

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 кібербезпеки для захисту
корпоративної мережі від кіберзагроз”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22-2
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Слободенюк І.Р.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнова Т.В.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань ._12 _____“Інформаційні технології”
Спеціальність 125 “Кібербезпека”
Освітньо-професійна (освітньо-наукова) програма “Кібербезпека”

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

Слободенюку Іллі Руслановичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз*

2. Керівник роботи *Смірнова Тетяна Віталіївна, канд. техн. наук, доцент*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 129-02 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 кібербезпеки для захисту корпоративної мережі від кіберзагроз*

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 кібербезпеки в промислову експлуатацію.

6. Висновки

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

Структурна схема системи кібербезпеки *1 аркуш*

Функціональна схема системи кібербезпеки *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

Смірнова Т.В.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Слободенюк І.Р.
(прізвище та ініціали)

АНОТАЦІЯ

Слободенюк І.Р. Програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

Метою розробки є програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

Результат роботи – програмна реалізація системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

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: кібербезпека, захист корпоративної мережі від кіберзагроз

ABSTRACT

Slobodeniuk I.R. Software for a cybersecurity system to protect a corporate network from cyber threats. 125 Cybersecurity. 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 that is intended for a cybersecurity system to protect a corporate network from cyber threats.

The purpose of the development is software for a cybersecurity system to protect a corporate network from cyber threats.

The result of the work is a software implementation of a cybersecurity system to protect a corporate network from cyber threats.

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 PCs with Windows 10/11.

The program is developed in the Python environment.

Keywords: cybersecurity, corporate network protection from cyber threats

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.....	9
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	12
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	12
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	25
2.3 Розгорнута постановка завдання	30
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	31
3.1 Опис функціонування системи	31
3.2 Розробка структурної схеми.....	36
3.3 Розробка функціональної схеми	45
3.4 Розробка діаграми процесів.....	48
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	50
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	50
4.2 Захист розробленого програмного забезпечення.....	70
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	72
6 ОСНОВНІ ВИСНОВКИ.....	78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	80

					ВКРБ-125.26.0040.00.00.ПЗ			
Вим	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагро.</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>		Слободенюк І.Р.				Б		
<i>Перев.</i>		Смірнова Т.В.					1	88
<i>Н.контр.</i>		Коваленко А.С.				ЦНТУ КБ-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. У сучасному швидкозмінному цифровому світі бізнес постійно перебуває під загрозою кібератак, які можуть поставити під загрозу конфіденційні дані, порушити роботу та зашкодити репутації бренду. Організації будь-якого розміру повинні впроваджувати надійні рішення мережевої безпеки для захисту своєї ІТ-інфраструктури та забезпечення безперервності бізнесу.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

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

- Огляд існуючих систем для захисту корпоративної мережі від кіберзагроз.
- Дослідження системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.
- Програмна реалізація системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для захисту корпоративної мережі від кіберзагроз.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Відзначимо, що вище сформульовано основні вимоги до корпоративного VPN. На практиці вони можуть бути реалізовані (якщо ці вимоги не реалізовані, те це не корпоративна VPN) різним образом. Разом з тим, як відзначалося раніше, при побудові корпоративної VPN (як і будь-якого іншого засобу захисту для даних застосунків), одним з найважливіших завдань є завдання спрощення адміністрування.

Отже, як відзначалося, при побудові корпоративної VPN повинні бути вирішені два ключові завдання – реалізація розмежувальної політики доступу до корпоративних ресурсів і криптографічний захист віртуальних ("накладених" на існуюче телекомунікаційне встаткування) каналів зв'язку корпоративної мережі.

Реалізація розмежувальної політики доступу до корпоративних ресурсів

Коли мова заходить про реалізацію розмежувальної політики доступу до ресурсів, у першу чергу, необхідно визначитися з тим, що ж є суб'єктом і об'єктом доступу. Це дозволить визначити спосіб їхньої ідентифікації. У загальному випадку, як об'єктом, так і суб'єктом доступу (як правило, в VPN суб'єкт одночасно є й об'єктом доступу) може виступати або комп'ютер, при цьому доступ розмежовується між комп'ютерами, або користувач, відповідно доступ розмежовується між користувачами. Універсальність корпоративної VPN досягається в тому випадку, коли як суб'єкт і об'єкта може виступати як комп'ютер у складі корпоративної мережі, так і користувач – співробітник підприємства. Це, а також складність ідентифікації комп'ютерів у мережі по адресах (потрібні спеціальні пристрої – координатори мережі, а це додаткові витрати й додаткова складність адміністрування) обумовлює доцільність

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

включення спеціальної сутності "Ідентифікатор" (ніяк не зв'язаної ні з адресою комп'ютера, ні з обліковим записом), використовуваної для ідентифікації суб'єктів і об'єктів VPN. Залежно від способу зберігання ідентифікатора суб'єкта/об'єкта (на комп'ютері, наприклад, у реєстрі або у файлі, або на зовнішньому носії, надаваному користувачеві, наприклад, на електронному ключі, або на смарт-карті), тобто його приналежності (належить комп'ютеру або користувачеві), може бути реалізована розмежувальна політика доступу до ресурсів VPN для комп'ютерів або ж для користувачів.

Тепер, двома словами, про користувачів. По різних причинах, вони можуть мати різний ступінь довіри. Тому користувачів доцільно підрозділяти на користувачів з високим і низьким рівнями довіри. Користувачеві з низьким рівнем довіри доцільно дозволити передачу інформації тільки в рамках корпоративної мережі, тобто дозволити взаємодія тільки з комп'ютерами в складі VPN, трафік у якій шифрується. Користувачеві з високим рівнем довіри може знадобитися дозволити взаємодія, як з комп'ютерами VPN (по захищеному каналі зв'язку), так і з комп'ютерами зовнішньої мережі (тут інформація передається у відкритому виді). Оскільки сутність "Ідентифікатор" у загальному випадку може привласнюватися, як користувачеві, так і комп'ютеру, то у двох режимах (з можливістю виходу в зовнішню мережу й без такої можливості) можуть використовуватися й комп'ютери корпоративної мережі.

Процедуру ідентифікації здійснює сервер VPN (який по зрозумілих причинах може резервуватися з автоматичною реплікацією бази налаштувань на резервний сервер). На комп'ютери в складі VPN встановлюються клієнтські частини, основу яких становить мережний драйвер. Клієнтська частина блокує який-небудь доступ у мережу доти, поки не буде проведена ідентифікація (комп'ютера або користувача, відповідно, ідентифікатор розташовується або на комп'ютері, або на зовнішньому носії в користувача) на сервері. При ідентифікації комп'ютера процедура здійснюється автоматично, для ідентифікації користувача – йому необхідно ввести в комп'ютер ідентифікатор

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

(наприклад, вставити смарт-карту з ідентифікатором). Після ідентифікації на сервері, залежно від рівня довіри, що відповідає ідентифікатору, клієнтська частина дозволить взаємодію (комп'ютера або користувача) або тільки з комп'ютерами в складі VPN – на які також встановлена клієнтська частина, інформація при цьому буде передаватися в шифрованому виді, або в захищеному режимі (із шифрацією) з комп'ютерами VPN, у відкритому – тільки із зовнішніми стосовно VPN комп'ютерами. Відношення комп'ютера до VPN визначається взаємодією клієнтських частин по захищеному протоколі.

Таким чином, властиво віртуальна мережа (VPN) формується із состава комп'ютерів, на яких встановлена клієнтська частина. Для підключення до VPN необхідна ідентифікація комп'ютера, або користувача на сервері VPN. Реалізація ж розмежувальної політики доступу усередині VPN (розмежування доступу між сутностями "Ідентифікатор", які можуть привласнюватися як комп'ютерам – розмежування між комп'ютерами, так і користувача – розмежування між користувачами) здійснюється адміністратором на сервері (про те, як це робиться, трохи нижче).

Налаштування й експлуатація VPN помітно спрощуються. Наприклад, для підключення до VPN мобільного користувача в будь-якій точці земної кулі, досить наявності в нього комп'ютера, підключеного до мережі, на якому повинна бути встановлена клієнтська частина VPN, і ідентифікатора, що йому видасть адміністратор (ми поки говоримо тільки про реалізацію розмежувальної політики). Адміністратор же створюючи ідентифікатор, може відповідним чином призначити рівень довіри й визначити ті ідентифікатори (комп'ютери або користувачів) з якими в рамках VPN по захищеному протоколі зможе "спілкуватися" мобільний користувач. Ніяких координаторів для цього не потрібно, тому що адреса (який може бути різним при кожному віддаленому підключенні комп'ютера до мережі) не використовується як ідентифікуюча сутність.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

Реалізація криптографічного захисту віртуальних каналів зв'язку корпоративної мережі

Вище ми говорили, що основними вимогами до реалізації криптографічного захисту віртуальних каналів корпоративної мережі є:

- "прозоре" автоматичне (примусове для користувача) шифрування віртуальних каналів корпоративної мережі;
- централізоване генерування ключів шифрування адміністратором (користувач повинен бути виключений зі схеми адміністрування й керування VPN);
- відсутність ключа шифрування віртуальних каналів зв'язку в користувача й відповідно;
- неможливість доступу користувача до ключів шифрування.

Важливою умовою ефективності захисту є необхідність часткої зміни ключів шифрування віртуальних каналів. Це з урахуванням необхідності централізованого генерування ключів для всіх суб'єктів/об'єктів (обумовлених ідентифікаторами) корпоративної мережі, істотно ускладнює завдання адміністрування VPN.

Підхід до реалізації ключової політики полягає в наступному.

Кожний суб'єкт/об'єкт VPN характеризується парою ознак: ідентифікатор і ключ шифрування взаємодії із сервером VPN. Дана пара генерується адміністратором при створенні суб'єкта/об'єкта. Якщо суб'єктом/об'єктом VPN виступає комп'ютер, то ідентифікатор і ключ шифрування взаємодії із сервером VPN встановлюються на комп'ютері адміністратором при установці клієнтської частини (у процесі експлуатації по розсуду адміністратора дані параметри можуть бути змінені), якщо ж суб'єктом/об'єктом VPN виступає користувач, то згенерована адміністратором пара ознак ідентифікатор і ключ шифрування взаємодії із сервером VPN видаються користувачеві адміністратором на зовнішньому носії (Flash-пристрій, електронний ключ, смарт-карта).

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

До моменту ідентифікації суб'єкта/об'єкта клієнтською частиною VPN на сервері, на комп'ютері не зберігається якої-небудь інформації про ключі шифрування віртуальних каналів. Ключі шифрування віртуальних каналів генеруються сервером при ідентифікації суб'єктів/об'єктів VPN автоматично, тобто навіть адміністратор безпеки не має ключову інформацію. Здійснюється це в такий спосіб. При ідентифікації суб'єкта/об'єкта VPN на сервері, для ідентифікуємого суб'єкта/об'єкта сервером автоматично генеруються ключі шифрування (кожна пара взаємодіючих суб'єктів/об'єктів VPN має свій ключ шифрування) з іншими суб'єктами/об'єктами VPN. Дана інформація (ключі шифрування даного комп'ютера з іншими активними комп'ютерами в складі VPN) сервером у зашифрованому виді передається на ідентифікований комп'ютер (ідентифікованому користувачеві), де зберігається в оперативній пам'яті – ця інформація не доступна користувачеві. Одночасно на всі інші активні (ідентифіковані раніше) комп'ютери із складу VPN сервером видаються згенеровані ключі шифрування для взаємодії зі знову ідентифікованим суб'єктом/об'єктом. Таким чином, у кожний момент часу в оперативній пам'яті ідентифікованого комп'ютера в складі VPN зберігається таблиця із ключами шифрування трафіку з іншими активними (ідентифікованими) комп'ютерами в складі VPN (для кожної пари цей ключ свій). Дана таблиця поповнюється після ідентифікації кожного наступного суб'єкта/об'єкта. Зміна ключа шифрування здійснюється сервером автоматично при кожній наступній ідентифікації суб'єкта/об'єкта.

Таким чином, вся процедура генерації ключових пар повністю автоматизована, не вимагає участі адміністратора безпеки, ключі шифрування віртуальних каналів VPN не доступні не тільки користувачам корпоративної мережі, але й адміністраторові.

Розмежування ж доступу між суб'єктами/об'єктами в складі VPN (про що згадувалося раніше) реалізується тим, що при ідентифікації суб'єкта/об'єкта йому передаються ключі шифрування віртуальних каналів тільки з тими активними

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

суб'єктами/об'єктами, з якими адміністратором дозволена взаємодія даному суб'єктові/об'єкту. Клієнтська ж частина VPN, установлена на комп'ютері в складі VPN, дозволить здійснювати з його взаємодія тільки з тими активними суб'єктами/об'єктами, для взаємодії з якими отримані відповідні ключі шифрування із сервера VPN.

1.2 Область застосування

Отже, на початку роботи ми поставили перед собою досить складне завдання – створити корпоративну VPN, при цьому максимально спростивши її адміністрування (природно, що без зниження забезпечуваного рівня безпеки). Що ж нам удалося в підсумку одержати? У чому складаються завдання адміністрування VPN, адже, як відзначали раніше, безліч функцій адміністратора в VPN автоматизовано.

У своєму складі ПЗ містить:

- клієнтські частини, установлювані на комп'ютери, що включаються до складу VPN;
- серверні частини (основна й резервна), установлювані на виділені комп'ютери;
- АРМ адміністратора безпеки;
- може встановлюватися як на окремому комп'ютері, так і на сервері VPN.

Тепер про адміністрування. Насамперед, адміністраторові варто інсталиювати відповідне ПЗ.

На сервері необхідно створити базу суб'єктів/об'єктів VPN. Це реалізується з інтерфейсу серверної частини, наведеного на мал.1. Для кожного створеного суб'єкта необхідно вказати довірений він (тоді йому дозволяється взаємодія із зовнішньою мережею), або ні, також для завдання системного суб'єкта існує сутність "резервний сервер". Для створених суб'єктів сервером VPN автоматично генеруються його ідентифікатор і ключ шифрування взаємодії

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

із сервером VPN, які необхідно зберегти на зовнішньому носії (або на Flash-пристрої, якщо суб'єктом виступає комп'ютер, або на одному з обраних носіїв – електронний ключ або карта (може бути також і Flash-пристрій), якщо суб'єктом виступає користувач. Даний пристрій буде використовуватися користувач для його ідентифікації, з метою одержання доступу до віртуальних каналів VPN. Даний пристрій згодом адміністраторові необхідно буде передати відповідному співробітникові підприємства (користувачеві). Крім того, необхідно настроїти системні параметри сервера, задати алгоритм шифрування віртуальних каналів в VPN.

На комп'ютери в складі VPN інстальється клієнтська частина системи захисту. Після інсталяції задаються відповідні системні параметри, задається алгоритм шифрування, використовуваний в VPN, задається спосіб зберігання й уведення ідентифікатора суб'єкта і його ключа шифрування взаємодії із сервером VPN, параметри взаємодії з основним і резервним серверами VPN.

Налаштування корпоративної VPN завершене. Якщо суб'єктами доступу є користувачі (не комп'ютери), то після установки клієнтської частини на комп'ютер користувача, адміністратор повинен передати користувачеві ключ (карту) з ідентифікаційними даними й ключем шифрування взаємодії із сервером VPN (ці дані адміністратор завжди зможе змінити на сервері, відповідно видавши новий ключ (потрібно змінити вміст ключа) користувачеві).

У процесі функціонування від користувача (якщо він, а не комп'ютер, є суб'єктом VPN) потрібно лише підключати ключ (карту) до комп'ютера для ідентифікації, з метою одержання доступу до мережі, від адміністратора ж взагалі не потрібно ніяких додаткових дій (всі ключі шифрування між кожною парою суб'єктів на сервері генеруються автоматично, при кожному підключенні комп'ютера VPN до сервера VPN). Адміністраторові залишається тільки здійснювати функції контролю роботи користувачів в VPN.

