

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут комп'ютерних наук та управління проєктами
Кафедра інформаційних управляючих систем та технологій

"Допущений до захисту"

Завідувач кафедри ІУСТ



к.т.н, доц. Михелєв І.Л.

" ____ " _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти "магістр"

**на тему: Дослідження та розробка підсистеми безпечного віддаленого
доступу до корпоративної інформаційної системи**

Виконав: студент групи 6144 мз

 **Шумейко С.Л.**
(підпис)

Керівник роботи:

доцент кафедри ІУСТ, к.т.н.,
(посада, науковий ступінь вчене звання)

 **Михелєв І.Л.**
(підпис)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут комп'ютерних наук та управління проєктами
Кафедра інформаційних управляючих систем та технологій
Спеціальність 126 "Інформаційні системи та технології"
Освітня програма "Інформаційні системи та технології"

"ЗАТВЕРДЖУЮ"

Гарант освітньої програми

к.т.н, доц. Чернова Лб.С.

"_____" "_____" 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ на здобуття ступеня вищої освіти "магістр"

Студенту Шумейку Сергію Леонідовичу

(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження та розробка підсистеми безпечного віддаленого доступу до корпоративної інформаційної систем

Керівник роботи к.т.н., доцент Михелєв І.Л.

Затверджені наказом ректора № 1355-уч. від "14" листопада 2025 року.

2. Термін подання роботи: 15 грудня 2025 р.

3. Вихідні дані до проєкту (роботи) ДСТУ щодо обробки інформації, літературні джерела, технічна документація на існуючі аналоги систем, матеріали наукового стажування

4. Перелік питань, що належать до розробки (найменування розділів)

Дослідження підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи. Проєктування інформаційної підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи. Розробка інформаційної підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи. Техніко-економічне обґрунтування розробки. Охорона праці. Охорона навколишнього середовища

5. Перелік презентаційних матеріалів Недоліки роботи, постановка задачі, задачі дослідження, концепція підсистем безпечного віддаленого доступу до корпоративної інформаційної системи, Діаграма варіантів використання, Концептуальна модель даних, Діаграма послідовності, Фізичну структуру бази даних системи, Схема взаємодії модулів програмного забезпечення системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Михелєв І.Л., доцент	05.09.2024	22.12.2024
2	Михелєв І.Л., доцент	23.12.2024	15.06.2025
3	Михелєв І.Л., доцент	15.06.2025	25.09.2025
4	Михелєв І.Л., доцент	25.09.2025	14.11.2025
5	Михелєв І.Л., доцент	25.09.2025	14.11.2025
6	Михелєв І.Л., доцент	25.09.2025	14.11.2025

7. Дата видачі завдання 05 вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів роботи	Примітка
1	Дослідження та аналіз предметної галузі	22.12.2024	
2	Розробка концепції	15.03.2025	
3	Розділ з розробки проєктних рішень по системі (та її частинах)	15.06.2025	
4	Реалізація проєкту та розробка робочої документації	25.09.2025	
5	Обчислення економічної ефективності	14.11.2025	
6	Вирішення питань охорони праці та навколишнього середовища	14.11.2025	
7	Оформлення пояснювальної записки	14.11.2025	
8	Подання магістерської роботи на перевірку на плагіат	16.11.2025	
9	Подання магістерської роботи рецензенту	20.11.2025	
10	Подання магістерської роботи на державний захист	15.12.2025	

Студент


(підпис)

Шумейко С.Л.
(ПІБ)

Керівник роботи


(підпис)

Михелєв І.Л.
(ПІБ)

Анотація

У магістерській роботі проведено дослідження та розробку підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи. Проаналізовано сучасні загрози інформаційній безпеці, зокрема несанкціонований доступ, перехоплення даних, атаки типу «людина посередині» та компрометацію облікових записів. Виконано огляд існуючих технологій та протоколів захисту, зокрема VPN, SSL/TLS, багатофакторної автентифікації, систем управління ідентифікацією та доступом (IAM), а також механізмів контролю доступу на основі ролей (RBAC).

У роботі сформовано вимоги до підсистеми безпечного віддаленого доступу з урахуванням принципів конфіденційності, цілісності та доступності інформації. Запропоновано архітектуру підсистеми, що включає модулі автентифікації, авторизації, шифрування трафіку, журналювання подій та моніторингу безпеки. Реалізовано прототип підсистеми та проведено тестування її ефективності, продуктивності та стійкості до типових кіберзагроз. Отримані результати підтверджують доцільність впровадження розробленого рішення для підвищення рівня захисту корпоративної інформаційної інфраструктури.

Робота представлена у вигляді 75 сторінок машинного тексту, що має у своєму складі 16 рисунків, 13 таблиць і 3 додатків та список з 15 використаних джерел.

Ключові слова: інформаційна безпека, віддалений доступ, корпоративна інформаційна система, автентифікація, авторизація, VPN, шифрування, багатофакторна автентифікація, IAM, RBAC, кіберзагрози.

Abstract

The master's thesis is devoted to the research and development of a secure remote access subsystem for a corporate information system. Modern information security threats are analyzed, including unauthorized access, data interception, man-in-the-middle attacks, and credential compromise. A review of existing security technologies and protocols is conducted, including VPN, SSL/TLS, multi-factor authentication, Identity and Access Management (IAM) systems, and Role-Based Access Control (RBAC) mechanisms.

The thesis defines the functional and security requirements for the secure remote access subsystem based on the principles of confidentiality, integrity, and availability. A subsystem architecture is proposed, incorporating authentication, authorization, traffic encryption, logging, and security monitoring modules. A prototype of the subsystem is implemented and evaluated in terms of efficiency, performance, and resistance to common cyber threats. The obtained results demonstrate the feasibility and effectiveness of the proposed solution for enhancing the security level of corporate information infrastructure.

The work is presented in the form of 75 pages of typewritten text, which includes 16 figures, 13 tables, 3 appendices, and a list of 15 sources used.

Keywords: information security, remote access, corporate information system, authentication, authorization, VPN, encryption, multi-factor authentication, IAM, RBAC, cybersecurity threats.

ЗМІСТ

ВСТУП.....	10
РОЗДІЛ 1. ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПІДСИСТЕМИ БЕЗПЕЧНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ.....	12
1.1 Аналіз існуючих підсистем безпечного віддаленого доступу до корпоративної інформаційної системи	12
1.2 Формування вимог до підсистеми віддаленого доступу до інформаційної системи	14
1.2.1 Характеристика підсистеми віддаленого доступу до інформаційної системи ПТУ	17
1.2.2 Цілі, критерії й обмеження створення інформаційної підсистеми віддаленого доступу до інформаційної системи ПТУ	17
1.2.3 Функції та задачі підсистеми віддаленого доступу до системи ПТУ.....	17
1.3 Розробка концепції підсистеми віддаленого доступу до інформаційної системи ПТУ	18
1.3.1 Опис результатів вивчення підсистеми віддаленого доступу до інформаційної системи ПТУ	18
1.3.2 Аналіз вимог до підсистеми віддаленого доступу до інформаційної системи ПТУ	18
1.3.3 Розробка варіантів концепції підсистеми віддаленого доступу до інформаційної системи ПТУ	19
1.4 Концепція підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи	22
1.4.1 Вимоги, що впливають на якість підсистеми віддаленого доступу до інформаційної системи ПТУ	23
1.5. Вартісний аналіз	25
1.6 Постановка задачі.....	25
1.6.1 Загальні відомості	25
1.6.2 Призначення і мета створення підсистеми віддаленого доступу до інформаційної системи ПТУ	25
1.6.3 Вимоги до підсистеми віддаленого доступу до інформаційної системи ПТУ	25
1.6.4 Вимоги до функцій, які виконує підсистема віддаленого доступу до інформаційної системи ПТУ	26
1.6.5 Вимоги до інформаційного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ	27
1.6.6 Вимоги до програмного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ	27
1.6.7 Вимоги до технічного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ	28
1.6.8 Вимоги до документації підсистеми віддаленого доступу до інформаційної системи ПТУ	30

Висновки до розділу 1	30
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТЕХНІЧНОГО ПРОЕКТУ ДО ПІДСИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ «ПІДСИСТЕМА ТЕХНІЧНОГО ДОСТУПУ»	32
2.1.2 Схема функціональної структури.....	32
2.1.3 Опис функцій, що автоматизуються	37
2.1.4 Загальний опис системи	38
2.1.5 Захист системи від несанкціонованого доступу	39
2.2 Рішення з організаційного забезпечення	40
2.3 Рішення з інформаційного забезпечення	40
2.3.1 Опис інформаційного забезпечення системи	40
2.3.2 Концептуальна модель даних	41
2.3.3 Логічна структура бази даних.....	44
2.3.4 Фізична структура бази даних	44
2.5 Рішення з програмного забезпечення	48
2.5.1 Структура програмного забезпечення	49
Висновки до розділу 2	52
РОЗДІЛ 3. РОЗРОБКА ПІДСИСТЕМИ БЕЗПЕЧНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ.....	53
3.1 Фізична архітектура підсистеми.....	53
Висновки до розділу 3	55
РОЗДІЛ 4. ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ РОЗРОБКИ.....	56
4.1. Мета та необхідність техніко-економічного обґрунтування	56
4.2. Технічне обґрунтування	56
4.2.1. Вимоги до апаратного забезпечення	56
4.2.2. Вимоги до програмного забезпечення	56
4.3. Оцінка витрат на розробку	57
4.3.1. Витрати на оплату праці.....	57
4.3.2. Витрати на програмні засоби	57
4.3.3. Витрати на сервери та інфраструктуру	57
4.3.4. Загальні витрати	58
4.4. Очікувані вигоди від впровадження.....	58
4.4.1. Економія за рахунок оптимізації роботи персоналу	58
4.4.2. Нематеріальні вигоди.....	58
Висновки до розділу 4	58
РОЗДІЛ 5. ОХОРОНА ПРАЦІ	60
5.1. Загальні положення охорони праці в ІТ-сфері.....	60
5.2. Характеристика умов праці розробника	60
5.3. Вимоги до організації та ергономіки робочого місця	60
5.3.1. Організація робочої зони.....	60
5.3.2. Вимоги до монітора та периферії	61
5.3.3. Робочий стіл та крісло	61
5.4. Вимоги до освітлення та шуму	61
5.5. Електробезпека	61

5.6. Пожежна безпека.....	61
5.7. Психофізіологічні фактори та профілактика професійних ризиків.....	62
5.8. Заходи безпеки при роботі над розробкою підсистеми	62
Висновки до розділу 5	62
РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА.....	62
6.1. Загальні положення екологічної безпеки в ІТ-сфері	62
6.2. Аналіз можливого впливу проєкту на довкілля	63
6.3. Заходи щодо зменшення екологічного впливу під час розробки системи.....	63
6.3.1. Рациональне використання електроенергії	63
6.3.2. Віртуалізація та оптимізація серверних ресурсів	64
6.3.3. Зниження рівня електронних відходів	64
6.3.4. Зменшення паперового документообігу	64
6.4. Екологічні вимоги до обладнання та приміщень.....	64
6.4.1. Вимоги до серверної кімнати.....	64
6.4.2. Вибір енергоефективного обладнання.....	64
6.4.3. Санітарні норми.....	64
6.5. Заходи щодо зменшення негативного впливу підсистеми після її впровадження.....	65
6.5.1. Хмарна або віртуальна інфраструктура.....	65
6.5.2. Моніторинг енергоспоживання	65
6.5.3. Обмеження використання шкідливих матеріалів	65
6.6. Оцінка екологічної ефективності проєкту	65
Висновки до розділу 6	65
ВИСНОВКИ	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	69
ДОДАТОК А - Технічне завдання на розробку підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи	71
ДОДАТОК Б - Інструкція користувача для роботи з підсистемою безпечного віддаленого доступу до корпоративної інформаційної системи	74
ДОДАТОК В - Екранні форми розробки.....	76

ВСТУП

Стрімкий розвиток цифрових технологій, зростання обсягів корпоративних даних та масовий перехід організацій до гібридних або віддалених моделей роботи зумовлюють необхідність удосконалення засобів інформаційної безпеки. Сучасні компанії активно впроваджують віддалений доступ до своїх інформаційних систем, що забезпечує гнучкість бізнес-процесів, підвищує мобільність персоналу та знижує витрати на інфраструктуру. Однак розширення периметра доступу супроводжується зростанням кількості кіберзагроз: перехоплення трафіку, несанкціоноване втручання, компрометація облікових даних, експлуатація вразливостей мережевих протоколів. У таких умовах забезпечення надійного, стійкого та захищеного доступу користувачів до корпоративних ресурсів стає критичним фактором кіберстійкості організації.

Актуальність обраної теми зумовлена тим, що наявні рішення для віддаленого доступу не завжди враховують специфіку конкретної корпоративної архітектури, часто мають надмірну складність у налаштуванні або забезпечують недостатній рівень контролю доступу та моніторингу активності користувачів. У багатьох організаціях існує потреба у гнучких, масштабованих і адаптивних підсистемах, які дозволяють поєднати зручність використання з високими стандартами кіберзахисту. Тому розробка та дослідження підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи є важливим прикладним завданням, що має теоретичне та практичне значення.

Об'єкт дослідження — процеси забезпечення віддаленого доступу користувачів до корпоративної інформаційної системи.

Предмет дослідження — методи, моделі та програмно-апаратні засоби побудови підсистеми безпечного віддаленого доступу в корпоративному середовищі.

Мета роботи — дослідження сучасних технологій віддаленого доступу та розробка підсистеми, яка забезпечує захищене, надійне та контрольоване підключення користувачів до корпоративної інформаційної системи.

Для досягнення поставленої мети у роботі необхідно виконати такі **завдання**.

Проаналізувати сучасні методи, протоколи та технології організації безпечного віддаленого доступу в корпоративних мережах.

Дослідити існуючі рішення та визначити їх переваги, недоліки і можливості інтеграції в корпоративну інфраструктуру.

Розробити архітектуру підсистеми безпечного віддаленого доступу з урахуванням вимог інформаційної безпеки та корпоративної політики доступу.

Реалізувати програмний прототип підсистеми та забезпечити підтримку механізмів автентифікації, авторизації та шифрування даних.

Провести тестування розробленої підсистеми та оцінити її ефективність, надійність і стійкість до основних типів кіберзагроз.

Розробити рекомендації щодо впровадження підсистеми у корпоративне середовище та можливих напрямів її подальшого удосконалення.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПІДСИСТЕМИ БЕЗПЕЧНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1 Аналіз існуючих підсистем безпечного віддаленого доступу до корпоративної інформаційної системи

Підсистеми безпечного віддаленого доступу до корпоративних інформаційних систем забезпечують можливість авторизованого підключення користувачів до внутрішніх сервісів організації з будь-якої географічної точки. Найбільш поширеними рішеннями є V

PN-системи (IPsec, OpenVPN, WireGuard), засоби багатофакторної автентифікації (MFA), Zero Trust-платформи, а також системи централізованого управління доступом (IAM). Кожен із підходів має власну архітектуру, механізми шифрування та моделі контролю доступу, проте у практичній експлуатації такі системи виявляють низку типових обмежень та недоліків.

