

Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“___” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи забезпечення обміну
інформацією у корпоративній мережі на базі технології
DMVPN”

Виконав здобувач вищої освіти
IV курсу, групи КІ-22-2
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Куліш Д.І.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Марченко К.М.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність 123 "Комп'ютерна інженерія"
Освітньо-професійна (освітньо-наукова) програма "Комп'ютерна інженерія"

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 27 » лютого 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Кулішу Дмитру Ігоровичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN*

2. Керівник роботи *Марченко Костянтин Миколайович, канд. техн. наук, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 136-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту 23.05.2026 р.

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію.

6. Висновки

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Структурна схема системи *1 аркуш*

Функціональна схема системи *1 аркуш*

Діаграма процесів *1 аркуш*

Блок-схема алгоритму роботи додатку *2 аркуша*

7. Дата видачі завдання « 27 » лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.03.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2026 р.	
3.	Розробка моделі компонента	20.03.2026 р.	
4.	Розробка структур даних	25.03.2026 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026 р.	
6.	Програмування алгоритмів	10.04.2026 р.	
7.	Оформлення ПЗ	17.04.2026 р.	
8.	Попередній захист роботи	23.05.2026 р.	

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Марченко К.М.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Куліш Д.І.
(прізвище та ініціали)

АНОТАЦІЯ

Куліш Д.І. Програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Метою розробки є програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Результат роботи – програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, DMVPN

ABSTRACT

Kulish D.I. Software for the information exchange system in a corporate network based on DMVPN technology. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed, which is intended for the information exchange system in a corporate network based on DMVPN technology.

The purpose of the development is software for the information exchange system in a corporate network based on DMVPN technology.

The result of the work is the software implementation of the information exchange system in a corporate network based on DMVPN technology.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with software are provided.

The program can be used on a PC with Windows 10/11 OS.

The program was developed in the Python environment.

Keywords: computer engineering, DMVPN

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	4
1.1 Призначення системи.....	4
1.2 Область застосування.....	5
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	7
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	7
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	21
2.3 Розгорнута постановка завдання	25
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	27
3.1 Опис функціонування системи	27
3.2 Розробка структурної схеми.....	31
3.3 Розробка функціональної схеми	38
3.4 Розробка діаграми процесів.....	45
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	47
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	47
4.2 Захист розробленого програмного забезпечення.....	61
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	64
6 ОСНОВНІ ВИСНОВКИ.....	72
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	

					ВКРБ-123.26.0047.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>	Куліш Д.І.					Б	1	81
<i>Перев.</i>	Марченко К.М.							
<i>Н.контр.</i>	Коваленко А.С.					ЦНТУ КІ-22-2		
<i>Затв.</i>	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AH	—	автентифікуючий заголовок
CA	—	сертифікаційне співтовариство
DES	—	Data Encryption Standard
DoS	—	атака "Відмова в обслуговуванні"
DOI	—	область інтерпретації
ESP	—	Інкапсуляція зашифрованих даних
HTTPS	—	зашифрований http
IAB	—	координаційна рада мережі Internet
IDS	—	система, яка автоматизує процес перегляду подій
IETF	—	проблемна група проектування Internet
IKE	—	протокол обміну ключами за замовчуванням для ISAKMP
IKMP	—	протоколу керування ключами прикладного рівня
IPsec	—	комплект протоколів захисту інформації по IP
ISAKMP	—	механізми узгодження атрибутів використовуваних протоколів
ISP	—	постачальник послуг Internet
MAC	—	коди на перевірку цілісності
MD5	—	дайджест повідомлення
Oakley	—	сесійні ключі на комп'ютери мережі Інтернет
PFS	—	ідеальна пряма безпека
PRF	—	псевдовипадкова функція
SA	—	Security Association
SKIP	—	команда підготовки наступної команди
SPI	—	індекс параметрів безпеки
SPD	—	база даних політики безпеки
SSL	—	протокол захищених сокетів
TCP	—	транспортний протокол
VPN	—	віртуальні приватні мережі

ВСТУП

Актуальність теми. Динамічний багатоточковий VPN (DMVPN) став високомасштабованим та гнучким рішенням для підключення розподілених мереж, що робить його особливо привабливим для тактичних розгортань, де підключення часто є динамічним, переривчастим та обмеженим за ресурсами. Використовуючи IPsec для шифрування та автентифікації, DMVPN створює безпечну мережу, що перекриває базовий транспорт. Однак унікальні вимоги тактичних середовищ, такі як агресивні умови експлуатації, потенційна фізична компрометація пристроїв, обмежена пропускна здатність та необхідність швидкого розгортання, створюють значні складнощі безпеки, що виходять за рамки типових корпоративних сценаріїв.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.
- Дослідження системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.
- Програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

DMVPN (Dynamic Multipoint Virtual Private Network – динамічна багатоточкова віртуальна приватна мережа, відмінно підходить для рішення цього завдання. У чому ж перевага використання цієї технології, скажемо, перед класичним VPN? Ця технологія є подальшим розвитком VPN компанією Cisco Systems – технологія об'єднання приватних мереж через публічні мережі.

Для об'єднання приватних мереж, як правило, використовується побудова тунелів через суспільні мережі. У звичайному варіанті необхідно набудовувати тунель для кожного з'єднання, тобто якщо ви хочете одержати повнозв'язну мережу з N вузлів потрібно налаштувати $N(N-1)/2$ тунелів. У певний момент таких зв'язків стає занадто багато й доводиться використовувати топологію типу «зірка». У цьому випадку весь трафік проходить через центральний вузол, що не додає йому продуктивності. Уже не говорячи про те, що у випадку його відмови вся мережа розсипається.

От у такій ситуації й приходить на допомогу DMVPN. Суть технології полягає в тому, що на кожному вузлі мережі настраюється тільки один тунельний інтерфейс, що і організує потім необхідну кількість тунелів автоматично, перетворюючи топологію мережі з «зірки» у повнозв'язну. Незважаючи на те, що в даній технології все-таки передбачене виділення центрального вузла, кінцеві вузли також організують між собою тунелі. В остаточному підсумку, після сходження такої мережі, навіть побудованої за технологією «зірка», центральний вузол уже не несе такої важливої ролі, і у випадку його відмови кінцеві вузли можуть продовжувати між собою взаємодіяти по вже встановлених тунелях (якщо, звичайно ж, мережа провайдеру дозволяє).

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1.2 Область застосування

Динамічний багатоточковий VPN (DMVPN) – це потужна технологія, яка поєднує кілька функцій Cisco, включаючи тунелі Generic Routing Encapsulation (GRE), Next Hop Resolution Protocol (NHRP) та IPsec, для створення масштабованої та гнучкої архітектури VPN. У конфігурації DMVPN центральний маршрутизатор-«хаб» забезпечує підключення для кількох маршрутизаторів-«спиць». Співроз'єми можуть динамічно встановлювати прямі тунелі між спицями без необхідності проходження через концентратор, що значно підвищує ефективність та зменшує затримку в mesh-топології [1]. Таке динамічне створення тунелів на вимогу робить DMVPN ідеальним для середовищ, де кінцеві точки часто змінюють місцезнаходження або стан підключення, наприклад, у військових, екстрених або мобільних операціях – отже, «тактичне розгортання».

Забезпечення безпеки тунелів DMVPN IPsec у тактичних розгортаннях є багатогранним завданням, що вимагає комплексної та адаптивної системи безпеки. Динамічний, обмежений ресурсами та потенційно агресивний характер цих середовищ підвищує важливість кожного засобу контролю безпеки. Зосереджуючись на надійних криптографічних параметрах IPsec, встановлюючи безпечні та масштабовані практики управління ключами, ретельно посилюючи мережеві пристрої та впроваджуючи ретельні можливості моніторингу та реагування на інциденти, організації можуть значно зменшити унікальні ризики, пов'язані з тактичним DMVPN.

Як фахівцю з мережевих технологій, наша роль полягає не лише в тому, щоб просто забезпечити підключення, а й у тому, щоб кожне з'єднання було захищене за своєю суттю. Проактивне проектування, постійна перевірка та здатність швидко реагувати на інциденти безпеки – це не просто найкращі практики, а критично важливі вимоги у вимогливому ландшафті тактичних мережевих операцій. Дотримання цих принципів, викладених у доменах CySA+,

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

дозволяє нам створювати стійкі та надійні комунікаційні інфраструктури, які витримують найскладніші загрози.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

К6ПЗ_2026

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти

Знайти VPN-сервіс, що захистить вас від всіх онлайн-погроз і забезпечить необхідний рівень приватності, здається практично неможливим завданням. У цей час на ринку представлені сотні VPN-сервісів, і кожний з них заявляє про себе як про кращий.

Виявлено, що ряд невеликих VPN-сервісів, які не мають у своєму розпорядженні рекламні бюджети великих брендів, працюють краще, якісніше й надійніше багатьох більше відомих VPN.

Після строгих і навіть причепливих тестів з'ясувалося також, що деякі популярні VPN-сервіси насправді марні, а інші й зовсім небезпечні.

Провівши всі ці перевірки, у даній роботі можемо із чистою совістю представити вам рейтинг 10 кращих VPN-сервісів, які захистять вас і ваші дані, а також нададуть блискавично швидкі підключення.

NordVPN

VPN-сервіс №1 2020 року

- Виділені сервери для завантаження торрентів: так, тут є сервери, настроєні спеціально для роботи з P2P-трафіком.
- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, HBO GO, Amazon Prime Video, Showtime, Sling TV.
- Є застосунки для: Windows, macOS, Linux, Android, iOS, BlackBerry, роутерів, Raspberry Pi, Android TV, Chrome, Firefox.
- Відношення до логів: строга безлогова політика.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7



Рисунок 2.1 – Інтерфейс користувача NordVPN

NordVPN – це VPN для ПК і смартфонів, що у даній роботі рекомендуємо в першу чергу. Він надає комплексні послуги, у нього відмінний функціонал і чудова якість роботи – і все це буде доступно вам по винятково доступній ціні, що мало хто ще зможе вам запропонувати.

Шифрування AES-256 і підтримка протоколів OpenVPN і IKEv2/IPSec захистить і сховає ваш трафік. Сервіс зареєстрований у Панамі, тому NordVPN не має нічого загального з розвідальнянсом «14 очей» і підозрілими законами про зберігання даних. Така «прописка» сервісу дозволяє не вести запис конфіденційних даних користувачів. Ті, хто хотів би зберегти інкогніто в інтернеті, оцінять.

У величезну серверну мережу NordVPN входять більше 5 400 серверів в 60+ країнах, при цьому мережа регулярно розширюється. Також цей провайдер володіє спеціальними серверами для роботи з подвійним шифруванням,

виділеними IP-адресами, а також підключеннями типу Tor-через-VPN (ідеальний варіант для користувачів Tor).

Безпечний перегляд потокових трансляцій (стрімів) і роздача торрентів – це завдання, які в Nord VPN вирішуються в 1 клік. Завдяки DNS-налаштуванням спеціального режиму роботи SmartPlay, застосунок NordVPN автоматично надає надійний доступ і відмінну швидкість, коли ви відкриваєте Netflix і інші стрімінгові сервіси.

Режим CyberSec – унікальна функція NordVPN, що забезпечує захист від шкідливого ПЗ й що дозволяє блокувати рекламу. Просунуті налаштування обфускації дозволять вам установити VPN-підключення навіть із території країни, що активно обмежує вільний доступ в Інтернет (наприклад, у Китаї). Також вам не прийдеться турбуватися про VPN-витоки, так як NordVPN надає дві незалежні функції екстреного відключення від Мережі (Kill switch) і дає можливість задати власні налаштування DNS для профілактики витоків даних.

Якщо вам коли-небудь знадобиться допомога, ви можете сміло покластися на службу підтримки користувачів, доступну в онлайн-чаті 24/7. Більше того, в NordVPN є просто величезна база знань, звідки ви зможете почерпнути чимало корисного про сервери й установку застосунків.

Цей сервіс не підійде вам, якщо:

– Ви збираєтеся оплатити його послуги через PayPal.

Що можна сказати в підсумку? У даній роботі вважаємо, що NordVPN – це кращий VPN-сервіс для всіх і кожного, однак відсутність можливості оплати через PayPal все-таки розчаровує. Ви можете перевірити на ділі його зручні інтерфейси й видатні функції на 6 пристроях відразу, скориставшись 30-денною гарантією повернення засобів.

До слова – в NordVPN зараз іде просто відмінна акція! Скористайтесь 70% знижкою при оформленні передплати на NordVPN за допомогою цих промо-кодів.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

ExpressVPN

VPN-сервіс №2 у загальному й беззастережному лідері в плані швидкості.

- Виділені сервери для завантаження торрентів: немає (всі сервери підтримують P2P-трафік).

- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, DAZN, HBO GO, Amazon Prime Video, Showtime, Sling TV.

- Є застосунки для: Windows, macOS, Linux, Android, iOS, BlackBerry, роутери, Raspberry Pi, Chrome, Firefox, Safari, PlayStation, Xbox, Apple TV, Nintendo Switch, Amazon Fire TV, Samsung Smart TV, Roku, Chromecast, Nvidia Shield.

- Відношення до логів: строга безлогова політика.

- У даній роботі тестували десятки VPN з різних локацій на предмет швидкості підключення, і ExpressVPN був беззастережним лідером.

В ExpressVPN є 3 000+ високошвидкісних серверів в 160 країнах. Це найшвидший VPN у нашій рейтингу, а тому він ідеально підходить для торрентів і стрімів.

Функція роздільного туннелювання дозволить вам налаштувати роботу ExpressVPN під себе й вибрати, трафік яких застосунків і сервісів необхідно шифрувати. Це дуже корисно, якщо ви хочете мати доступ до локального й іноземному контенту на тому самому пристрої.

Більше того: ExpressVPN допоможе вам одержати доступ до улюбленого контенту навіть на тих платформах, які не підтримують VPN-підключення. Функція MediaStreamer дозволить вам забути про обмеження на доступ до контенту на телевізорах Smart TV, Amazon Fire TV, Apple TV і навіть ігрових приставках.

ExpressVPN підтримує P2P-трафік на всіх своїх серверах, так що вам не прийде нічого набудовувати для використання торрентів. Функція Smart Location, доступна в додатках, автоматично вибере для вас самий підходящий сервер.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

ExpressVPN пропонує 256-бітне шифрування й підтримку OpenVPN на всіх платформах, що забезпечує бездоганний захист. Також ви будете захищені від витоків DNS за допомогою функції Network Lock – екстреного відключення підключення. TrustedServer – це інноваційна технологія ExpressVPN, що забезпечує кожному серверу в мережі сервісу однаковий рівень захисту й своєчасне відновлення ПЗ. Ця новинка дозволяє істотно знизити ймовірність зіткнення з різними кіберзагрозами. Технологія TrustedServer також дозволяє серверам ExpressVPN працювати, використовуючи тільки оперативну пам'ять. Так як серверам нічого не доводиться записувати на жорсткі диски, те після перезавантаження на пристроях не залишиться взагалі ніяких даних – у принципі. Це дозволяє домогтися безпрецедентного рівня приватності й захисту.

ExpressVPN стабільно обходить блокування Великого китайського файрволу, так що це кращий варіант для роботи з китайським сегментом Мережі.

З онлайн-чатом, готовим прийти на допомогу 24/7 і докладними інструкціями з установки для безлічі підтримуваних платформ, служба підтримки користувачів ExpressVPN також показує гідний рівень.

Цей сервіс не підійде вам, якщо:

- Ви шукаєте дешевий VPN. Послуги ExpressVPN коштують майже у два рази більше, ніж послуги деяких інших VPN-сервісів у цьому рейтингу.

ExpressVPN – це відмінне сполучення швидкості, бездоганної надійності в роботі й конфіденційності, що виразно коштує своїх грошей. Ви зможете перевірити ExpressVPN на ділі без якого-небудь ризику, скориставшись 30-денною гарантією повернення грошей. Але вам навряд чи захочеться повертати гроші: цей VPN може з легкістю задовольнити запити навіть самих вимогливих користувачів.

