

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 моніторингу та виявлення
відхилень у роботі апаратно-програмних компонентів
комп’ютерної системи”

Виконав здобувач вищої освіти
IV курсу, групи КІ-23-МБ
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Крічфалуші А.О.
« ____ » _____ 2026 р.

Керівник проекту
кандидат фізико-математичних наук, доцент
_____ Якименко Н.М.
« ____ » _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань ._12 _____“Інформаційні технології”
Спеціальність 123 “Комп’ютерна інженерія”
Освітньо-професійна (освітньо-наукова) програма “Комп’ютерна інженерія”

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

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

Крічфалуші Андрію Олександровичу

(прізвище, ім’я, по батькові)

1. Тема роботи *Програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп’ютерної системи*

2. Керівник роботи *Якименко Наталія Миколаївна, кандидат фізико-математичних наук, доцент*

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

затверджені наказом вищого навчального закладу № 126-02 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 моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп’ютерної системи*

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

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію.

6. Висновки

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

Структурна схема системи 1 аркуш

Функціональна схема системи 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

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

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Якименко Н.М.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Крічфалуші А.О.
(прізвище та ініціали)

АНОТАЦІЯ

Крічфалуші А.О. Програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

Метою розробки є програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

Результат роботи – програмна реалізація системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

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

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

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

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, моніторинг та виявлення відхилень, апаратно-програмні компоненти, комп'ютерна система

ABSTRACT

Krichfalushi A.O. Software for the monitoring system and detection of deviations in the operation of hardware and software components of a computer system. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed, which is intended for the monitoring system and detection of deviations in the operation of hardware and software components of a computer system.

The purpose of the development is software for the monitoring system and detection of deviations in the operation of hardware and software components of a computer system.

The result of the work is the software implementation of the monitoring system and detection of deviations in the operation of hardware and software components of a computer system.

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: computer engineering, monitoring and detection of deviations, hardware and software components, computer system

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	7
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	7
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	31
2.3 Розгорнута постановка завдання	34
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	36
3.1 Опис функціонування системи	36
3.2 Розробка структурної схеми.....	38
3.3 Розробка функціональної схеми	40
3.4 Розробка діаграми процесів.....	42
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	44
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	44
4.2 Захист розробленого програмного забезпечення.....	55
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	57
6 ОСНОВНІ ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	68

					ВКРБ-123.26.0034.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи	Літ.	Аркуш	Аркушів
Розроб.	Крічфалуші А.О.					Б	1	78
Перев.	Якименко Н.М.							
Н.контр.	Коваленко А.С.					ЦНТУ КІ-23-МБ		
Затв.	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ІТ	—	інформаційні технології
КС	—	комп'ютерна система
НС	—	надзвичайна ситуація
ОС	—	операційна система
ПЗ	—	програмне забезпечення
ПЕОМ	—	персональна електронна обчислювальна машина
AVSP	—	Anti-Virus Software Protection

К6ПЗ_2026

ВСТУП

Актуальність теми. Система моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи, яка розробляється у даній роботі, призначена для захисту комп'ютерної системи від шкідливих програм. Глобальний ринок антивірусного (AV) програмного забезпечення має значне значення в сучасній цифровій екосистемі, оскільки кіберзагрози продовжують розвиватися у складності та масштабі. Зростаюча цифровізація в різних галузях, поряд із поширенням підключених пристроїв, посилила потребу в надійних заходах кібербезпеки. Зростання кількості складних шкідливих програм, програм-вимагачів та фішингових атак стимулює попит на передові AV-рішення, здатні виявляти та пом'якшувати ці ризики в режимі реального часу. Крім того, нормативно-правові рамки, що вимагають захисту даних та конфіденційності, спонукають організації інвестувати в надійне антивірусне програмне забезпечення для забезпечення відповідності вимогам та захисту конфіденційної інформації. Збільшення кількості віддалених працівників та збільшення використання хмарних обчислень ще більше посилили вразливості, що робить комплексний антивірусний захист необхідним як для окремих осіб, так і для підприємств. Оскільки кібератаки стають все більш частими та руйнівними, ринок спостерігає зростаючий акцент на методах виявлення на основі штучного інтелекту та поведінки, щоб передбачити та запобігти порушенням до того, як виникне пошкодження. Загалом, глобальна важливість ринку AV-програмного забезпечення полягає в його вирішальній ролі у збереженні цілісності даних, підтримці безперервності роботи та зміцненні довіри до цифрової інфраструктури в усьому світі.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