Аналіз основних існуючих рішень

IPsec-VPN. Цей стандарт широко застосовується для створення тунелів між віддаленими користувачами та корпоративною мережею. Використовує набори протоколів AH та ESP, забезпечує надійне шифрування та контроль цілісності.

Недоліками роботи є складність налаштування та супроводження, особливо в умовах великої кількості користувачів. Високе навантаження на сервери через обробку криптографічних операцій. Уразливість до DoS-атак при масовому встановленні тунелів. Залежність від коректної конфігурації мережевої інфраструктури (NAT, маршрутизація).

OpenVPN. Поширене програмне рішення, що працює з TLS та SSL, має високу гнучкість і кросплатформність. Недоліками в роботі є залежність від окремих служб сертифікації (CA), потреба постійного оновлення сертифікатів. Потенційне зниження продуктивності при використанні слабких клієнтських пристроїв. Відсутність вбудованих механізмів тонкої політики доступу (не розмежовує доступ до конкретних ресурсів — лише до мережі в цілому).

WireGuard. Новітній VPN-протокол із сучасною криптографією та спрощеною конфігурацією. Недоліком в роботі є недостатня зрілість для великих

корпоративних систем (деякі функціональні можливості ще розвиваються). Відсутність стандартних засобів керування сертифікатами та політиками доступу.

Обмежена інтеграція з корпоративними рішеннями IAM.

Корпоративні системи багатофакторної автентифікації (MFA: Google Authenticator, Duo, Microsoft Authenticator). Дозволяють знизити ризики компрометації облікових записів. Недоліком є залежність від мобільних пристроїв та інтернет-з'єднання користувача. Можливість фішингових атак, спрямованих на перехоплення одноразових кодів. Відсутність повного захисту мережеских каналів — MFA лише доповнює інші технології. Zero Trust Network Access (ZTNA) — Zscaler, Cloudflare Access, Google BeyondCorp. Архітектура відмовляється від традиційних VPN-тунелів, забезпечуючи контроль доступу на рівні окремих ресурсів. Недоліком є складність інтеграції у традиційні підприємства з великою та застарілою інфраструктурою. Висока вартість ліцензування та потреба в фахівцях для налаштування політик безпеки. Залежність від хмарних сервісів, що може бути неприйнятним для організацій з критичними даними. Системи управління ідентичністю та доступом (IAM — Okta, Azure AD, Keycloak). Забезпечують централізовану автентифікацію, авторизацію та контроль ролей. Недоліком цієї системи є складність інтеграції з локальними корпоративними системами. Висока вартість розгортання та супроводу. Імовірність єдиної точки відмови — при недоступності IAM блокується вся система доступу.

Загальні недоліки існуючих підсистем

У ході аналізу виявлено низку типових проблем, притаманних більшості сучасних рішень. Складність керування доступами у великих організаціях, особливо при постійній зміні штату. Недостатня гнучкість у розмежуванні доступу до конкретних сервісів, коли VPN відкриває доступ до широкого сегменту мережі.

Висока залежність від якісних каналів зв'язку, що знижує ефективність роботи у віддалених регіонах. Можливість компрометації ключів і сертифікатів, особливо при порушенні політик безпеки користувачами. Відсутність єдиного інтегрованого рішення, що одночасно забезпечує шифрування, автентифікацію,

аудит та зручне управління. Проблеми масштабування, коли кількість одночасних підключень перевищує проєктні можливості системи. Низький рівень автоматизації моніторингу та виявлення аномалій, що ускладнює швидке реагування на загрози.

Висока вартість комерційних рішень, яка обмежує їх використання малими підприємствами.

1.2 Формування вимог до підсистеми віддаленого доступу до інформаційної системи

Підсистема віддаленого доступу до інформаційної системи «Підсистема технічного управління» (ПТУ) є інформаційною підсистемою, яка призначена для автоматизації роботи користувачів ПТУ. Функції, що автоматизуються підсистемою, пов'язані з організацією робочого часу користувачів, обліком відвідування й успішності ОПР.

Інформаційна підсистема віддаленого доступу до інформаційної системи Підсистема технічного управління (ПТУ) є середовищем, складовими елементами якого є комп'ютери, об'єднані в комп'ютерні мережі, програмні продукти, бази даних, люди, різного роду технічні і програмні засоби зв'язку і т.д. Основна мета інформаційної підсистеми — організація збереження, обробки і передачі інформації. Інформаційна підсистема являє собою людино-комп'ютерне оточення (систему) для обробки інформації. Інформаційна підсистема, що розробляється, є розподіленою, тобто для її функціонування, крім програм-клієнтів, необхідна наявність хоча б одного сервера програм. Програмне забезпечення сучасних інформаційних підсистем має наступні логічні рівні

- Рівень користувача (інтерфейс і сервіси користувача);
- Прикладний рівень (прикладні сервіси);
- Рівень даних (сервіси доступу до даних і сховище даних).

Опишемо функції кожного рівня:

- Рівень користувача: відображає дані і дозволяє користувачу редагувати їх за допомогою віконного інтерфейсу (реалізується засобами підсистеми інтерфейсу користувача операційної системи).

- Прикладний рівень: тут реалізовані бізнес-правила й обмеження на дані (перевірка коректності даних). І хоча його сервіси використовуються презентаційним рівнем, він не прив'язаний до якого-небудь клієнта – сервіси прикладного рівня доступні будь-якому клієнту. Бізнес-правила виражаються у формі прикладних алгоритмів і т.д. Обмеження на дані гарантують точність і цілісність інформації, що зберігається. Бізнес-правила звичайно реалізуються окремим модулем на централізованому сервері, що дає можливість доступу до нього відразу декільком клієнтам.

- Рівень даних: прикладний рівень не має інформації про те, як і де зберігаються дані, які він обробляє. У цьому питанні він покладається на сервіси доступу до даних, що виконують всю роботу з отримання і передачі даних. Сервіси доступу до даних також реалізуються у виді ізольованих модулів, які знають про місце збереження інформації. Кожен модуль доступу до даних, як правило, відповідає і за цілісність сховища (наприклад, реляційної бази даних). Для багаторівневих програм у якості сховища інформації підходять сервера баз даних (MS SQL Server, Oracle, Sybase, MySQL, PostgreSQL і ін.), необхідні для обслуговування даних у таблицях і високопродуктивної виборки інформації.

Реалізація функцій інформаційної системи неможлива без знання орієнтованих на неї інформаційних технологій. Нижче представлений опис технологій, які використовуються на кожному рівні інформаційної системи, що розробляється.

Технології рівня користувача: Програмний-інтерфейс

Серед особливостей засобів створення Java-додатків, цікавих в плані створення корпоративних рішень, слід назвати засоби підвищення продуктивності праці розробників, засоби підтримки колективної роботи, підтримку різних етапів життєвого циклу програм, як попередніх створенню коду додатків (таких як управління вимогами, моделювання даних і додатків), так і наступних за ним (тестування, впровадження та супровід), можливості, пов'язані з повторним використанням моделей і коду, підтримку засобів і стандартів створення

розподілених додатків і їх інтеграції (включаючи підтримку стандарту J2EE і Web-сервісів XML), а також можливість створення мобільних рішень, у тому числі підтримку стандарту J2ME. Сучасні інструменти розробки Java-додатків, як правило, володіють різними засобами підвищення продуктивності праці програмістів. Тут ми не будемо зупинятися на таких вже звичних речах, як колірне виділення синтаксичних конструкцій, візуальні редактори користувальницьких інтерфейсів, підтримка створення додатків з базами даних (у разі Java - за допомогою універсального механізму доступу до даних JDBC, Java DataBase Connectivity) або наявність коштів звичайної і віддаленого налагодження, - зараз без них жоден інструмент для розробки додатків не має шансів зайняти скільки-небудь значимої позиції на ринку. З коштів, наявність яких не є очевидним, в першу чергу відзначимо засоби рефакторінга - автоматичного внесення супутніх змін в код при перейменуванні класів (наприклад, зміна коду, що містить посилання на перейменований клас) і зміні параметрів методів, автоматичного додавання конструкцій try ... catch навколо блоку коду з урахуванням можливих винятків, які можуть відбутися при виклику методів, що містяться в цьому блоці, а також інших дій, пов'язаних з автоматичним внесенням змін в код, що вкрай необхідно при колективній роботі над великими проектами і при повторному використанні коду. Крім цього, до корисних особливостей Java-інструментів можна віднести засоби створення тестових класів, засоби конвертації файлів SQLJ1 в Java-код, різні засоби, що спрощують генерацію тестів і поставку додатків, а також наявність майстрів створення Web-додатків, Web-сервісів, генерації коду на підставі WSDL2-описів. Говорячи про підтримку проектування додатків, слід підкреслити, що створення Java-додатків масштабу підприємства зараз практично немислимо без застосування засобів UML-моделювання. Такі кошти можуть бути включені безпосередньо до складу продукту або підтримуватися на рівні інтерфейсів до них; при цьому найбільш переважним є наявність засобів UML-моделювання у вигляді модулів, вбудованих в середу розробки і підтримуючих синхронне зміна моделей і коду.

Технології рівня даних: Сервер баз даних (MySQL-server). Технології прикладного рівня: Java DataBase Connectivity

1.2.1 Характеристика підсистеми віддаленого доступу до інформаційної системи ПТУ

Об'єктом автоматизації є підсистема віддаленого доступу до інформаційної системи ПТУ, пов'язана з роботою користувачів ПТУ та ОНР. Існуюча інформаційна система (її комп'ютеризована версія перебуває в стадії розробки) має потребу в створення єдиної бази даних для централізованого збереження інформації й автоматизованих робочих місць для співробітників. Об'єкт автоматизації сам по собі є інформаційною системою, для автоматизації роботи якої потрібно створення власної бази даних і програмного забезпечення для користувачів і адміністратора. Об'єкт автоматизації – інформаційна підсистема віддаленого доступу до інформаційної системи ПТУ – вирішує задачі пов'язані з обліком виконання проєктів, організацією робочого часу користувачів і інше.

1.2.2 Цілі, критерії й обмеження створення інформаційної підсистеми віддаленого доступу до інформаційної системи ПТУ

Метою розробки є підвищення ефективності роботи інформаційної підсистеми, збільшення продуктивності і поліпшення умов праці користувачів шляхом автоматизації функцій, які вони виконують.

Основні критерії створення інформаційної підсистеми.

- Соціальний критерій. Інформаційна система розрахована на користувачів з різною комп'ютерною підготовкою. Необхідний зручний і інтуїтивно зрозумілий інтерфейс для роботи з нею.
- Економічний критерій. Автоматизована інформаційна підсистема створюється для ПТУ безкоштовно.
- Критерій безпеки. Підсистема повинна бути безпечною з погляду збереження й обробки даних. Утрата даних може привести до серйозних збоїв у роботі системи. Необхідний захист системи від несанкціонованого втручання.

1.2.3 Функції та задачі підсистеми віддаленого доступу до системи ПТУ

Задачею інформаційної підсистеми, що створюється, є автоматизація наступних функцій користувачів.

- Облік успішності роботи над проєктом.
- Облік часу участі в проєкті .
- Допомога в організації робочого часу.

Для створення інформаційної підсистеми необхідно розробити єдину базу даних для збереження інформації про користувачів і ОПР, про відвідування, про розклад користувачів і іншу. Для роботи з підсистемою користувачі повинні мати відповідне програмне забезпечення. Також повинно бути передбачене програмне забезпечення для адміністрування системи.

1.3 Розробка концепції підсистеми віддаленого доступу до інформаційної системи ПТУ

1.3.1 Опис результатів вивчення підсистеми віддаленого доступу до інформаційної системи ПТУ

Інформаційна підсистеми віддаленого доступу до інформаційної системи ПТУ вирішує задачі, що пов'язані з автоматизацією праці користувачів ПТУ. Для створення підсистеми потрібна розробка бази даних, програмного забезпечення для користувачів і адміністраторів, а також прийняття рішень по інших видах забезпечення. Основні задачі, що вирішує інформаційна підсистема «Віддаленого доступу для системи ДТУ» пов'язані з обліком успішності та відвідування ОПР, видачею завдань, організацією робочого часу користувачів.

Розробка автоматизованої інформаційної підсистеми «Реєстрація ОПР ДТУ» дозволить підвищити ефективність і якість праці користувачів, поліпшити умови їхньої праці.

1.3.2 Аналіз вимог до підсистеми віддаленого доступу до інформаційної системи ПТУ

Крім функціональних вимог до інформаційної підсистеми (облік успішності ОПР, облік відвідування ОПР, організація розкладу вчителя), необхідно врахувати вимоги до підсистеми в цілому:

- Простий і зручний інтерфейс користувача.

- Багатокористувачева робота.
- Висока продуктивність.
- Надійність.
- Конфіденційність інформації.

Аналізуючи зазначені вище вимоги, можна зробити висновок, що інформаційна система повинна мати/підтримувати:

- Багаторівневу архітектуру.
- Сучасні серверні платформи і програмне забезпечення.
- Ефективні методи доступу до даних.
- Забезпечити простоту модернізації, можливість повторного використання програмного забезпечення (коду).

1.3.3 Розробка варіантів концепції підсистеми віддаленого доступу до інформаційної системи ПТУ

Виходячи з аналізу вимог до інформаційної підсистеми, її функціональних характеристик, фізичної архітектури і технологій для розробки, можна розробити концепцію інформаційної підсистеми. Основними компонентами підсистеми є:

- серверна платформа і серверне програмне забезпечення;
- система управління базами даних;
- клієнтська платформа і клієнтське програмне забезпечення;
- засоби розробки;
- мережне середовище;
- технічні засоби.

Від вибору перерахованих компонентів залежить ефективність інформаційної підсистеми. Розглянемо кожен компонент інформаційної підсистеми.

Серверна платформа і серверне програмне забезпечення

Необхідну функціональність, надійність, безпеку і продуктивність інформаційної підсистеми можуть забезпечити наступні операційні системи (у порядку збільшення продуктивності і функціональності):

- Windows 2000 Server.
- Windows 2000 Advanced Server.
- Windows 7
- Windows 8
- Linux

Windows 2000 Advanced Server має всі можливості Windows 2000 Server, а також додаткові можливості (підтримка кластерів, підтримка більшої кількості оперативної пам'яті і мікропроцесорів). Windows 2000 Advanced Server має кращу продуктивність і надійність, але можливості цієї операційної системи набагато перевищують максимальні вимоги до інформаційної системи, що розробляється, тому немає необхідності купувати більш дорогу інформаційну систему, якщо її можливості не будуть використані повною мірою.