CyberGhost

Кращий VPN для початківців.

- Виділені сервери для завантаження торрентів: є.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, DAZN, HBO GO, Amazon Prime Video, Sky Go.
- Є застосунки для: Windows, macOS, Linux, Android, iOS, роутери, Raspberry Pi, Chrome.
- Відношення до логів: строга безлогова політика.
- Якщо ви шукаєте сервіс із інтуїтивно зрозумілим інтерфейсом і зручним дизайном, то CyberGhost може стати для вас ідеальним VPN.

Цей румунський сервіс дасть вам все необхідне: просунуте шифрування, повна відсутність логів і доступ до значної серверної мережі (5 600 серверів в 89 країнах). З застосунками, захищеними від витоків даних, і додатковою функцією екстреного відключення kill-switch цей VPN можна сміло назвати стабільним і безпечним.

Команда CyberGhost затверджує, що встановити й почати працювати з їхнім сервісом можна в один клік. Крім автоматичного підключення до найшвидшого сервера, у додатку можна знайти сервери, настроєні спеціально для стрімінгу й завантаження торрентів, і за допомогою яких ви зможете одержати доступ до американського каталогу контенту Netflix, Hulu і іншим популярним сервісам. Мабуть, це й справді простий VPN для щоденного використання.

Крім того, працювати з базовими й просунутими налаштуваннями застосунки дуже просто. Ви зможете задати власні правила роботи й налаштувати опції підключення.

Хоча він і уступає у швидкості підключення NordVPN і ExpressVPN, CyberGhost все-таки забезпечує досить швидкі підключення для того, щоб без проблем дивитися потокові трансляції й завантажувати торренти. Якщо під час роботи із сервісом ви зіткнетесь з якими-небудь технічними проблемами, за допомогою можна звернутися в онлайн-чат.

Цей сервіс не підійде вам, якщо:

- Вам потрібний VPN, що працює в Китаї. На даний момент CyberGhost не може обійти Великий китайський файрвол.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

У даній роботі вважаємо, що CyberGhost – це простий VPN, що відмінно справляється зі своїми завданнями. Як наслідок, це ще один відмінний VPN-варіант, по праву що займає 3-є місце в нашому рейтингу.

Surfshark

Кращий VPN для великої родини й малого бізнесу.

- Виділені сервери для завантаження торрентів: немає (P2P-трафік підтримується всіма серверами).

- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, HBO GO, Amazon Prime Video, ESPN.

- Є застосунки для: Windows, macOS, Linux, Android, iOS, роутери, Chrome, Firefox, Amazon Fire TV.

- Відношення до логів: строга безлогова політика.

Surfshark – це відносно новий VPN-сервіс, що вже встиг стати популярним.

Незважаючи на те, що Surfshark – новачок на ринку VPN, він пропонує дуже рідкий бонус – можливість підключити необмежену кількість пристроїв. Якщо ви хочете захистити гаджети всієї вашої родини (або ж ви самі використовуєте безліч пристроїв з можливістю виходу в Мережу), то варіанта краще вам просто не знайти.

Звичайно, у даній роботі б не стали розглядати Surfshark всерйоз, не надавай цей сервіс послуги дійсно високого рівня. Тут ви знайдете роздільне туннелювання, подвійне шифрування, екстрене відключення від Мережі й спеціальний режим роботи CleanWeb, що блокує рекламу й шкідливе ПЗ. Додаткові налаштування приховання трафіку доступні в режимі NoBorders, а режим Camouflage не дозволяє відслідковувати, що ви використовуєте VPN, а не пряме підключення.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

Зростаюча серверна мережа Surfshark містить у собі понад 1041 серверів більш ніж в 61 країнах. Це значить, що у вас завжди буде швидкий і надійний доступ до потрібного контенту.

Цей сервіс не підійде вам, якщо:

- Вам потрібно встановити VPN на роутер – в Surfshark немає окремого застосунки для роутерів.

У загальному говорячи, Surfshark – це вражаючий VPN-сервіс із преміум-функціями й простими, але, у той же час, стильними застосунками. Крім того, ви можете знайти по-справжньому вигідні пропозиції, скориставшись відмінними знижками на довгострокові тарифні плани й 30-денною гарантією повернення грошей.

PrivateVPN

Кращий бюджетний VPN.

- Виділені сервери для завантаження торрентів: ні, але P2P-трафік підтримується серверами в Британії.

- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, HBO GO, Amazon Prime Video.

- Є застосунки для: Windows, macOS, Linux, Android, iOS, роутери.

- Відношення до логів: строга безлогова політика.

PrivateVPN – це доступний сервіс із відмінною репутацією. Він надає доступ до компактної мережі з 150+ серверів, що належать самої компанії й установлених в 59 країнах і більш ніж 80 різних локаціях.

Цей шведський сервіс прикладає всі необхідні зусилля для захисту конфіденційності користувальницьких даних. Незважаючи на те, що місце реєстрації сервісу не саме вдале (Швеція входить у розвідальнянс «14 очей»), PrivateVPN у принципі не зможе передати комусь ваші дані, так як принципово не веде логи. Його прості й зручні застосунки дають доступ до шифрування AES-256 і підтримують різні протоколи, у тому числі визнаний галузевий стандарт – OpenVPN.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

Крім екстреного відключення, PrivateVPN пропонує захист від витоків даних IPv6 і DNS. Також у додатку можна активувати спеціальний «режим невидимості», розроблений для обходу блокувань підключення через VPN і глибокої перевірки пакетів даних, за рахунок чого ви одержите необмежений доступ до Всесвітньої павутини.

Звичайно, цей сервіс не може похвастати тисячами серверів і дуже просунутими функціями, однак це не заважає PrivateVPN залишатися відмінним варіантом для всіх, хто просто хоче обійти блокування доступу до свого улюбленого контенту. Він підтримує P2P-трафік на своїх британських серверах і навіть пропонує спеціальні сервери для доступу до Netflix і іншим популярним стрімінговим сервісам. Вражаючі швидкості підключень від PrivateVPN – гарантія того, що ви не зштовхнетеся з лагами й буферизацією: просто виберіть потрібний режим і приступайте до перегляду!

Цей сервіс не підійде вам, якщо:

- Вам потрібний VPN з більшою кількістю серверів.

Якщо ви шукаєте бюджетний сервіс із доступними цінами як на короткострокові, так і на довгострокові тарифи, PrivateVPN може стати для вас відмінним варіантом. 30-денна гарантія повернення грошей забезпечить вам досить часу, щоб випробувати цей VPN на ділі.

IPVanish

Відмінні застосунки й стабільні швидкості.

- Виділені сервери для завантаження торрентів: немає.

- Відкриває доступ до: Netflix, BBC iPlayer.

- Є застосунки для: Windows, macOS, Linux, Android, iOS, Windows Phone, роутери, Chromebook, Amazon Fire TV.

- Відношення до логів: строга безлогова політика.

Баланс між безпекою й швидкістю доступу робить сервіс IPVanish цілком гідним VPN, що заслуговує вашої уваги. Більше 1 200 серверів, відмінний потенціал обходу блокувань і надійний захист трафіку – цей сервіс може багато

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

чого вам запропонувати. 256-бітне шифрування й безліч VPN-протоколів, у тому числі OpenVPN, роблять IPVanish безпечним, а функція екстреного відключення й захист від витоків DNS/IPv6 гарантує вам і вашому трафіку постійний захист.

Швидкість підключень тут не тільки висока, але й стабільна, так що вам не прийде нервувати через дратівні обриви підключення або плаваючої швидкості. Як приємний бонус, IPVanish не дуже давно вдосконалив свої сервери для доступу до Netflix, оптимізувавши й поліпшивши їх.

IPVanish підтримує P2P-трафік і SOCKS 5-проксі, що дозволяє швидко завантажувати торренти. Так, сервіс зареєстрований у США (і, відповідно, повинен підкорятися вимогам DMCA), але це не заважає йому дотримуватися строгої безлогової політики, так що навіть американська «прописка» не повинна відлякувати аматорів торрентів.

IPVanish також надає доступ до додаткових налаштувань обфускації й IP-адрес(наприклад, ви можете з певною періодичністю одержувати нова IP-адресу). Все це, а також доступна 24/7 служба підтримки й 10 одночасних підключень у рамках однієї підписки дозволяють сервісу виділитися із числа інших VPN. Хотілося б, звичайно, щоб термін дії гарантії повернення грошей був побільше, але навіть 7 днів – це набагато краще, ніж нічого.

Цей сервіс не підійде вам, якщо:

- Ви ставите вартість VPN у главу кута.

IPVanish – не найдешевший сервіс, однак його ціна повністю виправдана відмінним функціоналом.

Hotspot Shield

Надійний захист і вільний доступ до потокових трансляцій.

- Виділені сервери для завантаження торрентів: немає.
- Відкриває доступ до: Netflix, Hulu, BBC iPlayer, Amazon Prime Video.
- Є застосунки для: Windows, macOS, Android, iOS, Chrome.
- Ведення логів: так (протягом VPN-сесій ведуться логи підключень, також збираються певні дані в маркетингових цілях).

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

Платний VPN-сервіс від Hotspot Shield, він же Hotspot Shield Premium, надасть вам доступ до більш ніж 2 500 серверам по усьому світі, а також до стильних застосунків і швидких підключень. Але чи коштує воно того?

Мабуть, що так! Цей VPN стане гідним вибором для звичайних користувачів, адже тут використовується відмінне шифрування (128/ 256-бітне) і власна розробка – протокол Catapult Hydra (заснований на OpenSSL).

Hotspot Shield стискає потоковий трафік, що поліпшує доступ до Netflix і дозволяє забути про буферизацію.

Що ж стосується функцій, то тут є екстрене відключення від Мережі й...нічого більше. Немає ні можливості задіяти користувацькі DNS, ні додаткових налаштувань для торрентів. І нехай навіть P2P-трафік тут підтримується, вам краще вибрати інший VPN-сервіс із цього списку, якщо торренти для вас – основний пріоритет.

Незважаючи на відмінну якість роботи в цілому, Hotspot Shield не можна включити в число безлогових VPN-сервісів. Додайте сюди реєстрацію в США, щоб зробити однозначно сумний вивід: ви будете легкою мішенню для копірайтних тролів і запитів DMCA. Для жителів США це актуально подвійно.

Цей сервіс не підійде вам, якщо:

- Ви шукаєте VPN для торрентів.

Нехай навіть в Hotspot Shield є свої недоліки, він був, є й залишається популярним, надійним і доступним VPN-сервісом. У даній роботі радимо перевірити його на практиці, скориставшись 45-денною гарантією повернення грошей.

UltraVPN

№1 у плані користувацької підтримки.

- Спеціальний режим для роботи з торрентами: немає.
- Відкриває доступ до: Netflix, Hulu, HBO GO.
- Підтримується на: Windows, macOS, Android, iOS, Fire TV.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

– Ведення логів: так (сервіс збирає IP-адреси, дані про місце розташування й відомості про пристрій, однак не веде логи активності).

UltraVPN – це бюджетний сервіс із відмінною користувацькою підтримкою. Скажемо так – ви зможете зв'язатися з нею навіть по телефоні!

Сервіс управляє мережею з 100+ серверів в 55+ локаціях по усьому світі. Проводячи тести, у даній роботі з'ясували, що цей сервіс відкриває доступ до Netflix, Hulu і HBO GO. Його сервери забезпечують швидкі підключення, так що з буферизацією у даній роботі практично не зіштовхувалися.

UltraVPN забезпечує надійний захист користувацьких даних, застосовуючи протокол OpenVPN і 256-бітне шифрування. На жаль, у нього та ж проблема, що й в Hotspot Shield – ім'я їй «логи». Знову ж, це американська компанія, тобто вона зареєстрована на території розвідальняса «14 очей». Результат? Цей VPN не варто розглядати як основний варіант, якщо ви хочете домогтися повної анонімності.

Перевагою UltraVPN можна назвати просту установку й зручність роботи як з настільними, так і з мобільними застосунками.

Не використовуйте цей сервіс, якщо:

– Ви шукаєте VPN, здатний відкрити доступ до BBC iPlayer за межами UK.

Що ж можна сказати в підсумку? Якщо вам потрібний швидкий VPN-сервіс для перегляду стрімів, обов'язково зверніть увагу на UltraVPN. Ви зможете протестувати його, нічим не ризикуючи, скориставшись 30-денною гарантією повернення грошей від сервісу.

VyprVPN

Вражаючий і недешевий VPN-сервіс для настільних пристроїв.

– Виділені сервери для завантаження торрентів: немає.

– Відкриває доступ до: Netflix, Hulu, BBC iPlayer.

– Є застосунки для: Windows, macOS, Android, iOS, роутери, Android TV, QNAP, Blackphone, Anonabox.

– Відношення до логів: строга безлогова політика.

VyprVPN пропонує своїм користувачам два різних тарифи, але якщо у вас є пристрій під керуванням ОС Windows або Mac, те вам потрібний тариф Premium.

Крім доступу до 700+ серверів і строгої безлогової політики, VyprVPN Premium дозволить вам скористатися своєю добре відомою функцією – протоколом Chameleon власної розробки.

Будучи поліпшеною версією OpenVPN, Chameleon надає додатковий захист і допомагає ще ефективніше обходити блокування доступу по географічній ознаці. Як наслідок, VyprVPN – це відмінний варіант для тих, хто хоче обійти геообмеження Netflix і інших популярних стрімінгових сервісів.

На жаль, протокол Chameleon доступний тільки в додатках для настільних пристроїв. Втім, базовий застосунок VyprVPN також забезпечує достатні приватність і якість роботи й для мобільних пристроїв. Застосунок захищений від витоків даних, мають стильний інтерфейс і, що важливіше всього, зручні й прості.

VyprVPN складно назвати бюджетним сервісом, однак відмінними знижками при оформленні передплати на довгостроковий тариф доступні гарні знижки. VyprVPN надає 30-денну гарантію повернення грошей, так що ви зможете перевірити сервіс на ділі, нічим не ризикуючи.

Цей сервіс не підійде вам, якщо:

– Ви хочете оплатити VPN-послуги біткоїнами або іншою криптовалютою.

– Ви шукаєте VPN із цілодобово доступної техпідтримкою.

VyprVPN довів, що це надійний сервіс, що цінує користувальницьку конфіденційність.

ZenMate

Простий VPN-сервіс, що справляється зі своїми завданнями.

- Виділені сервери для завантаження торрентів: немає (але P2P-трафік дозволений).
- Відкриває доступ до: Netflix.
- Є застосунки для: Windows, macOS, Android, iOS, Chrome, Firefox, Opera.
- Відношення до логів: строга безлогова політика.

І наш рейтинг замикає сервіс, що сміло можна назвати простим, якщо не базовим. ZenMate мало чим виділяється на тлі інших сервісів у цьому списку, однак у даній роботі поставили його на почесне 10-е місце не без причини.

За досить помірну ціну ZenMate захистить вас за допомогою протоколу OpenVPN і строгої безлогової політики, а також відкриє доступ до більш ніж 290 серверів в 30 країнах. P2P-трафік підтримується, нехай і без окремого режиму роботи для завантаження торрентів, а швидкість підключень досить висока щоб дивитися стріми у форматі HD без яких-небудь проблем.

Є отут і функція екстреного відключення від Мережі, так що ваші конфіденційні дані не залишаться без захисту у випадку обриву підключення. Треба сказати, що в минулому користувачі ZenMate часто страждали від обривів зв'язку, але після ряду поліпшень і відновлень ZenMate став як ніколи стабільним.

Якщо для вас важливо мати доступ до техпідтримки через онлайн-чат, то ZenMate VPN вас, швидше за все, розчарує – у сервісу є тільки система тікетів. Втім, компетентні співробітники техпідтримки відповідають швидко й докладно.

Нам подобається, що VPN-сервіси стають усе краще й краще. ZenMate – саме один з них: після істотного поліпшення якості роботи цей VPN-сервіс став досить гарний, щоб одержати місце в числі кращих провайдерів 2020 року.

Цей сервіс не підійде вам, якщо:

- Ви шукаєте VPN для стрімів. Zenmate надає доступ тільки до Netflix.