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

- Огляд існуючих систем моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.
- Дослідження системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.
- Програмна реалізація системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Інвестиційні можливості на ринку антивірусного (AV) програмного забезпечення розширюються завдяки зростаючому попиту на інноваційні рішення безпеки, що реагують на кіберзагрози, що розвиваються. Одним з основних напрямків є інтеграція технологій штучного інтелекту та машинного навчання для підвищення точності та швидкості виявлення загроз. Ці інтелектуальні системи пропонують прогнозу аналітику та можливості автоматизованого реагування, залучаючи інвестиції, спрямовані на створення адаптивних та масштабованих AV-рішень. Крім того, зростання використання мобільних пристроїв та впровадження Інтернету речей відкрило нові ринки для спеціалізованих антивірусних продуктів, розроблених для захисту різноманітних платформ та середовищ.

Ще однією ключовою сферою для інвестицій є зростаючий акцент на хмарних антивірусних сервісах. Хмарні рішення безпеки забезпечують гнучкість, оновлення в режимі реального часу та знижені витрати на інфраструктуру, що робить їх привабливими для підприємств будь-якого розміру. Інвестори також орієнтуються на малі та середні підприємства (МСП), які дедалі більше усвідомлюють важливість кібербезпеки, але часто не мають власних ресурсів. Крім того, регуляторний тиск та зростання впровадження кіберстрахування спонукають компанії вдосконалювати свої системи безпеки, створюючи додаткові можливості для інвесторів підтримувати антивірусні технології наступного покоління та комплексні пакети безпеки.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

1.2 Область застосування

Ринок антивірусного (AV) програмного забезпечення готовий до стабільного зростання завдяки постійному розвитку технологій кібербезпеки та зростанню рівня загроз. Зростання кількості кіберзлочинів у всьому світі спонукає організації впроваджувати більш складні AV-рішення, які пропонують проактивний та багаторівневий захист. Очікується, що ринок отримає вигоду від постійних інновацій, таких як хмарні антивірусні платформи, можливості виявлення та реагування на кінцеві точки (EDR) та інтеграція з ширшими екосистемами безпеки. Крім того, зростаюча обізнаність про ризики кібербезпеки як серед споживачів, так і серед підприємств підживлює попит на зручне та ефективне антивірусне програмне забезпечення.

Заглядаючи в майбутнє, перспективи ринку антивірусного програмного забезпечення виглядають багатообіцяючими, оскільки технологічні розробки та регуляторні вимоги зближуються, посилюючи потребу в комплексних інструментах кіберзахисту. Зростаюче впровадження штучного інтелекту та автоматизації в антивірусних продуктах, ймовірно, покращить ефективність прогнозування загроз та реагування, що дозволить швидше стримувати порушення. Крім того, розширення ініціатив цифрової трансформації та зростання впровадження підключених пристроїв ще більше розширять масштаби ринку. Постійний розвиток кіберзагроз стимулюватиме стабільні інвестиції та інновації, гарантуючи, що ринок антивірусного програмного забезпечення залишається критичним компонентом глобальної інфраструктури кібербезпеки.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

Існують сотні антивірусів, які стверджують про першокласний захист за надзвичайно низькими цінами – важко знати, який з них справді ефективний. Саме тому я ретельно протестував усі провідні антивіруси, оцінюючи їх за виявленням шкідливого програмного забезпечення, швидкістю, функціями та вартістю. До цього списку потрапили лише найкращі.

Сучасні антивіруси пропонують більше, ніж просто сканер, пропонуючи брандмауери, блокувальники фішингу, VPN, менеджери паролів, батьківський контроль, спеціальний захист для мобільних пристроїв тощо.