Таким чином, Windows 2000 Server – це найбільш оптимальний вибір для інформаційної системи, що розробляється. Windows 2000 Server може підтримувати оперативну пам'ять до 4Гб (128Мб – мінімальна; 256Мб – рекомендується), до чотирьох мікропроцесорів (мінімальний CPU – 133МГц) і жорсткий диск від 2Гб і більше. Усе це додасть інформаційній системі широкі можливості по нарощуванню продуктивності і забезпечить високу масштабуємість.

На сервері баз даних повинна бути встановлена серверна система управління базами даних (СУБД).

Необхідна сучасна серверна реляційна СУБД, що має високу продуктивність, здатна працювати з великими обсягами інформації і підтримує стандарт SQL-92. Крім того, СУБД повинна працювати під управлінням Windows. Серверними СУБД, що задовольняють зазначеним вимогам, на сьогодні є:

- MS SQL Server 2000.
- MySQL 3.23.
- PostgreSQL 7.
- Sybase (SQL Anyware Studio 8).
- Oracle 9i (Standard Edition чи Enterprise Edition).

- IBM Informix Dynamic Server 9.3 (Standard Engine).

Клієнтська платформа і клієнтське програмне забезпечення

На клієнтських машинах може використовуватися будь-яка операційна система з можливістю встановлення віддаленого мережного з'єднання і графічним інтерфейсом. Операційні системи, що рекомендуються – MS Windows 98/Me/2000/XP, Linux.

Технічні засоби серверів повинні задовольняти вимогам операційної системи і СУБД до обладнання. Конфігурація кожного сервера може бути наступною:

- Мікропроцесор класу Pentium IV 2000 МГц і вище.
- Оперативна пам'ять RAM 256 Мб і більше.
- Жорсткий диск з вільним місцем 5 Гб і більше (сервер баз даних повинен мати жорсткий диск з більшим обсягом вільного місця – 8 Гб і більше).
- Мережна карта Ethernet (не менше 10 Мбіт/с).

Технічні засоби клієнтських машин повинні відповідати вимогам операційної системи, що використовується. Конфігурація комп'ютера користувача може бути наступною:

- Мікропроцесор класу Pentium IV 2000 МГц і вище.
- Оперативна пам'ять RAM 128 Мб і більше.
- Жорсткий диск з вільним місцем 5 Гб і більше.

Варіанти концепції інформаційної системи

Таким чином, розглянувши компоненти підсистеми і вибравши найбільш оптимальні, можна визначити кілька варіантів концепції інформаційної підсистеми «Віддаленого доступу для системи ДТУ» (див. таблицю 1.1). У таблиці використані наступні скорочення:

- ПЗ – програмне забезпечення.
- ОС – операційна система.
- СУБД – система управління базами даних.

Таблиця 1.1 – Варіанти концепції інформаційної системи

№	ПЗ сервера доступу до даних (ОС)	ПЗ сервера баз даних (ОС, СУБД)	Засоби розробки
1	Linux(Ubuntu)	Linux(Ubuntu) , MySQL Server	JDK

Крім того, кожен варіант концепції підсистеми має відповідне технічне (описане вище) і організаційне забезпечення. Причому, і технічне, і організаційне забезпечення будуть однаковими для усіх варіантів, оскільки обране інформаційне забезпечення має приблизно однакові вимоги до апаратних ресурсів і обслуговування.

При виборі варіантів концепції інформаційної підсистеми, були враховані наступні особливості:

Краще на всіх серверах встановлювати однакову операційну систему, тому що їх легше буде підтримувати.

СУБД MySQL підтримує вкладені запити (стандартний дистрибутив) і трохи втрачає в продуктивності при роботі під управлінням Windows-систем Linux-систем.

Використовувати СУБД Oracle нераціонально – вона має високі вимоги до системних ресурсів, а її можливості не будуть використані повною мірою.

1.4 Концепція підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи

Концепція підсистеми безпечного віддаленого доступу полягає у створенні комплексного технологічного рішення, що забезпечує надійне, контрольоване та захищене підключення користувачів до корпоративної інформаційної системи незалежно від їхнього розташування, типу пристрою або каналу зв'язку. В умовах зростання кіберзагроз, поширення віддаленої та гібридної роботи, використання хмарних сервісів і мобільних пристроїв виникає потреба у формуванні нової моделі доступу, яка базується не на захисті периметра, а на принципах нульової довіри, багаторівневої автентифікації та адаптивного контролю дій користувачів.

Запропонована концепція передбачає створення підсистеми, що інтегрується в корпоративну IT-інфраструктуру та забезпечує захист комунікацій за допомогою сучасних криптографічних протоколів, сегментацію доступу відповідно до ролей, а також постійний моніторинг активності користувачів. Підсистема має включати механізми багатфакторної автентифікації, динамічного управління політиками доступу, перевірки цілісності клієнтських пристроїв і шифрування трафіку між користувачем і корпоративними сервісами.

Концепція розробки передбачає створення програмного прототипу, який реалізовує ключові функції: автентифікацію, авторизацію, шифрування даних, захист від несанкціонованого доступу, журналювання подій та аналіз безпекових інцидентів. Основою архітектури має бути модульність, що дає змогу масштабувати підсистему, адаптувати її до вимог різних корпоративних середовищ і інтегрувати з існуючими рішеннями, зокрема IAM, SIEM і засобами моніторингу.

Запропонована концепція орієнтована на підвищення рівня інформаційної безпеки організації шляхом зменшення ризиків, пов'язаних із віддаленим доступом, мінімізації людського фактору, забезпечення відповідності нормативним вимогам та створення надійного середовища для обміну даними. Реалізація такої підсистеми сприятиме підвищенню кіберстійкості підприємства, оптимізації процесів управління доступом та забезпеченню безпечної взаємодії співробітників із корпоративними ресурсами.

1.4.1 Вимоги, що впливають на якість підсистеми віддаленого доступу до інформаційної системи ПТУ

Якість інформаційної підсистеми і якість програмного забезпечення не піддаються точному визначенню і виміру. На даний момент, не існує ні метрології якості інформаційних систем, ні реальних методів оцінки якості програмного забезпечення, ні методів оцінки якості процесу проектування, розробки і впровадження. Проте, задача поставлена і вимагає вирішення. Складемо список

вимог (критеріїв), що можуть впливати на якість інформаційної системи (частина з них взята зі стандарту ІСО-9126):

- Здатність підвищити ефективність роботи ПТУ.
- Функціональність.
 - Відповідність призначенню.
 - Точність.
 - Повнота інформації.
 - Здатність взаємодіяти із середовищем.
 - Відповідність нормам.
 - Безпека (захист від взлому даних і інших злочинних дій).
- Надійність.
 - Зрілість ("обкатаність").
 - Стійкість до відмов.
 - Стійкість до помилок користувача.
 - Здатність відновлюватися після збоїв.
- Масштабуємість.
- Придатність до використання.
 - Зрозумілість.
 - Вивчаємість.
 - Зручність і простота в роботі.
- Ефективність.
 - Продуктивність і час відгуку.
 - Споживання ресурсів.
- Супроводжуємість.
 - Аналізуємість (діагностика причин помилок і зіставлення з первісним кодом).
 - Придатність до змін.
 - Стабільність.
 - Тестуємість.

Потрібно відзначити, що виконання всіх зазначених вимог ще не гарантує якість інформаційної підсистеми. Також, невідповідність системи якій-небудь вимозі не говорить про те, що підсистема неякісна. Як уже говорилося вище, не існує формальних методів оцінки якості інформаційної підсистеми.

1.5. Вартісний аналіз

Для розробки даної системи було використано безкоштовне (Open Source) програмне забезпечення, завдяки цьому ми не маємо витрат.

1.6 Постановка задачі

1.6.1 Загальні відомості

Потрібно розробити автоматизовану інформаційну підсистему для автоматизації функцій, які виконуються користувачі/працівники ПТУ. Замовником виступає корпорація та ОПР. Назва розробки: **Дослідження та розробка підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи**

1.6.2 Призначення і мета створення підсистеми віддаленого доступу до інформаційної системи ПТУ

Призначенням підсистеми є автоматизація функцій, які виконуються ОПРи, а також створення єдиної бази даних, у якій буде зберігатися вся інформація про поточну академічну успішність і відвідування занять учнями, а також інша інформація. У майбутньому, ця база даних може служити для адміністративних цілей.

Метою створення системи є підвищення продуктивності і поліпшення умов праці користувачів.

1.6.3 Вимоги до підсистеми віддаленого доступу до інформаційної системи ПТУ

Режим роботи підсистеми повинен відповідати режиму роботи співробітників (користувачів) ПТУ, інструментарій віддаленого доступу повинен функціонувати цілодобово. У режимі роботи системи повинні бути передбачені інтервали для проведення профілактичних і технічних робіт.

Рівень комп'ютерної підготовки користувачів повинен відповідати рівню «користувач ПЕОМ». Супроводження інформаційної підсистеми повинно здійснюватися штатними фахівцями ПТУ.

Компоненти системи повинні мати можливості для модернізації і розвитку в межах обраних технологій, що лежать у її основі, або навіть до їх часткової заміни.

Цільове призначення системи повинне зберігатися протягом часу остаточного застарівання технічного, програмного, інформаційного й організаційного забезпечення.

1.6.4 Вимоги до функцій, які виконує підсистема віддаленого доступу до інформаційної системи ПТУ

Інформаційна підсистема повинна володіти наступними функціональними характеристиками:

- 1) Аутентифікація користувача.
- 2) Ідентифікація користувача (надання користувачу тільки тих даних, які необхідні йому для виконання своєї роботи).
- 3) Конфіденційність передачі даних по комп'ютерній мережі.
- 4) Облік успішності ОНР:
 - додавання проведеного заняття (уроки);
 - виставлення оцінок учням, які виконали завдання;
 - зміна оцінок учням, які виконали завдання;
 - вилучення оцінок.
- 5) Облік відвідування занять учнями:
 - додавання проведеного заняття (уроку);
 - додавання відмітки про відсутність учня на занятті;
 - вилучення відмітки про відсутність учням на занятті.
- 6) Видача завдань учням:
 - додавання нових завдань (лабораторних, домашніх і інших робіт);
 - вилучення існуючих завдань;
 - зміна існуючих завдань.

- 7) Надання користувачу (вчителю) інформації про його розклад занять.
- 8) Надання зручного інтерфейсу:
 - однакове представлення інформації незалежно від платформи і програмного забезпечення машини користувача;
 - сортування даних;
 - проста навігація;
 - можливості настройки шрифтів інтерфейсу й інших параметрів інтерфейсу;
 - можливість збереження параметрів інтерфейсу між сеансами роботи;
 - можливість автоматичного заповнення полів форм.
- 9) Надання можливості створення паперових звітів про видані завдання, успішність і відвідування ОПР; друк розкладу занять, які проводить керівник.
- 10) Ведення записної книжки (щоденника) вчителя.
 - додавання запису;
 - зміна запису;
 - вилучення запису.

1.6.5 Вимоги до інформаційного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ

Підсистема повинна бути відкритою (використовувати існуючі стандарти), тобто мати властивості мобільності. Система повинна підтримувати розподілену багаторівневу архітектуру для забезпечення масштабуємості.

Підсистема повинна забезпечувати захист даних за допомогою аутентифікації та ідентифікації користувачів, захисту каналів зв'язку (шифрування даних), фізичного захисту обладнання.

У якості програмного забезпечення сервера бази даних необхідно використовувати серверну СУБД. Необхідно використовувати стандартні можливості СУБД із метою підтримки переносимості.

1.6.6 Вимоги до програмного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ

Інформаційна система включає кілька серверів (сервер з бізнес логікою; сервер із сервісами доступу до даних; сервер баз даних) і клієнтські машини.

Вимоги до програмного забезпечення сервера баз даних:

- Операційна система: ОС Linux (Ubuntu 12.04)
- Створена база даних яка відповідає запитам відповідно до інформаційної підсистеми.

Вимоги до програмного забезпечення сервера доступу до даних:

- Операційна система: ОС Linux (Ubuntu 12.04).

Вимоги до програмного забезпечення сервера баз даних:

- Операційна система: ОС Linux (Ubuntu 12.04)
- Сервер баз даних: рекомендується використання MySQL Server.

Вимоги до програмного забезпечення клієнтської машини:

- Операційна система: будь-яка операційна система з можливістю установки віддаленого мережного з'єднання і графічним інтерфейсом. Операційні системи, що рекомендуються – ОС Linux (Ubuntu 12.04).

1.6.7 Вимоги до технічного забезпечення підсистеми віддаленого доступу до інформаційної системи ПТУ

Інформаційна підсистема включає кілька серверів (сервер з бізнес логікою; сервер із сервісами доступу до даних; сервер баз даних) і клієнтські машини.

Вимоги до технічного забезпечення сервера баз даних

Для коректної та стабільної роботи підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи сервер баз даних має відповідати низці технічних вимог, що забезпечують надійну обробку запитів, високу доступність, стійкість до навантажень та захист інформації. Сервер баз даних обслуговує критично важливі функції — зберігання облікових записів користувачів, політик доступу, журналів аудиту, криптографічних ключів та службових даних системи, тому його технічні характеристики повинні відповідати високим стандартам продуктивності та безпеки.

1. Вимоги до обчислювальних ресурсів

Процесор (CPU) багатоядерний процесор із частотою від 2.5 ГГц та підтримкою інструкцій апаратного прискорення криптографічних операцій (AES-NI).

Рекомендовано 8–16 ядер, архітектура x86-64.

Оперативна пам'ять (RAM) мінімум 16 ГБ, рекомендовано 32–64 ГБ залежно від кількості користувачів та обсягів журналів. Пам'ять має підтримувати ECC для захисту від помилок.

2. Вимоги до системи зберігання даних

Тип накопичувача твердотільні накопичувачі (SSD) з інтерфейсом NVMe або SATA III для мінімізації затримок у роботі із транзакційними даними.

Обсяг мінімум 500 ГБ, рекомендовано 1 ТБ і більше, з урахуванням журналів аудиту та резервних копій.

Організація дискової підсистеми

Використання RAID-масивів рівнів RAID 1 або RAID 10 для підвищення відмовостійкості та швидкодії.

3. Вимоги до мережевої інфраструктури

Пропускна здатність мережевого інтерфейсу — не менше 1 Gbps, рекомендовано 10 Gbps для корпоративних інфраструктур.

Підтримка сучасних мережевих протоколів та технологій захисту (802.1X, VLAN, фільтрація трафіку).

Можливість ізоляції сервера БД у окремому сегменті мережі (DMZ або внутрішній захищений сегмент).

4. Вимоги до фізичної та апаратної безпеки

Розміщення сервера у серверному приміщенні з контролем доступу.

Наявність безперебійного живлення (UPS) з можливістю живлення серверних систем протягом не менше 30 хвилин.

Блоки живлення з підтримкою N+1 резервування.

Система охолодження серверної для підтримки робочої температури.

5. Вимоги до надійності та відмовостійкості

Підтримка технологій віртуалізації (наприклад, VMware ESXi, Hyper-V, Proxmox), що дозволяє розміщення БД у кластерному середовищі.