На закінчення відзначимо, що метою даної роботи не був детальний опис який-небудь конкретної корпоративної VPN. Ми постаралися сформулювати

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

вимоги до побудови корпоративної VPN і розглянути підходи до рішення одного із ключових завдань реалізації засобу захисту в даних застосунках – завдання спрощення адміністрування. На наш погляд, чітке позиціонування засобу захисту (у роботі мова йде про корпоративний VPN), наслідком чого з'явилася розробка й опублікування відповідних вимог до його побудови, допоможе розібратися споживачеві в представленому на ринку засобів захисту різноманітті подібних засобів. На наш погляд, засобів побудови VPN саме для корпоративних застосунків на сьогоднішній день дуже мало – одиниці. Більшість рішень може тією чи іншою мірою ефективно використовуватися для побудови часток VPN – для особистого використання. Ті ж засоби, які орієнтовані на корпоративне використання, відрізняються високою складністю не тільки властиво засобів захисту, але і їхнього адміністрування. У даній роботі ми також спробували показати, що завдання спрощення адміністрування корпоративної VPN може бути вирішена, причому вирішено досить ефективно.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для захисту корпоративної мережі від кіберзагроз, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

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

Є причина, по якій за використання безкоштовних VPN-сервісів не просять грошей: ви в кожному разі заплатите, просто по-іншому. Ви заслуговуєте не зіштовхуватися з обмеженнями трафіку, що дратує рекламою й небезпечними вірусами. У даній роботі протестували 100+ безкоштовних VPN-сервісів і знайшли 7 з них, які забезпечать вам високу швидкість підключення, відмінну сумісність зі стримінговими сервісами, а також гідний рівень безпеки, якому можна довіряти. Онлайн-конфіденційність – це ваше невід'ємне право, тому ви не повинні за неї платити. Наша сімка кращих безкоштовних VPN-сервісів гарантує захист і анонімний перегляд веб-сайтів, і за все це не потрібно буде платити. Тут немає ніяких вивертів: просто завантажте своє безкоштовне VPN-застосунок і виходите в Мережу. Як правило, вибір між безкоштовним і платним застосунками очевидний. Навіщо платити за те, що можна одержати безкоштовно? Але з VPN-застосунками все не так просто. Зрештою, не буває безкоштовного сиру: ви завжди заплатите тим або іншим способом. Коли мова заходить про безкоштовний VPN-сервіси, такою платою може стати низька швидкість підключення, необхідність дивитися дратівну рекламу, небезпечні віруси або навіть витік ваших конфіденційних даних.

VPN-провайдери користуються дуже простою хитрістю: вони обмежують безкоштовну версію свого застосунка настільки, що ви не зможете нормально користуватися необхідними послугами, поки не перейдете на платну. У підсумку, коли ви утомитеся від постійної буферизації, обмеженого вибору серверів і відсутності можливості дивитися Netflix, ви, швидше за все, зволієте заплатити.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

Найкращі з безкоштовних VPN-сервісів пропонують послуги, які практично так само гарні; фактично, вони гарні настільки, що вам, швидше за все, навіть не прийде переходити на платну версію. Ми рекомендуємо вам вибрати безкоштовний VPN-сервіс, з яким ви зможете:

- одержати доступ до геоблокованому контенту (тобто контенту, що недоступний у вашому регіоні);
- радуватися блискавичній швидкості підключення;
- бути впевненими, що ваші дані не зберігаються в логівих журналах.

Кращі безкоштовні VPN-сервіси:

1. NordVPN: ідеальний варіант для подорожей менш ніж на місяць або знайомства з VPN-технологіями.
2. Hotspot Shield: стабільний, швидкий і надійний VPN-сервіс, якщо ви не плануєте дивитися кіно й серіали онлайн.
3. Windscribe: ідеальний варіант для аматорів стримінгових сервісів, яких не дратує буферизація.
4. hide.me: гарний вибір, якщо ви не плануєте користуватися ним для роботи з торрент-трекерами.
5. Proton: надійний VPN-сервіс без обмеження трафіку, але не працює з торрент-трекерами.
6. Opera: відмінний безкоштовний VPN-сервіс, але тільки як розширення для веб-браузера.
7. TunnelBear: гарний вибір, якщо ви піклуєтеся про свої онлайн-безпеки й не плануєте використовувати багато трафіку.

У чому підступ з безкоштовними VPN-сервісами?

Більшість безкоштовних VPN-сервісів мають обмеження: наприклад, обмежений вибір серверів, низькі швидкості підключення або обмежений трафік. Більше 65% із протестованих нами безкоштовних VPN-сервісів не дають користувачам можливість дивитися серіали й фільми онлайн і працювати з торрент-мережами, а деякі ще й навмисно сповільнюють підключення. Так, ви

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

нічого не платите, але навряд чи вас задовольнять такі послуги. VPN-провайдери створюють видимість, що ви одержуєте їхні послуги безкоштовно. Насправді ж ви самі ризикуєте виявитися товаром. Багато користувачів повідомляли нас, що безкоштовні VPN-провайдери крали їх конфіденційні дані, а потім продавали третім особам.

Це піднімає інше гостре питання. Навіть безкоштовний VPN-сервіс у першу чергу повинен допомагати користувачам зберігати анонімність у мережі, але тільки по-справжньому безпечні сервіси насправді зможуть це зробити. На жаль, безліч безкоштовних VPN-сервісів являють собою лише ще одну, причому серйозну, погрозу вашої безпеки.

Ваші дані можна продати, тільки якщо перед цим їх кудись зберегти. Багато безкоштовних VPN-сервісів не мають безлогової політики безпеки, тобто вони можуть просто відслідковувати ваші дані, зберігати їх і, як наслідок, піддавати вас ризику. Безкоштовні сервіси також сумно відомі як джерела спама, реклами й вірусів.

Ми протестували сотні безкоштовних VPN-застосунків, і деякі з них, здається, були занадто гарні, щоб бути справжніми. Це викликало в нас певні підозри, тому ми докладніше вивчили самі нереалістичні пропозиції провайдерів.

Факти, що відкрилися, нас шокували: виявляється, багато безкоштовних VPN-сервісів зареєстровані в Китаї, у тій самій країні, чий уряд прийняв самі строгі закони об інтернет-цензурі. У політиках конфіденційності деяких із цих провайдерів прямо написаний, що даних користувачів будуть зберігатися й передаватися стороннім організаціям. Якщо хочете захистити своє право на конфіденційність, тримаєтеся подалі від будь-яких VPN-сервісів, зареєстрованих у Китаї.

Є ще одна дуже важлива причина, по якій варто триматися подалі від безкоштовних VPN-сервісів. Бізнесмени й маркетологи знають, що користувачі хочуть максимально спростити собі життя. Вони припускають, що раз вже вам сподобалася безкоштовна версія, ви рано або пізно перейдете на платний

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

тарифний план. У чому проблема? Кращий безкоштовний VPN-сервіс – це далеко не завжди те ж саме, що й кращий платний. І вже зовсім точно це не краще співвідношення ціни і якості. Багато безкоштовних сервісів пропонують дорогі тарифні плани, у яких ви одержите доступ до середнього по якості й можливостям функціоналові, у той час як інші сервіси, хоч і не мають безкоштовної версії, пропонують набагато кращі послуги по більше привабливій ціні. Якщо залишитися зі своїм «знайомим» провайдером до кінця, може так вийти, що ви переплатите за гірші послуги й залишитеся із другосортними VPN-підключеннями замість того, щоб насолоджуватися одним із кращих сервісів на ринку.

1. NordVPN

Спробуйте наш варіант №1 серед VPN-сервісів безкоштовно протягом 30 днів: необмежений вибір серверів, доступ до стримінговим сервісів і торрент-сайтам



Рисунок 2.1 – Інтерфейс користувача NordVPN

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

NordVPN – не безкоштовний сервіс. Фактично, це преміум-сервіс, що пропонує одні із самих просунутих можливостей. Так чому ж він потрапив у наш список кращих безкоштовних VPN-сервісів?

NordVPN пропонує 30-денну гарантію повернення грошей без зайвих питань. Це означає, що ви можете користуватися ним безкоштовно протягом місяця й при цьому зовсім нічим не ризикувати.

Це ідеальний варіант, якщо вам потрібно VPN-застосунок на короткий проміжок часу. Якщо ви їдете кудись менше ніж на місяць, можна встановити застосунок NordVPN, щоб безкоштовно справлятися з геоблоками й цензурою.

Це також відмінний спосіб насолодитися необмеженим доступом до стримінгових сервісів і першокласних функцій забезпечення безпеки, не оформляючи передплату на дорогий тарифний план. Нарешті, якщо ви просто хочете зрозуміти, чому так багато людей обожають VPN-додатки, але самі ви поки ще не готові платити, не варто покладатися на повільний, ненадійний безкоштовний застосунок.

Замість цього безкоштовно перевірте на ділі застосунок NordVPN. Якщо вам воно сподобається так само сильно, як цим користувачам, переходите на платну підписку, а якщо ні, то підписку можна швидко скасувати.

Застосунок NordVPN доступні для наступних пристроїв, ОС і веб-браузерів:

- Android, Windows, macOS, iOS, Android TV, Linux, Chrome і Firefox.

Переваги NordVPN:

- Стабільний доступ до Netflix, так що ви ніколи не пропустите важливу серію.
- Більш ніж 5 100 серверів в 60 країнах.
- Гарантія блискавичних швидкостей підключення.
- Просунуті протоколи безпеки, шифрування даних військового рівня, а також функція екстреного відключення від Інтернету.

– Гарантія повної конфіденційності, оскільки сервіс зареєстрований у країні, що не входить у розвідальнянськи «5/9/14 око».

2. Hotspot Shield

Для оплати не потрібна банківська карта, швидкі швидкості підключення, обмеження трафіку 500 Мб у день.

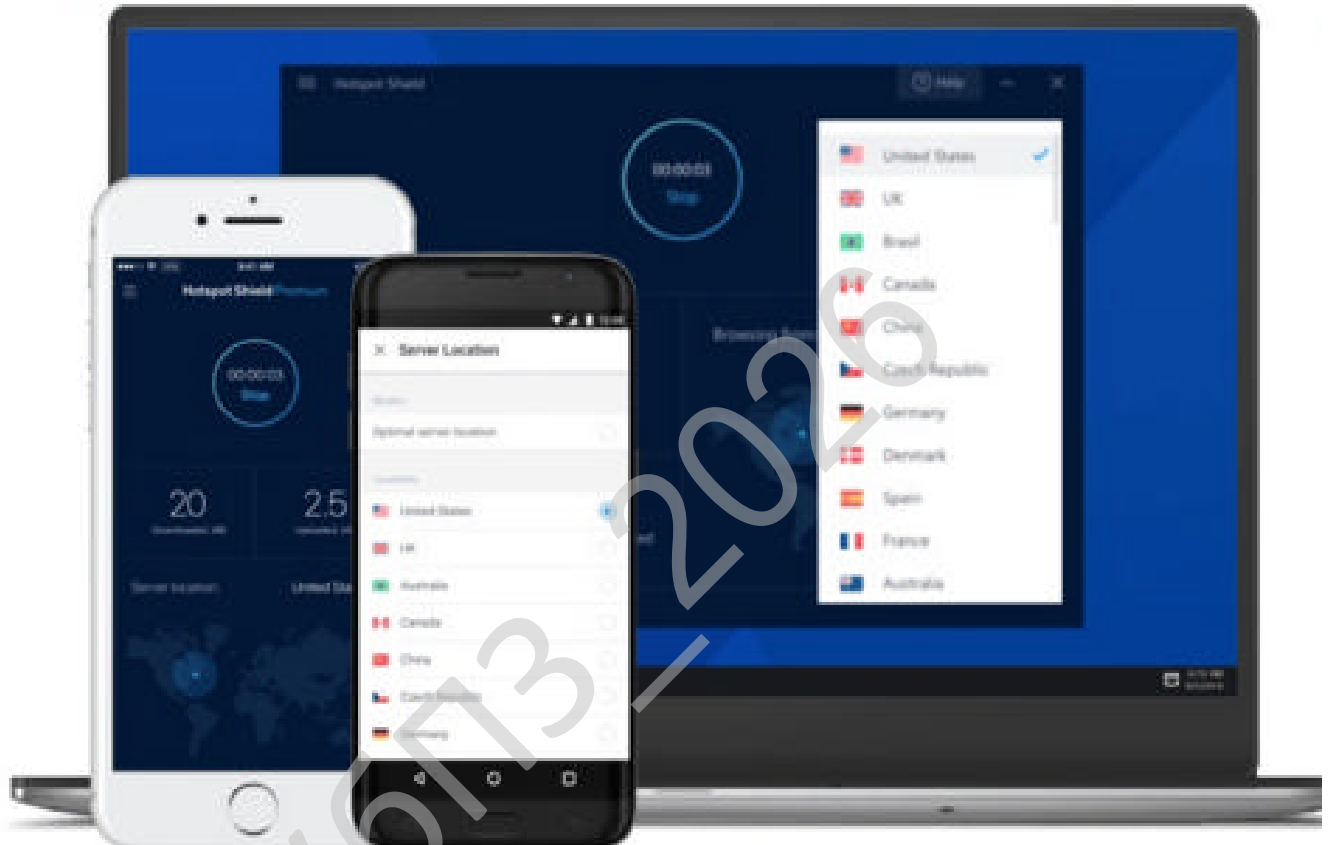


Рисунок 2.2 – Інтерфейс користувача Hotspot Shield

Hotspot Shield – кращий вибір серед безкоштовних VPN за версією наших читачів. У безкоштовній версії вам гарантовані блискавичні швидкості підключення, шифрування даних військового рівня й, як результат, швидкий і безпечний перегляд веб-сайтів.

Застосунки Hotspot Shield сумісні з усіма ОС, сам сервіс дотримується безлогової політики й пропонує техпідтримку для всіх платформ. Ви зможете

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

одержати доступ до геоблокованого контенту з будь-якої точки світу, використовуючи будь-який пристрій.

Безкоштовна версія обмежена всього 500 Мб трафіку в день. Незважаючи на те, що цього не вистачить для перегляду Netflix або завантаження більших торрент-файлів, вам точно буде цього досить для безпечного перегляду веб-сайти, де б ви не перебували.

Ви зможете підключити тільки один пристрій до безкоштовного аккаунту Hotspot Shield, також буде обмежена кількість доступних серверів. Безкоштовна версія існує за рахунок реклами, так що ви будете часто неї дивитися!

Застосунка Hotspot Shield доступні для:

- Windows, Android, macOS, iOS і Chrome.

Плюси безкоштовної версії:

- Швидкі підключення гарантують пошук у Мережі без затримок.
- Безлогова політика конфіденційності означає, що ваша історія запитів захищена від сторонніх очей.

- Шифрування даних військового рівня захистить вашу активність у Мережі.

Мінуси безкоштовної версії:

- Неможливо дивитися відео на стримінгових сервісах, тобто ви можете пропустити нові серії своїх улюблених серіалів.

- Трафік обмежений 500 Мб у день (це приблизно два невеликих відео на YouTube).

- Багато реклами, тобто прийде часто перериватися.

3. Windscribe

Щедрий ліміт даних в 10 Гб, підтримує торрент-мережі, завжди безкоштовно.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18



Рисунок 2.3 – Інтерфейс користувача Windscribe

Сервіс Windscribe потрапив у наш список кращих безкоштовних VPN завдяки щедрому ліміту використання даних у цілих 10 Гб. Щомісяця безкоштовні передплатники одержують 10 Гб трафіку й можуть одержати додаткові 5 Гб, написавши у Твіттере про компанію. Можна також додатково одержати 1 Гб безкоштовного трафіку щомісяця, приводячи друзів.

Більшість серверів Windscribe підтримують торрент-мережі.

Як платні, так і безкоштовні передплатники мають доступ до всіх функцій і можливостей сервісу Windscribe, включаючи режим R.O.B.E.R.T (блокувальник реклами й шкідливих програм). Компанія має докладну політику конфіденційності, у якій чітко описане, які данні вони зберігають, а також безлогову політику. Сервіс Windscribe також може похвалитися майстерним захистом і шифруванням даних.

Windscribe пропонує користувачам десктопний застосунок і розширення для веб-браузера. Інтерфейс програми дружелюбний і зрозумілий, тут є кілька способів техпідтримки на вибір, включаючи онлайн-чат і посібника з налаштування.

Крім обмеження трафіку, безкоштовний аккаунт Windscribe обмежує вас кількістю доступних серверів – усього в 10 з 50 доступних країнах. Почитайте, що користувачі думають про сервіс Windscribe.

Windscribe доступний на наступних платформах:

– macOS, iPhone, Windows, Linux, Chrome і Firefox.

Плюси безкоштовної версії:

– Підтримує торрент-мережі для необмеженого доступу до ваших улюблених розваг.