Але багато антивірусів не працюють так, як рекламується – вони мають низький рівень виявлення шкідливого програмного забезпечення, не блокують шкідливі сайти послідовно, а їхні додаткові функції погано розроблені та практично марні (незважаючи на додаткову вартість).

Norton 360 – найкращий антивірус для Windows, Android та iOS

Norton 360 пропонує неперевершений захист від вірусів та шкідливих програм. Це добре розроблений та добре підтримуваний пакет інтернет-безпеки, який захищає ваші пристрої та особисту інформацію, і він добре працює на всіх операційних системах. Це найкращий вибір для домашніх користувачів, які шукають повний, інтуїтивно зрозумілий антивірус з одними з найкращих засобів кіберзахисту.

Переваги:

- Ідеальне виявлення шкідливих програм.
- VPN з необмеженим трафіком.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

- Чудовий батьківський контроль.
- Хмарне сховище (до 500 ГБ).

Недоліки:

- Без безкоштовного плану.

Механізм сканування Norton працює на основі евристичного аналізу та машинного навчання, що дозволяє йому сканувати, знаходити та видаляти всі найновіші та найсучасніші типи шкідливих програм. Він отримав 100% рейтинг захисту під час усіх моїх тестів, постійно перевершуючи вбудовані антивіруси (наприклад, Microsoft Defender).

Повне сканування Norton було швидшим, ніж у будь-якого іншого конкурента, і зайняло лише 14 хвилин, але за ці 14 хвилин я помітив невелике уповільнення системи – хоча цього було недостатньо, щоб суттєво вплинути на мій робочий процес. Крім того, я не отримав багато хибних прапорців (безпечні програми, які помилково позначені як небезпечні).

Він також має широкий спектр додаткових функцій, які чудово працюють:

- Безпечний брандмауер.
- Менеджер паролів.
- Захист від фішингу (включаючи режим анонімного перегляду веб-сторінок).
- VPN (з необмеженим трафіком).
- Моніторинг темної мережі.
- Захист від крадіжки особистих даних.
- Інструменти оптимізації.
- Батьківський контроль.
- Сповіщення безпеки Wi-Fi (лише для Android та iOS).
- Хмарне сховище (до 500 ГБ).
- Захист від програм-вимагачів.
- І багато іншого...

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

Захист від фішингу в Norton чудовий. Він постачається як розширення для браузера, яке надійно блокує фішингові сайти, надаючи вам детальну інформацію про кожен сайт, який воно забороняє вам відвідувати. Він також має вбудований захист онлайн-банкінгу та безпечну пошукову систему, яка пропонує кольорове кодування результатів пошуку. Нарешті, є безкоштовний браузер під назвою Private Browser, який інтегрує різні інструменти для підвищення безпеки та конфіденційності.

Мені подобається, що менеджер паролів Norton безкоштовний. Він генерує, зберігає та автоматично заповнює паролі, тому вам ніколи не доведеться їх запам'ятовувати. На жаль, йому бракує спільного доступу до паролів та вбудованого автентифікатора TOTP, які пропонують деякі окремі конкуренти, але він добре виконує основні функції.

Мені дуже подобаються програми Norton для Android та iOS. Обидві версії мають фільтр спаму, VPN, безпеку Wi-Fi, веб-захист та багато іншого. Програма для Android навіть постачається з блокувальником реклами та відстеження, а також чудовим інструментом, який виділяє програми з нав'язливими дозволами. Версія для iOS менш функціональна, але це стосується всіх антивірусів.

Захист від крадіжки особистих даних також справді хороший. Продукти Norton LifeLock (для користувачів у вибраних країнах) пропонують різні рівні захисту та відшкодування, включаючи покриття до 3 мільйонів доларів викрадених коштів, особистих витрат та витрат на адвоката/експерта.