Можливість масштабування (горизонтального або вертикального) залежно від збільшення кількості користувачів.

Використання регулярного резервного копіювання (full/incremental), зберігання копій на окремому носії.

6. Вимоги до програмної сумісності та безпеки

Сервер має підтримувати встановлення СУБД, рекомендованих для систем безпечного доступу (PostgreSQL, MySQL/MariaDB, MS SQL Server).

Наявність оновленої серверної операційної системи зі строгою політикою безпеки (наприклад, Ubuntu Server LTS, Debian, RHEL, Windows Server).

Підтримка апаратного модулю TPM 2.0 для захищеного зберігання ключів (за потреби).

Можливість використання TLS 1.3 для захисту трафіку між підсистемами.

1.6.8 Вимоги до документації підсистеми віддаленого доступу до інформаційної системи ПТУ

Необхідна наявність наступних документів:

- Загальний опис системи.
- Керівництво користувача.
- Інструкція з формування і ведення бази даних.
- Керівництво адміністратора з установки програмного забезпечення на серверах.
- Програма і методика випробувань.
- Текст програми

Висновки до розділу 1

У першому розділі було здійснено системний аналіз теоретичних засад організації віддаленого доступу до корпоративних інформаційних систем та визначено ключові вимоги до побудови безпечних каналів взаємодії між користувачами та корпоративними ресурсами. Розглянуто архітектурні принципи сучасних технологій захищеного доступу, зокрема VPN-рішень, Zero Trust-

підходу, систем багатфакторної автентифікації та механізмів управління ідентичністю та правами доступу.

Проведений огляд показав, що розвиток цифрової інфраструктури та зростання кількості віддалених робочих місць суттєво збільшують ризики несанкціонованого доступу, перехоплення даних та кібератак на корпоративні мережі. Традиційні рішення забезпечують базову конфіденційність і цілісність інформації, проте мають низку обмежень, пов'язаних зі складністю налаштування, недостатньою масштабованістю, відсутністю гнучкого управління політиками доступу та потребою у підвищеному рівні контролю за автентифікацією.

На основі аналізу встановлено, що для ефективного та безпечного віддаленого доступу необхідно використовувати комплексний підхід, який поєднує криптографічний захист каналів зв'язку, централізоване управління правами, багаторівневу автентифікацію, постійний моніторинг активності та автоматизоване виявлення аномалій. Саме така інтегрована модель забезпечує стійкість до сучасних загроз, підтримує масштабування та дозволяє адаптувати підсистему до особливостей конкретної корпоративної інфраструктури.

Отже, результати розділу 1 створюють методологічне підґрунтя для подальшого проєктування та розробки підсистеми безпечного віддаленого доступу, визначають її функціональні вимоги та окреслюють ключові напрямки підвищення інформаційної безпеки корпоративної системи.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТЕХНІЧНОГО ПРОЕКТУ ДО ПІДСИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ «ПІДСИСТЕМА ТЕХНІЧНОГО ДОСТУПУ»

2.1 Загальносистемні рішення

2.1.1 Схема організаційної структури

Інформаційна підсистема віддаленого доступу до системи Підсистема технологічного управління проєктантів розробляється для Підсистема технологічного управління проєктантів. Схема організаційної структури Підсистема технологічного управління проєктантів представлена на рисунку 2.1.



Рисунок 2.1 – Концепція підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи

Користувачами системи, що розробляється, будуть співробітники підприємства.

2.1.2 Схема функціональної структури

Для уточнення функціональності інформаційної системи, виявлення схеми функціональної структури, визначення підсистем (модулів), які входять до її

складу, і вивчення динаміки роботи системи в цілому необхідно побудувати функціональну модель.

Функціональна модель описує обчислення в системі. Вона показує, яким чином вихідні дані обчислюються по вхідним даним, не розглядаючи порядок чи спосіб реалізації обчислень. Функціональна модель складається з набору діаграм потоків даних, що показують потоки значень від зовнішніх входів через операції і внутрішні сховища даних до зовнішніх виходів.

Діаграми потоків даних (Data Flow Diagrams – DFD) є основним засобом моделювання функціональних вимог підсистеми при проектуванні. З їхньою допомогою ці вимоги розбиваються на функціональні компоненти (процеси) і представляються у виді мережі, зв'язаної потоками даних. Головна мета таких засобів – продемонструвати, як кожен процес перетворить свої вхідні дані у вихідні, а також, виявити відносини між цими процесами. Далі при побудові DFD буде використовуватися нотація Гейна-Сарсона (Gane-Sarson).

Джерела інформації (зовнішні сутності) породжують інформаційні потоки (потоки даних), що переносять інформацію до підсистем чи до процесів. Ті у свою чергу перетворюють інформацію і породжують нові потоки, що переносять інформацію до інших процесів чи підсистемам, накопичувачів даних чи зовнішніх сутностей – споживачів інформації. Таким чином, основними компонентами діаграм потоків даних є:

- зовнішні сутності;
- процеси;
- накопичувачі даних;
- потоки даних.

Зовнішня сутність являє собою матеріальний предмет чи фізичну особу, що представляє собою джерело чи приймач інформації. Для системи, що розробляється, зовнішніми сутностями є:

- Керівник (користувач).
- ОПР (користувач)

Для системи, що розробляється, основні процеси на DFD пов'язані з аутентифікацією керівник або ОПР, отримання інформації про групи, проєктантів. Задачами адміністратора системи: ведення бази даних і налагодження системи для коректної аутентифікації.

Накопичувач даних являє собою абстрактний пристрій для збереження інформації, яку можна в будь-який момент помістити в накопичувач і через якийсь час знову взяти, причому способи запису і зчитування можуть бути будь-якими [3]. Накопичувачами даних у даній системі є:

- База даних системи (зберігає всю інформацію проєктантів).
- Файли аутентифікації (зберігають логіни та паролі керівник та ОПР).

Потік даних визначає інформацію, яка передається через деяке з'єднання від джерела до приймача.

Важливу специфічну роль у моделі грає спеціальний вид діаграми потоків даних – контекстна діаграма, що моделює систему найбільш загальним чином. Контекстна діаграма відображає інтерфейс системи з зовнішнім світом, а саме, інформаційні потоки між системою і зовнішніми сутностями, з якими вона повинна бути зв'язана. Контекстна діаграма підсистеми віддаленого доступу для системи Підсистема технологічного управління проєктантів представлена на рисунку 2.2.



Рисунок 2.2 – Контекстна діаграма потоків даних Інформаційної підсистеми віддаленого доступу для системи ПТУ

Проведемо декомпозицію потоків даних, показаних на рисунку 2.2 (див. таблицю 2.1).

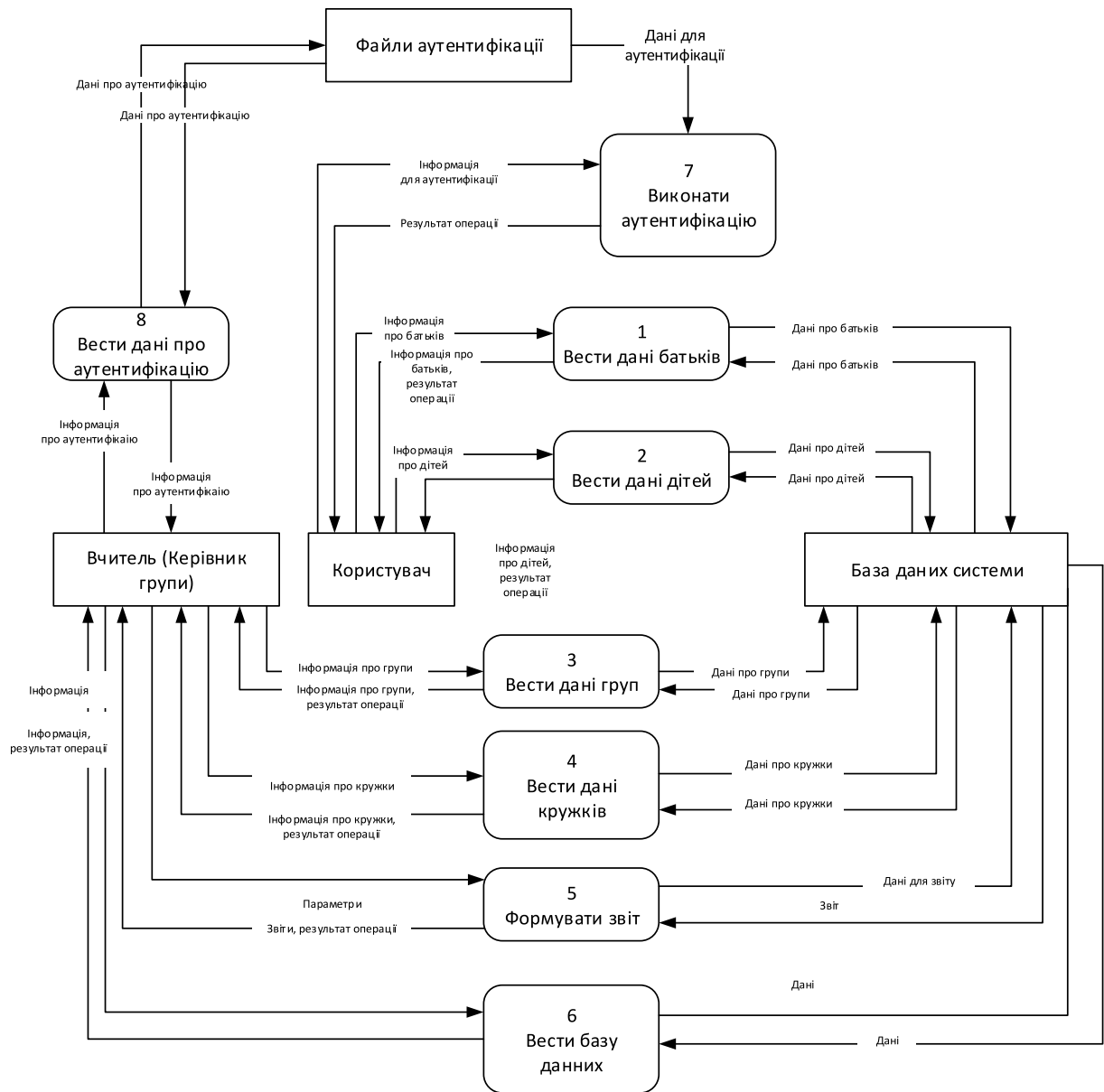
Таблиця 2.1 – Декомпозиція потоків даних для контекстної DFD

Потоки даних на контекстній діаграмі	Потоки на діаграмі першого рівня
Інформація від вчителя.	Інформація для аутентифікації. Інформація про групи проєктантів. Інформація про співробітників.
Інформація для вчителя.	Інформація про розклад по групам. Інформація про співробітників даної групи. Інформація про керівників даної групи.
Інформація від користувача.	Інформація. Інформація про аутентифікацію.
Інформація для користувача.	Інформація. Інформація про аутентифікацію.

Для продовження аналізу функціонального моделі підсистеми будуються діаграми наступних рівнів. При цьому процеси піддаються декомпозиції, існуючі "абстрактні" потоки даних трансформуються в потоки, що представляють обмін даними на більш конкретному рівні.

DFD першого рівня будується як декомпозиція процесів, що присутні на контекстній діаграмі. DFD першого рівня представлена на рисунку 2.3.

Можна провести подальшу декомпозицію процесів на діаграмі потоків даних першого рівня, однак зараз опишемо тільки декомпозицію деяких процесів.



Процес «Вести дані замовників»:

Процес «Вести дані користувачів»:

Процес «Вести дані груп»:

- Редагувати інформацію про проєктанті даної групи.
- Додати нового проєктанта до групи.

Процес «Вести дані активних проєктів»:

Вивести на екран звіт про кількість проєктантів у вибраному проєкті.

Вивести на екран інформацію стосовно керівника проєкту.

Вивести на екран інформацію безпосередньо про проєкт(дата початку та кінець)

Таким чином, функціональність системи цілком визначена. Подальша декомпозиція процесів приведе до опису алгоритмів роботи окремих програмних модулів, що входять до складу програмного забезпечення системи.

2.1.3 Опис функцій, що автоматизуються

Первісні дані

При розробці функціональної частини проєкту використовувалися наступні документи:

- Відомість з особистими даними проєктантів та керівників.
- Відомість з розподілу проєктантів по групам.
- Відомість про соціальне становище проєктантів.

Усі ці документи ведуться (керівниками груп). Для кожної групи проєктантів і предмета заводяться окремі відомості. Складність полягає в тому, що стандартів на ці документи немає. Кожний керівник вирішує сам для себе як повинен виглядати кожен документ, оскільки вся інформація в цих документах використовується тільки самим вчителем для прийняття рішень. Опишемо кожен документ по окремоті, включивши в нього необхідні елементи (поля, записи), що зустрічаються найбільш часто.

Документ «Відомість з особистими даними проєктантів та їх ОПР» повинна містити інформацію про проєктантів (прізвище, ім'я, по батькові), ОПР(П.І.Б., телефон, адреса, посада, статус) номер групи проєктантів,

Документ «Відомість з розподілу проєктантів по групах» повинен містити інформацію про групу (П.І.Б. керівника групи, номер групи), П.І.Б. проєктантів у даній групі.

Документ «Відомість про соціальне становище проєктантів» повинен містити інформацію про соціальне становище проєктантів: прізвище, ім'я, по батькові, номер групи проєктантів, назву предмета.

Цілі розробки системи і автоматизовані функції

Ціль розробки системи – збільшення продуктивності і поліпшення умов праці керівник шляхом автоматизації функцій, які вони виконують.

Автоматизовані функції, що виконує керівник:

Регістрація нових проєктантів.

Ведення інформації про проєктантів.

Ведення інформації про групи.

Вигода від створення інформаційної підсистеми віддаленого доступу для системи Підсистема технологічного управління проєктантів також полягає в тому, що інформація буде зберігатися в єдиній базі даних, вона буде систематизована і придатна для подальшої обробки. Цю інформацію зможуть надалі використовувати інші інформаційні системи.

2.1.4 Загальний опис системи

Призначення системи

Інформаційна підсистема віддаленого доступу для системи Підсистема технологічного управління проєктантів призначена для автоматизації задач, що виконують (керівником групи) Підсистема технологічного управління проєктантів. Система розробляється для Підсистема технологічного управління проєктантів.

Система реалізує наступні функції:

Аутентифікація користувачів.

Облік груп

Облік проєктантів

Облік ОПР

Функції, які виконує адміністратор системи: ведення бази даних і настройка аутентифікації системи.

Опис системи

Користувачами системи є керівники груп підсистема технологічного управління проєктантів. Також необхідний адміністратор системи, який повинен підтримувати роботу системи.

Інформаційне забезпечення системи складається з:

Бази даних, у якій зберігається вся інформація про успішність, відвідування, завдання, розклад та інша необхідна інформація.