Мінуси безкоштовної версії:

– Трафік обмежений 10 Гб на місяць (але це більше щедра пропозиція, чим у більшості інших безкоштовних сервісів).

– Обмежено доступ до мережі серверів у порівнянні із платною версією.

– Поки VPN-застосунок підключений, збираються деякі дані.

4. hide.me

Обмеження трафіку 2 Гб, підтримка торрент-сетей.

hide.me пропонує спрощене, але надійний безкоштовний застосунок. Ви одержите 2 Гб безкоштовного трафіку щомісяця, всі переваги протоколів безпеки сервісу hide.me, а також вибір з п'яти країн, до серверів у які можна підключитися. Тільки один з них перебуває в Європі.

На жаль, у вас не буде доступу до Netflix з hide.me. При цьому сервіс підтримує торрент-мережі, що робить його популярним серед користувачів.

Команда сервісу hide.me дійсно вірить у безкоштовні послуги, так що вони не обмежують безкоштовних передплатників. У вас буде цілодобовий доступ до служби техпідтримки й можливість переглядати сайти без реклами. Сервіс

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

hide.me дотримуються безлогової політики, надійно шифрує дані, підтримує різні протоколи безпеки, захищаючи вас і вашу конфіденційність.

Застосунок hide.me доступні для наступних платформ:

– Android, Windows, macOS, iOS, Linux, Chrome, Firefox, Windows Phone, Amazon Fire OS, а також його можна встановити на роутер.

Плюси безкоштовної версії:

– Гарні швидкості підключення для швидкого завантаження файлів і сайтів.

– Безлогова політика гарантує захист вашої конфіденційності.

– Безлімітні за часом безкоштовні послуги, тобто вам не прийде згодом переходити на платну версію.

Мінуси безкоштовної версії:

– Обмеження трафіку скромними 2 Гб на місяць.

– Доступ тільки до обмеженої кількості серверів.

– Обмежений трафік = обмежена кількість сайтів, що переглядаються, і відео.

5. ProtonVPN

Обмежена кількість серверів, необмежена пропускна здатність мережі. Хоча сервіс ProtonVPN пропонує якісні преміум-послуги, безкоштовна VPN-версія здається досить застарілою. Так, у вас буде необмежений трафік для одного пристрою, але при цьому у вас будуть проблеми зі швидкістю, що сповільнюється навмисно, підключення.

Ви не зможете дивитися Netflix з безкоштовним аккаунтом ProtonVPN. Тут є кілька серверів, які оптимізовані для роботи з торрентами. Втім, безкоштовні передплатники мають обмежений доступ до серверів країн, де підтримуються P2P-мережі.

Застосунок ProtonVPN просто використовувати, адже тут інтуїтивно зрозумілий інтерфейс, воно підходить для різноманітних платформ, що дуже подобається користувачам. Компанія також пропонує дуже надійні функції

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

забезпечення безпеки, включаючи потужне шифрування даних і протоколи безпеки. Це значить, що ваша онлайн-активність залишиться в таємниці від сторонніх, як і ваші дані.



Рисунок 2.4 – Інтерфейс користувача ProtonVPN

Застосунок ProtonVPN сумісний з наступними платформами:

– Android, Windows, macOS, iOS і Linux.

Плюси безкоштовної версії:

– Необмежений трафік означає, що ви будете під захистом у будь-який час.

– Безлогова політика й закони про захист конфіденційності Швейцарії задають високий рівень безпеки.

– Відмінні функції забезпечення безпеки.

Мінуси безкоштовної версії:

– Обмежена мережа серверів – доступ тільки до серверів у трьох країнах.

– Повільні підключення, тобто повільне завантаження сайтів і файлів.

– Неможливо зайти на торрент-трекери або стримінгові сервіси, так що у вас не буде доступу до улюблених розваг.

6. Opera

Необмежений перегляд веб-сайтів, безкоштовно назавжди.

Opera не є VPN-сервісом. Компанія створює веб-браузери, щоб Інтернет був відкритим, безкоштовним і безпечним.

Веб-браузер Opera доступний для платформ Windows, Mac, Linux і Android. Тут є убудований блокувальник реклами й VPN-розширення, а також захист від вірусів і інші можливості захисту конфіденційності користувачів. VPN-розширення приховує вашу особистість, даючи можливість анонімно переглядати веб-сайти; це особливо корисно при використанні суспільних мереж Wi-Fi.

Почитайте, що реальні користувачі думають про браузер Opera.

7. TunnelBear

Надійний захист, безкоштовно назавжди, обмежений трафік – усього 500 Мб на місяць.

Якщо ви недавно дізналися про VPN-сервіси, то безкоштовна версія TunnelBear – це відмінний варіант, з якого можна почати. Нашим читачам подобається дружелюбний інтерфейс цього застосунку, у якому є анімовані ведмеді. Ви зможете підключитися до серверів в 22+ країнах і насолоджуватися відмінними швидкостями підключення.

Сервіс TunnelBear дуже серйозно відноситься до анонімності й безпеки своїх користувачів. Цей VPN-сервіс перевіряється незалежними компаніями, використовує 256-бітне AES-шифрування й гарантує, що ніякі ваші дані не зберігаються в логівих журналах. Це значить, що ваша особистість буде схована від сторонніх.

Безкоштовний аккаунт TunnelBear розрахований усього на 500 Мб трафіку щомісяця (але ви можете заробити додатковий 1 Гб, написавши про сервіс у Твіттер). Цей VPN-сервіс не має доступу до Netflix і інших стримінгових сайтів, так що ви не зможете переглядати геоблокований контент із його допомогою.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

Застосунка TunnelBear доступні для:

– Android, Windows, macOS, iOS, Chrome, Firefox і Opera.

Плюси безкоштовної версії:

– Гарні швидкості підключення гарантують перегляд веб-сайтів без довгих завантажень.

– Ніяких логових журналів, потужне шифрування даних, – ви завжди будете захищені.

– Ніякої реклами, так що ніщо вас не буде відволікати.

Мінуси безкоштовної версії:

– Відсутність доступу до стримінговим сервісів, так що ніяких серіалів і музики.

– Трафік обмежений усього 500 Мб на місяць.

– Невелика мережа серверів у порівнянні з іншими VPN-провайдерами.

Як підсумок можна сказати, що можна знайти трохи гарних безкоштовних VPN-сервісів. При цьому, що й говорити, навіть самі безпечні безкоштовні сервіси не можна назвати абсолютно надійними. Найкращі безкоштовні сервіси просто не можуть зрівнятися із кращими платними.

VPN-сервіс преміум-класа дасть вам доступ до більше надійних функцій захисту, а також стримінговим сайтам і торрент-трекерам. А ще, на відміну від більшості безкоштовних VPN-сервісів, які обмежують ваш трафік, преміум-сервіси пропонують необмежений трафік. Ви зможете одержати доступ до більшого числа сервісів у більшому числі країн і насолоджуватися більше швидкими швидкостями підключення.

Найкраще з такими преміум-сервісами, що ви завжди можете спробувати їх безкоштовно. Більшість із них мають безкоштовний пробний період, а також гарантію повернення грошей, якщо вам щось не сподобається. Ви зможете переконатися, що сервіс вам підходить на всі 100%.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Python – динамічна інтерпретована об'єктно-орієнтована скриптова мова програмування із строгою динамічною типізацією. Офіційний сайт мови програмування Python <https://www.python.org/>. Python – багатоцільова мова програмування, яка дозволяє писати код, що добре читається. Відносний лаконізм мови Python дозволяє створити програму, яка буде набагато коротше свого аналога, написаного на іншій мові. Python – багатоплатформова мова програмування. Це означає, що програми на Python можна запускати в різних операційних системах без будь-яких змін.

Ще однією перевагою Python є його стандартна бібліотека, яка встановлюється разом з Python і містить готові інструменти для роботи з операційною системою, веб-сторінками, базами даних, різними форматами даних, для побудови графічного інтерфейсу програм тощо. Програми, написані на мові програмування Python, можуть бути як невеликими скриптами, так і складними системами. Python абсолютно безкоштовний.

Швидкість виконання коду Python

Один з можливих недоліків Python – швидкість виконання коду. Python не є компільованою мовою. Код на Python спочатку компілюється у внутрішній байт-код, який потім виконується інтерпретатором Python. У більшості випадків при використанні Python виходять програми повільніші в порівнянні з такими мовами, як С.

Втім, сучасні комп'ютери мають таку обчислювальну потужність, що для більшості застосунків швидкість розробки важливіша швидкості виконання, а програми на Python зазвичай пишуться набагато швидше.

Окрім того, Python легко розширюється модулями, написаними на С або С++. Такі модулі можуть використовуватися для виконання частин програми, що створюють інтенсивне навантаження на процесор.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

Використання Python

Python використовується для різних цілей: для створення ігор і веб-застосунків, розробки внутрішніх інструментів для різноманітних проектів. Мова також широко застосовується в науковій області для досліджень і розв'язування прикладних завдань.

Застосування мови програмування Python:

1. BitTorrent – протокол для обміну даними.
2. Ubuntu Software Center – вільне програмне забезпечення для пошуку, установки і видалення пакунків в системі Ubuntu Linux.
3. Blender – програма для створення тривимірної комп'ютерної графіки, що включає засоби моделювання, анімації, вимальовування, пост-обробки відео, а також створення відеоігор.
4. GIMP – растровий графічний редактор, із підтримкою векторної графіки.
5. World of Tanks.
6. Вільна енциклопедія Вікіпедія.
7. Пошукова система Google.
8. DropBox – файловий хостинг, що включає персональне хмарне сховище, синхронізацію файлів і програму-клієнт.
9. YouTube – популярне відеосховище.

Версії Python

Мови програмування з часом змінюються – розробники додають в них нові можливості, а також виправляють помилки. Так з'являються різні версії мови. Наприклад, код написаний на Python 2 у більшості випадків не буде працювати у версії Python 3 без внесення додаткових змін.

Процесор є найважливішим компонентом в комп'ютері. Одна з основних функцій процесора – це обробка даних згідно комп'ютерної програми, яка є списком інструкцій, шляхом виконання арифметичних і логічних операцій над фрагментами даних.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

Кожна інструкція в програмі – це команда, яка «повідомляє» процесору, яку операцію він повинен виконати. Процесор комп'ютера може розуміти лише ті інструкції, які написані на машинній мові. Машинна мова – це штучна мова, створена для передачі команд комп'ютеру. За допомогою машинної мови створюються ефективні програми, оскільки розробник отримує доступ до всіх можливостей процесора. Машинна мова – мова низького рівня.

Інструкція машинної мови існує для кожної операції, яку процесор здатний виконати – є інструкція для додавання чисел, є інструкція для віднімання чисел і т.д. Увесь набір інструкцій, який центральний процесор може виконати, відомий як набір інструкцій процесора.

Наприклад, у вас є певна програма, яка зберігається на диску вашого комп'ютера. Для виконання програми, ви здійснюєте подвійний клік на значку програми. Це змушує програму копіюватися з диска в оперативну пам'ять, після чого процесор комп'ютера виконує копію програми, яка знаходиться в оперативній пам'яті.

Коли процесор виконує інструкції програми, він бере участь у процесі, який є відомим як цикл `fetch – decode – execute` (отримати – декодувати – виконати). Цей цикл виконується для кожної інструкції у програмі і складається з трьох кроків:

Отримати

Програма – це послідовність інструкцій на машинній мові. Першим кроком циклу є завантаження (отримання) наступної інструкції з пам'яті в процесор.

Декодувати

Інструкція машинної мови – це двійкове число, яке представляє команду, що повідомляє процесору виконати певну операцію. На цьому кроці процесор декодує інструкцію, яку було «витягнуто» з пам'яті, для визначення того, яка операція повинна виконуватись.

Виконати

Останній крок циклу – виконати операцію.

Хоча процесор комп'ютера розуміє тільки машинну мову, людині непрактично писати програми на машинній мові. Така програма може мати тисячі або навіть мільйони бінарних інструкцій, і написання такої програми буде дуже обтяжливим процесом.

З цієї причини була створена мова асемблера як альтернатива машинній мові. Замість використання двійкових чисел для написання інструкцій, мова асемблера використовує короткі слова, відомі як мнемокоди.

Незважаючи на те, що мова асемблера не вимагає двійкових інструкцій, як у випадку машинної мови, проте вона вимагає високих знань про процесор. Використовуючи мову асемблера, навіть для найпростішої програми, необхідно написати велику кількість інструкцій.

Мова програмування високого рівня дозволяє створювати складні програми, не знаючи, як працює процесор, і не записуючи великої кількості інструкцій низького рівня. Крім того, більшість мов програмування високого рівня використовують слова, які легко зрозуміти.

Python – одна із популярних сучасних мов програмування високого рівня. Python – інтерпретована мова програмування. Python – це високорівнева інтерпретована мова програмування, на відміну від C++, яка є прикладом компільованої мови програмування. Назва Python відноситься як до мови програмування, так і до інтерпретатора – комп'ютерної програми, яка зчитує початковий код (написаний на Python) і виконує інструкції (команди).

Для перекладу мови високого рівня на машинну мову доступні два типи програм:

1. Компілятор.
2. Інтерпретатор.

Завантаження Python

Версії інтерпретатора Python для різних операційних систем доступні для безкоштовного завантаження за адресою <https://www.python.org/downloads>.

Середовище програмування для Python

Для написання програм використовують текстові редактори або інтегровані середовища розробки, які включають в себе різні інструменти для роботи з кодом: засіб для написання коду (текстовий редактор), інтерактивний інтерпретатор, відлагоджувач тощо.

Текстові редактори та інтегровані середовища програмування для Python:

- IDLE – стандартний редактор Python. Встановлюється разом з Python для користувачів Windows, окремим пакунком для користувачів Linux.
- Notepad++ – безкоштовний текстовий редактор початкового коду, який підтримує велику кількість мов, в тому числі і Python. Лише для користувачів Windows.
- Visual Studio Code – це легкий, але потужний редактор початкового коду, який розповсюджується безкоштовно і доступний у версіях для платформ Linux, Windows і macOS.
- PyScripter – інтегроване середовище розробки для мови програмування Python. Для користувачів Windows. Поширюється безкоштовно.
- Wing IDE 101 – вільне інтегроване середовище для Python, розроблене для навчання програмістів-початківців. Для користувачів Linux, Windows і macOS. Поширюється безкоштовно.
- Geany – вільний текстовий редактор з базовими елементами інтегрованого середовища розробки, доступний для операційних систем Linux, Windows і macOS.
- PyCharm – інтегроване середовище розробки для мови програмування Python. PyCharm є власницьким програмним забезпеченням. Наявна безкоштовна версія Community з усіченим набором можливостей. Для користувачів Linux, Windows і macOS.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

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

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 кібербезпеки 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 кібербезпеки 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-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Розглянемо основні підходи для захисту корпоративної мережі від кіберзагроз.

CYTAS

CYTAS надає інтегрований пакет послуг мережевої безпеки, розроблений для вирішення найактуальніших загроз, з якими стикається бізнес сьогодні. Поєднуючи передові технології з експертним моніторингом та розвідкою загроз, CYTAS допомагає організаціям ефективно виявляти, запобігати та реагувати на кіберзагрози.

Їхні рішення захищають від шкідливого програмного забезпечення, програм-вимагачів, фішингових атак, внутрішніх загроз та несанкціонованого доступу, забезпечуючи безперебійну роботу бізнесу. CYTAS також пропонує індивідуальні стратегії безпеки для підприємств, малого та середнього бізнесу та спеціалізованих секторів, що робить захист їхньої мережі масштабованим та адаптованим до потреб кожної компанії.

Ключові характеристики рішень мережевої безпеки CYTAS:

- Комплексний моніторинг мережі та виявлення загроз.
- Розширені технології брандмауера та запобігання вторгненням.
- Захист кінцевих точок та управління вразливостями.
- Інтеграція хмарних та гібридних мережевих систем безпеки.
- Експертні консультації з безпеки та реагування на інциденти.

Впроваджуючи послуги мережевої безпеки CYTAS, компанії отримують цілісну систему захисту, яка поєднує технології, досвід та постійний моніторинг, щоб залишатися стійкими до кіберзагроз, що постійно змінюються.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

Брандмауери наступного покоління (NGFW)

Хоча CYTAS надає повний пакет безпеки, компанії також покладаються на брандмауери нового покоління для створення безпечного мережевого периметра. На відміну від традиційних брандмауерів, брандмауери нового покоління пропонують обізнаність на рівні додатків, запобігання вторгненням та перевірку зашифрованого трафіку, забезпечуючи комплексний захист від складних загроз.