Перевірити ZenMate на ділі можна, скориставшись безкоштовним 7-денним пробним періодом і 30-денною гарантією повернення грошей.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – це об'єктно-орієнтована мова програмування високого рівня загального призначення з відкритим кодом. Це визначення може бути важким для новачків, тому розглянемо кожну характеристику окремо, щоб зрозуміти, що вона означає:

- Відкритий вихідний код: це безкоштовно та доступно для подальших покращень, таких як додавання корисних функцій або виправлення помилок.
- Об'єктно-орієнтована: заснована не на функціях, але в об'єктах з певними атрибутами й методами.
- Високий рівень: зручний для людини, а не для комп'ютера.
- Загальне призначення: можна використовувати для створення будь-яких програм.

Ця мова використовується в будь-якому програмному забезпеченні, про яке ви тільки можете подумати. Ви можете використовувати його для створення веб-сайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу та багато іншого. Також застосовується в науці про дані, аналізі даних, машинному навчанні, інженерії даних, веб-розробці, розробці програмного забезпечення та інших галузях.

Переваги та недоліки Python

Переваги:

– Її легко читати, вчити та писати. Це мова програмування високого рівня з англійським синтаксисом. Це полегшує читання та розуміння коду. Її дійсно легко зрозуміти і вивчити, тому багато людей рекомендують Python новачкам. Вам потрібно менше рядків коду для виконання того ж завдання в порівнянні з іншими основними мовами, такими як C/C++ та Java.

– Підвищує продуктивність. Це дуже продуктивна мова. Завдяки її простоті розробники можуть зосередитися на розв'язанні проблеми. Їм не

потрібно витрачати багато часу на розуміння синтаксису або поведінку мови програмування. Ви пишете менше коду та виконуєте більше завдань.

– Інтерпретована мова. Python мова, що інтерпретується, а це означає, що вона безпосередньо виконує код по рядку. Якщо сталася помилка, вона зупиняє подальше виконання та повідомляє про її виникнення. Вона показує лише одну помилку, навіть якщо у програмі їх кілька. Це спрощує налагодження.

– Динамічно типізована. Python не визначає тип змінної, доки ми не запустимо код. Вона автоматично надає тип даних, коли відбувається процес виконання. Фахівець може не турбуватися про оголошення змінних та типи даних.

– Безкоштовна та з відкритим вихідним кодом. Ця мова постачається під схваленою OSI ліцензією з відкритим вихідним кодом. Це робить його безкоштовним для використання та розповсюдження. Ви можете завантажити вихідний код, змінити його та навіть розповсюджувати свою версію. Це корисно для організацій, які хочуть використати свою версію для розробки.

– Підтримка великих бібліотек. Стандартна бібліотека Python є величезною, ви можете знайти майже всі функції, необхідні для вашого завдання. Таким чином ви не залежите від зовнішніх бібліотек.

– Портативність. У багатьох мовах, таких як C/C++, потрібно змінити свій код, щоб запустити програму на різних платформах. З Python все інакше. Ви тільки пишете один раз і запускаєте її будь-де.

Недоліки:

– Низька швидкість. Вище ми обговорювали, що це інтерпретована мова з динамічною типізацією. Порядкове виконання коду часто призводить до повільного виконання. Динамічна природа Python також є причиною її низької швидкості, оскільки їй доводиться виконувати додаткову роботу при виконанні коду. Тому вона не підходить для цілей, де швидкість важливий аспект проєкту.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

– Неєфективна для пам'яті. Ця мова програмування використовує великий обсяг пам'яті, це може бути недоліком при створенні програм, коли віддають перевагу оптимізації пам'яті.

– Слабка у мобільних обчисленнях. Python зазвичай використовується у серверному програмуванні. Ми не бачимо – її на стороні клієнта або в мобільних програмах з таких причин: вона не заощаджує пам'ять і має повільну обчислювальну потужність у порівнянні з іншими мовами.

– Доступ до бази даних. Програмувати на цій мові легко, але коли ми взаємодіємо з базою даних, її не вистачає. Рівень доступу до бази даних у Python примітивний та недостатньо розвинений у порівнянні з іншими популярними технологіями.

– Помилки виконання. Це мова з динамічною типізацією, тому тип даних змінної може змінюватись у будь-який час. Змінна, що містить ціле число, у майбутньому може містити рядок, що може призвести до помилок виконання.

Застосування Python:

– Для аналізу даних. Дані стали цінним активом у будь-якій сучасній галузі, і більшість компаній зацікавлені у збиранні, обробці та аналізі релевантних даних, щоб витягти з них цінну інформацію для бізнесу. І тут Python виходить за межі будь-якої конкуренції. Python особливо цінна тим, що крім великої стандартної бібліотеки надає величезний набір додаткових модулів, розроблених спеціально для аналітичних цілей. Найвідоміші бібліотеки Python для аналізу даних – це pandas і NumPy . Ці інструменти дозволяють робити з вашими даними майже все, наприклад, очищати і аналізувати їх, вивчати статистику або візуалізувати приховані тенденції у ваших даних.

– Для візуалізації даних. Візуалізація даних – це окрема частина аналізу даних, яка допомагає нам подавати інформацію, необроблену чи очищену, у більш змістовній формі. Тут Python знову входить у гру, пропонуючи широкий спектр інструментів візуалізації даних. Найпопулярніші з них – matplotlib і

заснований на ній seaborn. Використовуючи їх, ми можемо створювати буквально всі види візуалізації: від найпростіших до складніших.

– Для машинного навчання. Машинне навчання (ML) є основою більшості завдань науки даних. Він є областю штучного інтелекту, пов'язаною з використанням алгоритмів, що дозволяють машинам вивчати закономірності та тенденції на основі історичних даних, щоб робити прогнози на основі невідомих даних. – Використовуючи методи ML, ми можемо створювати моделі, які можуть точно передбачити швидкість відтоку клієнтів компанії, оцінити ризик виникнення у людини певного захворювання, визначити оптимальне розташування автомобілів таксі й т.д. За допомогою Python ми можемо побудувати модель ML, використовуючи лише три рядки коду.

– Для розробки програмного забезпечення. Крім свого багатостороннього застосування в галузях науки про дані, Python використовується на кожному етапі розробки програмного забезпечення, включаючи контроль складання, автоматичну безперервну компіляцію, прототипування, відстеження помилок, тестування та обслуговування програмного забезпечення. За допомогою цієї мови можемо створювати аудіо- або відеопрограми на основі методів штучного інтелекту, машинного навчання, API (інтерфейсів прикладного програмування), GUI (графічних інтерфейсів) або будь-якого іншого типу програмного забезпечення.

– Для веброзробки. У той час як для створення візуальної частини вебсайту ми переважно будемо використовувати такі мови, як HTML, CSS та JavaScript, для його невидимої частини ми часто вибираємо Python. Серед масштабних вебсайтів та програм, створених за допомогою цієї мови, варто згадати Google, Facebook, Instagram, YouTube, Dropbox та Reddit.

– Для автоматизації задач/скриптингу. Це відмінний інструмент для написання програм для автоматизації різних завдань, що повторюються. Цей процес називається скриптингом. Зокрема, можна робити скрипти для роботи з файлами та папками. Наприклад, можна створювати, перейменовувати,

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

перетворювати, розділяти, об'єднувати або видаляти файли, перевіряти їх на наявність помилок. Ви також можете використовувати автоматизацію Python для пошуку та завантаження інформації з Інтернету, заповнення та надсилання онлайн-форм та надсилання регулярних повідомлень або електронних листів.

Яким фахівцям потрібно володіти Python:

- Фахівець з даних.
- Аналітик даних.
- Інженер даних.
- Інженер з машинного навчання.
- Журналіст даних.
- Архітектор даних.
- Повний стек веб-розробника.
- Backend-розробник.
- DevOps-інженер.
- Інженер-програміст.

Можемо зробити висновок, що Python ще довго буде популярною мовою, хоч і має низку недоліків. Цю мову використовують для створення вебсайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу, аналізу даних, машинного навчання, інженерії даних та для багатьох інших областей. Це перспективна і затребувана навичка, яка необхідна у всіх галузях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

В процесі розробки випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформулювати висновки про виконаний обсяг робіт та одержані результати.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

DMVPN – це власне рішення Cisco, яке спрощує керування VPN, дозволяючи прямий зв'язок між віддаленими сайтами без необхідності формування постійних статичних тунелів. Воно використовує:

- mGRE (багатоточковий GRE): Для динамічного створення тунелів.
- NHRP (протокол вирішення наступного стрибка): для зіставлення публічних IP-адрес із приватними.
- IPSec: Для безпечного шифрування тунельного трафіку.

DMVPN поділяється на три фази залежно від того, як обробляється трафік і які протоколи маршрутизації можна використовувати.

DMVPN Фаза 1: Тільки Hub-and-Spoke

- Весь трафік проходить через хаб.
- Немає прямого спілкування між людьми.
- Статична або динамічна маршрутизація на бабі.

Фаза 2 DMVPN: Динамічні тунелі між спостереженнями

- Дозволяє прямі тунелі між спицями.
- Протокол маршрутизації ввімкнено (EIGRP/OSPF/BGP).
- Потрібне перенаправлення NHRP.

Фаза 3 DMVPN: Покращена маршрутизація за допомогою скорочень Spoke:

- Використовує підсумовування маршруту зі скороченнями NHRP.
- Більш масштабований та ефективний.
- Чудово підходить для великих корпоративних VPN.

1. Чи можна використовувати OSPF замість EIGRP в DMVPN?

Так, ви можете використовувати OSPF з DMVPN, але EIGRP зазвичай є

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

кращим через кращу сумісність з динамічною поведінкою DMVPN. Ось чому:

- EIGRP ефективніше обробляє мережі NBMA.
- EIGRP не залежить від ролей DR/BDR, на відміну від OSPF.
- EIGRP підтримує підсумовування маршрутів та маршрутизацію тупиків

більш гнучко між фазами.

У середовищах з кількома вузлами або великомасштабних середовищах EIGRP спрощує маршрутизацію та зменшує проблеми з конвергенцією.

2. Чи спілкуються представники безпосередньо на етапі DMVPN 1?

Ні, на першому етапі весь зв'язок має проходити через хаб-маршрутизатор. Тунелі між точками не будуються динамічно:

- Існують лише статичні тунелі типу «точка-багато точок».
- Спицеві компоненти реєструються в хабі за допомогою NHRP, але хаб пересилає весь трафік.

Якщо вам потрібні тунелі з прямим з'єднанням спиць, розгляньте можливість переходу на Фазу 2 або Фазу 3.

3. Чи обов'язковий IPsec у DMVPN?

Не зовсім, але дуже рекомендується:

- DMVPN без IPsec функціонально можливий, але небезпечний.
- На практиці більшість розгортань використовують IPsec для шифрування та забезпечення цілісності.
- IPsec захищає трафік через публічний Інтернет або MPLS, коли потрібна конфіденційність даних.

У Cisco IOS інтеграція IPsec з DMVPN відбувається безперешкодно, використовуючи конфігурації захисту на основі профілів або тунелів.

4. Чому варто використовувати DMVPN Phase 3 замість Phase 2?

DMVPN Phase 3 є кращим варіантом у великих мережах, оскільки він:

- Підтримує підсумовування маршрутів на хабі.
- Дозволяє переадресацію/скорочення повідомлень NHRP, що забезпечує динамічні тунелі між сполучниками навіть зі зведеними маршрутами.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

– Пропонує кращу масштабованість та покращений контроль над шляхами маршрутизації.

На відміну від Фази 2, Фаза 3 уникає маршрутизації чорних дір під час використання підсумовування.

5. Чи можу я імітувати DMVPN в EVE-NG?

Так. Лабораторії DMVPN повністю підтримуються в EVE-NG, за умови використання:

- Маршрутизатори Cisco IOS (наприклад, c7200, IOSv, CSR1000v).
- Зображення, що підтримують NHRP, IPsec та протоколи маршрутизації.

Поради щодо симуляції:

- Використовуйте щонайменше одну маточину та дві спиці.
- Тестування топологій фаз 1, 2 та 3 за допомогою EIGRP та OSPF.
- Перевірте зіставлення NHRP та поведінку тунелів за допомогою інструментів CLI.

6. Як перевірити стан тунелю в DMVPN?

Ви можете використовувати такі команди CLI:

`show dmvpn`

Відображає зіставлення NHRP, стани тунелів та статус вузла.

`show crypto session`

Перевіряє тунелі IPsec (ISAKMP та IPsec SA).

`show ip nhrp`

Перелічує вирішені адреси наступного вузла та інформацію про вузли.

Ці команди допомагають діагностувати проблеми з тунелем і перевірити успішну реєстрацію та шифрування.

7. Яка роль NHRP у DMVPN?

NHRP (протокол вирішення наступного вузла) є основним компонентом DMVPN. Він:

- Зіставляє тунельні IP-адреси з реальними (NBMA) IP-адресами.
- Дозволяє динамічну реєстрацію спиць на концентраторі.

– У Фазі 2 та 3 він підтримує скорочення між спицями за допомогою переадресації повідомлень.

Коротше кажучи, NHRP діє як ARP для тунелів і є важливим для динамічного з'єднання.

8. Як DMVPN обробляє резервне копіювання?

DMVPN підтримує конфігурації з кількома хабами, що дозволяє:

– Первинні/вторинні хаби, що використовують динамічні пріоритети реєстрації NHRP.

– Перемикає на резервний хаб, якщо основний стає недоступним.

Порада щодо налаштування: використовуйте різні IP-адреси джерел тунелю та реєстрації NHRP для кожного хаба.

Ви також можете поєднувати протоколи маршрутизації (наприклад, EIGRP/OSPF) з об'єктами відстеження для безперешкодного перемикання на резервний комп'ютер.

9. Чи може DMVPN працювати через LTE або широкосмуговий доступ?

Так, DMVPN добре працює через будь-який транспорт на основі IP, зокрема:

- Широкосмуговий доступ (кабельний, DSL).
- 4G/5G LTE.
- Публічний інтернет.

Просто переконайтеся, що пристрої:

- Може формувати публічні тунелі на основі IP-адрес.
- Дозволити UDP 500/4500 (для IPsec).
- Чи підтримують NAT-T, якщо задіяно NAT?

Це робить DMVPN ідеальним для філій з ненадійними або мобільними WAN-з'єднаннями.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

3.2 Розробка структурної схеми

Хоча DMVPN пропонує гнучкість, його інтеграція в тактичні середовища створює унікальні проблеми безпеки, які вимагають більш ретельного підходу, ніж типові корпоративні VPN.

1.1 Різні проблеми безпеки під час тактичного розгортання:

- Несприятливе операційне середовище: пристрої можуть бути розгорнуті у фізично незахищених місцях, що збільшує ризик фізичного доступу, втручання або захоплення.

- Динамічні та непередбачувані топології: Тактичні мережі часто змінюються в міру переміщення підрозділів, розгортання нових пристроїв або вилучення існуючих. Це ускладнює керування статичними політиками безпеки та може призвести до тимчасових вразливостей.

- Обмеження ресурсів: Обмежена пропускна здатність, потужність та обчислювальні ресурси тактичних пристроїв можуть обмежувати використання функцій безпеки з високим навантаженням на процесор або комплексного ведення журналу, що впливає на архітектуру безпеки та набори інструментів.

- Періодичне підключення: Часті відключення та повторні підключення можуть ускладнити керування ключами, встановлення тунелів та моніторинг безпеки в режимі реального часу.

- Підвищений ризик фізичного зламу: тактичні пристрої більш схильні до втрати, крадіжки або навмисного зламу з боку зломисників. Це безпосередньо впливає на цілісність та конфіденційність усієї мережі DMVPN, якщо їх належним чином не захистити.

- Внутрішні загрози: Персонал, який має прямий доступ до тактичних пристроїв, навіть якщо він авторизований, становить значну загрозу, якщо його дані будуть скомпрометовані або зломисні.