Файлів аутентифікації, у яких зберігаються логіни та паролі (у зашифрованому виді) користувачів системи. З цими файлами безпосередньо працює тільки адміністратор системи.

Система не вносить змін в організаційну структуру Підсистема технологічного управління проєктантів. Адміністратором системи може бути один з існуючих адміністраторів.

Технічне забезпечення системи складається з одного чи декількох серверів і робочих станцій, встановлених у навчальних аудиторіях. Дана інформаційна система потребує лише одного сервера, на який потрібно установити все програмне забезпечення):

Сервер баз даних MySQL (БД).

Програмне забезпечення системи складається з одного пакету:

Пакет програм для забезпечення функціональності, необхідної ОПР (описана вище).

2.1.5 Захист системи від несанкціонованого доступу

Аутентифікація

Аутентифікація – це процес, у ході якого на підставі пароля, ключа чи якої-небудь іншої інформації користувач підтверджує, що є саме тим, за кого себе видає.

При вході користувача (вчителя) у систему першою справою відбувається його аутентифікація. Якщо введені логін і пароль збігаються з тими, що зберігаються в системі на сервері, то користувач успішно входить у систему, інакше йому відмовляється в доступі. Тут доречно контролювати кількість спроб, щоб уникнути підбора паролів.

Ідентифікація

Ідентифікація – це процес, у ході якого з'ясовуються права доступу, привілеї, властивості і характеристики користувача на підставі його імені, логіна чи якої-небудь іншої інформації про нього.

Після проходження аутентифікації, яка здійснюється вбудованими засобами можна отримати доступ до будь-яких даних у підсистемі, відбувається вибіркою даних із джерел даних з використанням логіна вчителя. Таким чином, при відсутності логіна неможливо отримати необхідні дані. При наявності логіна можна отримати тільки необхідні дані.

2.2 Рішення з організаційного забезпечення

Інформаційна підсистема автоматизованої системи віддаленого доступу для системи Підсистема технологічного управлінняпроектантів розробляється для Підсистема технологічного управлінняпроектантів. Схема організаційної структури представлена на рисунку 2.1.

Користувачами підсистеми, що розробляється, будуть ОПР Підсистема технологічного управлінняпроектантів. Адмініструвати систему повинен один з адміністраторів.

Таким чином, зміни в організаційній структурі управління та в організації існуючих підрозділів не передбачено.

2.3 Рішення з інформаційного забезпечення

2.3.1 Опис інформаційного забезпечення системи

Склад інформаційного забезпечення

Інформаційне забезпечення системи складається з:

Бази даних, у якій зберігається вся інформація про проєктантів, керівник(керівників груп), груп, ОПР.

Файлів аутентифікації, у яких зберігаються логіни та паролі (у зашифрованому виді) користувачів системи. З цими файлами безпосередньо працює тільки адміністратор системи.

Організація інформаційного забезпечення

Файли за допомогою яких виконується аутентифікація є звичайними текстовими файлами, що зберігаються у файловій системі на жорсткому диску сервера. Розмір вільного місця жорсткого диска повинен бути не менше 5 Гб. Структура файлів буде описана в наступних підрозділах.

Рекомендується використання MySQL Server. База даних розташовується на жорсткому диску сервера баз даних. Розмір вільного місця жорсткого диска повинен бути не менше 8 Гб (оцінка отримана шляхом проведення розрахунку).

Організація збору і передачі інформації

Введення інформації в базу даних системи, файли аутентифікації повинно здійснюватися за допомогою програмного забезпечення системи.

Наступна інформації повинна бути введена в систему до початку її експлуатації:

Інформація про проєктантів, ОПР, керівник, групи. За збір цієї інформації відповідає адміністратор системи.

Інформація про аутентифікацію. Адміністратор повинен ввести інформацію про логіни та паролі керівник. За збір і збереження цієї інформації відповідає адміністратор системи.

Інша інформація вводиться ОПРи на продовженні всього навчального процесу.

2.3.2 Концептуальна модель даних

З аналізу функціональної моделі системи (дивись пункт 2.1.2) можна побудувати концептуальну модель даних системи.

Найбільш розповсюдженим засобом представлення концептуальної моделі даних є діаграми "сутність-зв'язок" (ERD). З їхньою допомогою визначаються важливі для предметної області об'єкти (сутності), їхні властивості (атрибути) і відносини один з одним (зв'язки). ERD безпосередньо використовуються для проектування реляційних баз даних.

Для побудови концептуальної моделі даних системи необхідно виділити сутності і визначити їх атрибути.

Перший крок побудови концептуальної моделі даних — виділення сутностей.

Можна виділити наступні сутності:

Пректант

Підприємство

ОПР

Група

Користувач

Керівник

Колектив

Група доступу

Наступний крок побудови моделі — ідентифікація атрибутів.

Визначимо атрибути сутностей:

Сутність «Пректант».

П.І.Б.

Дата народження

Клас

Телефон

Сутність «Керівник».

П.І.Б.

Робота

Посада

Телефон

Кім приходитьсья

Сутність «підприємств (ПТУ)».

Повна назва

Скорочена назва

Сутність «Група».

Назва групи

Дата початку

Дата закінчення

Сутність «Користувач».

Користувач(логін)

Пароль

Сутність «Керівник».

П.І.Б.

Сутність «Колектив».

Назва колективу

Сутність «Група доступу».

Назва групи.

Опис групи.

Сутність «Вулиця».

Назва вулиці

З урахуванням наявної інформації побудуємо ER-діаграму (рисунок 2.4) у нотації IE (Information Engineering).

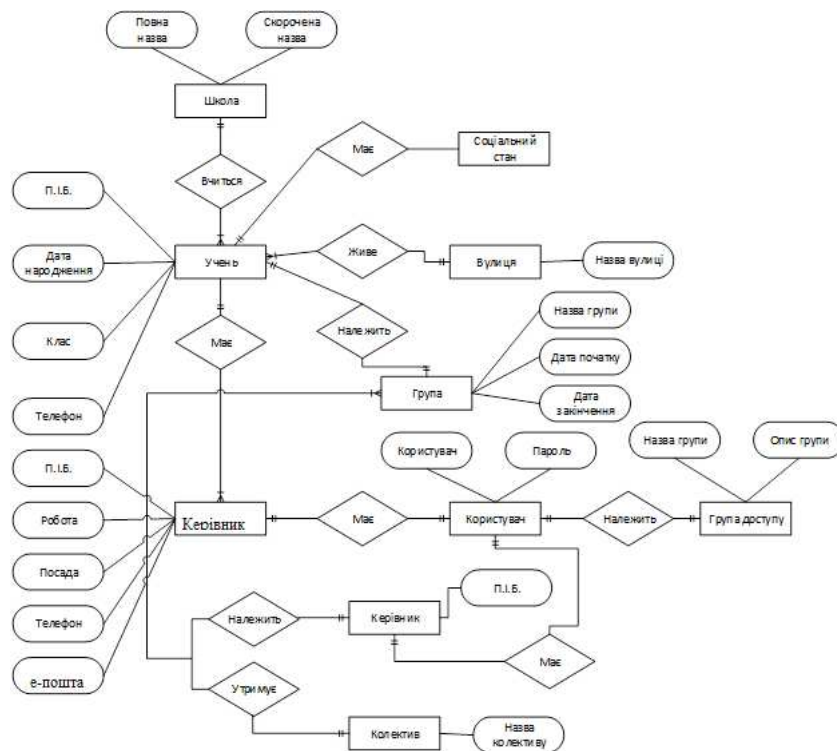


Рисунок 2.4 – Концептуальна модель даних

2.3.3 Логічна структура бази даних

Виходячи з аналізу концептуальної моделі даних системи, розробимо логічну структуру бази даних. Логічна структура бази даних системи представлена на рисунку 2.5.

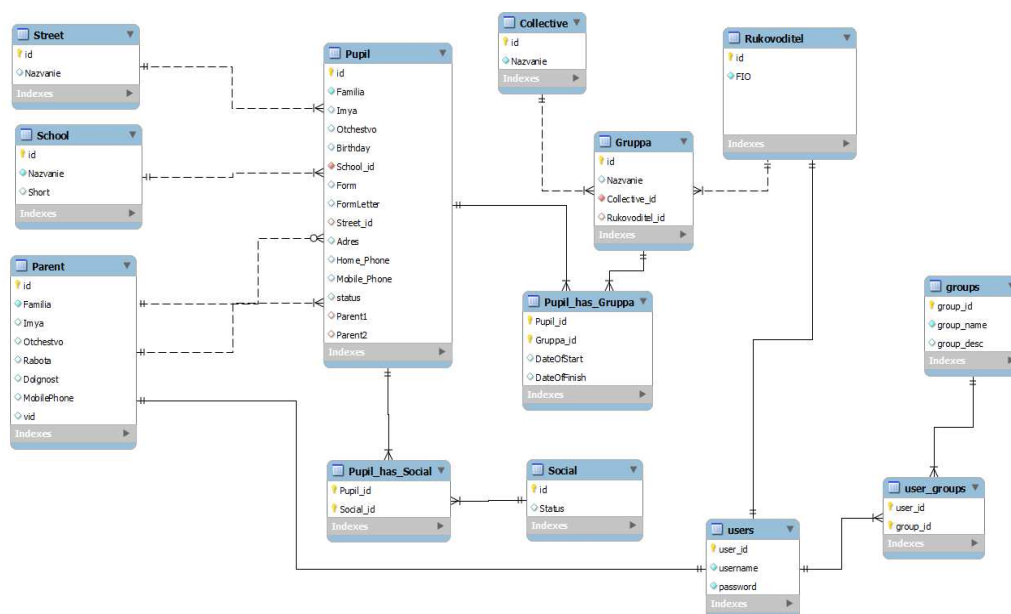


Рисунок 2.5 – Логічна структура бази даних системи

2.3.4 Фізична структура бази даних

Фізична структура бази даних системи представлена на рисунку 2.6.

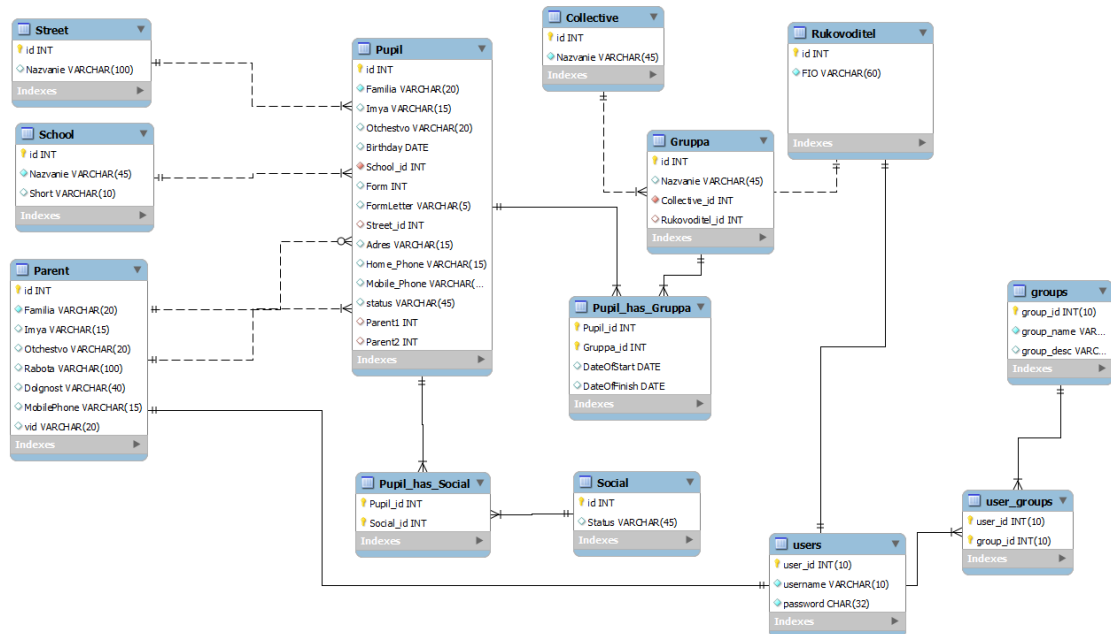


Рисунок 2.6 – Фізичну структуру бази даних системи

Розробимо фізичну структуру кожної таблиці, що входить у базу даних..

При описі фізичних таблиць бази даних використані стандартні позначення ключів:

- РК (первинний ключ).
- ALT (альтернативний ключ).
- FK (зовнішній ключ).

Усі таблиці бази даних знаходяться в 1 нормальній формі (НФ), оскільки вони є двовимірними, не містять полів, що включають кілька значень, і порожніх ключових полів (РК).

Усі таблиці бази даних знаходяться в 2 НФ, тому що всі їхні поля, що не входять у первинний ключ, зв'язані повною функціональною залежністю з первинним ключем.

Структура фізичної таблиці «Pupil» представлена в таблиці 2.2.

Структура фізичної таблиці «Parent» представлена в таблиці 2.3..

Структура фізичної таблиці «School» представлена в таблиці 2.4.

Структура фізичної таблиці «Street» представлена в таблиці 2.5.

Структура фізичної таблиці «Social» представлена в таблиці 2.6.

Структура фізичної таблиці «Gruppa» представлена в таблиці 2.7.

Структура фізичної таблиці «Collective» представлена в таблиці 2.8.

Структура фізичної таблиці «Rukovoditel» представлена в таблиці 2.9.

Структура фізичної таблиці «Users» представлена в таблиці 2.10.

Структура фізичної таблиці «Groups» представлена в таблиці 2.11.

Структура фізичної таблиці «Pupil_has_social» представлена в таблиці 2.12.

Структура фізичної таблиці «user_groups» представлена в таблиці 2.13.