Основні характеристики NGFW:

- Обізнаність та контроль застосунку.
- Інтегрована система запобігання вторгненням (IPS).
- Розширений захист від шкідливих програм та програм-вимагачів.
- Глибока перевірка пакетів зашифрованого трафіку.
- Інтеграція аналітики загроз.

NGFW гарантують, що лише легітимний трафік досягає критично важливих систем, захищаючи конфіденційні дані та покращуючи загальний стан безпеки мережі.

Системи виявлення та запобігання вторгненням (IDPS)

Системи виявлення та запобігання вторгненням (IDPS) є важливими для виявлення та зупинки спроб несанкціонованого доступу та зловмисної діяльності в мережі. У той час як брандмауери блокують зовнішні загрози, IDPS відстежує внутрішній трафік на предмет підозрілої поведінки та потенційних порушень у режимі реального часу. Цей дворівневий підхід гарантує нейтралізацію загроз до того, як вони зможуть поставити під загрозу чутливі системи.

Основні характеристики IDPS:

- Виявлення загроз та оповіщення в режимі реального часу.
- Автоматизоване реагування для запобігання порушенням.
- Виявлення на основі поведінки та сигнатур.
- Комплексний журнал реєстрації та звітності.
- Інтеграція з SIEM-системами (системами управління інформацією та

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

подіями безпеки).

IDPS допомагає компаніям залишатися проактивними, виявляти та запобігати потенційним атакам, що є критично важливим для захисту конфіденційних даних, дотримання нормативних вимог та забезпечення загальної цілісності мережі.

Віртуальні приватні мережі (VPN)

Віртуальна приватна мережа (VPN) шифрує інтернет-трафік між пристроєм та мережею, забезпечуючи безпечний віддалений доступ. Зі зростанням популярності віддаленої роботи та хмарних операцій VPN стали важливим компонентом стратегії мережевої безпеки компанії.

Основні характеристики VPN:

- Наскрізне шифрування для безпечного зв'язку.
- Анонімний перегляд та захист від перехоплення.
- Віддалений доступ для співробітників та партнерів.
- Підтримка кількох пристроїв та платформ.
- Відповідність нормативним стандартам, таким як HIPAA або GDPR.

VPN дозволяють компаніям зберігати конфіденційність даних та операційну безпеку, навіть коли співробітники працюють поза традиційним офісним середовищем.

Рішення для безпеки кінцевих точок

Кінцеві точки, включаючи ноутбуки, мобільні пристрої та сервери, часто є найслабшою ланкою в мережевій безпеці. Рішення для безпеки кінцевих точок забезпечують захист на рівні пристрою, запобігаючи шкідливим програмам, програмам-вимагачам та несанкціонованому доступу до мережі.

Основні характеристики захисту кінцевих точок:

- Захист від шкідливих програм та антивірус.
- Контроль пристроїв та шифрування.
- Поведінкова аналітика для виявлення аномалій.
- Централізоване управління для великих мереж.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

- Інтеграція з інструментами моніторингу мережі.

Забезпечуючи безпеку кінцевих точок, компанії знижують ризик порушень, спричинених людською помилкою, втратою пристроїв або компрометацією облікових даних, посилюючи загальну стратегію захисту.

Безпечні шлюзи електронної пошти

Електронна пошта залишається найпоширенішим вектором атаки для кіберзлочинців. Безпечні шлюзи електронної пошти (SEG) запобігають потраплянню фішингу, спаму та шкідливого програмного забезпечення до поштових скриньок співробітників, захищаючи мережу від компрометації.

Основні характеристики безпечних шлюзів електронної пошти:

- Виявлення та фільтрація загроз у режимі реального часу.
- Розширений захист від фішингу та спуфінгу.
- Можливості запобігання втраті даних (DLP).
- Блокування спаму та шкідливого програмного забезпечення.
- Детальні журнали активності електронної пошти та звіти.

Групи підтримки клієнтів (SEG) є важливими для будь-якої організації, яка значною мірою залежить від електронного спілкування, забезпечуючи як безпеку даних, так і дотримання нормативних стандартів.

Рішення для хмарної безпеки

Зі стрімким впровадженням хмарних технологій, організації повинні захищати програми, дані та інфраструктуру, розміщені в хмарних середовищах. Рішення для хмарної безпеки забезпечують видимість, контроль та захист у публічних, приватних та гібридних хмарах.

Ключові характеристики хмарних рішень для безпеки:

- Безперервний моніторинг хмарних робочих навантажень.
- Керування ідентифікацією та доступом (IAM).
- Шифрування даних у стані спокою та під час передачі.
- Розвідка загроз та виявлення аномалій.
- Звітність про відповідність галузевим стандартам.

Хмарна безпека гарантує, що бізнес може використовувати масштабованість та гнучкість хмарних обчислень, дотримуючись при цьому суворих стандартів безпеки та захищаючи конфіденційні дані.

Створення стійкої системи мережевої безпеки у 2026 році

У сучасному цифровому середовищі бізнес стикається з безпрецедентними кіберзагрозами, починаючи від складного шкідливого програмного забезпечення та програм-вимагачів і закінчуючи внутрішніми загрозами та фішинговими атаками. Впровадження комплексної стратегії мережевої безпеки більше не є необов'язковим, воно має вирішальне значення для безперервності бізнесу, дотримання нормативних вимог та захисту конфіденційних даних.

7 найкращих рішень для мережевої безпеки, починаючи з CYTAS, провідного постачальника передових послуг кібербезпеки, пропонують організаціям інструменти, досвід та захист, необхідні для захисту від загроз, що постійно змінюються. Від брандмауерів наступного покоління до хмарних рішень безпеки, кожен рівень відіграє ключову роль у підтримці цілісності вашої мережі.

Організації повинні застосовувати багаторівневий підхід, поєднуючи технології, політики та обізнаність співробітників. Інвестуючи в безпеку кінцевих точок, системи запобігання вторгненням, VPN, безпечні шлюзи електронної пошти та хмарну безпеку, компанії створюють стійку інфраструктуру, здатну протистояти як внутрішнім, так і зовнішнім атакам.

Більше того, партнерство з перевіреною фірмою з кібербезпеки, такою як CYTAS, гарантує, що компанії не лише отримають доступ до передових технологій безпеки, але й отримають переваги від експертних порад, індивідуальних рішень та проактивного моніторингу. Такий стратегічний підхід мінімізує вразливості, захищає конфіденційну інформацію та дає компаніям змогу впевнено працювати у все більш взаємопов'язаному світі.

У 2026 році компанії, які надають пріоритет комплексній безпеці мережі, отримають конкурентну перевагу, захистять свою репутацію та збережуть довіру

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

з клієнтами, партнерами та співробітниками. Безпека – це не одноразове зусилля; це постійне зобов'язання, яке розвивається разом із технологіями, ландшафтом загроз та потребами бізнесу.

3.2 Розробка структурної схеми

Кожна сучасна організація покладається на цифрові мережі для ефективної роботи. Від хмарних платформ і внутрішніх баз даних до пристроїв співробітників і віддалених з'єднань, мережі зараз є основою бізнес-операцій. Однак та сама зв'язок, яка підвищує продуктивність, також створює серйозні ризики для безпеки. Кіберзагрози розвиваються з безпрецедентною швидкістю, і зловмисники постійно шукають слабкі місця в мережах, щоб викрасти дані, порушити роботу систем або отримати несанкціонований доступ.

Таким чином, мережева безпека стала одним із найважливіших елементів кіберстійкості. Підприємства повинні забезпечити захист своїх мереж як від зовнішніх атак, так і від внутрішніх вразливостей. Одне порушення може призвести до фінансових втрат, шкоди репутації, юридичних наслідків та збоїв у роботі. Оскільки цифрова трансформація продовжує поширюватися в усіх галузях, потреба в надійному захисті мережі зростає з кожним роком.

У даному розділі досліджується роль мережевої безпеки в сучасному бізнесі, пояснюючи, як організації можуть створювати стійкі мережеві засоби захисту, розуміти нові кіберзагрози та впроваджувати ефективні стратегії захисту. Мета полягає в тому, щоб надати чітке та практичне розуміння, яке допоможе особам, що приймають рішення, зрозуміти, як надійна мережева безпека сприяє довгостроковій операційній стабільності.

Розуміння мережевої безпеки в цифрову епоху

Мережева безпека стосується технологій, процесів і політик, розроблених для захисту мереж від несанкціонованого доступу, неправильного використання або збоїв. Вона включає широкий спектр захисних механізмів, таких як

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

брандмауери, шифрування, системи виявлення вторгнень, управління ідентифікацією та моніторинг мережі. Основна мета полягає в тому, щоб забезпечити доступ до мережевих ресурсів лише авторизованим користувачам і пристроям, одночасно запобігаючи використанню вразливостей зловмисниками.

У сучасному цифровому середовищі мережі більше не обмежуються офісною інфраструктурою. Бізнес працює в гібридних середовищах, що включають хмарні платформи, системи віддаленої роботи, мобільні пристрої та інтеграції зі сторонніми розробниками. Ця розширена екосистема збільшила складність захисту мереж організації. Прогалина в безпеці будь-якого підключеного компонента може наразити всю систему на кіберзагрози.

Ефективні служби кібербезпеки повинні використовувати стратегічний підхід. Їхня методологія починається з оцінки вразливостей у цифровій інфраструктурі організації, а потім розробки заходів безпеки, що зміцнюють загальну стійкість. Аналізуючи потенційні ризики та впроваджуючи захисні заходи на ранній стадії, підприємства можуть значно зменшити свій вплив кіберзагроз.

Розуміння постійно мінливої природи кіберзагроз є важливою частиною сучасної мережевої безпеки. Зловмисники часто використовують неправильно налаштовані системи, застаріле програмне забезпечення, слабкі методи автентифікації та людські помилки. До поширених загроз належать зараження шкідливим програмним забезпеченням, атаки програм-вимагачів, фішингові кампанії, внутрішні загрози та розподілені атаки типу «відмова в обслуговуванні». Ці атаки можуть проникати в мережі, красти конфіденційні дані або порушувати бізнес-операції.

Тому сучасна мережева безпека зосереджена на постійному моніторингу та виявленні загроз. Команди безпеки аналізують мережеву активність у режимі реального часу, щоб виявити незвичайні закономірності, які можуть свідчити про атаку. Коли виявляється підозріла поведінка, запускаються механізми швидкого реагування, щоб стримати загрозу та мінімізувати збитки.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

Ще одним важливим елементом захисту мережі є дотримання нормативних актів та законів про захист даних. Багато галузей повинні дотримуватися суворих правил щодо конфіденційності даних та інформаційної безпеки. Надійна стратегія безпеки мережі допомагає організаціям підтримувати відповідність вимогам, а також захищати довіру клієнтів.

Чому надійна мережева безпека є важливою для бізнесу

Надійна мережева безпека – це не просто технічна вимога, а фундаментальний компонент безперервності бізнесу. Організації значною мірою залежать від цифрового зв'язку та обміну даними, що робить їх привабливими мішенями для кіберзлочинців. Без належних заходів безпеки зловмисники можуть отримати доступ до конфіденційної інформації, порушити роботу послуг або маніпулювати системами для отримання фінансової вигоди.

Одна з головних причин важливості мережевої безпеки – це захист конфіденційних даних. Підприємства зберігають великі обсяги конфіденційної інформації, включаючи записи клієнтів, фінансові дані, інтелектуальну власність та операційну інформацію. Якщо ці дані будуть скомпрометовані, наслідки можуть бути серйозними. Витік даних часто призводить до юридичних санкцій, регуляторних розслідувань та втрати довіри клієнтів.

Ще одним важливим фактором є операційна надійність. Мережі підтримують критично важливі бізнес-процеси, такі як комунікація, хмарні сервіси, платіжні системи та інструменти для внутрішньої співпраці. Коли кібератаки порушують роботу цих мереж, операції можуть зупинитися. Добре захищена мережа гарантує, що системи залишатимуться доступними та функціональними навіть за виникнення загроз.

Проактивний моніторинг загроз та оцінка вразливостей є важливими для підтримки безпеки мереж. Їхні консалтингові послуги з кібербезпеки зосереджені на виявленні слабких місць та зміцненні систем, перш ніж зловмисники зможуть їх використати. Такий проактивний підхід дозволяє організаціям підтримувати стійкість у постійно мінливому середовищі загроз.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

Мережева безпека також відіграє ключову роль у захисті репутації організації. В епоху цифрових технологій новини про кібератаку швидко поширюються та можуть значно зашкодити довірі до бренду. Клієнти очікують, що компанії захищатимуть їхні персональні дані та цифрову взаємодію. Демонстрація твердої відданості безпеці допомагає зміцнити довіру та впевненість між клієнтами та партнерами.

Фінансовий захист – це ще один важливий фактор. Кібератаки можуть спричинити прямі фінансові втрати через шахрайство, виплату викупу та витрати на відновлення системи. Крім того, компанії можуть зіткнутися з непрямыми збитками через простої в роботі та втрату клієнтів. Тому інвестування в надійну мережеву безпеку є стратегічним рішенням, яке захищає як фінансову стабільність, так і довгострокове зростання.

Основні компоненти безпечної мережевої інфраструктури

Побудова безпечної мережі вимагає багаторівневого підходу, який поєднує різні технології та методи безпеки. Кожен рівень усуває різні вразливості та гарантує, що зловмисники стикаються з кількома перешкодами під час спроби проникнення в систему.

Брандмауери є одним із найважливіших компонентів мережевої безпеки. Вони контролюють вхідний та вихідний мережевий трафік і забезпечують дотримання заздалегідь визначених правил безпеки. Фільтруючи трафік на основі цих правил, брандмауери запобігають несанкціонованому доступу та блокують підозрілу активність. Сучасні брандмауери також мають розширені можливості, такі як глибока перевірка пакетів та фільтрація на рівні програм.

Шифрування – ще один важливий захід безпеки. Воно захищає дані, перетворюючи їх у нечитабельний формат, який можуть розшифрувати лише уповноважені сторони. Шифрування гарантує, що навіть якщо зловмисники перехоплять дані під час передачі, вони не зможуть отримати доступ до їхнього вмісту без правильних ключів шифрування. CyberMount пропонує послуги

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		39

шифрування, призначені для захисту конфіденційної інформації та забезпечення конфіденційності в цифровому зв'язку.

Віртуальні приватні мережі також відіграють важливу роль у безпечному мережевому зв'язку. VPN створює зашифрований тунель між користувачами та мережею, захищаючи дані під час їх передавання через Інтернет. Це особливо важливо для віддалених працівників, які отримують доступ до ресурсів компанії із зовнішніх мереж. Шифруючи з'єднання, VPN запобігають перехопленню конфіденційної інформації зловмисниками.

Керування ідентифікацією та доступом – ще один важливий компонент мережевої безпеки. Ця система гарантує, що користувачі мають доступ лише до ресурсів, необхідних для їхніх ролей. Такі методи, як багатофакторна автентифікація, додають додаткові рівні перевірки, що значно ускладнює зловмисникам компрометацію облікових записів. Навіть якщо пароль викрадено, додаткові кроки перевірки запобігають несанкціонованому доступу.

Технології постійного моніторингу та виявлення загроз також сприяють безпеці мережевої інфраструктури. Системи управління інформацією про безпеку та подіями аналізують мережеві журнали та виявляють підозрілу поведінку. Коли виявляються аномалії, команди безпеки можуть швидко реагувати, щоб стримувати потенційні загрози до їх ескалації.

Зрештою, обізнаність співробітників щодо безпеки є часто недооціненим, але важливим елементом захисту мережі. Людська помилка залишається основною причиною кіберінцидентів. Навчальні програми, що навчають персонал фішингу, соціальній інженерії та безпечним практикам, можуть значно зменшити ризик порушень, спричинених помилками або маніпуляціями.

Роль безперервного моніторингу та реагування на інциденти

Кіберзагрози не дотримуються передбачуваного графіка. Зловмисники постійно досліджують мережі в пошуках вразливостей, і навіть добре захищені системи можуть зазнати спроб вторгнення. Ця реальність робить постійний

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

моніторинг та швидке реагування на інциденти важливими компонентами мережевої безпеки.