VPN від Norton – один з моїх улюблених VPN-провайдерів у комплекті з антивірусом у 2026 році. У жодному з тарифних планів VPN немає обмежень щодо даних, і всі користувачі отримують доступ до серверів у 29 країнах. Ви також захищені 256-бітним AES-шифруванням та політикою відмови від ведення журналів. Інші функції включають функцію автоматичного вимкнення, роздільне тунелювання та блокувальник реклами.

Загалом, Norton пропонує більше функцій, ніж майже будь-який конкурент, і всі вони чудово працюють. Він проходить щорічні перевірки,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

відповідає всім основним нормам конфіденційності даних і має програми для всіх основних операційних систем (він навіть працював на Chromebook мого колеги, незважаючи на офіційну підтримку).

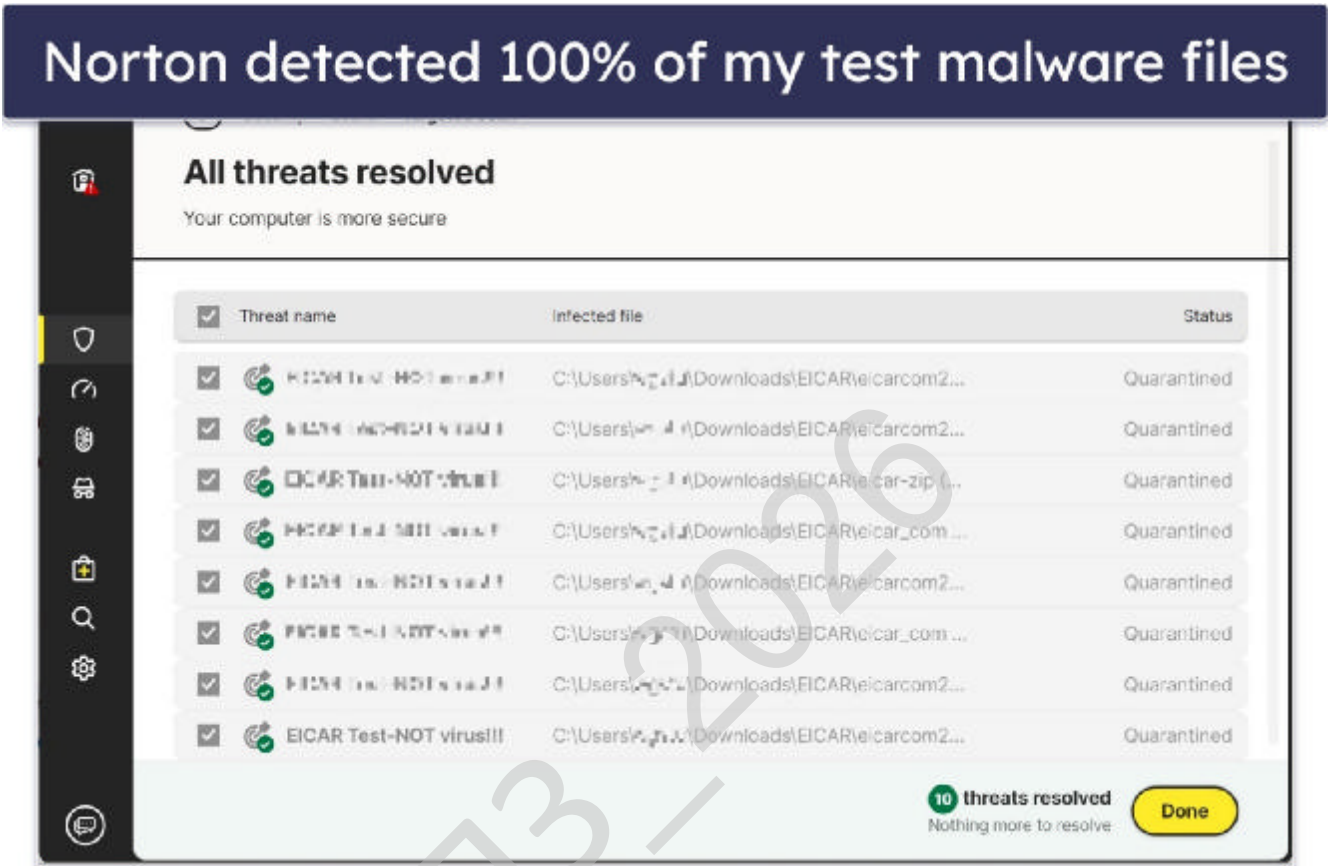


Рисунок 2.1 – Інтерфейс користувача Norton

Ви можете отримати базовий захист для 1 пристрою з планом AntiVirus Plus (1310 гривень/рік), але я вважаю, що 360 Deluxe – це найкращий пакет для більшості користувачів. Він коштує 2180 гривень/рік і включає VPN, моніторинг даркнету, хмарне сховище та багато іншого. Щоб скористатися повним пакетом захисту від крадіжки особистих даних Norton, вам знадобиться підписка LifeLock, яка починається від 3050 гривень/рік. На всі плани поширюється 60-денна гарантія повернення грошей.

Norton 360 забезпечує найкращий антивірусний захист у 2026 році. Він пропонує один із найпотужніших пакетів кібербезпеки, повний захист від усіх

шкідливих загроз та безліч чудових додаткових функцій, таких як VPN (з необмеженим обсягом даних), менеджер паролів, безпечне хмарне сховище, батьківський контроль та багато іншого. Ви можете спробувати Norton без ризику з 60-денною гарантією повернення грошей.

TotalAV – найкращий за простотою використання (дуже зручний для початківців)

TotalAV має чудовий антивірусний сканер і кілька справді корисних додаткових функцій, і все це всередині дуже інтуїтивно зрозумілої панелі інструментів, що робить його чудовим вибором для початківців. Однак TotalAV також включає багато опцій налаштування, які оцінять досвідчені користувачі.