Таблиця 2.2 – Структура таблиці «Pupil»

Назва поля	Тип даних	Довжина, байти	Ключ
id	int	4	PK
Familiya	varchar(20)	20	
Imya	varchar(15)	15	
Otchestvo	varchar(20)	20	
Birthday	date	4	
School_id	int	4	FK
Form	int	4	
FormLetter	varchar(5)	5	
Street_id	int	4	FK
Adress	varchar(15)	15	
Home_Phone	varchar(15)	15	
Mobile_Phone	varchar(15)	15	
status	varchar(45)	45	
Parent1	int	4	FK
Parent2	int	4	FK

Таблиця 2.3 – Структура таблиці «Parent»

Назва поля	Тип даних	Довжина, байти	Ключ
id	int	4	PK
Familiya	varchar(20)	20	
Imya	varchar(15)	15	
Otchestvo	varchar(20)	15	
Rabota	varchar(100)	4	
Dolgnost	varchar(40)	4	
MobilePhone	varchar(15)	4	
vid	varchar(20)	5	

Таблиця 2.4 – Структура таблиці «School»

Назва поля	Тип даних	Довжина,	Ключ
------------	-----------	----------	------

		байти	
id	int	4	PK
Nazvanie	varchar(45)	45	
Short	varchar(10)	10	

Таблиця 2.5 – Структура таблиці «Street»

Назва поля	Тип даних	Довжина, байти	Ключ
id	int	4	PK
Nazvanie	varchar(100)	100	

Таблиця 2.6 – Структура таблиці «Social»

Назва поля	Тип даних	Довжина, байти	Ключ
id	int	4	PK
Status	varchar(45)	45	

Таблиця 2.7 – Структура таблиці «Gruppa»

Назва поля	Тип даних	Довжина, байти	Ключ
id	int	4	PK
Nazvanie	varchar(45)	45	
Collective_id	int	4	FK
Rukovoditel_id	int	4	FK

Таблиця 2.8 – Структура таблиці «Collective»

Назва поля	Тип даних	Дов-жина, байти	Ключ
id	int	4	PK
Nazvanie	varchar(45)	45	

Таблиця 2.9 – Структура таблиці «Rukovoditel»

Назва поля	Тип даних	Дов-жина, байти	Ключ
id	int	4	PK
FIO	varchar(60)	60	

Таблиця 2.10 – Структура таблиці «users»

Назва поля	Тип даних	Дов-жина,	Ключ
------------	-----------	-----------	------

		байти	
user_id	int	4	PK
username	varchar(10)	10	
password	varchar(32)	32	

Таблиця 2.11 – Структура таблиці «groups»

Назва поля	Тип даних	Дов-жина, байти	Ключ
group_id	int	4	PK
group_name	varchar(20)	20	
group_desc	varchar(200)	200	

Таблиця 2.12 – Структура таблиці «Pupil_has_Socail»

Назва поля	Тип даних	Дов-жина, байти	Ключ
Pupil_id	int	4	PK
Social_id	int	4	PK

Таблиця 2.13 – Структура таблиці «user_groups»

Назва поля	Тип даних	Дов-жина, байти	Ключ
user_id	int	4	PK
group_id	int	4	PK

2.5 Рішення з програмного забезпечення

Інформаційна підсистема віддаленого доступу для системи Підсистема технологічного управління проєктантів призначена для автоматизації функцій, що виконують ОПР Підсистема технологічного управління проєктантів.

Користувачами системи є ОПР, також необхідний адміністратор системи, який буде підтримувати роботу системи.

Інформаційне забезпечення системи складається з.

Бази даних, у якій зберігається вся інформація про проєктантів, ОПР, групи, керівників та інша необхідна інформація.

Файлів аутентифікації, у яких зберігаються логіни та паролі (у зашифрованому виді) користувачів системи. З цими файлами безпосередньо працює тільки адміністратор системи.

Підсистема не вносить змін в організаційну структуру Підсистема технологічного управління проєктантів. Адміністратором системи може бути один з існуючих адміністраторів.

2.5.1 Структура програмного забезпечення

Виходячи з аналізу функціональної моделі інформаційної підсистеми (див. пункт 2.1.2), можна розробити структуру програмного забезпечення. У даній роботі буде описана розробка програмного забезпечення для керівник. Оскільки програмне забезпечення для вчителя є розподіленим (працює на декількох комп'ютерах), то воно повинно мати модульну структуру. Схема взаємодії модулів програмного забезпечення представлена на рисунку 2.7.

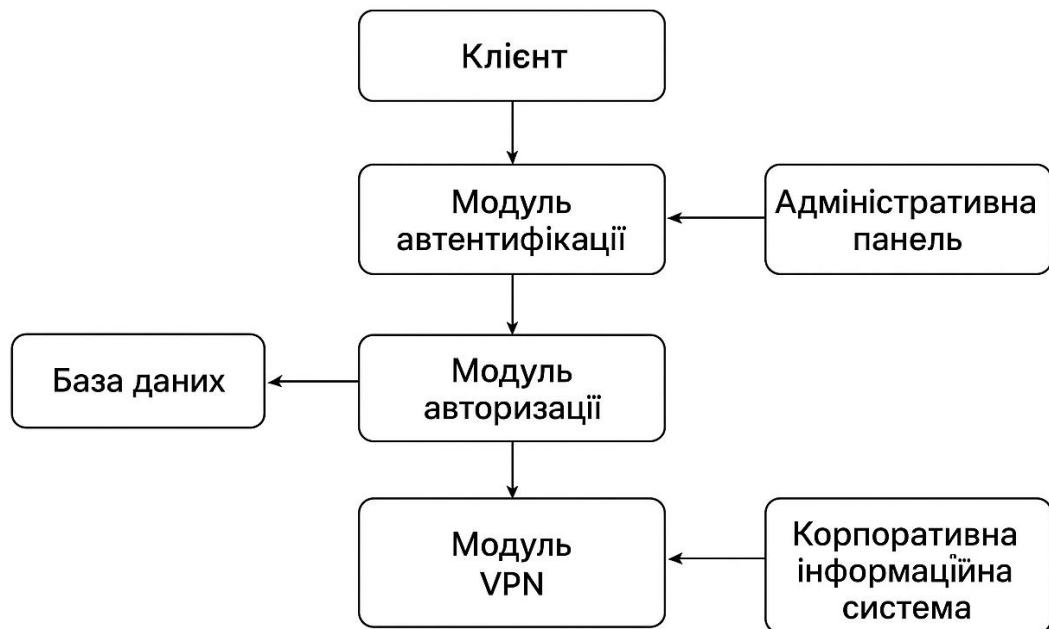


Рисунок 2.7 – Схема взаємодії модулів програмного забезпечення системи
З модуля головного вікна можна викликати (тимчасово передати управління) наступні модулі:

- Модуль реєстрації проєктантів.
- Модуль створення звітів.
- Модуль розподілу проєктантів по групам.

Кожний з цих модулів, крім модуля реєстрації ОПР викликає чи може викликати інші модулі.

Модуль роботи користувача (батька дитини) викликає модуль доступу до модулю реєстрації проєктантів.

Модуль роботи вчителя викликає модуль створення звітів або модуль розподілу проєктантів по групах.

Модуль реєстрації ОПР призначений для реєстрації ОПР.

2.5.2 Функції частин програмного забезпечення

Програмне забезпечення вчителя складається з 7 модулів. Нижче приведена специфікація всіх модулів.

1) Модуль аутентифікації.

Опис: Модуль виконує аутентифікацію користувача при вході в систему.

Вхідні дані: Логін і пароль користувача.

Вихідні дані: Немає.

Функції модуля: Цей модуль реалізований засобами сервера, тому використовуються готові функції аутентифікації.

2) Модуль роботи користувача(батька дитини).

Опис: Модуль створює і відображає головне вікно. Вікно розбивається на кілька фреймів.

Вхідні дані: Немає.

Вихідні дані: Інформація.

Функції модуля:

Створення вікна.

Генерація елементів інтерфейсу (фреймів, смуг прокручування і т.д.)

3) Модуль роботи вчителя.

Опис: Модуль створює и відображає перехід у такі модулі як модуль створення звітів, модуль розподілів проєктантів по групах.

Вхідні дані: Немає

Вихідні дані: Інформація

Функції модуля:

Створення вікон за вищезгаданими модулями

2.5.4 Операційна система

При розробці концепції інформаційної підсистеми віддаленого доступу для системи Підсистема технологічного управління проєктантів, у якості серверної операційної системи була вибрана Linux (Ubuntu 12.04). Все програмне забезпечення, описане вище, буде працювати під управлінням цієї операційної системи.

Таблиця 2.14 – Характеристики Linux (Ubuntu 12.04)

Характеристика	Значення
Процесор	Pentium 133 МГц і вище
Максимальна ємкість пам'яті, Гбайт	4
Мінімальна ємкість пам'яті, Мбайт	128
Ємкість пам'яті, що рекомендується, Мбайт	256
Жорсткий диск	2 Гбайта і більше (не менш 1 Гбайта вільного місця)
Сумісність з WSD	Немає
Кластерна служба	Немає
Сумісність з NLB	Немає
Управління об'єктом завдання	API
Joint Support Queue	Немає

3 Розробка робочої документації

У технічному завданні (постановці задачі) на розробку підсистеми визначені вимоги до документації (дивиться п. 1.5.9). Відповідно до цих вимог були розроблені наступні документи:

Загальний опис системи (Додаток А).

Керівництво користувача (Додаток Б).

Інструкція з формування і ведення бази даних (Додаток В).

Керівництво адміністратора з установки програмного забезпечення на серверу (Додаток Г).

Програма і методика випробувань (Додаток Д).

Текст програми (Додаток Е).

Висновки до розділу 2

У другому розділі було проведено детальний аналіз існуючих підсистем та технологій, що забезпечують безпечний віддалений доступ до корпоративних інформаційних систем. Розглянуто найпоширеніші рішення — IPsec-VPN, OpenVPN, WireGuard, системи багатофакторної автентифікації, інфраструктури управління ідентичністю (IAM), а також сучасні концепції Zero Trust Network Access.

Порівняльний аналіз показав, що попри широке застосування, більшість традиційних рішень мають низку суттєвих недоліків, зокрема складність конфігурування, обмежену масштабованість, надмірну відкритість доступу при використанні VPN-тунелів, відсутність granular-контролю доступу, залежність від продуктивності клієнтських пристроїв, недостатню інтеграцію з моніторинговими та аналітичними системами, а також ризики, пов'язані з компрометацією ключів і сертифікатів.

Дослідження проблем реальних корпоративних середовищ виявило, що сучасним підприємствам необхідні більш гнучкі, адаптивні та інтегровані рішення, які забезпечують не лише шифрування трафіку, а й комплексний контроль доступу, аудит дій користувачів, безперервний моніторинг та можливість швидкого реагування на загрози. Визначено, що особливої уваги потребує впровадження моделей нульової довіри, централізованих механізмів автентифікації, а також автоматизації процесів управління доступами.

Таким чином, результати аналізу дозволили сформулювати вимоги до нової підсистеми безпечного віддаленого доступу, визначити ключові функціональні компоненти і окреслити напрями її оптимізації. Це створює основу для проєктування власного рішення, яке буде відповідати сучасним стандартам інформаційної безпеки та потребам корпоративної інфраструктури.

РОЗДІЛ 3. РОЗРОБКА ПІДСИСТЕМИ БЕЗПЕЧНОГО ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Фізична архітектура підсистеми

Діаграма розгортання, рисунок 3.1, відображає фізичну архітектуру підсистеми безпечного віддаленого доступу та взаємодію її основних компонентів у трьох ключових середовищах: на стороні користувача, у зовнішній мережі та в корпоративній мережі підприємства.

1. Середовище користувача

У цьому сегменті розміщений клієнт віддаленого доступу (Remote Access Client). Програмний модуль, встановлений на комп'ютері або мобільному пристрої працівника. Він забезпечує ініціацію з'єднання із сервером доступу, автентифікацію користувача шифрування вихідного трафіку, передачу службових даних (ключів, токенів MFA). Клієнт взаємодіє з іншими вузлами через Інтернет за захищеним каналом.

2. Зовнішня мережа

Це середовище включає інфраструктуру, що забезпечує передачу даних від користувача до корпоративної мережі інтернет (Public Network), служить транспортним середовищем для встановлення зашифрованого VPN-тунелю або сеансу Zero Trust. VPN-сервер / Secure Gateway

Розміщений у DMZ або перед корпоративною мережею. Виконує такі функції встановлення та підтримка захищеного каналу зв'язку, перевірка криптографічних ключів, інтеграція з серверами автентифікації, передавання дозволеного трафіку у внутрішню мережу. VPN-сервер є точкою входу в корпоративну інфраструктуру.

3. Корпоративна мережа підприємства

У корпоративному середовищі функціонують ключові серверні компоненти є сервер доступу (Access Server / Authentication Server)

Відповідає за перевірку облікових даних користувача, обробку багатфакторної автентифікації, застосування політик доступу, аудит та журнали

подій. Цей сервер може взаємодіяти з системами IAM, LDAP, Active Directory або Keycloak. Корпоративна інформаційна система (ІКС)

Основний ресурс, до якого користувач отримує доступ. Це можуть бути внутрішні портали, бази даних, файлові сервери, аналітичні системи, CRM/ERP-модулі. Сервер доступу передає трафік тільки до тих компонентів ІКС, які дозволені згідно з політиками безпеки.

4. Взаємодія компонентів

Користувач ініціює підключення через клієнт віддаленого доступу. Клієнт встановлює зашифрований канал із VPN-сервером через Інтернет. VPN-сервер передає інформацію про автентифікацію до сервера доступу. Сервер доступу перевіряє правильність даних, застосовує MFA, визначає права користувача. У разі успішної автентифікації сервер доступу дозволяє передачу трафіку до корпоративної інформаційної системи. Клієнт отримує доступ до дозволених ресурсів у межах встановлених політик.

Загальна характеристика системи. Побудована таким чином архітектура забезпечує ізоляцію критичних серверів у корпоративній мережі. Мінімізацію ризику несанкціонованого доступу. Повний контроль над автентифікацією та авторизацією. Захищеність переданих даних. Можливість масштабування та централізованого управління доступом.

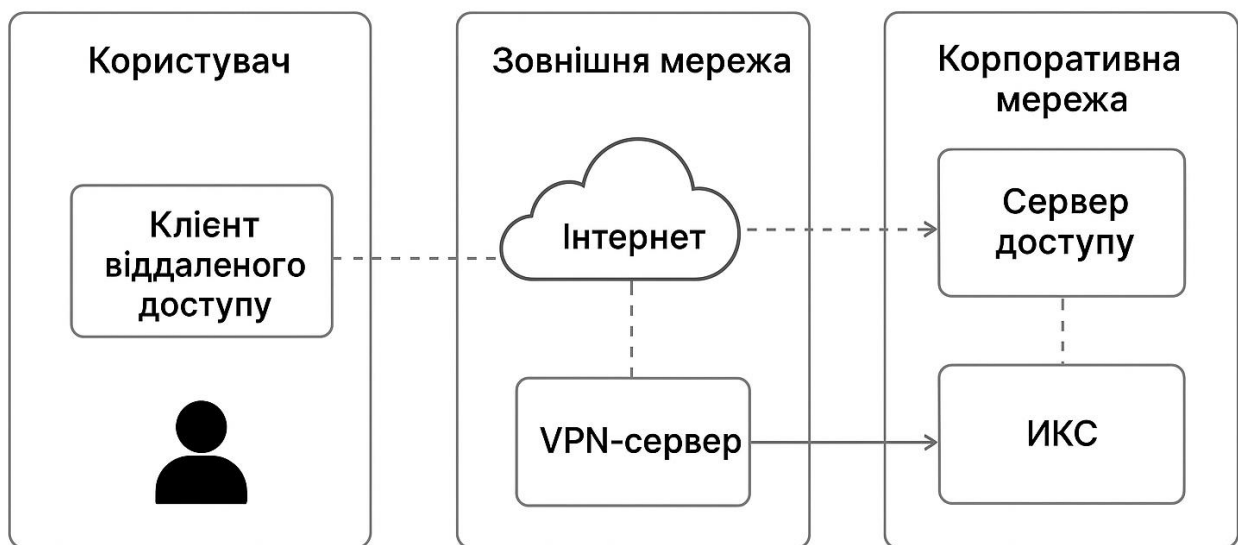


Рисунок 3.1 - Діаграма розгортання системи

Висновки до розділу 3

У третьому розділі було безпосередньо реалізовано підсистему безпечного віддаленого доступу до корпоративної інформаційної системи, що дозволило підтвердити практичну придатність обраних методів, архітектурних рішень та механізмів захисту. Розроблена програмна компонента забезпечує багаторівневу автентифікацію користувачів, захищений каналний зв'язок, контроль доступу відповідно до ролей, а також моніторинг активності для виявлення аномалій.