- Обмежене централізоване управління: у високорозподілених та мобільних операціях централізоване управління безпекою та встановлення

виправлень у режимі реального часу може бути складним, що призводить до потенційних прогалин в управлінні вразливостями.

Ці виклики підвищують важливість надійної конфігурації IPsec, безпечного управління ключами, пильного моніторингу та стійкого реагування на інциденти.

2. Вразливості та ландшафт загроз

Характерні риси тактичних розгортань DMVPN у поєднанні зі складнощами IPsec та маршрутизації створюють певний набір вразливостей та загроз, які аналітики з кібербезпеки повинні розуміти.

2.1 Поширені вразливості

– Слабкі криптографічні параметри IPsec: використання застарілих або слабких алгоритмів шифрування (наприклад, DES, 3DES), коротких ключів або незахищених алгоритмів хешування (наприклад, MD5) робить тунелі вразливими до атак методом грубої сили або криптоаналізу. Відсутність ідеальної прямої секретності (PFS) означає, що один скомпрометований ключ може розшифрувати минулий та майбутній трафік.

– Незахищені попередньо спільні ключі (PSK): Якщо PSK використовуються та є слабкими, повторно використовуються або неправильно керуються, їх можна легко скомпрометувати. У великих мережах DMVPN безпечне розповсюдження та оновлення PSK стає значним логістичним та безпековим тягарем.

– Вразливості NHRP: Протокол вирішення наступних переходів (NHRP), критично важливий для динамічних тунелів типу «спойлер-спойлер», може бути використаний. Без належної автентифікації зловмисник може впроваджувати шкідливі відповіді NHRP, перенаправляючи трафік або видаючи себе за законних спойлерів.

– Неправильна конфігурація маршрутизатора: помилки в списках контролю доступу (ACL), протоколах маршрутизації (наприклад, OSPF, EIGRP через GRE) або наборах перетворень IPsec можуть ненавмисно відкрити діри в

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

безпеці, дозволяючи несанкціонованому трафіку або маршрутній інформації проходити через тунель. Це поширена вразливість.

– Відсутність захисту площини управління: Недостатній захист інтерфейсів управління маршрутизатора (Telnet/SSH, SNMP, HTTP/HTTPS) може дозволити несанкціонований доступ до конфігурацій пристроїв, що потенційно може призвести до компрометації тунелю.

– Вразливості програмного забезпечення: помилки або не виправлені вразливості в операційній системі маршрутизатора (наприклад, Cisco IOS XE) можуть бути використані для отримання контролю над пристроєм, що призводить до повного злому тунелю DMVPN. Це критична область управління загрозами.

2.2 Суб'єкти загроз та їхня тактика:

– Змагальні національні держави/організована злочинність: високорозвинені суб'єкти можуть атакувати тактичні мережі для збору розвідувальних даних, руйнування системи або отримання стратегічної переваги. Вони використовують складні методи, такі як фізична компрометація, криптоаналіз та експлойти нульового дня.

– Внутрішні загрози: Невдоволені співробітники або персонал з скомпрометованими даними, який має законний доступ, можуть навмисно впроваджувати вразливості, витікати ключі або вимикати функції безпеки.

– Глушители/перешкоди: Некіберзагрози, такі як радіочастотне (РЧ) глушіння, можуть порушувати базове з'єднання, що призводить до періодичних збоїв тунелів та потенційного переходу до менш безпечних методів зв'язку.

– Перехоплення та маніпулювання пакетами: Зловмисники, що діють поблизу тактичних підрозділів, можуть перехоплювати та аналізувати зашифрований трафік (для криптоаналізу) або намагатися впроваджувати шкідливі пакети, якщо перевірки цілісності IPsec слабкі або автентифікація обійдена.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

Поєднання цих вразливостей та загроз підкреслює критичну потребу в надійній та адаптивній системі безпеки для DMVPN у тактичних середовищах.

3. Стратегії пом'якшення наслідків та найкращі практики

Захист тунелів DMVPN IPsec у тактичних розгортаннях вимагає багаторівневого підходу, який охоплює конфігурацію, керування ключами, посилення захисту пристроїв та безперервний моніторинг.

3.1 Надійна конфігурація IPsec:

– Надійні криптографічні параметри: Завжди використовуйте найнадійніше доступне шифрування IPsec (наприклад, AES-256) та алгоритми хешування (наприклад, SHA-384 або SHA-512). Налаштуйте ідеальну пряму секретність (PFS) за допомогою надійних груп Діффі-Хеллмана (DH) (наприклад, група 19 або 20), щоб гарантувати, що компрометація одного сеансового ключа не призведе до компрометації минулих або майбутніх сеансових ключів [2].

– Автентифікація на основі сертифікатів (PKI): Надайте пріоритет використанню інфраструктури відкритих ключів (PKI) для автентифікації однорангових IPsec над попередньо спільними ключами. PKI забезпечує набагато масштабованіший та безпечніший метод перевірки особи та обміну ключами, особливо в середовищах з численними спіцями. Це спрощує ротацію та скасування ключів. Якщо PSK неминучі, переконайтеся, що вони довгі, складні, унікальні для кожного тунелю (де це можливо) та безпечно зберігаються.

– Захист від повторного відтворення: Переконайтеся, що захист IPsec від повторного відтворення ввімкнено, щоб запобігти повторному відтворенню захоплених пакетів зловмисниками для переривання роботи послуг або імітації легітимного трафіку.

– Виявлення неактивних вузлів (DPD): налаштуйте DPD для швидкого виявлення неактивних або невідповідальних вузлів IPsec, що дозволяє розібрати тунель та запобігти марнуванню ресурсів або ризикам безпеки через застарілі тунелі.

3.2 Управління ключами та їх розподіл:

– Автоматизована ротація ключів: для IPsec на основі PKI впроваджуйте автоматизовані процеси реєстрації та поновлення сертифікатів. Для PSK встановіть суворі політики регулярної ручної ротації та безпечних методів розповсюдження, мінімізуючи втручання людини та ризики.

– Безпечне зберігання ключів: Ключі, особливо PSK, повинні безпечно зберігатися на пристроях. Використовуйте апаратні модулі безпеки (HSM) або модулі довіреної платформи (TPM), якщо вони доступні на тактичних платформах, для захисту криптографічних ключів.

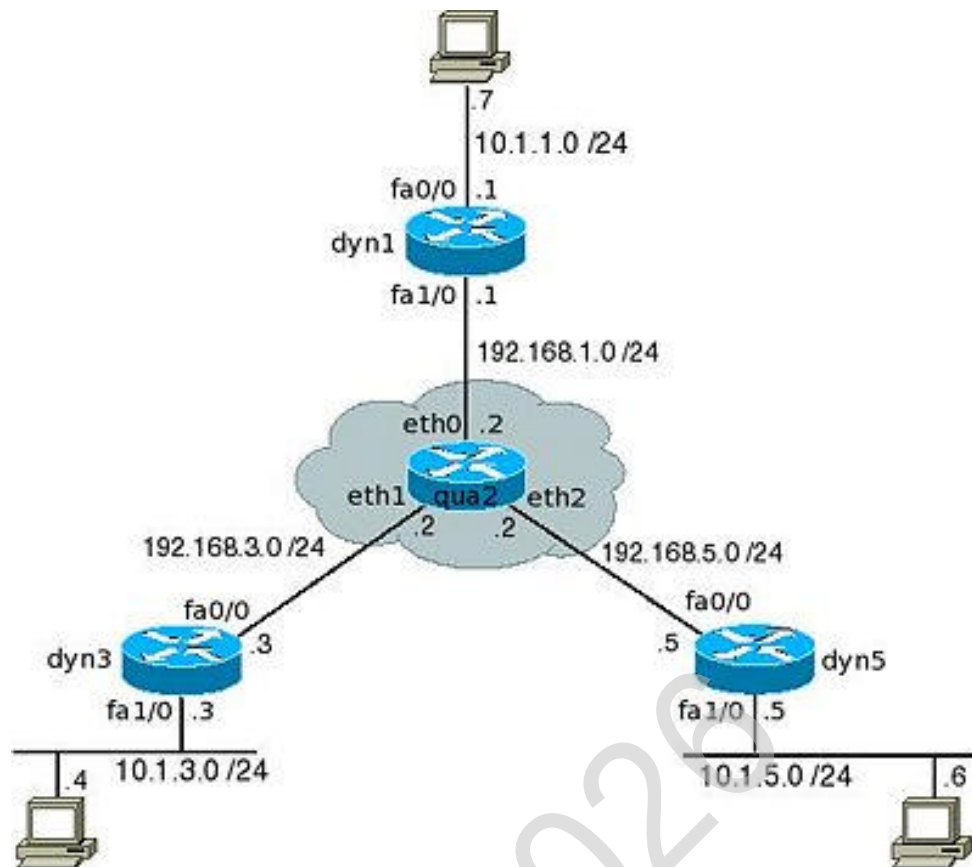
– Криптографічні гнучкі політики: Розробляйте криптографічні політики, які дозволяють легко оновлюватися до сильніших алгоритмів у разі появи нових загроз або збільшення обчислювальної потужності.

3.3 Захист пристроїв та контроль доступу:

– Захист площини управління (MPP): Впроваджуйте суворий MPP на всіх хабових та спицевих маршрутизаторах. Обмежте доступ до управління (SSH/HTTPS) довіреними мережами, використовуйте надійні паролі та налаштуйте керування доступом на основі ролей (RBAC). Вимкніть непотрібні служби та протоколи [3].

– Перевірка безпечного завантаження та цілісності: якщо обладнання підтримує цю функцію, увімкніть механізми безпечного завантаження, щоб переконатися, що операційна система не була підроблена перед її завантаженням. Регулярно перевіряйте цілісність образу IOS/OS маршрутизатора.

– Сегментація мережі (VRF-Lite): Навіть у рамках тактичних розгортань розгляньте використання VRF-lite на спицевих маршрутизаторах для сегментації конфіденційного управлінського або критично важливого трафіку від загального користувацького трафіку. Це обмежує радіус вибуху в разі компрометації.



Початок налаштування системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN

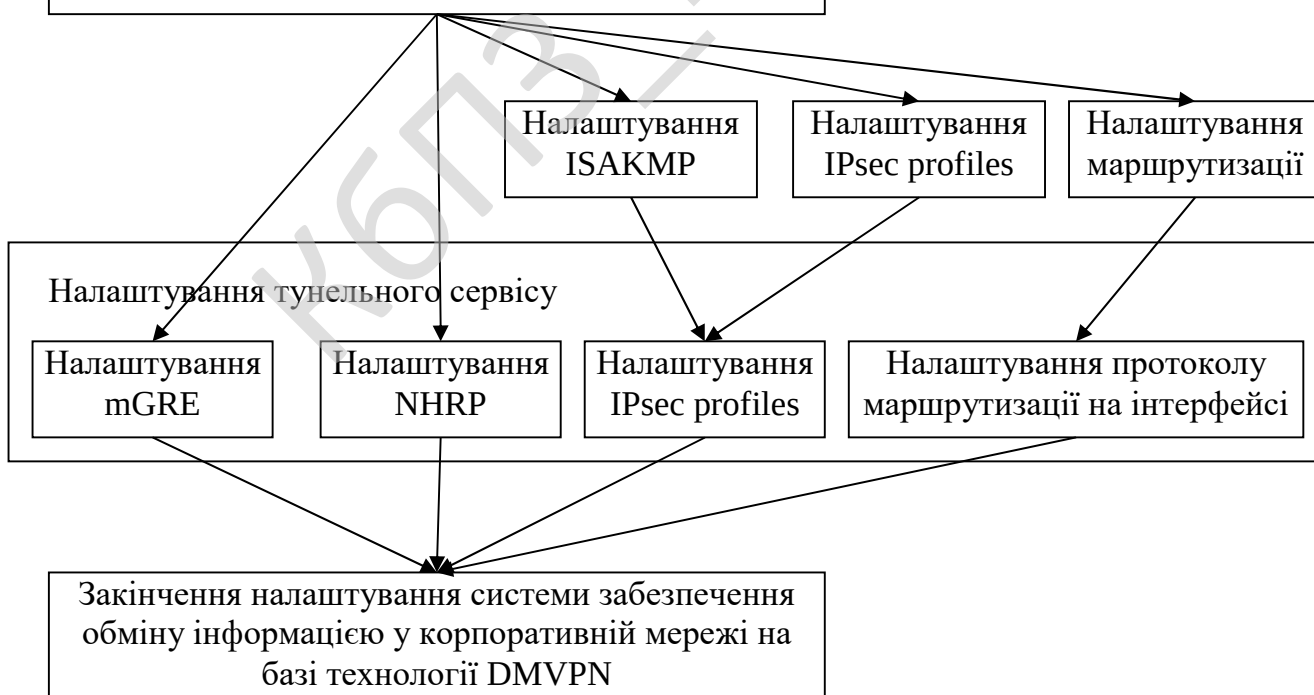


Рисунок 3.1 – Структурна схема системи

– Доступ з найменшими привілеями: Застосовуйте принцип найменших привілеїв до трафіку, що проходить через тунелі DMVPN. Використовуйте детальні ACL на інтерфейсах hub та spoke, щоб дозволити лише необхідний трафік та протоколи. Обмежте оголошення протоколів маршрутизації лише необхідними підмережами.

– Заходи фізичної безпеки: Використовуйте засоби фізичної безпеки для тактичних пристроїв, де це можливо. Це включає пломби із захистом від несанкціонованого доступу, надійні корпуси та моніторинг несанкціонованого доступу.

3.4 Моніторинг, ведення журналу та реагування на інциденти:

– Комплексне ведення журналу: Налаштуйте детальне ведення журналу для змін стану тунелю IPsec, збоїв автентифікації, оновлень протоколу маршрутизації та спроб входу. Надсилайте журнали до централізованої системи SIEM, де це можливо, навіть через переривчасті з'єднання. Надайте пріоритет критичним сповіщенням для негайного повідомлення. Це життєво важливо для операцій безпеки.

– Моніторинг NetFlow/IPFIX: Використовуйте NetFlow або IPFIX для збору даних про потік трафіку через тунелі DMVPN. Це може допомогти виявити аномальні моделі трафіку, неочікувані підключення або несанкціоновану передачу даних.

– Регулярні аудити безпеки: Проводьте періодичні аудити безпеки конфігурацій DMVPN на всіх пристроях, щоб забезпечити відповідність політикам безпеки та виявити неправильні конфігурації.

– Інтеграція даних про загрози: інтегруйте канали даних про загрози для виявлення відомих шкідливих IP-адрес або шаблонів атак, які можуть бути спрямовані на інфраструктуру DMVPN. Це допомагає в управлінні загрозами.

– Посібники з реагування на інциденти: Розробіть конкретні посібники з реагування на інциденти для сценаріїв компрометації DMVPN. Вони повинні окреслювати кроки для:

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

- Виявлення: Як ідентифікувати ознаки компрометації тунелю (наприклад, збої автентифікації, аномалії маршрутизації).
- Стимування: Кроки для ізоляції скомпрометованих спиць або сегментів без порушення всієї тактичної мережі.
- Видалення: Процедури для перекодування тунелів, перетворення образів пристроїв або анулювання сертифікатів.
- Відновлення: Кроки для відновлення безпечних операцій.
- Аналіз після інциденту: Висновок з досвіду для покращення майбутніх розгортань, особливо в середовищах з обмеженими ресурсами.

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Нижче розглянемо її більш докладно. У системі використовуються наступні протоколи. В основу програмного забезпечення створення VPN підключень покладені протоколи забезпечення безпеки інформації IPsec та SSL.

Заголовок АН

Автентифікуючий заголовок (АН) є звичайним опціональним заголовком і, як правило, розташовується між основним заголовком пакета IP і полем даних. Наявність АН ніяк не впливає на процес передачі інформації транспортного й більш високого рівнів. Основним і єдиним призначенням АН є забезпечення захисту від атак, пов'язаних з несанкціонованою зміною вмісту пакета, і в тому числі від підміни вихідної адреси мережного рівня. Протоколи більш високого рівня повинні бути модифіковані з метою здійснення перевірки автентичності отриманих даних.