Безперервний моніторинг включає аналіз мережевого трафіку, системних журналів та поведінки користувачів для виявлення незвичайної активності. Служби безпеки використовують передові аналітичні інструменти та автоматизовані системи для виявлення закономірностей, які можуть свідчити про кібератаку. Ці системи можуть виявляти аномалії, такі як неочікувані передачі даних, незвичайні спроби входу або підозріла активність пристроїв.

Важливий моніторинг в режимі реального часу як частина комплексної стратегії безпеки. Їхні керовані служби безпеки забезпечують цілодобовий спостереження за IT-інфраструктурою, що дозволяє організаціям швидко виявляти загрози та реагувати на них. Безперервний моніторинг дозволяє вирішувати потенційні ризики до того, як вони переростуть у серйозні інциденти.

Стратегії виявлення та реагування на інциденти розроблені для стримування та нейтралізації кіберзагроз після їх виявлення. Ці стратегії включають процедури аналізу інцидентів, ізоляції уражених систем та відновлення нормальної роботи. Мета полягає в мінімізації збитків та забезпеченні продовження бізнес-діяльності з мінімальними перебоями.

Ефективний план реагування на інциденти також включає протоколи зв'язку та процедури відновлення. Організації повинні бути готові інформувати зацікавлені сторони, розслідувати першопричину інцидентів та вживати коригувальних заходів для запобігання подібним подіям у майбутньому.

Стратегії реагування на інциденти часто включають передові технології, такі як автоматизований аналіз загроз та моніторинг на основі штучного інтелекту. Ці інструменти можуть обробляти великі обсяги мережевих даних та виявляти потенційні загрози швидше, ніж лише ручний аналіз.

Регулярне тестування планів реагування на інциденти також є важливим. Симуляційні вправи дозволяють організаціям оцінювати свою готовність та

вдосконалювати процедури реагування. Відпрацьовуючи сценарії реагування, команди можуть реагувати ефективніше під час реальних інцидентів.

Нові тенденції в мережевій безпеці та захисті від загроз

Ландшафт кібербезпеки постійно змінюється під впливом нових технологій та дедалі складніших кібератак. Підприємства повинні адаптувати свої стратегії мережевої безпеки для реагування на нові загрози та технологічні розробки.

Однією з важливих тенденцій є впровадження моделей безпеки Zero Trust. Традиційні підходи до безпеки часто спираються на захист периметра, який припускає, що користувачі внутрішньої мережі є надійними. Однак сучасні загрози часто виникають через скомпрометовані внутрішні облікові записи або пристрої. Архітектура Zero Trust усуває це припущення та вимагає постійної перевірки всіх користувачів і пристроїв перед наданням доступу. Такий підхід значно знижує ризик несанкціонованої діяльності в мережі.

Хмарні обчислення також трансформували методи мережевої безпеки. Багато організацій тепер зберігають дані та запускають програми на хмарних платформах, а не на локальній інфраструктурі. Хоча хмарні середовища пропонують гнучкість та масштабованість, вони також створюють нові проблеми безпеки. Захист хмарних робочих навантажень вимагає спеціалізованого моніторингу, управління конфігурацією та стратегій відповідності, щоб забезпечити безпеку даних.

Штучний інтелект та машинне навчання все частіше використовуються для посилення систем кіберзахисту. Ці технології аналізують мережеву активність та виявляють закономірності, які можуть свідчити про зловмисну поведінку. Автоматизуючи процеси виявлення та реагування на загрози, системи безпеки на основі штучного інтелекту можуть реагувати швидше, ніж традиційні підходи.

Ще однією тенденцією, що розвивається, є інтеграція безпеки в усі цифрові системи. Замість того, щоб розглядати безпеку як окрему функцію,

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

організації впроваджують практики безпеки в усю свою технологічну інфраструктуру. Такий підхід гарантує, що міркування безпеки враховуються під час проектування системи, розробки програмного забезпечення та операційних процесів.

Дотримання нормативних вимог також формує майбутнє мережевої безпеки. Уряди та регуляторні органи запроваджують суворіші вимоги щодо захисту даних та кіберстійкості. Тому організації повинні забезпечити відповідність своїх стратегій безпеки нормативно-правовим базам, що постійно змінюються.

Розробка довгострокової стратегії мережевої безпеки

Розробка надійної стратегії мережевої безпеки вимагає ретельного планування та постійного вдосконалення. Кіберзагрози швидко розвиваються, і заходи безпеки повинні адаптуватися відповідно. Організації повинні почати з проведення комплексних оцінок ризиків, які виявляють вразливості та потенційні вектори атак у їхній інфраструктурі.

Рекомендуємо почати з детального аудиту кібербезпеки, щоб оцінити поточні заходи безпеки та виявити слабкі місця. Ці оцінки надають цінну інформацію про те, як можна зміцнити мережі та які області потребують негайної уваги.

Успішна стратегія також передбачає впровадження багаторівневих заходів безпеки, які захищають мережі з різних боків. Поєднання таких технологій, як брандмауери, шифрування, управління ідентифікацією та інструменти моніторингу, створює надійну систему захисту, яку зловмисникам важко обійти.

Навчання співробітників є ще одним важливим компонентом довгострокової безпеки. Навчальні програми допомагають співробітникам розпізнавати кіберзагрози та застосовувати безпечні цифрові практики. Коли співробітники розуміють, як відбуваються кібератаки, вони стають активною частиною оборонної стратегії організації.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

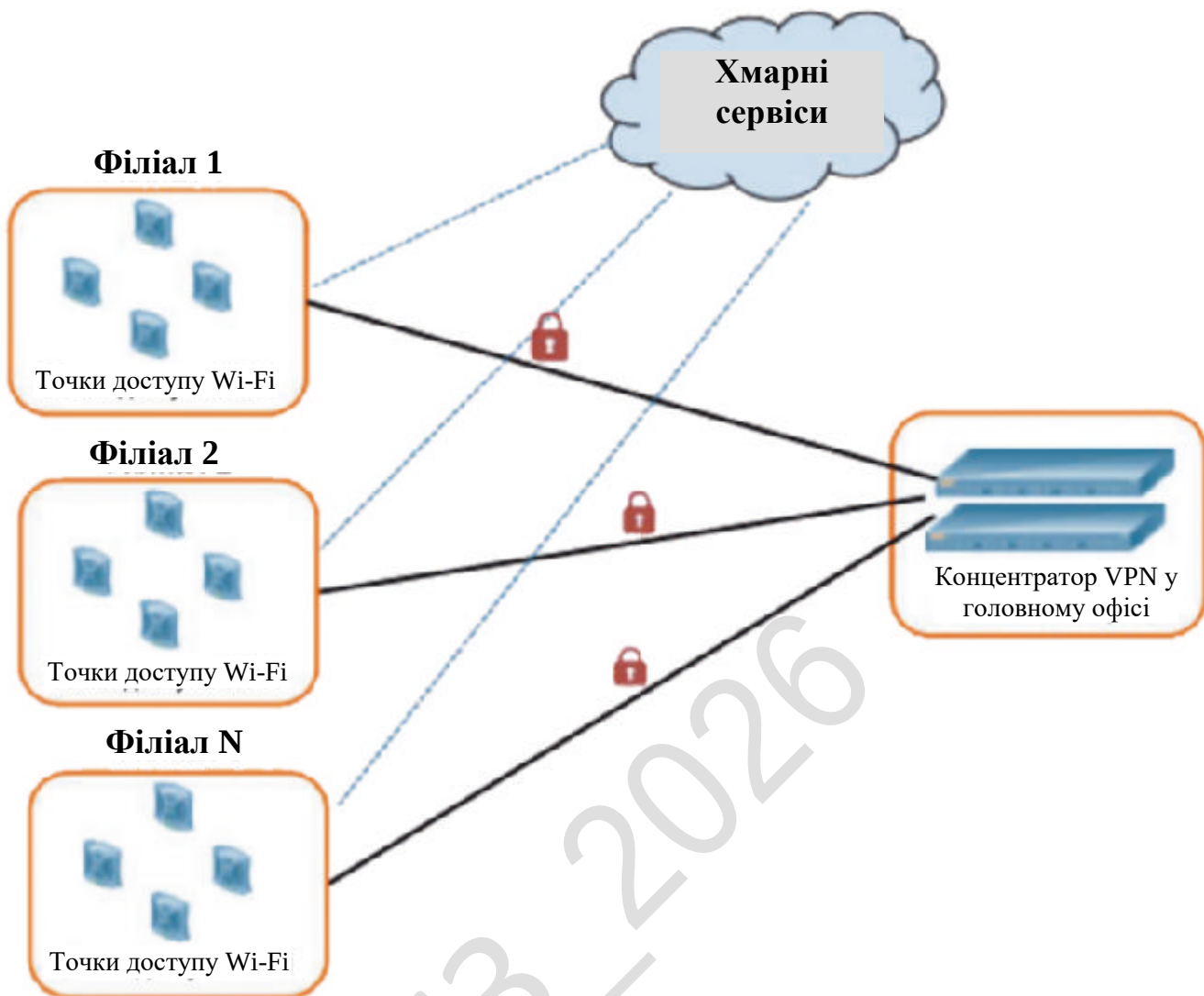


Рисунок 3.1 – Структурна схема системи

Організації також повинні встановити чіткі політики безпеки та структури управління. Ці політики визначають прийнятне використання технологій, вимоги до захисту даних та процедури реагування на інциденти безпеки. Чітко визначені політики гарантують, що всі співробітники дотримуються послідовних практик безпеки.

Регулярні аудити безпеки та оновлення необхідні для підтримки надійного захисту. Технології швидко розвиваються, і застарілі системи можуть містити вразливості, якими можуть скористатися зловмисники. Оновлення програмного

забезпечення, встановлення патчів для систем та перегляд конфігурацій безпеки допомагають забезпечити захист мереж.

Співпраця з досвідченими фахівцями з кібербезпеки також може посилити стратегії безпеки. Експерти-консультанти надають цінну інформацію про нові загрози та передовий досвід, допомагаючи організаціям випереджати кіберризики.

Висновок

Мережева безпека стала одним із найважливіших пріоритетів для сучасних організацій. Оскільки бізнес дедалі більше покладається на цифрову інфраструктуру, ризики, пов'язані з кіберзагрозами, продовжують зростати. Захист мереж вимагає комплексного підходу, який поєднує передові технології, стратегічне планування, постійний моніторинг та обізнаність співробітників.

Надійна мережева безпека гарантує захист конфіденційних даних, безперебійну роботу бізнес-операцій та збереження довіри організацій до своїх клієнтів і партнерів. Завдяки впровадженню багаторівневих заходів безпеки, застосуванню проактивних методів моніторингу та постійному інформуванню про нові загрози, компанії можуть створювати стійкі мережі, здатні протистояти сучасним кібератакам.

3.3 Розробка функціональної схеми

Віртуальна приватна мережа (Virtual Private Network, VPN) – це технологія, що дозволяє створити закриту високошвидкісну приватну мережу поверх мережі Інтернет для забезпечення анонімності й безпеки її користувачів. Використовуючи VPN, можна вийти в Інтернет через сервер, розташований в іншій державі, і одержати доступ до контенту, що заблокований у країні.

Ваше з'єднання захищає зашифрований тунель, тому ваші дані не зможуть перехопити різні шахраї, хакери та інші сторонні особи. Це неперевершений захист для ваших даних у небезпечних цифрових джунглях.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

VPN споконвічно використовувався як безпечний спосіб віддаленого доступу до локальної офісної мережі для співробітників різних великих компаній. VPN відкриває можливість насолодитися перевагами VPN всім бажаною, на будь-якому пристрої.

Як VPN захищає вашу конфіденційність

Звичайно ви підключаєтеся до Мережі через постачальника відповідних послуг – Інтернет-провайдеру. Ваш провайдер підключає вас до будь-якого сайту, що ви хочете відвідати. Весь ваш Інтернет-трафік проходить через сервери провайдеру, а виходить, провайдер може його переглядати.

Коли ви використовуєте VPN, ви підключаєтеся до VPN-сервера через надійно зашифрований тунель. Це значить, що всі дані, якими ви обмінюєтеся із цим VPN-сервером, може розшифрувати тільки цей сервер і ваш комп'ютер.

VPN строго дотримується принципу «Ніяких записів» – ніякі ваші дані не відслідковуються, не збираються й нікому не розкриваються. Навіть ми самі не знаємо, що ви робите в Мережі.

Захистіть свою конфіденційність

Не так багато інформації в Інтернеті дійсно є особистою – ваша онлайн-активність відслідковується урядовими службами, постачальниками рекламних послуг, власниками сайтів і т.п.

Обійдіть гео-блокування

Багато власників авторських прав містять із онлайн-ресурсами ліцензійні угоди, згідно яким їх контент дозволяється демонструвати винятково на певних територіях.

Захистіть свої особисті дані

Кожна ваша дія в Мережі по суті є процесом передачі даних. Завдяки VPN, ви зможете контролювати цей процес і зробити його безпечним.

Заощаджуйте з віртуальною релокацією

Багато сервісів пропонують різні ціни жителям різних країн. Наприклад, ваше місцезнаходження може серйозно вплинути на ціну квитка на літак.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46



Рисунок 3.2 – Функціональна схема системи

У такий спосіб на підставі всього вищенаведеного в даній роботі була розроблена функціональна схема, що складається з наступних блоків:

1. Блок системних параметрів:

- Алгоритм шифрування, використовуваний в VPN.
- Спосіб зберігання й уведення ідентифікатора суб'єкта і його ключа шифрування взаємодії із сервером VPN.

- Параметри взаємодії з основним і резервним серверами VPN.

2. Блок функціональних параметрів:

- Доступ до будь-якому контенту.
- Приховує ваше місце розташування (IP-адресу).
- Приховує вашу особистість від шахраїв.
- Працює із браузерами (Chrome, Firefox).
- Працює з різними пристроями (смартфони, планшети, консолі).
- Працює з іграми й застосунками.
- Шифрує вашу діяльність, захищає від хакерів.
- Захищає вас від шкідливих програм і фішингових тактик.
- Постійно міняє віртуальне місце розташування (IP-адресу).
- Високошвидкісний серфінг і перегляд потокового контенту.

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.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		48

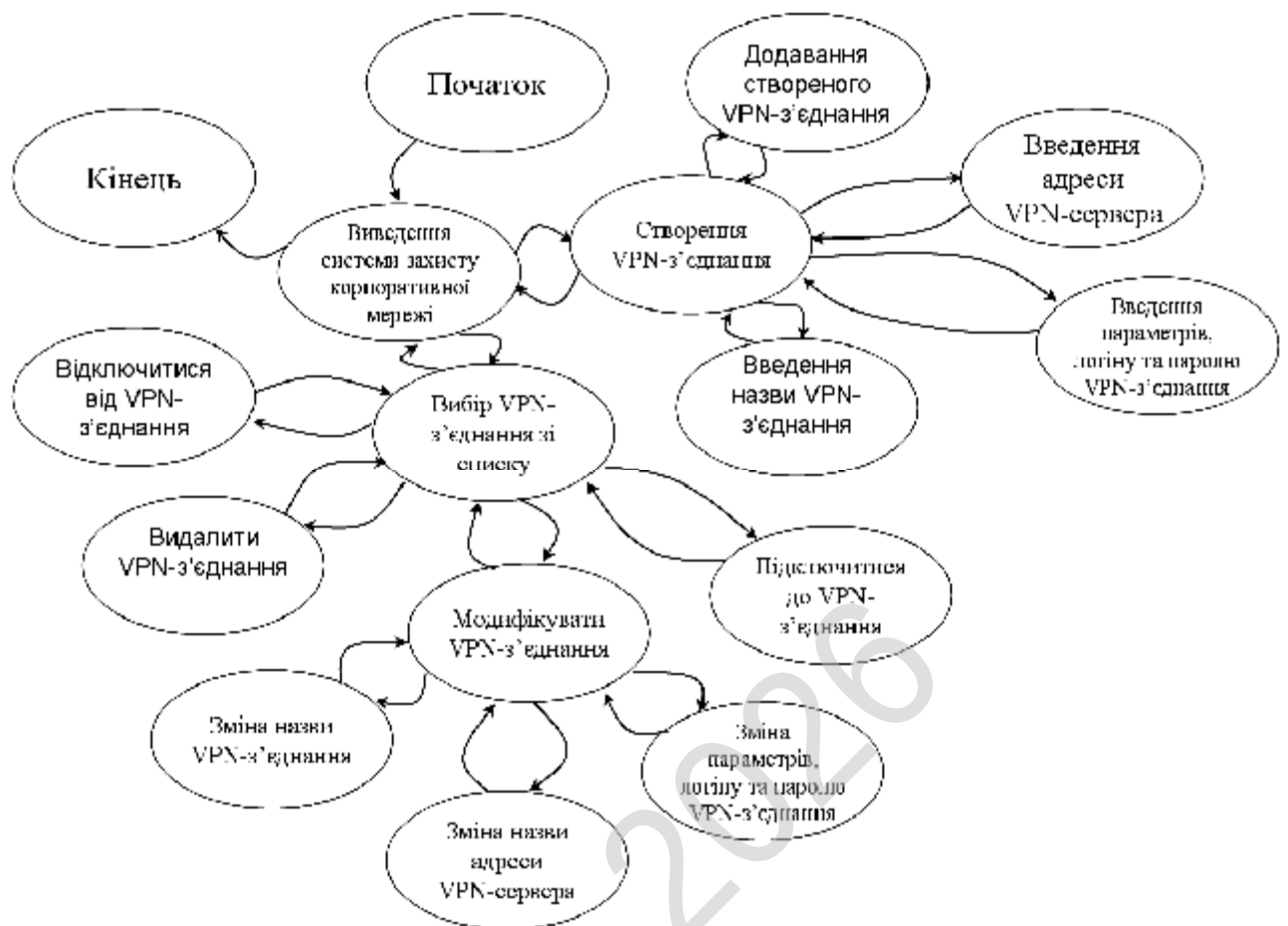


Рисунок 3.3 – Діаграма взаємодії процесів

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).