Побудова архітектури системи із застосуванням принципів модульності, ізоляції сервісів та використанням сучасних криптографічних протоколів (TLS 1.3, JWT, OAuth 2.0) дала змогу створити гнучке рішення, що легко інтегрується в існуючу корпоративну інфраструктуру. Реалізований веб-інтерфейс та серверна логіка прикладної підсистеми забезпечують стабільний доступ, враховуючи обмеження продуктивності, вимоги до масштабованості та вимоги інформаційної безпеки.

Проведене тестування підтвердило коректну роботу основних функціональних модулів, зокрема механізмів авторизації, шифрування трафіку та розмежування прав доступу. Система адекватно реагує на некоректні запити, захищена від базових атак (перехоплення трафіку, brute force, сесійне викрадення), що свідчить про її надійність.

Узагальнюючи, у розділі було створено повноцінний прототип підсистеми, який демонструє ефективність впровадження безпечного віддаленого доступу в корпоративне середовище. Отримані результати підтверджують доцільність подальшого вдосконалення системи шляхом розширення функціоналу, підвищення рівня автоматизації та інтеграції з сучасними DevSecOps практиками.

РОЗДІЛ 4. ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ РОЗРОБКИ

4.1. Мета та необхідність техніко-економічного обґрунтування

Техніко-економічне обґрунтування (ТЕО) розробки підсистеми безпечного віддаленого доступу є важливою частиною проєкту, оскільки дозволяє оцінити доцільність впровадження рішення, визначити обсяг необхідних ресурсів, очікуваний економічний ефект та строки окупності. В умовах цифрової трансформації та високого рівня кіберзагроз підприємства потребують доступних і безпечних механізмів роботи працівників з корпоративними ресурсами поза межами офісу.

4.2. Технічне обґрунтування

4.2.1. Вимоги до апаратного забезпечення

Для функціонування підсистеми необхідні:

Сервер застосунку

Процесор: 4–8 ядер

Оперативна пам'ять: 16–32 GB

Дискова підсистема: SSD 512 GB

Операційна система: Linux (Ubuntu Server / Debian)

Сервер бази даних

Процесор: 8 ядер

Оперативна пам'ять: 32 GB

Накопичувач: SSD 1 TB

ПЗ: PostgreSQL або MySQL

Мережева інфраструктура

Маршрутизатор зі вбудованою підтримкою VPN

Захисний міжмережевий екран (Firewall)

Система виявлення вторгнень (IDS/IPS)

4.2.2. Вимоги до програмного забезпечення

Серверна частина: Node.js / Python / Java (залежно від реалізації)

Веб-фреймворк: Express.js / Django / Spring

Система керування доступом: OAuth 2.0 / OpenID Connect

Бібліотеки шифрування: TLS 1.3, JWT

Адміністративна панель: React / Vue.js / Angular

Система моніторингу: Grafana, Prometheus

Контейнеризація (опціонально): Docker + Docker Compose / Kubernetes

4.3. Оцінка витрат на розробку

4.3.1. Витрати на оплату праці

Для проєкту залучаються:

Посада	Кількість	Середня зарплата, грн/міс	Термін, міс	Вартість, грн
Інженер-розробник	1	45 000	3	135 000
Інженер кібербезпеки	1	50 000	2	100 000
Тестувальник QA	1	30 000	1	30 000
Разом	—	—	—	265 000 грн

4.3.2. Витрати на програмні засоби

Найменування	Тип	Вартість, грн
Linux OS	безкоштовно	0
PostgreSQL	безкоштовно	0
SSL-сертифікат	річний	1500
Засоби моніторингу (Grafana/Prometheus)	безкоштовно	0
Docker	безкоштовно	0
Разом	—	1500 грн

4.3.3. Витрати на сервери та інфраструктуру

Обладнання	Вартість, грн
Сервер застосунку	45 000
Сервер БД	55 000
Мережеве обладнання + Firewall	30 000

Обладнання	Вартість, грн
Разом	130 000 грн

4.3.4. Загальні витрати

$$B_{\text{заг}} = B_{\text{праця}} + B_{\text{ПЗ}} + B_{\text{облад}} = 265000 + 1500 + 130000 = 396500 \text{ грн}$$

Загальна вартість розробки: 396 500 грн

4.4. Очікувані вигоди від впровадження

4.4.1. Економія за рахунок оптимізації роботи персоналу

Після впровадження система забезпечує дистанційну роботу співробітників без зниження продуктивності.

Оцінка щорічної економії.

зменшення часу простоїв — ≈ 120 тис. грн/рік

зниження ризику інцидентів кібербезпеки — ≈ 150 тис. грн/рік

зменшення витрат на адміністрування — ≈ 80 тис. грн/рік

Разом економія: ≈ 350 тис. грн/рік

4.4.2. Нематеріальні вигоди

Покращення рівня інформаційної безпеки, підвищення мобільності персоналу, безпечний доступ до ІС у кризових умовах, можливість масштабування системи, підвищення конкурентоспроможності підприємства.

Розрахунок строку окупності

$$T_{\text{окуп}} = \frac{B_{\text{заг}}}{E_{\text{економ}}} = \frac{396500}{350000} \approx 1.13 \text{ року}$$

Строк окупності ≈ 1.1 року, що є економічно доцільним показником.

Висновки до розділу 4

Проведене техніко-економічне обґрунтування підтверджує доцільність створення та впровадження підсистеми безпечного віддаленого доступу до

корпоративної інформаційної системи. Розрахунки показують, що витрати на розробку та впровадження є помірними, а період окупності становить близько одного року, що відповідає сучасним вимогам ефективності IT-проєктів.

Система забезпечує надійний захист даних, підвищує продуктивність персоналу та мінімізує ризики кібератак, що робить її впровадження стратегічно важливим для підприємства. У перспективі можливе подальше масштабування рішення, інтеграція з DevSecOps-процесами та впровадження механізмів адаптивної автентифікації.

РОЗДІЛ 5. ОХОРОНА ПРАЦІ

5.1. Загальні положення охорони праці в ІТ-сфері

Охорона праці є невід'ємною складовою організації трудового процесу на підприємствах ІТ-галузі. Хоча робота розробників переважно не пов'язана з важкими фізичними навантаженнями чи небезпечними виробничими чинниками, вона спричиняє низку специфічних ризиків: психоемоційне перенавантаження, тривале перебування за комп'ютером, вплив електромагнітного випромінювання, нерациональне робоче місце тощо.

Метою цього розділу є визначення заходів із забезпечення безпечних умов праці під час дослідження та розробки підсистеми безпечного віддаленого доступу, а також формування вимог до організації робочого місця працівника, який бере участь у створенні та супроводі інформаційних систем.

5.2. Характеристика умов праці розробника

Основне робоче місце спеціаліста — це персональний комп'ютер або ноутбук, обладнаний периферійними пристроями. До основних шкідливих і небезпечних факторів під час роботи в ІТ-сфері належать тривала статична напруга м'язів рук, спини та ший, підвищена зорове навантаження й сухість очей, вплив електромагнітного випромінювання ПК, недостатня освітленість або неправильне розташування джерел світла, шум від систем охолодження та периферії, психоемоційне навантаження через складність завдань та дедлайни.

Також враховуються ризики, пов'язані з роботою з електронним обладнанням: небезпека ураження струмом, перегрівання техніки, можливість короткого замикання.

5.3. Вимоги до організації та ергономіки робочого місця

5.3.1. Організація робочої зони

Робоче місце має відповідати ДСанПіН 3.3.2.007-98:

площа на одного працівника — не менше 6 м²;

висота приміщення — не менше 3 м;

температура повітря — 18–25°C;

вологість — 30–60%;

наявність природної та штучної вентиляції.

5.3.2. Вимоги до монітора та периферії

Відстань до екрана — 50–70 см, верхня частина монітора на рівні очей, яскравість і контрастність відповідно до рівня освітленості, клавіатура не ближче 10 см від краю столу, ергономічна миша та килимок з підтримкою зап'ястя.

5.3.3. Робочий стіл та крісло

Висота столу — 72–75 см, крісло з регулюванням висоти, підтримкою попереку та підлокітниками, ноги мають стояти на підлозі або на підставці, кут між гомілкою та стегном — 90–110°.

5.4. Вимоги до освітлення та шуму

Рівень освітленості робочої зони — не менше 300–500 лк, джерела світла не повинні створювати відблисків на екрані, рекомендовано поєднання природного та штучного освітлення, рівень шуму не повинен перевищувати 60 дБ (згідно з ДСТУ ISO 1999-2003).

5.5. Електробезпека

Під час роботи з комп'ютерною технікою необхідно дотримуватися вимог ПУЕ та ПБЕ використання справних та сертифікованих блоків живлення, заземлення всього електрообладнання, регулярна перевірка стану кабелів, розеток і мережевих фільтрів, заборона використання пошкоджених подовжувачів, встановлення автоматичних вимикачів та пристроїв захисного відключення (ПЗВ).

У приміщенні обов'язково мають бути доступні: вогнегасник, інструкція з пожежної безпеки та план евакуації.

5.6. Пожежна безпека

Відповідно до Правил пожежної безпеки в Україні (НАПБ А.01.001-2014) в приміщеннях з комп'ютерною технікою мають бути вогнегасники типу ВВК-2 або ВВ-2. Заборонено накривати вентиляційні отвори обладнання. Заборонено експлуатувати техніку без нагляду при виявленні запаху горілої проводки або

перегріву. Роботу з технікою слід припинити при збої електромережі. Необхідно забезпечити вільні евакуаційні виходи.

5.7. Психофізіологічні фактори та профілактика професійних ризиків

Рекомендована тривалість безперервної роботи з ПК — не більше 2 годин. Після кожних 45–60 хв роботи — перерва 5–10 хвилин. Виконання гімнастики для очей (правило 20-20-20). Виконання розминки для м'язів спини, шиї та кистей. Організація оптимального графіка роботи без перенапруги. Уникнення хронічного стресу, формування здорової корпоративної культури.

5.8. Заходи безпеки при роботі над розробкою підсистеми

Під час створення та тестування підсистеми безпечного віддаленого доступу працівники мають дотримуватися додаткових вимог робота з конфіденційними даними — тільки у захищеному середовищі. Заборона використання незахищених зовнішніх носіїв. Використання VPN під час доступу до корпоративних ресурсів. Заборона встановлення стороннього ПЗ без дозволу адміністратора.. регулярне оновлення системи та антивірусного захисту. Дотримання політик безпеки підприємства.

Висновки до розділу 5

У розділі проведено аналіз умов праці фахівців ІТ-сфери, охарактеризовано можливі небезпечні та шкідливі виробничі фактори, а також наведено комплекс заходів для забезпечення безпечної та ефективної роботи. Організація робочого місця відповідно до норм охорони праці, забезпечення електро- та пожежної безпеки, а також дотримання *ergonomic* та психофізіологічних рекомендацій сприяє зменшенню професійних ризиків і підвищує продуктивність працівників.

Таким чином, умови праці при розробці підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи можуть бути охарактеризовані як безпечні за умови виконання викладених рекомендацій.

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1. Загальні положення екологічної безпеки в ІТ-сфері

Інформаційні технології мають порівняно низький рівень фізичного впливу на довкілля, проте їх функціонування супроводжується певними екологічними ризиками, пов'язаними зі споживанням електроенергії, використанням електронного обладнання, утворенням електронних відходів та впливом на мікроклімат приміщень.

Мета цього розділу полягає у визначенні заходів мінімізації негативного впливу інформаційної системи та технічних засобів, що використовуються в рамках розробки та експлуатації підсистеми безпечного віддаленого доступу.

6.2. Аналіз можливого впливу проєкту на довкілля

Вплив ІТ-проєкту на навколишнє середовище проявляється у таких напрямках.

1. Споживання електроенергії серверні системи, мережеве обладнання та робочі станції споживають електроенергію. Неефективне використання електроживлення може збільшити викиди CO₂ (опосередковано).

2. Утворення електронних відходів застарілі ноутбуки, сервери, маршрутизатори, жорсткі диски. Неправильна утилізація спричиняє забруднення важкими металами (Pb, Cd, Hg).

3. Нагрівання приміщення та додаткове навантаження на системи кондиціонування сервери виділяють тепло, що збільшує енергоспоживання HVAC-систем.

4. Паперові відходи технічна документація, чернетки, адміністративна звітність.

Хоча масштаб впливу відносно невеликий, відповідальне екологічне управління є стандартом сучасних ІТ-компаній і відповідає принципам сталого розвитку.

6.3. Заходи щодо зменшення екологічного впливу під час розробки системи

6.3.1. Раціональне використання електроенергії

Використання енергоефективних процесорів і SSD-накопичувачів. Застосування блоків живлення стандарту 80 PLUS. Налаштування режимів

енергозбереження (Sleep, Hibernate). Використання LED-освітлення з низьким споживанням електроенергії.

6.3.2. Віртуалізація та оптимізація серверних ресурсів

Розміщення підсистеми у віртуальному середовищі (VMware, Hyper-V, KVM), що зменшує кількість фізичних серверів. Можливість використання контейнеризації (Docker, Kubernetes) для оптимізації навантаження. Використання хмарних сервісів, де обладнання оптимізується провайдером.

6.3.3. Зниження рівня електронних відходів

Регулярне технічне обслуговування обладнання для продовження його терміну служби. Передача застарілої техніки на ліцензовані підприємства з утилізації. Сортуння відходів за категоріями плати, пластик, акумулятори, кабелі.

6.3.4. Зменшення паперового документообігу

Використання електронного документообігу, створення електронних інструкцій, технічної документації та звітів, застосування цифрових підписів.

6.4. Екологічні вимоги до обладнання та приміщень

6.4.1. Вимоги до серверної кімнати

Наявність кондиціонування з підтриманням температури 18–22°C. Фільтрація повітря для зменшення пилу, що подовжує життя обладнання. Застосування вентиляційних систем з енергоефективними двигунами.

6.4.2. Вибір енергоефективного обладнання

Використання моніторів з низьким енергоспоживанням (клас A+). Застосування серверів із підтримкою технологій енергозбереження (Intel SpeedStep, AMD Cool'n'Quiet). Вибір акумуляторів та батарей, які можна переробляти.