Формат АН досить простий і складається з 96-бітового заголовка й даних змінної довжини, що складаються з 32-бітових слів. Назви полів досить ясно відбивають їхній зміст: Next Header указує на наступний заголовок, Payload Len представляє довжину пакета, SPI є показником на контекст безпеки й Sequence

Number Field містить послідовний номер пакета.

Послідовний номер пакета був введений в АН в 1997 році в ході процесу перегляду специфікації IPsec. Значення цього поля формується відправником і служить для захисту від атак, пов'язаних з повторним використанням даних процесу автентифікації. Оскільки мережа Інтернет не гарантує порядок доставки пакетів, одержувач повинен зберігати інформацію про максимальний послідовний номер пакета, що пройшов успішну автентифікацію, і про одержання деякого числа пакетів, що містять попередні послідовні номери (звичайно це число дорівнює 64).

На відміну від алгоритмів обчислення контрольної суми, застосовуваних у протоколах передачі інформації з лініям зв'язку, що комутуються або по каналах локальних мереж і орієнтованих на виправлення випадкових помилок середовища передачі, механізми забезпечення цілісності даних у відкритих телекомунікаційних мережах повинні мати засоби захисту від внесення цілеспрямованих змін. Одним з таких механізмів є спеціальне застосування алгоритму MD5: у процесі формування АН послідовно обчислюється хеш-функція від об'єднання самого пакета й деякого попередньо погодженого ключа, а потім від об'єднання отриманого результату й перетвореного ключа. Даний механізм застосовується за замовчуванням з метою забезпечення всіх реалізацій IPv6, принаймні, одним загальним алгоритмом, не підданим експортним обмеженням.

Заголовок ESP – інкапсуляція зашифрованих даних

У випадку використання інкапсуляції зашифрованих даних заголовок ESP є останнім у ряді опціональних заголовків, "видимих" у пакеті. Оскільки основною метою ESP є забезпечення конфіденційності даних, різні види інформації можуть вимагати застосування істотно різних алгоритмів шифрування. Отже, формат ESP може перетерплювати значні зміни залежно від використовуваних криптографічних алгоритмів. Проте, можна виділити наступні обов'язкові поля: SPI (SPI – Secutity Parameter Index – індекс параметра безпеки),

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		39

що вказує на контекст безпеки, поле порядкового номера, що містить послідовний номер пакета, і контрольна сума, призначена для захисту від атак на цілісність зашифрованих даних. Крім цього, як правило, у тілі ESP присутні параметри (наприклад, режим використання) і дані (наприклад, вектор ініціалізації) застосовуваного алгоритму шифрування. Частина ESP заголовок може бути зашифрована на відкритому ключі одержувача або на спільному ключі пари відправник-одержувач. Одержувач пакета ESP розшифровує ESP заголовок і використовує параметри й дані застосовуваного алгоритму шифрування для декодування інформації транспортного рівня.

Розрізняють два режими застосування ESP – транспортний і тоннельний.

Транспортний режим – використовується для шифрування поля даних IP пакета, що містить протоколи транспортного рівня (TCP, UDP, ICMP), який, у свою чергу, містить інформацію прикладних служб. Прикладом застосування транспортного режиму є передача електронної пошти. Всі проміжні вузли на маршруті пакета від відправника до одержувача використовують тільки відкриту інформацію мережного рівня й, можливо, деякі опціональні заголовки пакета (в IPv6). Недоліком транспортного режиму є відсутність механізмів приховання конкретних відправника й одержувача пакета, а також можливість проведення аналізу трафіку. Результатом такого аналізу може стати інформація про об'єми й напрямки передачі інформації, області інтересів абонентів, розташування керівників.

Тоннельний режим – припускає шифрування всього пакета, включаючи заголовки мережного рівня. Тоннельний режим застосовується якщо буде потреба приховання інформаційного обміну організації із зовнішнім миром. При цьому, адресні поля заголовка мережного рівня пакета, що використовує тоннельний режим, заповнюються міжмережним екраном організації й не містять інформації про конкретного відправника пакета. При передачі інформації із зовнішнього миру в локальну мережу організації як адреса призначення використовується мережна адреса міжмережного екрана. Після дешифрування міжмережним

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

екраном початкового заголовка мережного рівня пакет направляється одержувачеві.

Протокол ISAKMP/Oakley

Завдання алгоритмів IPsec – справа непроста, для цього потрібен протокол керування сеансом. Протокол ISAKMP (Internet Security Association Key Management Protocol) є рамковою основою для такого протоколу, а протокол Oakley – це вже конкретна реалізація його на цій основі, призначена для спільного використання з IPsec.

Протокол Oakley має більш широкий набір функціональних можливостей, ніж необхідно для керування IPsec-сеансами. Реалізація ISAKMP/Oakley являє собою функціональну підмножину, достатню, щоб забезпечити безпечний спосіб повідомлення автентифікованих даних для генерації ключів і SA-параметрів. Обмін по протоколу ISAKMP/Oakley відбувається у двох режимах (фазах): основному й швидкому. Відповідно до протоколу Oakley, обмін починається в основному й триває у швидкому режимі. У першому режимі встановлюються угоди SA для обміну даними по протоколу Oakley, а в другому – по протоколу IPsec.

На один обмін в основному режимі може доводитися кілька обмінів у швидкому, так як час існування SA-угоди для протоколу Oakley може бути більш тривалим, ніж для протоколу IPsec. Завдяки обмеженому строку існування SA-угод комбінування в сеансі основного й швидкого режимів забезпечує дуже потужний захисний механізм обміну ключами.

Обмін ключами в основному режимі здійснюється по методу Діффі-Хелмана (DH), що вимагає інтенсивного використання обчислювальних ресурсів. Цей метод є механізмом розподілу відкритих ключів для безпечного обміну секретною інформацією без застосування якої-небудь інформації, заздалегідь відомим обою сторонам. Тому ним активно користуються для встановлення безпечних сеансів зв'язку в тих випадках, коли необхідний динамічний захист і коли кіцеві системи не належать одній й тій же системі адміністративного керування. Наприклад, метод DH можна використовувати в електронній комерції

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

при встановленні з'єднання для передачі транзакцій між двома компаніями.

Хоча цей метод і вимагає більших обчислювальних ресурсів, при його застосуванні можливий компроміс між криптостійкістю алгоритму (при використанні менш довгих відкритих ключів) і необхідним об'ємом обчислень. Обмін ключами у швидкому режимі не вимагає великого об'єму обчислень, так як тут використовується набір простих математичних операцій. Існує обмеження припустимого числа швидких фаз, перевищення якого веде до того, що ключі, згенеровані в основній фазі, а потім використовувані у швидких фазах, виявляться під погрозою розкриття. На сьогоднішній день немає твердого правила, що визначає число швидких фаз на одну основну фазу; криптографи діють, керуючись загальними міркуваннями й з огляду на оперативну обстановку.

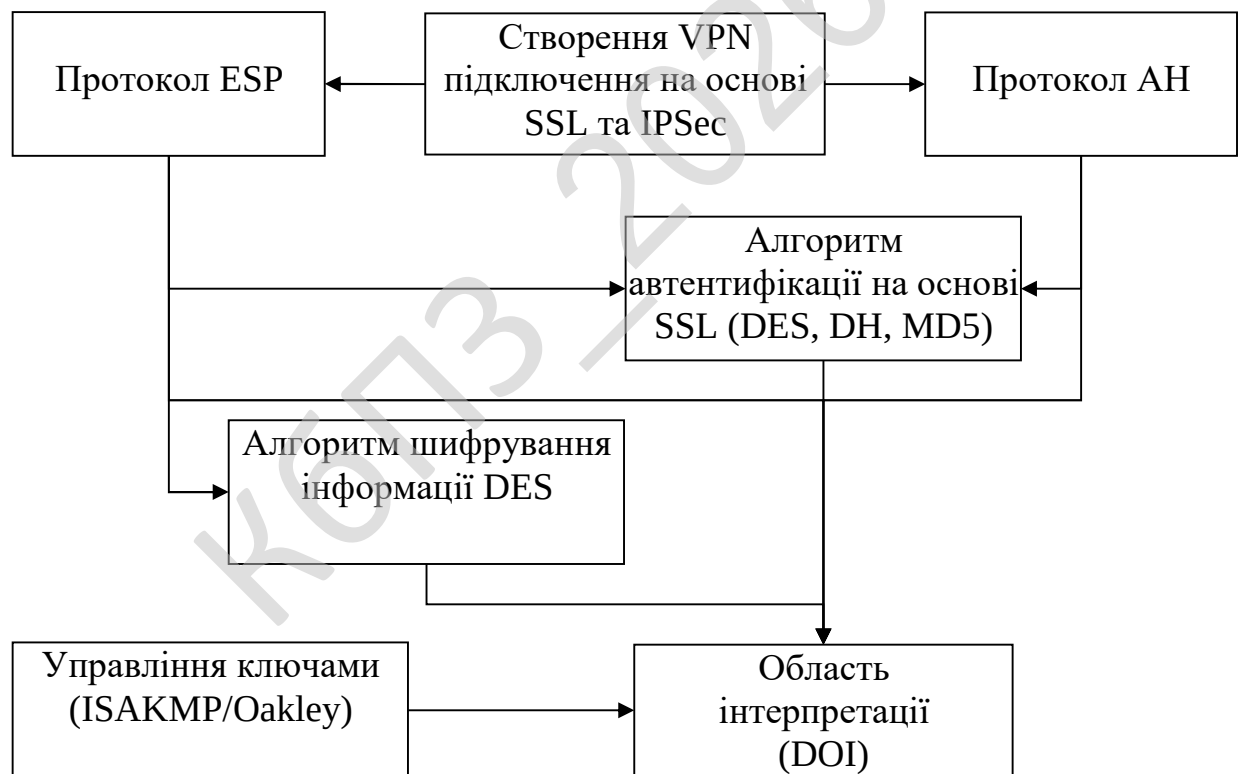


Рисунок 3.2 – Функціональна схема системи

В основному режимі обоє учасника обміну встановлюють SA-угоди для безпечного спілкування один з одним по протоколу Oakley. У швидкому режимі

SA-угоди встановлюються вже "від імені" протоколу IPsec або будь-якої іншої служби, який необхідні дані для генерації ключів або узгодження параметрів. Протокол Oakley розроблений таким чином, що він ніяк не пов'язаний з IPsec. Наприклад, для підвищення безпеки процесу встановлення сеансів його цілком можна використовувати разом із протоколом SSL (Secure Sockets Layer) версії 4.0 замість механізму обміну ключами SSL 3.0.

DOI – область інтерпретації

Протокол ISAKMP/Oakley не був спеціально розроблений для спільного використання із протоколом IPsec, тому виникає необхідність у так званій області інтерпретації (Domain Of Interpretation – DOI), що забезпечила б спільну роботу протоколів IPsec і ISAKMP/Oakley. Щоб інші протоколи також могли використовувати ISAKMP/Oakley, вони повинні мати власні DOI-області. У даний момент таких областей для інших протоколів не існує, але ситуація може змінитися на черговій конференції групи IETF або в тому випадку, якщо приватний розроблювач, наприклад фірма Netscape, вирішить використовувати цей механізм. Більш докладно про це можна прочитати в документі "The Internet Key Exchange (IKE)", розробленому робочою групою IP Security Protocol Working Group (<ftp://ftp.ietf.org/internet-draft/draft-ietf-ipsec-isakmp-oakley-06.txt>).

В основному режимі між сторонами погоджуються методи шифрування, хешування, автентифікації й так звана група DH (їх усього чотири), що визначає криптографічну стійкість алгоритму відкритого розподілу ключів. Перша група DH характеризується високою стійкістю й дозволяє використовувати стандарт DES, у той час як для другої й третьої груп варто застосовувати Triple DES. Оскільки в основному режимі іноді потрібно передавати до шести пакетів, то, наприклад, при використанні космічного сегмента з великою тимчасовою затримкою, DES краще застосовувати з більш сильною групою DH. Тоді перед виконанням чергового основного режиму, сполученого з інтенсивними обчисленнями й обміном пакетами, вам вдасться виконати більше обмінів у швидкому режимі.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

Коли SA-угода для обміну по протоколу Oakley устанавлюється в основному режимі, створюється ланцюжок випадкових біт, що використовують для генерації ключів. Також визначається тривалість (за часом або кількістю переданих даних) "життя" SA-угоди Oakley і дані для генерації ключів до того, як буде потрібно наступний обмін в основному режимі.

Швидкий режим простіше основного, і узгодження SA для IPsec здійснюється за допомогою трьох пакетів. IPsec-ключі створюються за допомогою простих операцій піднесення в ступінь переданих в основному режимі даних. У швидкому режимі погодяться також алгоритми шифрування й строки існування SA для IPsec-сеансів.

Згідно із цими строками визначається, як незабаром, залежно від часу або об'єму переданих даних, буде потрібно нове узгодження у швидкому режимі. Помітьте, є два різних строки існування SA-угоди. Основний режим задає його для протоколу Oakley, а швидкий – для обміну по протоколу IPsec. Як приклад пропонуємо значення цих параметрів для шифрування IPsec-сеансів за допомогою алгоритму DES: 15 хв або 10 Мбайт для швидкого режиму, і 60 хв або 40 Мбайт для основного. Ці числа варто збільшити для Triple DES і зменшити для ARCFour (в ARCFour застосовується 40-бітний, а в TripleDES – 112-бітний ключ). Такий підхід дозволяє збалансувати криптографічну стійкість сервісів IPsec і вартість накладних витрат на передачу пакетів ISAKMP/Oakley.

При генерації ключів в основному режимі сеанс можна примусово перервати на підставі відкликання сертифіката. Сертифікати кінцевих вузлів використовуються тільки під час основного режиму. Таким чином, при анулюванні одного із сертифікатів обмін перерветься тільки в основному режимі. Тимчасові обмеження, погоджені в основному й швидкому режимах, значно відрізняються друг від друга й залежать від типу даних і транзакцій, що використовують IPsec-з'єднання. Для правильного визначення цих обмежень із обліком, з одного боку, об'єму обчислень і навантаження на мережу, а з іншого боку – імовірності порушення захисту даних, потрібно деякий аналіз.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

Сполучення різних IPsec-механізмів забезпечує цілком безпечні з'єднання як між мережами, так і між кінцевими станціями. Оскільки практично всі постачальники підтримують ці стандарти, рано або пізно це приведе до виникнення середовища для реалізації безпечних з'єднань через Інтернет. Таким чином, протокол IPsec стане основним для безпечної е-комерції в Інтернет.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування).

Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи.

Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.

- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).

