applied-cryptography

8. Bishop M. Computer Security : Art and Science. 2nd ed. Boston : Addison-Wesley, 2018. 1184 p. URL: pearson.com/computer-security-art-and-science

9. Whitman M., Mattord H. Principles of Information Security. 7th ed. Boston : Cengage Learning, 2022. 656 p. URL: cengage.com/principles-of-information-security

10. Andress J. The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice. 3rd ed. Amsterdam : Elsevier, 2021. 288 p. DOI: 10.1016/C2019-0-03715-6

11. Harris S. CISSP All-in-One Exam Guide. 9th ed. New York : McGraw-Hill Education, 2021. 1456 p. URL: mheducation.com/cissp-all-in-one-exam-guide

12. Kizza J. M. Guide to Computer Network Security. 5th ed. Cham : Springer, 2020. 622 p. DOI: 10.1007/978-3-030-38141-7

13. Goodrich M. T., Tamassia R. Introduction to Computer Security. 2nd ed. Boston : Pearson, 2020. 544 p. URL: pearson.com/introduction-to-computer-security

14. Easttom C. Network Defense and Countermeasures. 3rd ed. Burlington : Jones & Bartlett Learning, 2022. 520 p

15. Kim D., Solomon M. Fundamentals of Information Systems Security. 4th ed. Burlington : Jones & Bartlett Learning, 2023. 650 p.

16. NIST Special Publication 800-46 Rev. 2. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. Gaithersburg : National Institute of Standards and Technology, 2020. URL: csrc.nist.gov/sp800-46r2

17. NIST Special Publication 800-63B. Digital Identity Guidelines : Authentication and Lifecycle Management. Gaithersburg : National Institute of Standards and Technology, 2023. URL: csrc.nist.gov/sp800-63b

18. NIST Special Publication 800-207. Zero Trust Architecture. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207

19. Cisco Systems. Cisco Secure Remote Access Design Guide. San Jose : Cisco Press, 2022. URL: cisco.com/secure-remote-access

20. VMware. Secure Remote Access Architecture Guide. Palo Alto : VMware Documentation, 2021. URL: docs.vmware.com/secure-remote-access

21. Microsoft Corporation. Microsoft Security Best Practices for Remote Work. Redmond : Microsoft Press, 2021. URL: learn.microsoft.com/security-remote-work

22. European Union Agency for Cybersecurity (ENISA). Remote Working Security Guidelines. Athens : ENISA, 2021. URL: enisa.europa.eu/remote-working-security-guidelines

23. Peltier T. Information Security Policies, Procedures, and Standards : Guidelines for Effective Information Security Management. Boca Raton : CRC Press, 2016. URL: routledge.com/information-security-policies-procedures-and-standards

24. Grimes R. A Data-Driven Computer Security Defense. Indianapolis : Wiley, 2017. URL: wiley.com/data-driven-computer-security-defense

25. Cisco Systems. Zero Trust Security Solution for Hybrid Work. San Jose : Cisco Systems, 2022. URL: cisco.com/zero-trust-hybrid-work

26. Palo Alto Networks. Zero Trust Security For the Hybrid Workforce. Santa Clara : Palo Alto Networks, 2022. URL: paloaltonetworks.com/zero-trust-hybrid-workforce

27. OWASP Foundation. OWASP Top 10 : The Ten Most Critical Web Application Security Risks. 2021. URL: owasp.org/www-project-top-ten

28. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force, 2018. DOI: 10.17487/RFC8446

29. RFC 4301. Security Architecture for the Internet Protocol. Internet Engineering Task Force, 2005. DOI: 10.17487/RFC4301

30. RFC 7296. Internet Key Exchange Protocol Version 2 (IKEv2). Internet Engineering Task Force, 2014. DOI: 10.17487/RFC7296

31. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. Gaithersburg : NIST, 2020. DOI: 10.6028/NIST.SP.800-207

32. Scarfone K., Souppaya M. Guide to Enterprise Telework and Remote Access Security. Gaithersburg : NIST, 2020. URL: nist.gov/telework-remote-access-security

33. Alshamrani A., Myneni S., Chowdhary A., Huang D. A Survey on Advanced Persistent Threats : Techniques, Solutions, Challenges, and Research Opportunities // IEEE Communications Surveys & Tutorials. 2019. Vol. 21, No. 2. P. 1851–1877. DOI: 10.1109/COMST.2019.2891891

34. Ahmad Z., Shahid Khan A., Wai Shiang C., Abdullah J., Ahmad F. Network Intrusion Detection System : A Systematic Study of Machine Learning and

Deep Learning Approaches // Transactions on Emerging Telecommunications Technologies. 2021. Vol. 32, No. 1. DOI: 10.1002/ett.4150

35. Tankard C. Advanced Persistent Threats and How to Monitor and Deter Them // Network Security. 2011. Vol. 2011, No. 8. P. 16–19. DOI: 10.1016/S1353-4858(11)70086-1

36. Allah Rakha N. Ensuring cyber-security in remote workforce: legal implications and international best practices. *International journal of law and policy*. 2023. Vol. 1, no. 3. URL: https://doi.org/10.59022/ijlp.43

37. Cybersecurity problems in organizations with remote work. *Modern information security*. 2025. Vol. 62, no. 2. URL: https://doi.org/10.31673/2409-7292.2025.020383

38. Garzia F., Sammarco E., Cusani R. Integrated access control system for ports. *Safe 2009*, Rome, Italy, 1–3 July 2009. Southampton, UK, 2009. URL: https://doi.org/10.2495/safe090301

39. Mistry H. K. Developing secure remote access: a policy framework for european organizations. *European journal of information technologies and computer science*. 2025. Vol. 5, no. 5. P. 1–6. URL: https://doi.org/10.24018/compute.2025.5.5.10123

40. Pagliusi P. S. Internet authentication for remote access : thesis. 2008. URL: http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.500040

41. Remote access authentication. *Complete book of remote access*. 2002. P. 213–224. URL: https://doi.org/10.1201/9781420000429-24

42. Security in remote access, based on zero trust model concepts and SSH authentication with signed certificates / C.-R. Iță et al. *Advanced topics in optoelectronics, microelectronics, and nanotechnologies XI*, Constanta, Romania, 25–28 August 2022 / ed. by M. Vladescu, I. Cristea, R. D. Tamas. 2023. URL: https://doi.org/10.1117/12.2643058

43. Seema K. BeyondTrust's password safe, privileged remote access, remote support, identity security insights, pathfinder overview. *International journal of*

innovative research and creative technology. 2025. Vol. 11, no. 3. P. 1–13. URL: https://doi.org/10.5281/zenodo.15437309

44. Zewdie T. G. Usable security case of remote web access. *Communications in computer and information science*. Cham, 2020. P. 491–501. URL: https://doi.org/10.1007/978-3-030-60700-5_62