Переваги:

- Чудовий захист у режимі реального часу.
- Розширені інструменти оптимізації системи.
- Швидкий VPN з необмеженим трафіком.
- Безпечний менеджер паролів.

Недоліки:

- Без брандмауера.
- Часті додаткові продажі.

Антивірусний сканер TotalAV швидкий і надійний, з майже ідеальним рівнем виявлення шкідливого програмного забезпечення. Сканер виявив більшість тестових шкідливих програм, від вірусів і троянів до програм-вимагачів. Подібно до Bitdefender, він не мав великого впливу на продуктивність системи під час сканування, але це також означає, що він виконується трохи довше, ніж трохи ресурсомісткіший Norton. Тим не менш, він видавав значно більше хибних прапорців, ніж Norton і Bitdefender.

WebShield від TotalAV запобігає відвідуванню небезпечних вебсайтів. Під час моїх тестів він блокував більшість фішингових вебсайтів, які я намагався відвідати. Ви також отримуєте доступ до Total Browser, безпечного браузер, який блокує рекламу та небезпечні сайти. Він навіть повідомляє вам, чи була

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

сторінка, яку ви відвідуєте, коли-небудь задіяна у витоку даних.

Крім того, TotalAV спрощує рутинне обслуговування, об'єднуючи їх в одне сканування. Це включає антивірусне сканування, сканування файлів cookie відстеження та очищення диска. Я ціную кількість часу, який це економить.

Мені особливо подобається оптимізатор продуктивності TotalAV. Повне сканування на віруси автоматично перевірятиме наявність небажаного програмного забезпечення для очищення та налаштувань для виправлення, але ви також можете сканувати виключно на наявність проблем із продуктивністю. Він очистив більше місця на моєму комп'ютері, ніж більшість інших конкурентів.

VPN від TotalAV надійний для щоденних завдань, що потребують підключення до локальних серверів. Він безпечний, працює з популярними стрімінговими сайтами та підтримує пристойну швидкість, але підключення до віддалених серверів значно знизило швидкість мого інтернету.