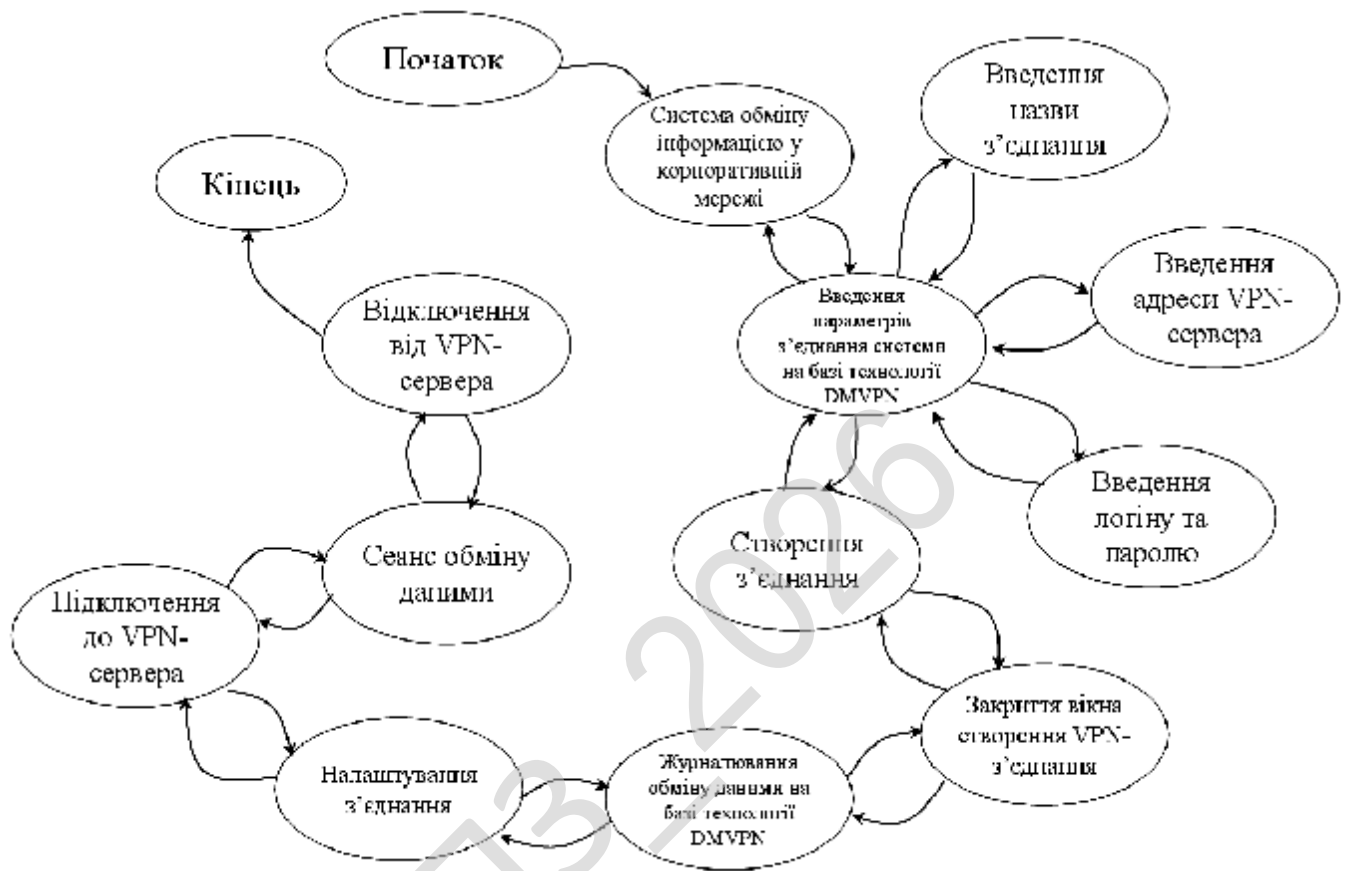


Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень. Було створено блок-схеми роботи системи. Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. Тому від точності і детальної блок-схеми залежить результат всієї програми. При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об'єктно-орієнтована що вимагає високого рівня декомпозиції задач на класи.

На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми. З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підсистеми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ. При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

Було використано наступні підходи UML: діаграма діяльності (діаграми поведінки типу); діаграма прецедентів (діаграми поведінки типу).

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

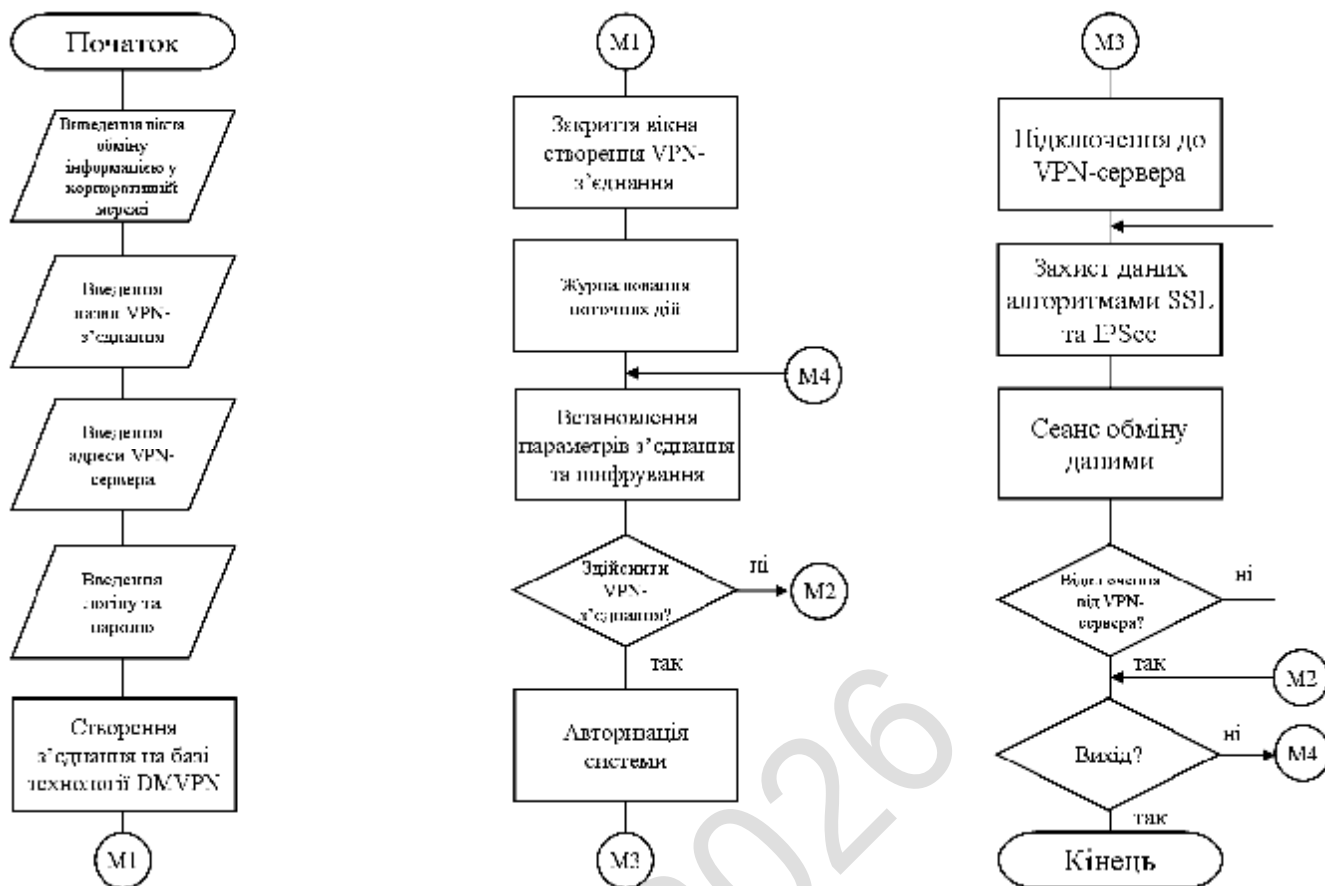


Рисунок 4.1 – Блок-схема основної програми

Діаграма діяльності. Це візуальне представлення графу діяльностей. Граф діяльностей є різновидом графу станів скінченного автомату, вершинами якого є певні дії, а переходи відбуваються по завершенню дій. Дія є фундаментальною одиницею визначення поведінки в специфікації. Дія отримує множину вхідних сигналів, та перетворює їх на множину вихідних сигналів.

Одна із цих множин, або обидві водночас, можуть бути порожніми. Виконання дії відповідає виконанню окремої дії. Подібно до цього, виконання діяльності є виконанням окремої діяльності, буквально, включно із виконанням тих дій, що містяться в діяльності. Кожна дія в діяльності може виконуватись один, два, або більше разів під час одного виконання діяльності. Щонайменше, дії мають отримувати дані, перетворювати їх та тестувати, деякі дії можуть вимагати певної послідовності.

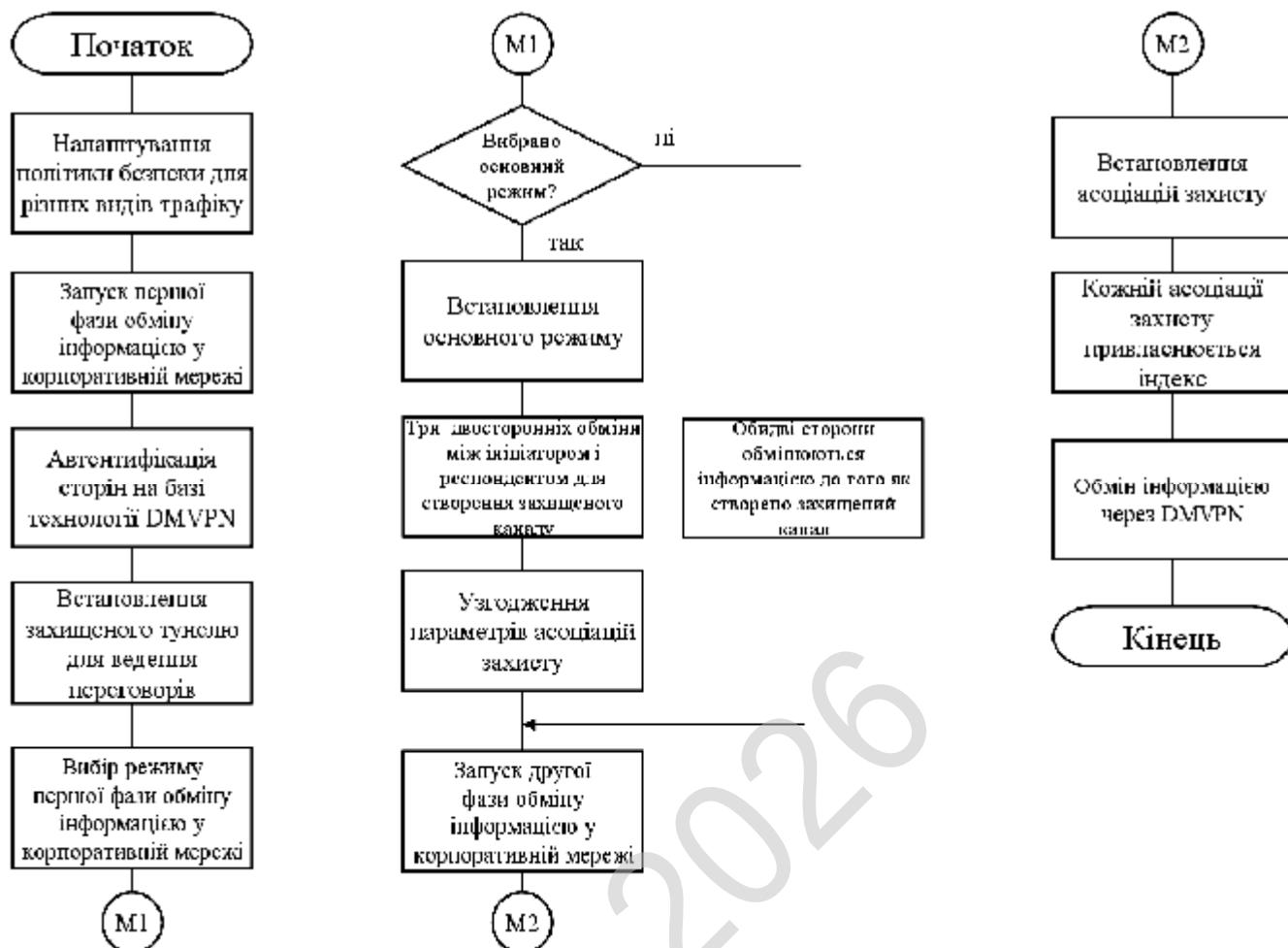


Рисунок 4.2 – Блок-схема роботи підпрограми

Специфікація діяльності (на вищих рівнях сумісності) може дозволяти виконання декількох (логічних) потоків, та існування механізмів синхронізації для гарантування виконання дій у правильному порядку.

Діаграма прецедентів це діаграма, на якій зображено відношення між акторами та прецедентами в системі. Також, перекладається як діаграма варіантів використання.

Діаграма прецедентів є графом, що складається з множини акторів, прецедентів (варіантів використання) обмежених границею системи (прямокутник), асоціацій між акторами та прецедентами, відношень серед прецедентів, та відношень узагальнення між акторами. Діаграми прецедентів відображають елементи моделі варіантів використання.

Суть даної діаграми полягає в наступному: проектована система представляється у вигляді безлічі сутностей чи акторів, що взаємодіють із системою за допомогою так званих варіантів використання. Варіант використання (use case) використовують для описання послуг, які система надає актору. Іншими словами, кожен варіант використання визначає деякий набір дій, який виконує система при діалозі з актором.

При цьому нічого не говориться про те, яким чином буде реалізована взаємодія акторів із системою.

У мові UML є кілька стандартних видів відношень між акторами і варіантами використання:

- асоціації (association relationship);
- включення (include relationship);
- розширення (extend relationship);
- узагальнення (generalization relationship).

При цьому загальні властивості варіантів використання можуть бути представлені трьома різними способами, а саме – за допомогою відношень включення, розширення і узагальнення.

Відношення асоціації – одне з фундаментальних понять у мові UML і в тій чи іншій мірі використовується при побудові всіх графічних моделей систем у формі канонічних діаграм.

Включення (include) у мові UML – це різновид відношення залежності між базовим варіантом використання і його спеціальним випадком. При цьому відношенням залежності (dependency) є таке відношення між двома елементами моделі, при якому зміна одного елемента (незалежного) приводить до зміни іншого елемента (залежного).

Відношення розширення (extend) визначає взаємозв'язок базового варіанта використання з іншим варіантом використання, функціональна поведінка якого задіюється базовим не завжди, а тільки при виконанні додаткових умов.

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних програм і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

Сервери є незалежними один від одного. Клієнти також функціонують паралельно і незалежно один від одного. Немає жорсткої прив'язки клієнтів до серверів. Більш ніж типовою є ситуація, коли один сервер одночасно обробляє запити від різних клієнтів; з іншого боку, клієнт може звертатися то до одного сервера, то до іншого. Клієнти мають знати про доступні сервери, але можуть не мати жодного уявлення про існування інших клієнтів.

Дуже важливо ясно уявляти, хто або що розглядається як «клієнт». Можна говорити про клієнтський комп'ютер, з якого відбувається звернення до інших комп'ютерів. Можна говорити про клієнтське та серверне програмне забезпечення. Нарешті, можна говорити про людей, які бажають за допомогою відповідного програмного та апаратного забезпечення отримати доступ до тієї чи іншої інформації.

Загальноприйнятим є положення, що клієнти та сервери – це перш за все програмні модулі. Найчастіше вони знаходяться на різних комп'ютерах, але бувають ситуації, коли обидві програми – і клієнтська, і серверна, фізично розміщуються на одній машині; в такій ситуації сервер часто називається локальним.

Модель клієнт-серверної взаємодії визначається перш за все розподілом обов'язків між клієнтом та сервером. Логічно можна відокремити три рівні операцій:

– рівень представлення даних, який по суті являє собою інтерфейс користувача і відповідає за представлення даних користувачеві і введення від нього керуючих команд;

– прикладний рівень, який реалізує основну логіку ПЗ і на якому здійснюється необхідна обробка інформації;

– рівень управління даними, який забезпечує зберігання даних та доступ до них.

Дворівнева клієнт-серверна архітектура передбачає взаємодію двох програмних модулів – клієнтського та серверного. В залежності від того, як між ними розподіляються наведені вище функції, розрізняють:

– модель тонкого клієнта, в рамках якої вся логіка ПЗ та управління даними зосереджена на сервері. Клієнтська програма забезпечує тільки функції рівня представлення;

– модель товстого клієнта, в якій сервер тільки керує даними, а обробка інформації та інтерфейс користувача зосереджені на стороні клієнта. Товстими клієнтами часто також називають пристрої з обмеженою потужністю: кишенькові комп'ютери, мобільні телефони та ін.

Типовим прикладом клієнт-серверної взаємодії є WWW. Існує величезна кількість веб-серверів, на яких розміщується та чи інша інформація. У найпростішому випадку ця інформація являє собою набір веб-сторінок, які можуть зберігатися на сервері у вигляді файлів, розмічених за допомогою мови розмітки HTML. Але ситуація, як правило, є складнішою; значна частина веб-ресурсів на сучасному етапі є динамічними, тобто вони не існують в заздалегідь підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Для того, щоб людина, яка працює в Інтернеті, могла переглянути ту чи іншу сторінку, на її комп'ютері повинно бути встановлено відповідне програмне забезпечення. Програми для перегляду веб-сторінок називаються браузером.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

Але, крім браузерів, до серверів можуть звертатися і інші клієнти, а саме – автономні програми. Вони можуть передбачати взаємодію з людиною, а можуть працювати в цілком автоматичному режимі. Типовим класом таких програм є роботи, призначені для автоматичного перегляду веб-ресурсів. Зокрема, роботи є важливим елементом пошукових систем і використовуються ними для перегляду сторінок і збору інформації про них.