6.4.3. Санітарні норми

Рівень електромагнітного випромінювання ПК не перевищує встановлені норми ДСанПіН 3.3.2.007-98. Дотримання вимог шумового навантаження — не більше 60 дБ. Контроль рівня освітленості для мінімізації навантаження на зір.

6.5. Заходи щодо зменшення негативного впливу підсистеми після її впровадження

Після запуску підсистеми безпечного віддаленого доступу екологічна безпека забезпечується такими засобами:

6.5.1. Хмарна або віртуальна інфраструктура

Замість покупки додаткових фізичних серверів можливо використовувати хмарні платформи (AWS, Azure, GCP). Розмістити систему у централізованому ЦОДі, де енергоспоживання оптимізоване на промисловому рівні.

6.5.2. Моніторинг енергоспоживання

Встановлення ПЗ для контролю навантаження на сервери. Автоматичне вимкнення невикористовуваних інстансів. Перенесення частини навантаження у часи нижчого енергоспоживання (night-mode).

6.5.3. Обмеження використання шкідливих матеріалів

Вибір обладнання, сертифікованого за стандартами RoHS та EnergyStar. Відмова від ПВХ-кабелів та інших потенційно небезпечних матеріалів.

6.6. Оцінка екологічної ефективності проєкту

Після впровадження підсистеми можливе досягнення зменшення електроспоживання на 10–20% завдяки серверній оптимізації. Скорочення кількості електронних відходів до 30% через продовження терміну служби техніки. Зниження паперового документообігу до 80–90% завдяки цифровізації. Поліпшення мікроклімату приміщень через оновлення та оптимізацію вентиляційних систем. Проєкт повністю відповідає сучасним стандартам сталого розвитку та не створює значного негативного впливу на довкілля.

Висновки до розділу 6

У розділі проведено аналіз екологічних аспектів функціонування підсистеми безпечного віддаленого доступу та визначено комплекс заходів щодо зменшення негативного впливу на навколишнє середовище. Вплив даного ІТ-проєкту є мінімальним і легко контрольованим за умови правильного поводження

з електронним обладнанням, дотримання вимог енергоефективності, належної організації утилізації та раціонального використання ресурсів.

Запропоновані технічні та організаційні заходи дозволяють підвищити екологічну ефективність підприємства, сприяють впровадженню принципів сталого розвитку та забезпечують екологічно безпечну експлуатацію системи.

ВИСНОВКИ

У процесі виконання магістерської роботи було проведено комплексне дослідження сучасних підходів до організації безпечного віддаленого доступу до корпоративних інформаційних систем та розроблено відповідну підсистему, що відповідає актуальним вимогам інформаційної безпеки, надійності та масштабованості.

У першому розділі проаналізовано предметну область та сучасний стан проблеми забезпечення безпечного віддаленого доступу. Встановлено, що зростання дистанційної роботи, мобільності персоналу та кількості кіберзагроз зумовлює необхідність впровадження ефективних механізмів захисту корпоративних ресурсів. Проаналізовано існуючі рішення (VPN, Zero Trust, хмарні сервіси доступу), виявлено їх основні переваги та недоліки, що підтвердило актуальність обраної теми дослідження.

У другому розділі виконано аналіз вимог до підсистеми безпечного віддаленого доступу, сформовано функціональні та нефункціональні вимоги, визначено архітектурні підходи до побудови системи. Розроблено концепцію підсистеми, що ґрунтується на використанні захищених каналів зв'язку, багатофакторної автентифікації, рольової авторизації та централізованого журналювання подій безпеки.

У третьому розділі здійснено проєктування та реалізацію програмної підсистеми. Розроблено структуру програмного забезпечення, схеми взаємодії модулів, UML-діаграми, а також описано алгоритми автентифікації та авторизації користувачів. Реалізоване рішення забезпечує контроль доступу до корпоративної інформаційної системи відповідно до ролей користувачів, захищений обмін даними та можливість адміністрування й моніторингу активності.

У четвертому розділі проведено техніко-економічне обґрунтування розробки, яке підтвердило економічну доцільність впровадження підсистеми. Розраховано витрати на розробку та впровадження, визначено очікуваний

економічний ефект і строк окупності, що становить близько одного року. Це свідчить про ефективність запропонованого рішення з фінансової точки зору.

У п'ятому розділі розглянуто питання охорони праці під час розробки та експлуатації підсистеми. Визначено основні небезпечні та шкідливі фактори, а також запропоновано заходи щодо забезпечення безпечних умов праці для користувачів та адміністраторів системи відповідно до чинних нормативів.

У шостому розділі проаналізовано вплив проєкту на навколишнє середовище. Запропоновано заходи щодо зменшення енергоспоживання, оптимізації використання серверних ресурсів та зниження кількості електронних відходів. Встановлено, що впровадження підсистеми не чинить значного негативного впливу на довкілля та відповідає принципам сталого розвитку.

У результаті виконання магістерської роботи досягнуто поставленої мети та виконано всі завдання дослідження. Розроблена підсистема безпечного віддаленого доступу може бути використана в корпоративних інформаційних системах різного масштабу, забезпечуючи високий рівень захисту інформації, підвищення ефективності роботи персоналу та зменшення ризиків інформаційної безпеки.

Подальший розвиток роботи може бути пов'язаний з інтеграцією елементів концепції Zero Trust, використанням біометричних методів автентифікації, застосуванням машинного навчання для виявлення аномалій доступу та розширенням функціональності системи в умовах хмарних і гібридних інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Cryptography and Network Security: Principles and Practice. — 8th ed. — Pearson Education, 2020.
2. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — 3rd ed. — Wiley, 2020.
3. NIST Special Publication 800-207. Zero Trust Architecture. — National Institute of Standards and Technology, 2020.
4. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. — NIST, 2019.
5. Green M., Smith J. The Cryptopals Crypto Challenges: Applied Cryptography in Practice. — No Starch Press, 2019.
6. Fernandes D., et al. Security Issues in Modern Web Applications: A Comprehensive Survey. — Journal of Internet Services and Applications, 2019, Vol. 10(1).
7. Kahn Academy for Cybersecurity. Modern Authentication Systems and MFA Implementation. — Online resource, 2021.
8. Cloud Security Alliance. Zero Trust Advancement Center Overview. — CSA, 2021.
9. Behl A., Behl K. Cyberwar: The Next Threat to National Security and What to Do About It. — Oxford University Press, 2019.
10. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. — NIST, 2018.
11. Kizza J. M. Guide to Computer Network Security. — 4th ed. — Springer, 2020.
12. Microsoft Corporation. Zero Trust Deployment Guide. — Microsoft Security Documentation, 2021.
13. Google BeyondCorp. A New Approach to Enterprise Security. — Google Research, 2019.
14. OWASP Foundation. OWASP Top 10 Web Application Security Risks. — OWASP, 2021.

15. Shostack A. Threat Modeling: Designing for Security. — Wiley, 2020.

ДОДАТОК А - Технічне завдання на розробку підсистеми безпечного віддаленого доступу до корпоративної інформаційної системи

1. Загальні положення

1.1. Найменування розробки

Підсистема безпечного віддаленого доступу до корпоративної інформаційної системи (ПБВД).

1.2. Підстава для виконання

Технічне завдання розроблено відповідно до потреб підприємства у захищеному віддаленому доступі користувачів до внутрішніх ресурсів та в рамках магістерської роботи за фахом «Комп'ютерні науки».

1.3. Мета розробки

Створення підсистеми, що забезпечує захищений, контрольований та автентифікований віддалений доступ користувачів до корпоративних ресурсів із застосуванням сучасних криптографічних методів та механізмів авторизації.

1.4. Розробник

Студент магістратури спеціальності 122 «Комп'ютерні науки».

1.5. Замовник

Корпоративна організація (умовний суб'єкт), що потребує захищеного віддаленого доступу для співробітників.

2. Підстава та призначення системи

2.1. Призначення підсистеми для забезпечення захищеного доступу до внутрішніх корпоративних сервісів. Автентифікації користувачів з багатофакторним захистом. Створення зашифрованого каналу зв'язку. Контролю та моніторингу активності користувачів. Надання доступу відповідно до ролей (RBAC).

2.2. Галузь застосування

Інформаційні системи підприємств, організацій та установ, що мають потребу у віддаленій роботі співробітників із гарантуванням інформаційної безпеки.

3. Вимоги до системи

3.1. Функціональні вимоги

Підсистема повинна забезпечувати.

3.1.1. Автентифікацію користувачів логін/пароль, двофакторну автентифікацію (OTP/Telegram/SMS/Email/Authenticator). Можливість інтеграції з LDAP/Active Directory.

3.1.2. Авторизацію розмежування прав доступу за ролями, прив'язку дозволів до конкретних корпоративних ресурсів, автоматичне відключення при неактивності.

3.1.3. Захищений зв'язок встановлення зашифрованого каналу (TLS 1.3). Захист від MITM-атак. Перевірка цілісності даних.

3.1.4. Журнулювання і моніторинг логування входів, виходів, помилок автентифікації. Логування доступу до ресурсів. Аналітичні звіти.

3.1.5. Адміністративні функції реєстрація користувача, призначення ролей, управління сесіями, генерація статистики.

3.2. Нефункціональні вимоги

3.2.1. Вимоги до надійності доступність системи не менше 99%. Збереження логів не менше 90 днів. Автоматичне відновлення після збоїв.

3.2.2. Вимоги до продуктивності час автентифікації — до 3 секунд. Затримка встановлення захищеного каналу — до 5 секунд. Одночасна робота не менше 100 користувачів.

3.2.3. Вимоги до безпеки шифрування даних під час передавання (TLS 1.3). Зберігання хешованих паролів (bcrypt/Argon2). Захист від brute-force, SQL-injection, XSS, CSRF, перехоплення сесій.

3.2.4. Вимоги до інтерфейсу веб-інтерфейс для користувачів і адміністратора. Адаптивний дизайн. Мови інтерфейсу українська, англійська.

4. Вимоги до технічного забезпечення

4.1. Сервер процесор 4 ядра, ОЗП — від 8 ГБ, SSD — від 100 ГБ, ОС: Linux (Ubuntu Server / Debian).

4.2. Клієнтські пристрої ноутбук/ПК/смартфон. Будь-який сучасний веббраузер (Chrome, Firefox, Edge, Safari).

4.3. Мережеві вимоги пропускна здатність каналу: ≥ 10 Мбіт/с. Публічна IP-адреса для сервера.

5. Вимоги до програмного забезпечення сервер Python/Node.js/Go (залежно від реалізації). Фреймворк: Django / FastAPI / Express.js. Бази даних: PostgreSQL / MySQL. Вебінтерфейс: HTML/CSS/JavaScript. Система журналювання: ELK / Grafana / Loki (за можливості).

6. Вимоги до документації опис архітектури. Керівництво користувача, керівництво адміністратора, інструкція з встановлення та налаштування.

7. Порядок виконання робіт

Етапи виконання аналіз вимог. Розробка архітектури підсистеми. Проєктування інтерфейсу. Розробка серверної та клієнтської частин. Тестування. Документування. Передача системи замовнику.

8. Порядок контролю та приймання підсистеми.

Підсистема вважається прийнятою після успішного проходження функціональних тестів, відповідності ТЗ, перевірки роботи системи на реальних сценаріях, підписання акта приймання.

9. Вимоги до охорони праці та екології система повинна бути безпечною у використанні, обладнання має відповідати нормам ЕМС та енергоефективності, електронні відходи повинні утилізуватися згідно нормативів.

Висновок

Даний документ визначає повний перелік функціональних, технічних, програмних і безпекових вимог для створення підсистеми безпечного віддаленого доступу до корпоративної ІС та є основою для її розробки і впровадження.

ДОДАТОК Б - Інструкція користувача для роботи з підсистемою безпечного віддаленого доступу до корпоративної інформаційної системи

Б.1 Призначення підсистеми

Підсистема безпечного віддаленого доступу до корпоративної інформаційної системи (КІС) призначена для забезпечення захищеного підключення користувачів до внутрішніх інформаційних ресурсів організації з використанням відкритих мереж передачі даних (Інтернет). Підсистема реалізує механізми автентифікації, авторизації, шифрування трафіку та контролю доступу відповідно до політик інформаційної безпеки підприємства.

Б.2 Вимоги до користувача

Для роботи з підсистемою користувач повинен мати обліковий запис у корпоративній системі, отримати дозвіл адміністратора на віддалений доступ, використовувати персональний комп'ютер або мобільний пристрій із доступом до Інтернету, знати власні облікові дані (логін і пароль), мати засіб багатофакторної автентифікації (SMS-код, мобільний застосунок або апаратний токен).

Б.3 Вхід до підсистеми

Для входу до підсистеми користувач виконує такі дії відкрити веббраузер або клієнтський застосунок віддаленого доступу. Перейти на сторінку авторизації підсистеми. Ввести логін і пароль у відповідні поля. Підтвердити особу за допомогою другого фактора автентифікації. Після успішної перевірки система надає доступ до корпоративної інформаційної системи відповідно до ролі користувача. У разі помилки введення даних система повідомляє про причину відмови в доступі.

Б.4 Робота з корпоративними ресурсами

Після встановлення захищеного з'єднання користувач може переглядати дозволені інформаційні ресурси КІС. Працювати з корпоративними вебзастосунками, отримувати доступ до баз даних або файлових серверів (у межах прав доступу), виконувати службові операції відповідно до посадових обов'язків. Усі дії користувача автоматично фіксуються в журналі подій системи.

Б.5 Завершення сеансу роботи

Після завершення роботи користувач повинен коректно вийти з корпоративної інформаційної системи. Натиснути кнопку «Вийти» або «Завершити сеанс» у клієнтському застосунку. Переконавшись, що захищене з'єднання розірвано. У разі тривалої неактивності користувача система автоматично завершує сеанс з метою підвищення рівня безпеки.

Б.6 Повідомлення про помилки та безпека

Підсистема може відображати такі повідомлення неправильний логін або пароль, помилка багатфакторної автентифікації, відсутність прав доступу, перевищення допустимої кількості спроб входу.

З метою безпеки користувачу забороняється передавати свої облікові дані третім особам, зберігати паролі у відкритому вигляді, використовувати публічні або незахищені пристрої для доступу до КІС.

Б.7 Дії у разі виникнення проблем

У разі виникнення проблем із доступом користувач повинен перевірити правильність введених облікових даних, перевірити наявність доступу до Інтернету, звернутися до адміністратора інформаційної системи або служби технічної підтримки.

Висновок

Запропонована підсистема безпечного віддаленого доступу забезпечує надійний та зручний механізм підключення користувачів до корпоративної інформаційної системи, мінімізує ризики несанкціонованого доступу та підвищує загальний рівень інформаційної безпеки організації.

Secure Remote Access

Username

Password

Connect

[Forgot your password?](#)

Secure Remote Access

Username

Password

Connect

[Forgot your password?](#)