Менеджер паролів досить непоганий. Total Password може безпечно зберігати ваші паролі та іншу конфіденційну інформацію в зашифрованому просторі. Ви отримуєте всі стандартні функції, такі як автоматичне збереження та автоматичне заповнення, налаштовуваний генератор паролів, синхронізацію між пристроями та багато іншого. Він показав себе дуже добре в моїх тестах, єдина моя скарга полягає в тому, що йому бракує спільного доступу до паролів. Проте, він містить деякі досить унікальні функції, такі як Secure Me – інструмент, який дозволяє вам віддалено виходити з облікових записів на всіх пристроях.

TotalAV сумісний з усіма основними пристроями та операційними системами, включаючи Chromebook. Мені подобається, що це один з небагатьох антивірусів, який працює з планшетами Kindle Fire. Єдиним недоліком є те, що я не зміг знайти інформацію про внутрішні аудити безпеки, як це було з Norton чи Bitdefender. Однак він регулює ваші дані відповідно до GDPR, що є однією з переваг.

Мій улюблений план – TotalAV Total Security, який охоплює до 8 пристроїв і коштує 2130 гривень на рік. Мені подобається, що він включає VPN,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

преміум-менеджер паролів і чудовий блокувальник реклами, окрім усіх інших функцій, згаданих вище. Якщо у вас обмежений бюджет, TotalAV Premium – це хороший пакет початкового рівня для користувачів, які хочуть захистити до 3 пристроїв, і він коштує 830 гривень на рік. Усі плани мають 30-денну гарантію повернення грошей.

TotalAV має потужний антивірусний механізм і хороший набір функцій у зручній панелі керування – я рекомендую TotalAV новачкам, яким просто потрібне щось безпечне, надійне та просте у використанні. Усі пакети TotalAV мають широкий спектр функцій і розроблені для максимальної зручності використання. Крім того, на всі покупки TotalAV надається 30-денна гарантія повернення грошей.

Bitdefender – найкращий для легкого сканування + безліч додаткових функцій

Bitdefender має високотехнологічний антивірусний механізм – він використовує величезну базу даних шкідливих програм, машинне навчання та штучний інтелект для виявлення та захисту від шкідливих програм ефективніше, ніж майже будь-який конкурент на ринку.

Переваги:

- Відмінні показники виявлення шкідливих програм.
- Низький вплив на систему.
- Безпечний браузер для онлайн-платежів.
- Захист веб-камери та мікрофона.

Недоліки:

- Обмежений VPN на більшості планів.
- Обмежені версії для Mac та iOS.

У моїх тестах Bitdefender знайшов та видалив усі шкідливі загрози з моєї системи. А оскільки всі сканування на наявність шкідливого програмного забезпечення відбуваються на хмарному сервері Bitdefender, на ваш пристрій не створюється жодного навантаження. Фактично, коли я протестував Bitdefender,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

середнє використання процесора становило 30% під час повного сканування системи та менше 1% під час роботи у фоновому режимі. Я також був радий бачити, що він майже не видавав жодних хибних прапорців.

Але Bitdefender – це не просто сканер шкідливих програм, це один із найповніших пакетів безпеки, що забезпечує найкращий захист як для комп'ютерів, так і для мобільних пристроїв, завдяки таким функціям, як:

- Захист веб-сторінок.
- Сканер вразливостей.
- Системний оптимізатор.
- VPN (200 МБ/щодня для більшості тарифних планів).
- Батьківський контроль.
- Менеджер паролів.
- Захист веб-камери.
- Захист від програм-вимагачів.
- Захист від крадіжки особистих даних.
- І багато іншого...

Веб-захист Bitdefender чудовий – вбудований захист від фішингу блокував переважну більшість фішингових сайтів під час мого тестування, а також є блокувальник відстеження. Я великий шанувальник Safepay, який є безпечним, зашифрованим вікном браузера для онлайн-банкінгу та покупок. Деякі плани навіть постачаються зі Scam Copilot, інструментом штучного інтелекту, який попереджає вас про нові шахрайські схеми, надає чат-бота, який може виявляти шахрайські схеми, тощо. Мені особливо подобається багаторівневий захист Bitdefender від програм-вимагачів, який додає шар захисту даних до ваших важливих файлів, щоб їх не можна було зашифрувати під час атаки програми-вимагача.