Для запиту до веб-сервера клієнтська програма повинна задати місцезнаходження комп'ютера, на якому розміщується серверна програма, назву потрібного документа і, можливо, інші дані, які специфікують запит. Мережа забезпечує знаходження сервера і передачу йому клієнтського запиту. Серверні програми обробляють цей запит, відповідь пересилається по мережі клієнтові.

Трирівнева клієнт-серверна архітектура, яка почала розвиватися з середини 90-х років, передбачає відділення прикладного рівня від управління даними. Відокремлюється окремий програмний рівень, на якому зосереджується прикладна логіка ПЗ. Програми проміжного рівня можуть функціонувати під управлінням спеціальних серверів ПЗ, але запуск таких програм може здійснюватися і під управлінням звичайного веб-сервера. Нарешті, управління даними здійснюється сервером даних.

Для роботи з системою користувач використовує стандартне програмне забезпечення – звичайний браузер. Це позбавляє його необхідності завантажувати та інсталиувати спеціальні програми (хоча інколи така необхідність все-таки виникає).

Але користувачеві слід надати в розпорядженні інтерфейс, який дозволяв би йому взаємодіяти з системою і формувати запити до неї. Форми, що визначають цей інтерфейс, розміщуються на веб-сторінках та завантажуються разом з ними.

Веб-оглядач формує запит та пересилає його до сервера, який здійснює обробку. При необхідності сервер викликає серверні програмні модулі, які забезпечують обробку запиту і в разі потреби звертаються до сервера даних.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

Сервер даних здійснює операції з даними, що зберігаються в системі та складають її інформаційну основу. Зокрема, він може здійснити вибірку з інформаційної бази відповідно до запиту та передати її модулю проміжного рівня для подальшої обробки. Дані, з якими працює сервер даних, найчастіше організовані як реляційна база даних.

Найчастіше веб-сервер і серверні модулі проміжного рівня розміщуються на одному комп'ютері, хоч і являють собою окремі і логічно незалежні програмні модулі.

На сучасному етапі для програмування модулів проміжного рівня використовується мова серверних сценаріїв PHP, а для управління даними – СУБД MySQL. Таким чином, зв'язку PHP-MySQL слід розглядати як стандартний інструмент для створення порівняно простих інтерактивних веб-сайтів та систем електронної комерції; близько 90% комерційних систем сьогодні створюється саме на цій основі. Водночас як засоби управління даними, так і middleware-засоби можуть бути найрізноманітнішими. Так, для створення серверних програм, крім PHP, широко застосовуються Java, Perl, Python, Delphi.

Взагалі, технології створення розподілених, зокрема веб-програм, стрімко розвиваються. Слід згадати про технології EJB (Enterprise Java Beans), CORBA, а також про .NET – порівняно нову ініціативу компанії Microsoft. Для зберігання даних та їх передачі часто використовується так звана розширювана мова розмітки XML (Extensible Markup Language).

Розглянемо протокол SNMP (Simple Network Management Protocol, простий протокол керування мережею) – це протокол керування мережами зв'язку на основі архітектури TCP/IP.

На основі концепції TMN в 1980–1990 р. різними органами стандартизації був вироблений ряд протоколів керування мережами передачі даних з різним спектром реалізації функцій TMN. До одного з типів таких протоколів керування належить Simple Network Management Protocol (SNMP).

SNMP – це технологія, покликана забезпечити керування й контроль за пристроями й програмами в мережі зв'язку шляхом обміну керуючою інформацією між агентами, що розташовуються на мережних пристроях, і менеджерами, розташованими на станціях керування. SNMP визначає мережу як сукупність мережних керуючих станцій й елементів мережі (головні машини, шлюзи й маршрутизатори, термінальні сервери), які спільно забезпечують адміністративні зв'язки між мережними керуючими станціями й мережними агентами. SNMP різних версій присвячений цілий ряд рекомендацій IETF (RFC).

Зазвичай при використанні SNMP присутні керовані та керуючі системи. До складу керованої системи входить компонент, який називається агентом, який відправляє звіти керуючій системі. По суті SNMP агенти передають управлінську інформацію на керуючі системи як змінні (такі як «вільна пам'ять», «ім'я системи», «кількість працюючих процесів» тощо).

Керуюча система може отримати достовірну інформацію через операції протоколу GET, GETNEXT і GETBULK. Агент може самостійно без запиту надсилати дані, використовуючи операцію протоколу TRAP або INFORM. Управляючі системи можуть також відправляти конфігураційні оновлення або контролюючі запити, використовуючи операцію SET для безпосереднього управління системою. Операції конфігурування та управління використовуються тільки тоді, коли потрібні зміни у мережній інфраструктурі. Операції моніторингу зазвичай виконуються на регулярній основі.

Змінні, доступні через SNMP, організовані в ієрархії. Ці ієрархії та інші метадані (такі як тип і опис змінної) описуються Базами Керуючої Інформації (Management Information Bases (MIBs)).

SNMP не визначає, яку інформацію (які змінні) керована система повинна надавати. Навпаки, SNMP використовує розширювану модель, в якій доступна інформація визначається Базами Керуючої Інформації (MIB – Management Information Base).

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

Бази Керуючої Інформації описують структуру керуючої інформації пристроїв. Вони використовують ієрархічний адресний простір імен, що містить унікальний ідентифікатор об'єкта (object identifier (OID)).

Грубо кажучи, кожен унікальний ідентифікатор об'єкта ідентифікує змінну, яка може бути прочитана чи встановлена через SNMP. MIB'и використовують нотацію, визначену в ASN.1.

Ієрархія MIB може бути зображена як дерево з безіменним коренем, рівні якого приписані різними організаціями. На найвищому рівні MIB OID'и належать різним організаціям, що займаються стандартизацією, в той час як на нижчих рівнях OID'и виділяються асоційованими організаціями. Ця модель забезпечує управління на всіх шарах мережної моделі OSI, адже MIB'и можуть бути визначені для будь-яких типів даних і операцій.

Керований об'єкт – це одна з будь-якого числа характеристик, специфічних для керованого пристрою. Керований об'єкт включає в себе один або більше екземплярів об'єкта (що ідентифікуються за OID), які насправді є змінними.

Існує два типи керованих об'єктів: Скалярні об'єкти визначають єдиний екземпляр об'єкта; Табличні об'єкти визначають множинні, пов'язані екземпляри об'єктів які групуються в таблицях MIB.

Прикладом керованого об'єкта може бути atInput, який є скалярним об'єктом що містить єдиний екземпляр об'єкта, ціле число, яке показує загальну кількість вхідних пакетів AppleTalk на мережний інтерфейс маршрутизатора.

Ідентифікатор об'єкта (OID) унікально ідентифікує керований об'єкт в ієрархії MIB.

В телекомунікаціях і комп'ютерних мережах, ASN.1 є стандартною гнучкою нотацією для опису структур даних, що служать для кодування, передачі і декодування даних. ASN.1 являє собою набір правил для опису структури об'єктів, незалежних від специфічних для обладнання методик кодування, і формальну нотацію, яка дозволяє уникнути неоднозначностей.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

ASN.1 це єдиний ISO та ITU-T стандарт, спочатку визначений у 1984 році як частина стандарту CCITT X.409: 1984. Пізніше, в 1988 році, завдяки його широкому застосуванню, він був виділений в окремий стандарт X.208. Значно переглянута версія 1995 року описана в X.680.

Адаптована підмножина ASN.1 Структура Керуючої Інформації (SMI) описана в протоколі SNMP для визначення наборів пов'язаних MIB об'єктів, також званих MIB модулями.

SNMP працює на прикладному рівні TCP/IP (сьомий рівень моделі OSI). Агент SNMP отримує запити по UDP-порту 161. Менеджер може посилати запити з будь-якого доступного порту джерела на порт агента. Відповідь агента буде відправлений назад на порт джерела на менеджері. Менеджер отримує повідомлення (Traps і InformRequests) по порту 162. Агент може генерувати повідомлення з будь-якого доступного порту. При використанні TLS або DTLS запити виходять по порту 10161, а пастки відправляються на порт 10162.

У SNMPv1 зазначено п'ять основних протокольних одиниць обміну (protocol data units – PDU). Ще дві PDU, GetBulkRequest і InformRequest, були введені в SNMPv2 і перенесені в SNMPv3.

Нижче перераховані сім протокольних одиниць обміну SNMP:

1. GetRequest. Запит від менеджера до об'єкту для отримання значення змінної або списку змінних. Необхідні змінні вказуються в полі variable bindings (розділ поля values при цьому не використовується). Отримання значень зазначеної змінної повинно бути виконано агентом як Атомарна операція. Менеджеру буде повернений Response (відповідь) з поточними значеннями.

2. SetRequest. Запит від менеджера до об'єкту для зміни змінної або списку змінних. Зв'язані змінні вказуються в тілі запиту. Зміни всіх зазначених змінних повинні бути виконані агентом як атомарна операція. Менеджеру буде повернений Response з (поточними) новими значеннями змінних.

3. GetNextRequest. Запит від менеджера до об'єкту для виявлення доступних змінних і їх значень. Менеджеру буде повернений Response зі

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

зв'язаними змінними для змінної, яка є наступною в базі MIB в лексикографічному порядку. Обхід всієї бази MIB агента може бути проведений ітераційним використанням GetNextRequest, починаючи з OID 0. Рядки таблиці можуть бути прочитані, якщо вказати в запиті OID-и колонок в пов'язаних змінних.

4. GetBulkRequest. Покращена версія GetNextRequest. Запит від менеджера до об'єкту для численних ітерацій GetNextRequest. Менеджеру буде повернений Response з декількома пов'язаними змінними, обійденими починаючи зі пов'язаної змінної (змінних) в запиті. Специфічні для PDU поля non-repeaters і max-repetitions використовуються для контролю за поведінкою відповіді. GetBulkRequest був введений в SNMPv2.

5. Response. Повертає зв'язані змінні і значення від агента менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest і InformRequest. Повідомлення про помилки забезпечуються полями статусу помилки і індексу помилки.

Ця одиниця використовується як відповідь і на Get-, і на Set-запити, в SNMPv1 називається GetResponse.

6. Trap. Асинхронне повідомлення від агента – менеджеру. Включає в себе поточне значення sysUpTime, OID, що визначає тип trap (пастки), і необов'язкові зв'язані змінні. Адресація одержувача для пасток визначається за допомогою змінних trap-конфігурації в базі MIB. Формат trap-повідомлення був змінений в SNMPv2 і PDU перейменували в SNMPv2-Trap.

7. InformRequest. Асинхронне повідомлення від менеджера менеджеру або від агента менеджеру. Повідомлення від менеджера менеджеру були можливі вже в SNMPv1 (за допомогою Trap), але SNMP зазвичай працює на протоколі UDP, в якому доставка повідомлень не гарантована, і не повідомляється про втрачені пакетах. InformRequest виправляє це зворотним відправленням підтвердження про отримання. Одержувач відповідає Response-му, що повторює всю інформацію з InformRequest. Цей PDU був введений в SNMPv2.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

NetBIOS (Network Basic Input/Output System) – протокол для роботи в локальних мережах на персональних ЕОМ типу IBM/PC, розроблений у вигляді інтерфейсу, який не залежить від фірми–виробника. Був розроблений фірмою Sytek Corporation за замовленням IBM в 1983 році. Він включає в себе інтерфейс сеансового рівня (англ. NetBIOS interface), в якості транспортних протоколів використовує TCP і UDP.

Особливістю NetBIOS є можливість його роботи поверх різних протоколів, найпоширенішими/відомими з яких є NetBEUI, IPX і стек протоколів TCP/IP; причому якщо старі версії Windows орієнтувалися на більш легкі в реалізації і менш ресурсомісткі NetBEUI і IPX, то сучасні Windows орієнтуються на TCP/IP.

При використанні NetBEUI і IPX NetBIOS сам забезпечує надійність доставки даних (функціональність SPX не використовувати), а при використанні TCP/IP надійність доставки забезпечує TCP, за що удостоївся окремого імені «NBT».

Інтерфейс NetBIOS являє собою типовий інтерфейс взаємодії програм (API) для забезпечення мережових операцій введення–виведення і управління транспортним протоколом.

Програми, що використовують NetBIOS API інтерфейс, можуть працювати тільки при наявності протоколу, що допускає використання такого інтерфейсу.

NetBIOS також визначає протокол, що функціонує на сеансовому/транспортному рівнях моделі OSI. Цей протокол використовується протоколами нижчих рівнів, такими як NBFP (NetBEUI) і NetBT для виконання мережових запитів вводу–виводу і операцій, описаних в стандартному інтерфейсному наборі команд NetBIOS.

Тобто, NetBIOS сам не підтримує виконання файлових операцій. Ця функція покладається на протоколи нижчих рівнів, а сам NetBIOS забезпечує тільки зв'язок з цими протоколами і NetBIOS API–інтерфейс.

Пакет NETBIOS створений для використання групою EOM. Підтримує як режим сесій (робота через з'єднання), так і режим дейтаграм (без встановлення з'єднання). 16-символьні імена об'єктів в NETBIOS розподіляються динамічно.

NETBIOS має власну DNS, яка може взаємодіяти з інтернетівськй. Ім'я об'єкта при роботі з NETBIOS не може починатися з символу *.

Додатки можуть знайти через NETBIOS потрібні їм ресурси, встановити зв'язок і послати або отримати інформацію. NETBIOS використовує для служби імен порт 137, для служби дейтаграм – порт 138, а для сесій – порт 139. Будь-яка сесія починається з NETBIOS-запиту, завдання IP-адреси і визначення TCP-порту віддаленого об'єкта, далі йде обмін NETBIOS-повідомленнями, після чого сесія закривається.

Сесія здійснює обмін інформацією між двома NETBIOS – додатками. Довжина повідомлення лежить в межах від 0 до 131 071 байт. Припустимо одночасне встановлення декількох сесій між двома об'єктами.

При організації IP-транспорту через NETBIOS IP-дейтаграмма вкладається в NETBIOS-пакет. Інформаційний обмін відбувається в цьому випадку без встановлення зв'язку між об'єктами. Імена NETBIOS повинні містити в собі IP-адреси. Так, частина NETBIOS-адреси може мати вигляд IP.XX.XX. XX.XX, де IP вказує на тип операції (IP через Netbios), а XX. XX. XX.XX – IP- адреса.

Система NETBIOS має власну систему команд (call, listen, hang up, send, receive, session status, reset, cancel, adapter status, unlink, remote program load) і примітивів для роботи з дейтаграммами (send datagram, send broadcast datagram, receive datagram , receive broadcast datagram).

Всі кінцеві вузли NETBIOS діляться на три типи:

- широкомовні («b») вузли;
- вузли точка-точка («p»);
- вузли змішаного типу («m»).

IP-адреса може асоціюватися з одним із зазначених типів. В-вузли встановлюють зв'язок зі своїм партнером за допомогою широкомовних запитів. Р-

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

і М-вузли для цієї мети використовують netbios сервер імен (NBNS) і сервер розподілу дейтаграм (NBDD).

NetBIOS забезпечує:

- реєстрацію і перевірку мережеских імен;
- встановлення і розрив з'єднань;
- зв'язок з підтвердженням доставки інформації;
- зв'язок без підтвердження доставки інформації;
- підтримку управління і моніторингу драйвера і мережевої карти.

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм LOKI_91. Механізм алгоритму LOKI_91 подібний DES (рисунок 4.3). Блок даних розщеплюється на ліву й праву половини й проходить 16 раундів, що досить нагадує DES. У кожному раунді права половина спочатку піддається операції XOR із частиною ключа, а потім розширювальній перестановці (таблиця 4.1).