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

Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень.

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.

Система керування базами даних (СКБД, Database Management System, DBMS) – набір взаємопов'язаних даних (база даних) і програм для доступу до цих даних. Надає можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

Першим поколінням СКБД прийнято вважати ієрархічні й мережеві системи. Ці системи отримали широке поширення в 1970-х роках, а першою комерційною системою цього типу була система IMS компанії IBM.

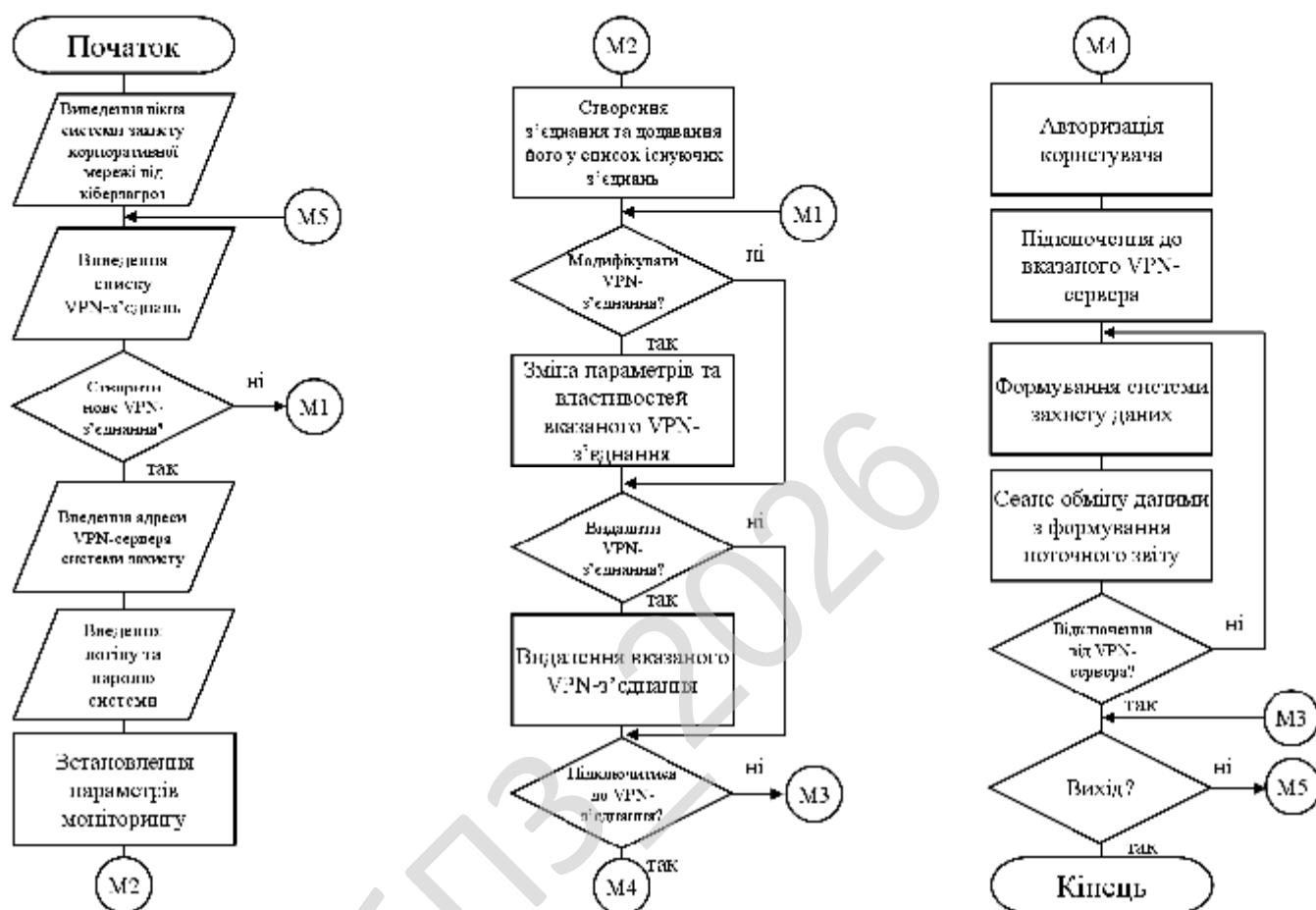


Рисунок 4.1 – Блок-схема основної програми

У 1980-х роках ці системи були витіснені системами другого покоління – повсюдно використовуваними і донині реляційними СКБД. У цих системах використовувалися непроцедурні мови управління даними (SQL) і передбачався значний ступінь незалежності даних. Реляційні системи внесли значні удосконалення в управління даними: графічний користувацький інтерфейс (GUI), клієнт-серверні застосунки, розподілені бази даних, паралельний пошук даних та інтелектуальний аналіз даних.

Але вже до кінця 1980-х років існуюча тоді реляційна модель перестала задовольняти розробників в силу низки обмежень. Відповіддю на зростаючу складність програм баз даних стали два нових напрямки розвитку СКБД: об'єктно-орієнтовані СКБД і об'єктно-реляційні СКБД.

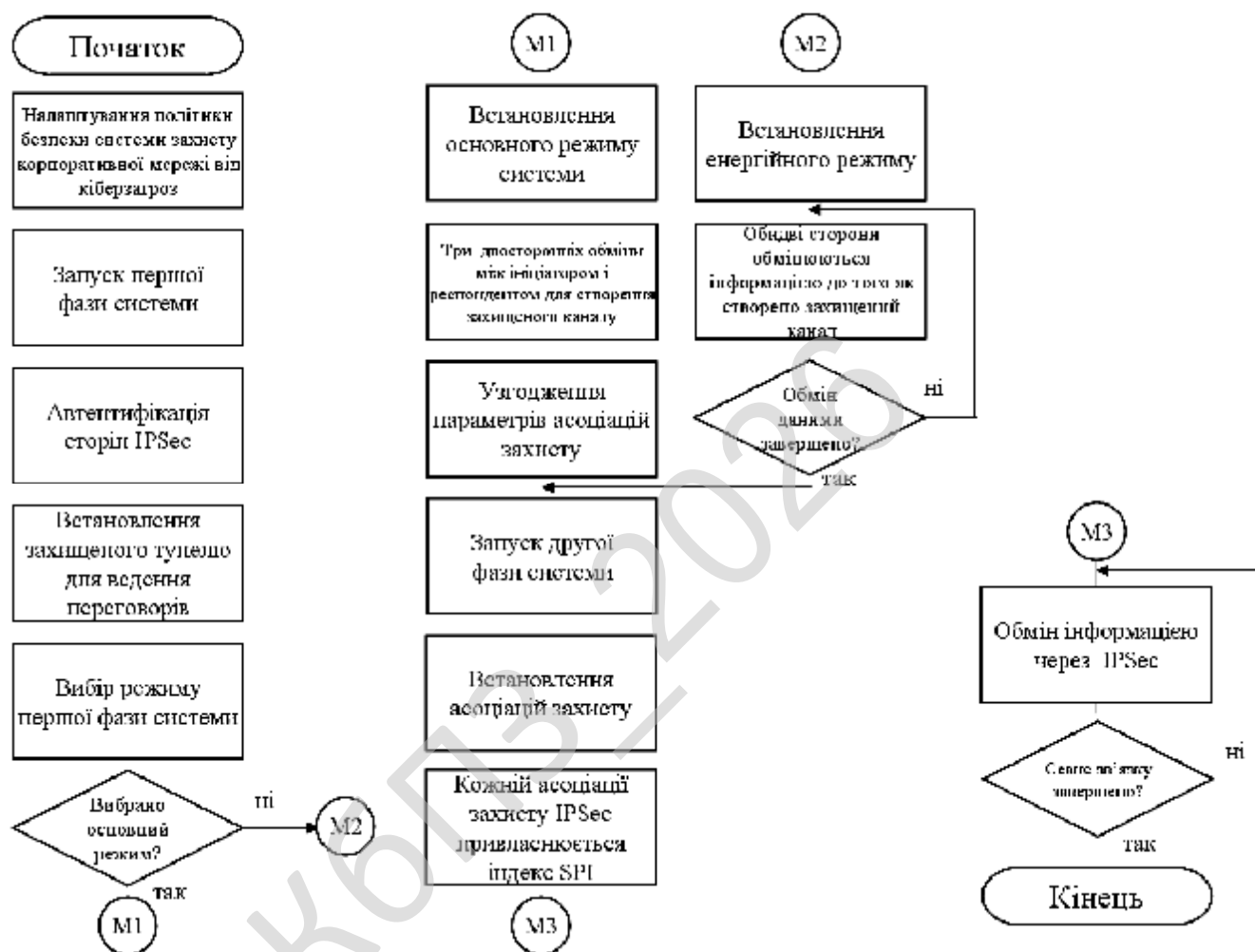


Рисунок 4.2 – Блок-схема роботи підпрограми

У 1991 був утворений консорціум ODMG, основною метою якого стало вироблення промислового стандарту об'єктно-орієнтованих баз даних. Між 1993 та 2001 роками ODMG опублікувала п'ять ревізій своїх специфікацій. Остання версія стандарту має індекс 3.0, після чого група розпустилася. До кінця 1990-х існувало близько десяти компаній, що виробляли комерційні продукти, що позиціонуються на ринку як ООСКБД. Найбільш відомими системами даного

класу стали Objectivity, Versant виробництва однойменних компаній, а також СКБД Jasmine, випущена компанією CA. Незважаючи на переваги, що дозволяють ефективніше вирішувати певний ряд завдань, об'єктно-орієнтовані системи так і не змогли завоювати значущу частку ринку СКБД, залишившись «нішевим» продуктом.

Постачальниками традиційних реляційних СКБД також була проведена значна робота з об'єднання об'єктно-орієнтованих і реляційних систем. Розробники постаралися розширити мову SQL, щоб включити в неї концепції об'єктно-орієнтованого підходу, зберігаючи переваги реляційної моделі (об'єктні розширення мови SQL були зафіксовані в стандарті SQL:1999).

Основний принцип – це еволюційний розвиток можливостей СКБД без поломки попередніх підходів та зі збереженням наступності з системами попереднього покоління.

Поняття СКБД третього покоління, якими, власне кажучи, і є об'єктно-реляційні СКБД, з'явилося після опублікування групою відомих фахівців в області баз даних «Маніфесту систем баз даних третього покоління». Основні принципи СКБД третього покоління, позначені в маніфесті:

Крім традиційних послуг з управління даними, СКБД третього покоління повинні забезпечити підтримку розвиненіших структур об'єктів і правил. Розвинутіша структура об'єктів характеризує засоби, необхідні для зберігання і маніпулювання нетрадиційними елементами даних (тексти, просторові дані, мультимедіа).

СКБД третього покоління повинні включити в себе СКБД другого покоління. Системи другого покоління внесли вирішальний вклад у двох областях – непроцедурний доступ за допомогою мови запитів SQL і незалежність даних. Ці досягнення обов'язково повинні враховуватися в системах третього покоління.

СКБД третього покоління повинні бути відкриті для інших підсистем. Це включає оснащення різноманітними інструментами підтримки прийняття рішень,

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

доступом з багатьох мов програмування, інтерфейсами до існуючих популярних систем і бізнес-застосунків, можливістю запуску програм з бази даних на іншій машині і розподілені СКБД. Весь набір інструментів і СКБД має ефективно функціонувати на різноманітних апаратних платформах з різними операційними системами.

Крім того, СКБД, що розраховує на широку сферу застосування, повинна бути оснащена мовою четвертого покоління (4GL).

У середині 1990 років було лише кілька дослідних прототипів СКБД, які поєднали найкращі риси реляційних і об'єктно-орієнтованих СКБД. Першим комерційним продуктом, якому були властиві об'єктно-реляційні риси, став Universal Server компанії Informix(згодом була поглинена IBM). В даний час більшість цих ідей вже втілено в реальних комерційних рішеннях, в тому числі і в продуктах основних постачальників СКБД (Oracle Database і IBM DB2).

Розвиток індустрії систем керування базами даних базується на значних фундаментальних наукових дослідженнях. Найчастіше, між самими дослідженнями та їхньою конкретною реалізацією в прикладних рішеннях минають роки, а іноді й десятиліття. Роботу в області управління даними проводять як університетські дослідницькі групи (MIT, Berkeley), так і центри розробок основних постачальників СКБД (Oracle, IBM, Microsoft). Інвестування в управління даними – це довгострокове, і разом з тим, вигідне вкладення коштів. В даний час дослідники мають у своєму розпорядженні засоби, що дозволяють ефективно реалізувати найскладніші запити, що маніпулюють терабайтами й петабайтами різних даних.

Основними тенденціями, які дали привід для проведення різних масштабних досліджень в області баз даних стали:

Експонентний ріст даних. Обсяг даних, у тому числі синтетичних, що генеруються автоматизованими системами, значно зріс. Збільшилося і число прикладних областей, в яких вимагається обробка великих обсягів даних. До таких областей тепер відносяться не тільки традиційні корпоративні програми,

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

пошук у веб, але також і наукові дослідження, обробка природних мов, аналіз соціальних мереж тощо.

Значне ускладнення структур використовуваних даних. Прості види даних у вигляді чисел і символьних рядків стали доповнятися численною мультимедійною інформацією, просторовими, процедурними даними та великою кількістю інших складних форматів.

Широке поширення дешевих високопродуктивних апаратних засобів. Щорічно ми спостерігаємо зростання обчислювальних можливостей мікропроцесорів, збільшення ємності і зниження вартості доступних і зручних в експлуатації пристроїв дискової оперативної пам'яті.

Активний розвиток засобів комунікації та «всесвітньої павутини» World Wide Web. WWW стає єдиним інформаційним середовищем, що пронизує весь світ і об'єднує величезне число користувачів та електронних пристроїв.

Поява нових важливих областей застосування СКБД. У першу чергу, це пов'язано з інтелектуальним аналізом даних, сховищами даних, а останнім часом – з паралельними обчисленнями і хмарними технологіями.

Основні характеристики СКБД

1. Контроль за надлишковістю даних.
2. Несуперечливість даних.
3. Підтримка цілісності бази даних (коректність та несуперечливість).
4. Цілісність описується за допомогою обмежень.
5. Незалежність прикладних програм від даних.
6. Спільне використання даних.
7. Підвищений рівень безпеки.

Можливості СКБД

1. Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language)).

2. Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)

3. Можна надавати контрольований доступ до БД за допомогою: Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД; Системи керування паралельною роботою прикладних програм, яка контролює процеси спільного доступу до БД; Система відновлення – дозволяє відновлювати БД до попереднього несуперечливого стану, що був порушений в результаті збою апаратного або програмного забезпечення.