Так само сканер вразливостей шукає невикористані оновлення Windows, застарілі програми та слабкі місця у вашій мережі Wi-Fi. Коли Bitdefender знаходить вразливість, він призначає їй рівень ризику та пропонує поради щодо

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

подальших дій. Наприклад, у мене на комп'ютері була застаріла версія Opera, і Bitdefender дозволив мені завантажити найновішу версію або видалити її.

VPN від Bitdefender також є одним з найкращих на ринку, забезпечуючи блискавично швидкий доступ до зашифрованих серверів по всьому світу. На жаль, на відміну від VPN від Norton, VPN від Bitdefender обмежує ваше щоденне використання даних на всіх планах, окрім найдорожчих.

Bitdefender пропонує кілька недорогих пакетів для всіх основних операційних систем, включаючи Windows, Mac, iOS, Android та ChromeOS. Він також відповідає низкою регуляторів даних, зокрема SOC2, HIPAA та ISO 27001. Bitdefender Antivirus Plus, ціна якого становить 1530 гривень на рік, має багато преміум-функцій Bitdefender (за винятком захисту веб-камери, батьківського контролю та менеджера паролів). Bitdefender Total Security охоплює до 5 пристроїв і додає батьківський контроль, брандмауер, інструменти оптимізації тощо за 2400 гривень на рік.

Щоб отримати VPN без обмеження трафіку, вам знадобиться Premium Security, який також включає Scam Copilot, блокувальник реклами та багато іншого. Вартість – 2830 гривень на рік.

Bitdefender пропонує хмарне сканування та безліч інструментів кібербезпеки за нижчою ціною, ніж більшість конкурентів. Я рекомендую Bitdefender, якщо ви шукаєте комплексний хмарний пакет кібербезпеки з додатковими функціями, такими як VPN, батьківський контроль та менеджер паролів. Ви можете випробувати Bitdefender без ризику з 30-денною гарантією повернення грошей.

McAfee – найкращий засіб для онлайн-безпеки (+ чудово підходить для сімей)

McAfee має широкий спектр функцій інтернет-безпеки, включаючи захист від шкідливих програм, захист від фішингу, менеджер паролів, VPN, а також моніторинг і покриття крадіжки особистих даних. Усі його функції прості у використанні та працюють саме так, як заявлено. Окрім покриття мобільних

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

пристроїв, він навіть має додаток для Chromebook.

Переваги:

- Надійний захист у режимі реального часу.
- Налаштовувані сканування.
- Очищення персональних даних.
- Необмежена кількість пристроїв у більшості тарифних планів.

Недоліки:

- Уповільнення роботи системи під час сканування.
- Базовий брандмауер.

Його чудовий захист від вірусів робить McAfee чудовим вибором – він показав ідеальний 100% рівень виявлення всіх зразків шкідливого програмного забезпечення під час моїх тестів. McAfee виявляв, блокував та видаляв як прості, так і складні загрози, включаючи віруси, трояни, шпигунські програми, кейлогери та руткіти. Хоча він видавав досить низьку кількість хибних прапорців, сканування було повільним порівняно з Norton та TotalAV, зі значно більшим впливом на мою систему. Я міг переглядати Інтернет, використовувати Microsoft Office та дивитися відео на YouTube, але не міг грати в ігри, що ресурсомістко використовують процесор.

Його антифішинговий захист також чудовий, він запобігає доступу до відомих фішингових сайтів та інших небезпечних веб-сторінок. Він визначив переважну більшість ризикованих сайтів, перевершуючи вбудований захист таких браузерів, як Chrome, Firefox та більшість конкуруючих антивірусів.

Ви також можете захистити свій телефон за допомогою мобільних додатків McAfee. Версії для iOS та Android містять VPN, веб-захист і сканер, який попереджає вас, якщо ви намагаєтеся підключитися до небезпечних мереж Wi-Fi. Є також унікальні функції, такі як захист від шахрайства, який попереджає вас про небезпечні посилання в електронних листах, текстових повідомленнях, соціальних мережах та веббраузерах.