Таблиця 4.1 – Перестановка з розширенням

4	3	2	1	32	31	30	29	28	27	26	25
28	27	26	25	24	23	22	21	20	19	18	17
20	19	18	17	16	15	14	13	12	11	10	9
12	11	10	9	8	7	6	5	4	3	2	1

48-бітовий вихід розділяється на чотири 12-бітових блоки. У кожному блоці виконується така підстановка з використанням S-блоку: береться кожний 12-бітовий вхід, 2 старших і 2 молодших біти використовуються для утворення номера r , а вісім внутрішніх біт утворюють номер c . Вихід S-блоку, O , має наступне значення: $O(r,c) = (c + ((r*17) \oplus 0xff) \& 0xff)^{31} \bmod P_r$.

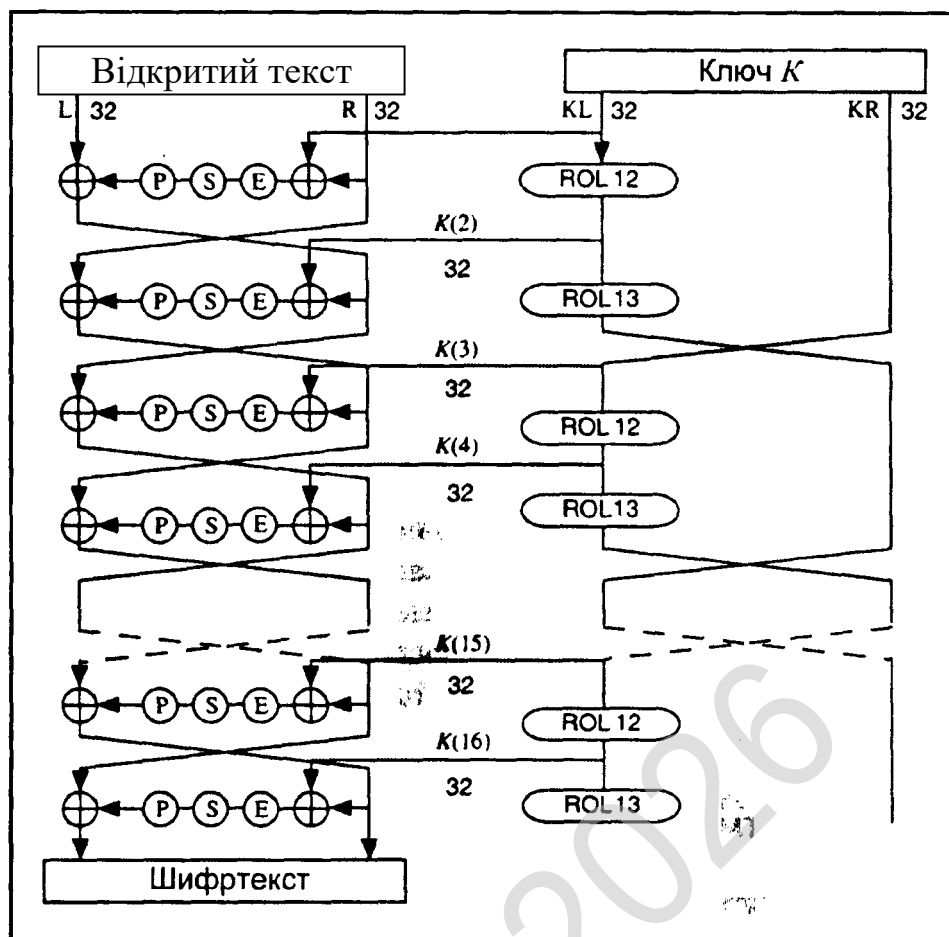


Рисунок 4.3 – Алгоритм LOKI91

Таблиця 4.2 – Значення P_r

r	1	2	3	4	5	6	7	8
P_r	375	379	391	395	397	415	419	425
r	9	10	11	12	13	14	15	16
P_r	433	445	451	463	471	477	487	499

Після цього чотири 8-бітових результати знову поєднуються, утворюючи 32-бітове число, що піддається операції перестановки, описаній в таблиці 4.3. Нарешті, для одержання нової лівої половини виконується операція XOR правої половини з колишньою лівою половиною, а ліва половина стає новою правою

половиною. Після 16 раундів для одержання остаточного шифртексту знову виконується операція XOR над блоком і ключем.

Таблиця 4.3 – Перестановка за допомогою Р-блоку

32	24	16	8	31	23	15	7	30	22	14	6	29	21	13	5
2	20	12	4	27	19	11	3	26	18	10	2	25	17	9	1

Підключи генеруються із ключа досить прямолінійно. 64-бітовий ключ розбивається на ліву й праву половини. На кожному раунді підключем служить ліва половина. Далі вона циклічно зрушується вліво на 12 або 13 біт, потім після кожних двох раундів ліва й права половини міняються місцями. Як і в DES, для зашифрування й розшифрування використовується один й той самий алгоритм із деякими змінами у використанні підключів.

К6ПЗ-2026

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1-5.5 зображено розроблене у бакалаврської дипломної роботі система забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий. Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма. На рисунку 5.1 зображено скриншот вікна створення VPN-з'єднання. На рисунку 5.2 зображено скриншот вікна створення VPN-з'єднання (введення параметрів з'єднання). На рисунку 5.3 зображено скриншот вікна створення VPN-з'єднання (завершення роботи). На рисунку 5.4 зображено скриншот ярлика створеного VPN-з'єднання на робочому столі.

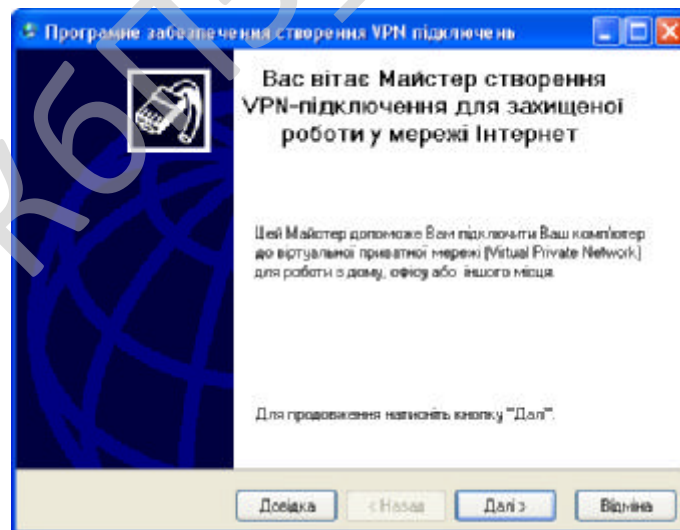


Рисунок 5.1 – Вікно створення VPN-з'єднання

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

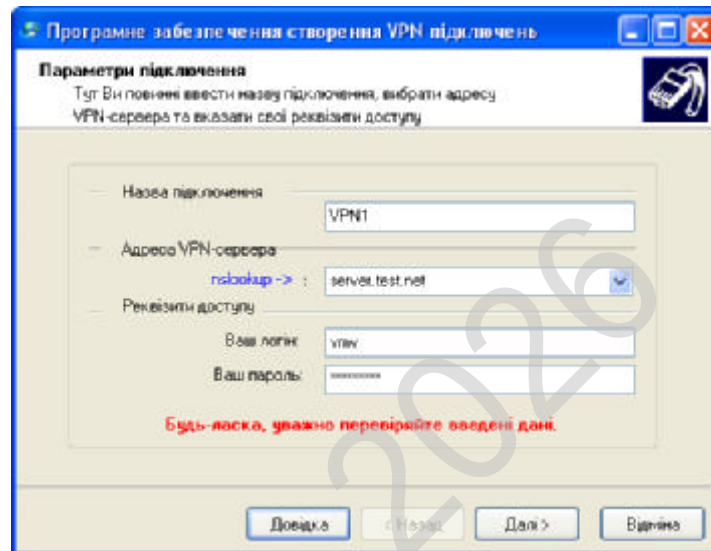


Рисунок 5.2 – Вікно створення VPN-з'єднання (введення параметрів з'єднання)

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити. Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

– Випуск.

- Встановлення та активація.
- Деактивація.
- Адаптація.
- Оновлення.
- Вмонтування.
- Відстежування версій.
- Видалення.
- Вилучення з обігу.

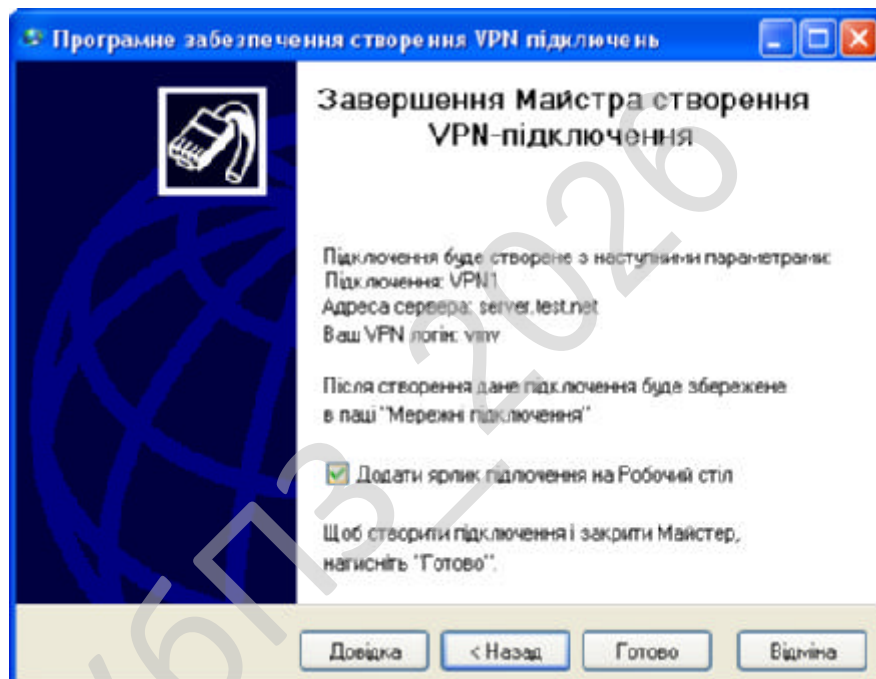


Рисунок 5.3 – Вікно створення VPN-з'єднання (завершення роботи)

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво

важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження;



Рисунок 5.4 – Іконка створеного VPN-з'єднання у папці «Мережні з'єднання»

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в ІТ рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

- відповідності поставленим вимогам;
- правильна відповідь для усіх можливих вхідних даних;
- виконання функцій за прийнятний час;
- практичність;
- сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування форматом білої скриньки засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

У цьому випадку формуються тестові варіанти, в яких:

- Гарантується перевірка всіх незалежних маршрутів програми.
- Знаходяться гілки True, False для всіх логічних рішень.
- Виконуються всі цикли (у межах їхніх кордонів та діапазонів).
- Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

- Кількість незалежних маршрутів може бути дуже велика.
- Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.
- У програмі можуть бути пропущені деякі маршрути.

– Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки" пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

– Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.

– Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

– При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

– Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

Проводилось тестування чорної скриньки.

Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

– Як виконуються функції програми.

– Як приймаються вихідні дані.

– Як виробляються результати.

– Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^{10} . Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чію поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

- Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ІТс).

- Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його ОТ).

Будь-який спосіб тестування «чорної скриньки» повинен:

- Виявити такі вхідні дані, які з високою ймовірністю належать набору ІТс.
- Сформулювати такі очікувані результати, які з високою ймовірністю є елементами набору ОТ.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

- Некоректних чи відсутніх функцій;
- Помилки інтерфейсу;
- Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних;

- Помилки характеристик (необхідна ємність пам'яті і т.д.);
- Помилки ініціалізації та завершення.

Обрано умови розповсюдження – Shareware.

Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70

(тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

В угоді про використання (ліцензії для кінцевого користувача, EULA) також може бути обумовлена заборона на комерційне або професійне (не тестове) її використання.

Основний принцип умовно-безплатного ПЗ – «спробуй, перш ніж купити» (try before you buy). ПЗ що поширюється як умовно-безплатний, надається користувачам безоплатно. Звичайно користувач платить тільки за час завантаження файлів через Інтернет або за носій (CD диск, флешку, ключ). Протягом певного терміну, що становить зазвичай тридцять днів, він може користуватися програмою, тестувати її, освоювати її можливості.

Якщо після закінчення цього терміну користувач вирішить продовжити використання ПЗ, він зобов'язаний купити його (zareestruvatisya), zaplativshi avtorovi певну суму.

В іншому випадку користувач повинен припинити використання ПЗ та видалити його зі свого комп'ютера.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докum.	Підпис	Дата		71

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.
- Досліджена система забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.
- На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створенні програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм LOKI_91.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Russ White & Ethan Banks «Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient, Modern Networks». 2017. – 832 p.
2. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». *Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка»* (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
3. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
4. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
5. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
6. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
7. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

8. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.

9. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.

10. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.

11. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». *CEUR Workshop Proceedings* Volume 3156, 2022, Pages 390-399.

12. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.

13. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.

14. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

15. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

16. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.

17. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

18. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

19. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

20. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		76

21. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.
22. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.
23. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.
24. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.
25. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
26. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
27. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.

28. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.

29. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019*, P. 395-399.

30. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

31. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352.

32. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019*, Pages 618-629.

33. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

34. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95

35. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у

комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки.* №4. С. 103-110. 2020.

36. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка.* № 3(7). С. 43-62. 2020.

37. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

38. О.А. Смірнов, П.С. Усік, «Дослідження перспектив використання технологічних рішень в мережах 5G» у *Кібербезпека та інформаційні технології: монографія.* – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

39. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». *Центральноукраїнський науковий вісник. Технічні науки.* № 2(33). с. 161-172, 2019.

40. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

41. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

42. Смірнов О.А., Дреєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

43. Дреєва Г.М., Смірнов О.А., Дреєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральнотраїнський науковий вїсник. Технїчні науки. № 1(32). с. 173-183, 2019.

44. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дреєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральнотраїнський науковий вїсник. Технїчні науки. № 1(32). с. 184-194, 2019.

45. Смірнов О.А., Смірнов С.А., Полїщук Л.І., Смірнова Т.В., Коноплицька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кїбербезпека: освіта, наука, технїка. – Том 3 № 3. – Кїїв: КУ ім. Бориса Грінченка. – 2019. – С. 63-87.

46. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посїбник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

47. Смірнов О.А., Котелянець В.В. Стїйкї до колїзїй стохастичнї моделї функціонування безпроводових сенсорних мереж. Вїсник інженерної академїї України, №3, с. 145-152, 2018

48. Смірнов О.А., Смірнов С.А., Дїдик А.К., Дреєв А.М. Алгоритми формування безлїчї маршрутів передачі метаданих у антивіруснї хмарнї системи. Збїрник наукових праць "Системи обробки інформації". - Випуск 5 (142). - Х.: ХУПС - 2016. - С. 148-152.

49. Смірнов О.А., Смірнов С.А. Дїдик А.К., Дреєв О.М. Моделї системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних системах. Збїрник наукових праць "Системи обробки інформації". - Випуск 3 (140). - Х.: ХУПС - 2016. - С. 36-39.

50. Смірнов О.А., Смірнов С.А., Дїдик А.К., Дреєв А.М. Спосїб контролю лїній зв'язку телекомунікаційної системи антивірусу. Збїрник наукових

					ВКРБ-123.26.0047.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		80

праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. - 2016. - С. 121-127.

51. Смірнов О.А., Смірнов С.А., Дідик А.К. Метод безпечної маршрутизації метаданих у хмарні антивірусні системи. Системи озброєння та військова техніка. - Випуск 2 (46) - Х.: ХУПС - 2016. - С. 146-149.

52. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.

53. Смірнов О.А., Кавун С.В., Коваленко О.В., Дреєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.

54. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

55. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.

56. Смірнов О.А., Мелешко Є.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник. – Кіровоград: КНТУ 2012. – 250 с.

57. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник. – Кіровоград: КНТУ 2012. – 454 с