Основні компоненти середовища СКБД

1. Апаратне забезпечення.
2. Програмне забезпечення.
3. Дані.
4. Процедури – інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.
5. Користувачі: адміністратори даних (керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних); розробники БД; прикладні програмісти; кінцеві користувачі.

Архітектура СКБД

Існує трирівнева система організації СКБД ANSI-SPARC, при якій існує незалежний рівень для ізоляції програми від особливостей представлення даних на нижчому рівні.

Рівні:

1. Зовнішній – представлення БД з точки зору користувача.
2. Концептуальний – узагальнене представлення БД, описує які дані зберігаються в БД і зв'язки між ними. Підтримує зовнішні представлення, підтримується внутрішнім рівнем.
3. Внутрішній – фізичне представлення БД в комп'ютері.

Логічна незалежність – повна захищеність зовнішніх моделей від змін, що вносяться в концептуальну модель.

Фізична незалежність – захищеність концептуальної моделі від змін, які вносяться у внутрішню модель.

SQLite – полегшена реляційна система керування базами даних. Втілена у вигляді бібліотеки, де реалізовано багато зі стандарту SQL-92.

Сирцевий код SQLite поширюється як суспільне надбання (public domain), тобто може використовуватися без обмежень та безоплатно з будь-якою метою. Фінансову підтримку розробників SQLite здійснює спеціально створений консорціум, до якого входять такі компанії, як Adobe, Oracle, Mozilla, Nokia, Bentley і Bloomberg.

З 2018р SQLite, як й JSON та CSV, рекомендований Бібліотекою Конгресу США формат зберігання структурованого набору даних. У 2005 році проект отримав нагороду Google-O'Reilly Open Source Awards.

Особливістю SQLite є те, що вона не використовує парадигму клієнт-сервер, тобто рушій SQLite не є окремим процесом, з яким взаємодіє застосунок, а надає бібліотеку, з якою програма компілюється і рушій стає складовою частиною програми.

Таким чином, як протокол обміну використовуються виклики функцій (API) бібліотеки SQLite. Такий підхід зменшує накладні витрати, час відгуку і спрощує програму.

SQLite зберігає всю базу даних (включаючи визначення, таблиці, індекси і дані) в єдиному стандартному файлі на тому комп'ютері, на якому виконується застосунок.

Простота реалізації досягається за рахунок того, що перед початком виконання транзакції весь файл, що зберігає базу даних, блокується; ACID-функції досягаються зокрема за рахунок створення файлу-журналу.

Кілька процесів або потоків можуть одночасно без жодних проблем читати дані з однієї бази. Запис в базу можна здійснити тільки в тому випадку, коли

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

жодних інших запитів у цей час не обслуговується; інакше спроба запису закінчується невдачею, і в програму повертається код помилки. Іншим варіантом розвитку подій є автоматичне повторення спроб запису протягом заданого інтервалу часу.

У комплекті постачання йде також функціональна клієнтська частина у вигляді виконуваного файлу `sqlite3`, за допомогою якого демонструється реалізація функцій основної бібліотеки. Клієнтська частина працює з командного рядка, і дозволяє звертатися до файлу БД на основі типових функцій ОС.

Завдяки архітектурі рушія можливо використовувати SQLite як на вбудовуваних (embedded) системах, так і на виділених машинах з гігабайтними масивами даних.

Особливості SQLite:

1. Транзакції атомарні, послідовні, ізольовані, і міцні (ACID) навіть після збоїв системи і збоїв живлення.
2. Встановлення без конфігурації – не потребує ані установки, ані адміністрування.
3. Реалізує значну частину стандарту SQL92.
4. База даних зберігається в одному крос-платформовому файлі на диску.
5. Підтримка терабайтних розмірів баз даних і гігабайтного розміру рядків і BLOBів.
6. Малий розмір коду: менше ніж 350KB повністю налаштований, і менш 200KB з опущеними додатковими функціями.
7. Швидший за популярні рушії клієнт-серверних баз даних для найпоширеніших операцій.
8. Простий, легкий у використанні API.
9. Написана в ANSI C, включена прив'язка до TCL; доступні також прив'язки для десятків інших мов.
10. Добре прокоментований сирцевий код зі 100% тестовий покриттям гілок.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

11. Доступний як єдиний файл сирцевого коду на ANSI C, який можна легко вставити в інший проект.

12. Автономність: немає зовнішніх залежностей.

13. Крос-платформовість: з коробки підтримується Unix (Linux і Mac OS X), OS/2, Windows (Win32 і WinCE). Легко переноситься на інші системи.

14. Сирці перебувають в суспільному надбанні.

15. Поставляється з автономним клієнтом інтерфейсу командного рядка, який може бути використаний для управління базами даних SQLite.

Інструменти створення та обслуговування БД

Створення та обслуговування БД можуть здійснюватись через текстову консоль SQL-командами або через спеціальні інструменти, у тому числі – з графічним інтерфейсом користувача.

Технології, що підтримують SQLite та мови програмування

Сама бібліотека SQLite написана мовою C. Проте є реалізація бібліотеки на JavaScript sql.js, яка дозволяє обробляти файли БД безпосередньо в браузері.

Для інших мов програмування розроблено механізм підключення й роботи з БД через цю бібліотеку: C++, Java, Python, Perl, PHP, Ruby, Haskell, Scheme, Smalltalk, Lua тощо. Засоби для роботи з Tcl включені в комплект постачання SQLite. Повний список наявних засобів можна знайти на сторінці проекту.

Web-інструментарії

У ряді інструментаріїв присутня можливість використання SQLite як бази даних, наприклад: Django; Java; PHP; Ruby on Rails; Trac; Symfony; Parser.

Багато програм підтримують SQLite як формат зберігання даних, зокрема:

1. Amarok – може використовувати бази даних SQLite як сховище музичної колекції.

2. Gajim – SQLite використовується для зберігання історії контактів.

3. Songbird (як застосунок, заснований на XULRunner 1.9)

4. Banshee.

5. F-Spot.

6. Платформа XUL на рушії Gecko 1.9, XULRunner 1.9 і, потенційно, всі застосунки, засновані на цій платформі, у тому числі й Firefox починаючи з версії 3.0.

7. Google Chrome.

8. Google Gears.

9. Mendeley – менеджер pdf-документів, академічний засіб для дослідження (реалізується desktop & web).

10. Zotero – менеджер інформації, бібліографічний менеджер, додаток Firefox.

Незважаючи на те що я працював над ПЗ один в реалізації програми я використовував підходи пришвидшення розробки на основі методологій Agile.

Гнучка розробка програмного забезпечення (Agile software development, agile-методи) – клас методологій розробки програмного забезпечення, що базується на ітеративній розробці, в якій вимоги та розв'язки еволюціонують через співпрацю між самоорганізовуваними багатофункціональними командами.

Гнучка розробка – найкращий засіб для підвищення продуктивності розробників програмного забезпечення.

Більшість гнучких методологій націлені на мінімізацію ризиків, шляхом зведення розробки до серії коротких циклів, що мають назву ітерацій, які зазвичай тривають один-два тижні. Кожна ітерація сама по собі виглядає як програмний проект в мініатюрі, і включає всі завдання, необхідні для видачі мінімального приросту за функціональністю: планування, аналіз вимог, проектування, кодування, тестування і документування. Хоча окрема ітерація, як правило, недостатня для випуску нової версії продукту, мається на увазі те, що гнучкий програмний проект готовий до випуску наприкінці кожної ітерації. Після закінчення кожної ітерації, команда виконує переоцінку пріоритетів розробки.

Agile акцентує увагу на безпосередньому спілкуванні «віч-на-віч». Більшість agile команд розташовані в одному офісі, його іноді називають bullpen. Як мінімум вона включає і «замовників» (замовники, які визначають продукт,

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

також це можуть бути менеджери продукту, бізнес аналітики або клієнти). Офіс може також включати тестувальників, дизайнерів інтерфейсу, технічних авторів і менеджерів.

Основною метрикою agile методів є робочий продукт. Віддаючи перевагу безпосередньому спілкуванню, agile-методи зменшують обсяг письмової документації в порівнянні з іншими методами. Це привело до критики цих методів як недисциплінованих.

Agile – родина процесів розробки, а не єдиний підхід в розробці програмного забезпечення, і визначається Agile Manifesto. Agile не включає практик, а визначає цінності та принципи, якими керуються успішні команди.

Agile Manifesto розроблений і прийнятий 17 розробниками 11-13 лютого 2001 року на лижному курорті The Lodge at Snowbird в горах Юти. Маніфест підписали представники наступних методологій Extreme programming, Scrum, DSDM, Adaptive software development, Crystal Clear, Feature driven development, Pragmatic Programming. Agile Manifesto містить 4 основні ідеї та 12 принципів. Примітно, що Agile Manifesto не містить практичних порад.

Основні ідеї:

- Особистості та їхні взаємодії важливіші, ніж процеси та інструменти;
- Робоче програмне забезпечення важливіше, ніж повна документація;
- Співпраця із замовником важливіша, ніж контрактні зобов'язання;
- Реакція на зміни важливіша, ніж дотримання плану.

Принципи, які роз'яснює Agile Manifesto:

- задоволення клієнта за рахунок ранньої та безперебійної поставки коштовного програмного забезпечення;
- вітання змін вимог навіть наприкінці розробки (це може підвищити конкурентоспроможність отриманого продукту);
- часта поставка робочого програмного забезпечення (кожен місяць або тиждень або ще частіше);

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

- тісне, щоденне спілкування замовника з розробниками впродовж всього проекту;
- проектом займаються мотивовані особистості, які забезпечені потрібними умовами роботи, підтримкою і довірою;
- рекомендований метод передачі інформації – особиста розмова (віч-на-віч);
- робоче програмне забезпечення – найкращий вимірник прогресу;
- спонсори, розробники та користувачі повинні мати можливість підтримувати постійний темп на невизначений термін;
- постійну увагу поліпшенню технічної майстерності та зручному дизайну;
- простота – мистецтво не робити зайвої роботи;
- найкращі технічні вимоги, дизайн та архітектура виходять у самоорганізованої команди;
- постійна адаптація до мінливих обставин.

Маніфест та Принципи гнучкої розробки містять високорівневі ідеї щодо того, як потрібно вибудовувати процес розробки програмного забезпечення, щоб успішно завершувати проекти й створювати команди, в яких приємно та цікаво працювати.

Документи визначають, що потрібно для цього зробити, але не говорять, як це зробити. По-іншому й не могло бути, оскільки Маніфест та Принципи народилися внаслідок консенсусу представників різних (хоча й споріднених) напрямів, які могли знайти спільну основу лише на рівні базових цінностей та принципів.

Критика. Багато керівників проектів, що працюють у традиційних методологіях на кшталт «водоспаду», критикують agile-методи.

Один з повторюваних пунктів критики: при agile-підході часто нехтують створенням «дорожньої карти» розвитку продукту, так само як і управлінням вимогами, в процесі якого і формується така «карта». Гнучкий підхід до управління вимогами не має на увазі далекосяжних планів (по суті, управління

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

вимогами просто не існує в даній методології), а має на увазі можливість замовника раптом і несподівано наприкінці кожної ітерації виставляти нові вимоги, що часто суперечать архітектурі вже створеного і поставленого продукту. Таке іноді призводить до катастрофічних «авралів» з масовим рефакторингом і переробками практично на кожній черговій ітерації.

Крім того вважається, що робота в agile мотивує розробників вирішувати всі прибулі завдання найпростішим і найшвидшим можливим способом, при цьому часто не звертаючи уваги на коректність коду з точки зору вимог базової платформи (підхід «працює, та й добре», при цьому не враховується, що може перестати працювати при найменшій зміні або ж породити важкі до відтворення дефекти після реального розгортання у клієнта). Це призводить до зниження якості продукту і накопиченню дефектів.

Методології. Існують методології, які дотримуються цінностей і принципів заявлених в Agile Manifesto, деякі з них:

1. Agile Modeling – набір понять, принципів і прийомів (практик), що дозволяють швидко і просто виконувати моделювання і документування в проектах розробки програмного забезпечення. Не включає в себе детальну інструкцію з проектування, не містить описів, як будувати діаграми на UML.

Основна мета – ефективне моделювання і документування; але не охоплює програмування та тестування, не включає питання управління проектом, розгортання і супроводу системи. Однак включає в себе перевірку моделі кодом.

2. Agile Unified Process (AUP) спрощена версія IBM Rational Unified Process (RUP), розроблена Скоттом Амблером, яка описує просте і зрозуміле наближення (модель) для створення програмного забезпечення для бізнес-додатків.

3 Agile Data Method – група ітеративних методів розробки програмного забезпечення, в яких вимоги та рішення досягаються в рамках співпраці різних крос-функціональних команд.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

4. DSDM заснований на концепції швидкої розробки додатків (Rapid Application Development, RAD). Являє собою ітеративний і інкрементний підхід, який надає особливого значення тривалій участі в процесі користувача/споживача.

5. Essential Unified Process (EssUP).

6. Екстремальне програмування (Extreme programming, XP).

7. Feature driven development (FDD) – функціонально-орієнтована розробка.

Використовуване в FDD поняття функції або властивості (feature) Системи досить близько до поняття прецеденту використання, використовуваному в RUP, істотна відмінність – це додаткове обмеження: «кожна функція повинна допускати реалізацію не більше, ніж за два тижні». Тобто якщо сценарій використання досить малий, його можна вважати функцією. Якщо ж великий, то його треба розбити на декілька відносно незалежних функцій.

8. Getting Real – ітераційний підхід без функціональних специфікацій, що використовується для веб-додатків. У даному методі спершу розробляється інтерфейс програми, а потім її функціональна частина.

9. OpenUP – це ітераційно-інкрементний метод розробки програмного забезпечення. Позиціюється, як легкий і гнучкий варіант RUP. OpenUP ділить життєвий цикл проекту на чотири фази: початкова фаза, фази уточнення, конструювання та передачі. Життєвий цикл проекту забезпечує надання зацікавленим особам та членам колективу точок ознайомлення і прийняття рішень впродовж усього проекту. Це дозволяє ефективно контролювати ситуацію і вчасно приймати рішення про задовільність результатів. План проекту визначає життєвий цикл, а кінцевим результатом є остаточний додаток.

10. Scrum встановлює правила керування процесом розробки та дозволяє використовувати вже існуючі практики кодування, коректуючи вимоги або вносячи тактичні зміни. Використання цієї методології дає можливість виявляти і усувати відхилення від бажаного результату на більш ранніх етапах розробки програмного продукту.

11. Бережлива розробка програмного забезпечення (lean software development). Використовує підходи з концепції бережливого виробництва.

Jira – була використана комерційна система відслідковування помилок, призначена для організації взаємодії з користувачами, хоча в деяких випадках використовується і для управління проектами. Розроблено компанією Atlassian, є одним з двох її основних продуктів (поряд з вікі-системою Confluence). Має веб-інтерфейс.

Назва системи отримано шляхом усічення слова «Gojira» – Японського імені монстра Годзилла, що, в свою чергу, є відсиланням до назви конкуруючого продукту – Bugzilla; створювалася в якості заміни Bugzilla і багато в чому повторює її архітектуру. Система дозволяє працювати з декількома проектами. Для кожного з проектів створює і веде схеми безпеки і схеми оповіщення.

До версії 3.13.5 (включно) розрізнялися редакції Enterprise, Professional і Standard, після – Залишилася тільки редакція Enterprise (для великих організацій).

Система заснована на Java EE і працює на кількох популярних системах управління базами даних і операційних системах.

Основний елемент обліку в системі – завдання (ticket або issue). Завдання містить назву проекту, тему, тип, пріоритет, компоненти і зміст. Завдання може бути розширена додатковими полями (також і нові призначені для користувача поля можуть бути визначені), додатками (наприклад – Фотографіями, скріншотами) або коментарями. Завдання може редагуватися або просто змінювати статус, наприклад, з «відкритий» в «закритий». Які переходи між станами можливі, визначається через настраюється потік операцій. Будь-які зміни в задачі записуються в журнал.

Jira має велику кількість можливостей конфігурації: для кожної програми може бути визначений окремий тип завдання з власним workflow, набором статусів, одним або декількома видами уявлення (screens). Крім того, за допомогою так званих «схем» можна визначити для кожного індивідуального Jira-проекту власні права доступу, поведінку і видимість полів і багато іншого.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

Завдяки універсальному підходу можна пристосувати Jira для багатьох непрофільних завдань, наприклад, керування вимогами, керування ризиками, аж до реалізації невеликої системи бронювання, автоматизації процесу рекрутингу.

Для інтеграції з зовнішніми системами підтримує інтерфейси SOAP, XML-RPC і REST. Поставляється із засобами інтеграції з такими системами управління версіями, як Subversion, CVS, Git, Clearcase, Team Foundation Server, Mercurial і Perforce.

Існують доповнення, що дозволяють вбудувати Jira в інтегровані середовища розробки, в тому числі Eclipse і IntelliJ IDEA. Перекладена багатьма мовами, включаючи російську, англійську, японську, німецьку, французьку, іспанську.

Для сторонніх розробників надаються кошти розробки розширень системи – плагінів. Розробники розширень можуть викладати плагіни для продажу на спеціальний розділ сайту Atlassian.

Є комерційним продуктом, який може бути ліцензований для роботи на локальному сервері або доступний в якості віддаленого додатки. Ціноутворення залежить від максимального числа користувачів, при цьому близько \$50 за користувача для локального і \$7 на місяць за користувача для віддаленого доступу є типовими цінами.

Для академічних і комерційних клієнтів доступний повний вихідний код під ліцензією розробника.

Для проектів з відкритим вихідним кодом Atlassian надає спеціальну безкоштовну ліцензію при дотриманні наступних правил:

- проект використовує ліцензії, схвалені Open Source Initiative;
- вихідний код проекту доступний для скачування;
- у проекту є публічно доступна веб-сайт;
- програмне забезпечення від Atlassian є на веб-сайті проекту.

Розглянемо визначення API. Це прикладний програмний інтерфейс (Application Programming Interface, API) – набір визначень підпрограм, протоколів взаємодії та засобів для створення програмного забезпечення.

Спрощено – це набір чітко визначених методів для взаємодії різних компонентів. API надає розробнику засоби для швидкої розробки програмного забезпечення. API може бути для веб-базованих систем, операційних систем, баз даних, апаратного забезпечення, програмних бібліотек.

Одним з найпоширеніших призначень API є надання набору широко використовуваних функцій, наприклад для малювання вікна чи іконок на екрані. API є абстрактним поняттям — програмне забезпечення, що пропонує деякий API, часто називають реалізацією (implementation) даного API. У багатьох випадках API є частиною набору розробки програмного забезпечення, водночас, набір розробки може включати як API, так і інші інструменти/апаратне забезпечення, отже ці два терміни не є взаємозамінювані.

Високорівневі API часто програють у гнучкості. Виконання деяких функцій нижчого рівня стає набагато складнішим, або навіть неможливим.

В об'єктно-орієнтованих мовах, прикладний програмний інтерфейс зазвичай включає в себе опис набору визначень класу, з набором форм поведінки, пов'язаних з цими класами. Це абстрактне поняття пов'язане з реальними функціями, які надані або надаватимуться, класами, які реалізуються в методах класу.

Прикладний програмний інтерфейс в даному випадку можна розглядати як сукупність всіх методів, які публічно доступні в класах (зазвичай званий інтерфейс класу). Це означає, що прикладний програмний інтерфейс вказує методи, за допомогою яких взаємодіє з об'єктами, отриманими з визначень класів і обробляє їх.

У більш загальному плані можна визначити Прикладний Програмний Інтерфейс як сукупність усіх видів об'єктів, які можна вивести з визначення класу, і пов'язаних з ними можливих варіантів поведінки.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

Наприклад: клас, що представляє Stack, може просто виставити публічно два методи Push() (для додавання нового елемента в стек) і Pop() (для вилучення останнього пункту, ідеально розташований на вершині стека).

У цьому випадку Прикладний Програмний Інтерфейс може бути інтерпретованим як два методи pop() і push(), або, більш широко, використовується варіант, коли можна використовувати елемент типу Stack, який реалізує поведінку стека, надаючи йому можливість для додавання / видалення елементів з вершини. Друга інтерпретація видається більш доречною в дусі об'єктно-орієнтованого підходу.

Якість документації, пов'язаної з Прикладним Програмним Інтерфейсом, є часто ключовим фактором, що визначає його успішність з точки зору простоти використання.

ППІ, як правило, пов'язаний із бібліотеками програмного забезпечення: ППІ описує і вказує очікувану поведінку в той час, як бібліотека є фактичною реалізацією даного набору правил. Один ППІ може мати декілька реалізацій (або жодної, будучи абстрактним) у вигляді різних бібліотек, які мають такий же інтерфейс.

Прикладний програмний інтерфейс також може бути пов'язаним з платформами програмування: платформа може бути заснована на кількох бібліотеках реалізує декілька інтерфейсів ППІ, але на відміну від звичайного використання ППІ, доступ до поведінки вбудований в платформу опосередкований шляхом розширення його змісту новими класами і вставлений в саму платформу. Крім того, загальний потік управління програми може бути під контролем абонента.

Прикладний програмний інтерфейс може бути також реалізацією протоколу.

Коли ППІ реалізує протокол, він може бути заснованим на проксі-методах віддалених викликів, що засновані на протоколі зв'язку. Роль ППІ може

заклучатися саме в тому, щоб приховати деталі транспортного протоколу. Наприклад: RMI є ППІ, який реалізує протокол або JRMP IIOP як RMI-IIOP.

Протоколи, як правило, розподіляються між різними технологіями і зазвичай дозволяють різним технологіям обмінюватися інформацією, діючи як абстракція між двома світами. ППІ, як правило, є специфічним для конкретної технології: звідси, інтерфейси даної мови не можуть бути використані на інших мовах, якщо виклики функції не будуть перетворені з конкретної адаптації бібліотеки.

Деякі мови, серед яких такі, що працюють на віртуальних машинах (наприклад: мови, сумісні з NET CLI середовища CLR і JVM сумісних мов у віртуальній машині Java) можуть ділитися програмними інтерфейсами.

У цьому випадку віртуальна машина дозволяє мові взаємодії завдяки спільному знаменнику віртуальної машини, що абстрагується від конкретної мови, використовувати проміжний байт-код і його мову.

При використанні прикладного програмного інтерфейсу в контексті веб-розробки, як правило, ППІ визначається набором повідомлень запиту HTTP, також визначається структура повідомлень-відповідей, зазвичай у розширенні мови розмітки XML або в форматі об'єктного запису JavaScript (JSON). У той час як прикладний програмний інтерфейс у Web історично був практично синонімом для веб-служби, останнім часом тенденція змінилась (так званий Web 2.0) на відхід від Simple Object Access Protocol (SOAP) на основі веб-сервісів і сервіс-орієнтованої архітектури (SOA) на більш прямі передачі репрезентативного стану (REST) стилів веб-ресурсів та ресурсів-орієнтованої архітектури (ROA).

Частина цієї тенденції пов'язана з рухом Семантичного веб-ресурсу до Опису Платформ (RDF), Концепції розвитку веб-технологій інженерних онтологій. Прикладні програмні інтерфейси у Web, що дозволяють комбінувати декількома прикладними програмними інтерфейсами в нові додатки називають гібридними.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм ДСТУ 28147:2009, що є класичним алгоритмом симетричного шифрування на основі мережі Фейстеля (рисунок 4.3). Даний алгоритм шифрує інформацію блоками по 64 біта (такі алгоритми називаються "блоковими"). Зміст мережі Фейстеля полягає в тому, що блок шифруємої інформації розбивається на два або більше субблоків, частина яких обробляється за певним законом, після чого результат цієї обробки накладається (операцією побітового додавання за модулем 2) на необроблювані субблоки. Потім субблоки міняються місцями, після чого обробляються знову й т.д. певне для кожного алгоритму число раз – раундів.

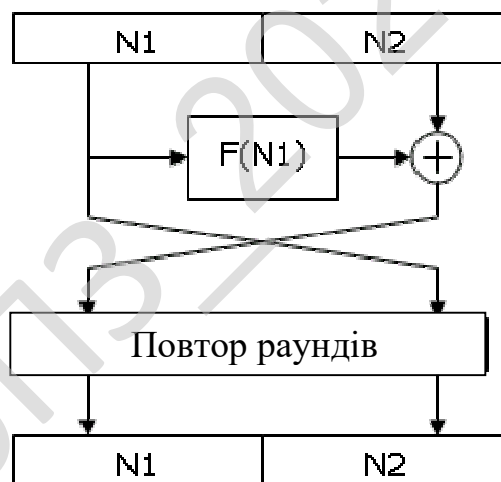


Рисунок 4.3 – Мережа Фейстеля

Основна відмінність алгоритмів симетричного шифрування друг від друга складається саме в різних функціях обробки субблоків. Дана функція часто називається "основним криптографічним перетворенням", оскільки саме вона несе основне навантаження при шифруванні інформації. Основне перетворення алгоритму ДСТУ 28147:2009 є досить простим, що забезпечує високу швидкодію алгоритму; у ньому виконуються наступні операції (рисунок 4.4).



Рисунок 4.4 – Основне перетворення алгоритму ДСТ 28147:2009

1. Додавання субблоку з певним фрагментом ключа шифрування за модулем 2^{32} . K_x – це 32-бітна частина ("підключ") 256-бітного ключа шифрування, якому можна представити як конкатенацію 8 підключів: $K = K_0K_1K_2K_3K_4K_5K_6K_7$. Залежно від номера раунду й режиму роботи алгоритму (про їх – нижче), для даної операції вибирається один з підключів.

2. Таблична заміна. Для її виконання субблок розбивається на 8 4-бітних фрагментів, кожний з яких прогоняється через свою таблицю заміни. Таблиця заміни містить у певній послідовності значення від 0 до 15 (тобто всі варіанти значень 4-бітні фрагменти даних); на вхід таблиці подається блок даних, числове подання якого визначає номер вихідного значення. Наприклад, подається значення 5 на вхід наступної таблиці: "13 0 11 74 91 10 143 5 122 15 8 6". У результаті на виході виходить значення 9 (оскільки 0 замінюється на 13, 1 – на 0, 2 – на 11 і т.д.).

3. Побітове циклічне зрушення даних усередині субблока на 11 біт уліво.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблена система кібербезпеки для захисту корпоративної мережі від кіберзагроз. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Верхнього меню: Файл; З'єднання; Безпека; Журнал; Параметри; Довідка.
- Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.
- Розділу обрання групи з'єднання з сервером.
- Розділу виведення результату роботи системи.

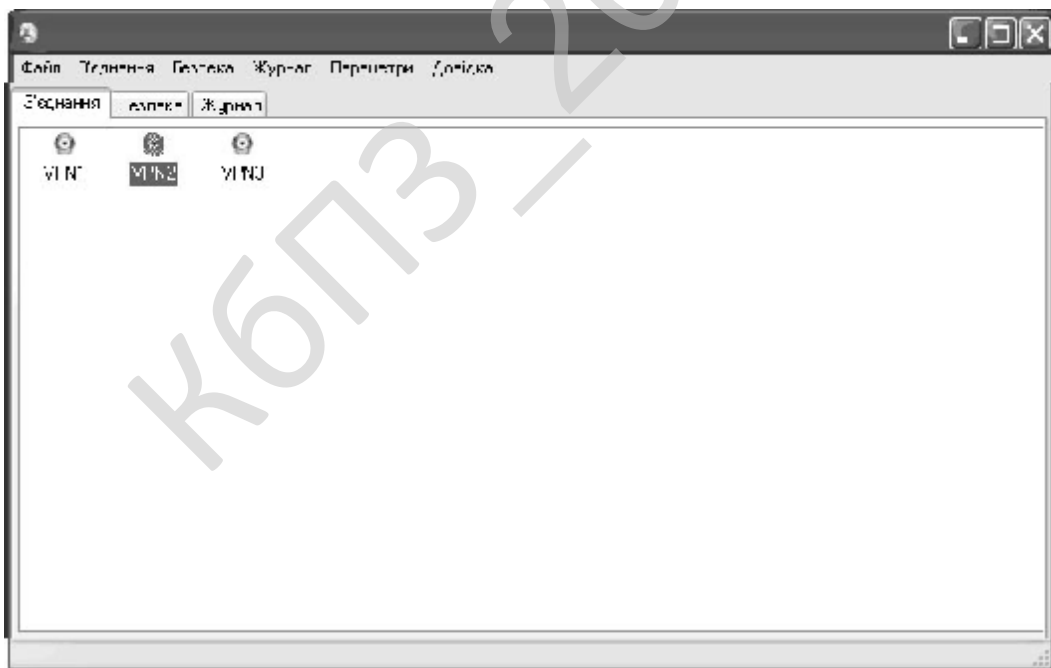


Рисунок 5.1 – Головне вікно ПЗ

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 5.2 зображено авторські дані розробленого програмного забезпечення.

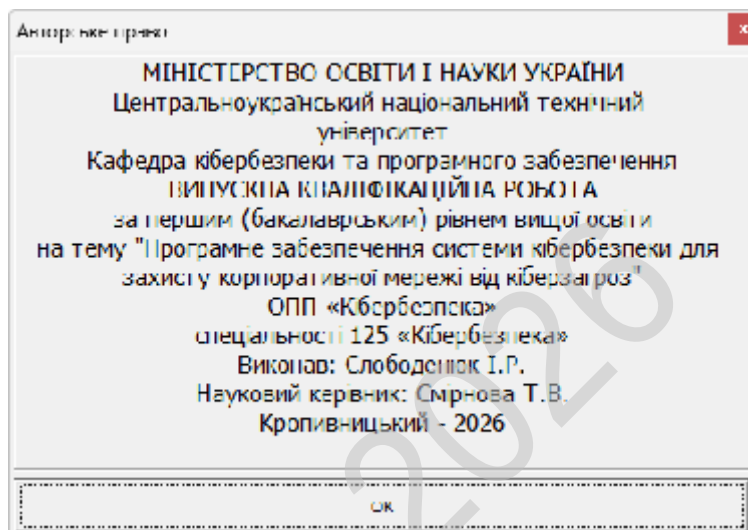


Рисунок 5.2 – Авторське право

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.

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

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

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.

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;

– 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.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

– Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

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 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.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

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.

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.
- помилок інтерфейсу.
- помилок у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
- помилок 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 (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 (zareєstrуватися), заплативши авторові певну суму.

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

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем для захисту корпоративної мережі від кіберзагроз.

- Досліджена система для захисту корпоративної мережі від кіберзагроз.

- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для захисту корпоративної мережі від кіберзагроз.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для захисту корпоративної мережі від кіберзагроз.

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 системи кібербезпеки для захисту корпоративної мережі від кіберзагроз. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід,

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

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 кібербезпеки 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 ДСТУ 28147:2009.

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-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
5. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		80

7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

9. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.

10. 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.

11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.

12. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем ІР-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.

13. 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.

14. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56
16. 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.
17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.
18. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
19. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.
20. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІІШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
21. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя*

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		82

кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

22. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

23. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.

24. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,

25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

26. 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.

27. 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.

					ВКРБ-125.26.0040.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		83

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

29. 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.

30. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021*, Cracow, Poland, 22-25 September 2021. P. 414-418

31. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

32. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020*, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

33. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings Volume 2805*, 2020, Pages 44-58.

34. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-

feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

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

36. 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.

37. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

38. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.

39. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.

40. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.

41. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I., Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 166-171.

42. 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.

43. 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.

44. 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.

45. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». *International Journal of Computer Network and Information Security (IJCNIS)*. Vol. 12, No. 3, 2020. PP.33-43.

46. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 646-660.

47. 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.

48. 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.

49. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during

Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019.

50. 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.

51. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», 2019 *IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019)*. 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209.

52. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18 - 21 September 2019. P.713-718.

53. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskiy, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P. 707-712.

54. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P.701-706.

55. Smirnov, O., Hu, Z., Vasiliu, Y., Sydorenko, V., Polishchuk, Y., «Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P.399-405.

56. 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.

57. Smirnov, O., Kuznetsov, A., Kiian, A., Babenko, B., Zhosan, H., Prokopovych-Tkachenko, D., «Soft Decoding Method for Turbo-Productive Codes», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019,* Lviv, Ukraine, 2-6 July, 2019, P. 129-134.

58. 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.

59. 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.

60. 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.

61. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», *CEUR Workshop Proceedings* Volume 2353, *CEUR Workshop Proceedings* 2019, Pages 873-884.