Батьківський контроль McAfee також є одним з найкращих на ринку –

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

окрім блокування небажаного та невідповідного контенту й програм, вони оснащені розширеним відстеженням місцезнаходження, що дозволяє відстежувати пристрій вашої дитини майже з ідеальною точністю (ця функція працює набагато краще, ніж інструменти Google або Apple для визначення місцезнаходження пристроїв).

Тарифні плани McAfee, вартість яких починається лише від 1740 гривень на рік, пропонують чудову цінність. Тарифний план Essential (1740 гривень на рік) передбачає покриття до 5 пристроїв, а сімейний пакет Premium (3050 гривень на рік) додає покриття засобом видалення брокера даних для необмеженої кількості пристроїв та батьківський контроль. Також є плани Advanced (3920 гривень на рік) та Ultimate (8700 гривень на рік), які додають покриття від крадіжки особистих даних на суму до 2 мільйонів доларів США та інші засоби захисту – на всі плани поширюється 30-денна гарантія повернення грошей.

McAfee пропонує чудовий захист в Інтернеті. Його антифішинговий та Wi-Fi захист надзвичайно хороший, він блокує всі ризиковані сайти та пропонує централізований контроль безпеки з мобільного додатку McAfee, а його батьківський контроль є одним з найкращих на ринку. Пакети McAfee включають 30-денну гарантію повернення грошей без зобов'язань.

Intego – найкращий варіант для комплексного захисту Mac

Intego – найкращий антивірус для macOS. Більшість антивірусних брендів зосереджені лише на захисті ПК з Windows, але Mac також потребує захисту. Усі антивірусні пакети Intego для Mac забезпечують високоякісні інструменти інтернет-безпеки та оптимізації для macOS, значно покращуючи вбудовані функції безпеки Apple.

Переваги:

- Інструменти оптимізації для Mac.
- Розширені параметри резервного копіювання Mac.
- Параметри безпеки мережі.

Недоліки:

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

- Потрібно 6 окремих програм.
- Немає багатоплатформного покриття.

Антивірусний движок Intego показав ідеальний рівень виявлення всіх тестових шкідливих програм (як для macOS, так і для ПК). А його сканування швидке – понад 300 000 файлів сканується менш ніж за годину. Мені дуже подобається, що наступні сканування займають лише кілька хвилин завдяки системі кешування файлів Intego, яка ігнорує вже перевірені файли (Norton використовує ту саму технологію для пропуску раніше перевірених файлів). Він має мінімальний вплив на систему та не має хибних прапорців.

Intego має деякі чудові функції, такі як:

- Захист від шкідливих програм у режимі реального часу.
- Інструменти для оптимізації та очищення Mac.
- Розширені параметри резервного копіювання Mac.
- Варіанти безпеки мережі.
- Батьківський контроль.

Мені також дуже подобається налаштовуваний брандмауер Intego – він контролює як вхідні, так і вихідні мережеві з'єднання та попереджає вас про програми, які намагаються підключитися до Інтернету. Брандмауер також автоматично налаштовує свої параметри залежно від вашого середовища – чи ви вдома, на роботі, чи використовуєте загальнодоступну мережу Wi-Fi.

Intego має цікаві додаткові функції – мені подобається, як ви можете підключити зовнішній диск або пристрій iOS до вашого Mac та просканувати його за допомогою антивірусного сканера Intego. Це позбавляє вас необхідності отримувати кілька антивірусних пакетів для захисту ваших пристроїв iOS.

Тарифний план Intego Mac Premium Bundle чудовий – він містить усі найкращі функції Intego, включаючи інструменти оптимізації диска та батьківський контроль. Також є план Mac Internet Security, але в ньому відсутні чудові інструменти оптимізації Intego. Починаючи з 870 гривень на рік, Intego трохи дорожчий за конкурентів, але знову ж таки, більшість конкурентів

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

пропонують лише базові програми для користувачів Mac. Усі плани розраховані на використання до 5 комп'ютерів Mac і підкріплені 30-денною гарантією повернення грошей.

Intego також має продукт для Windows, антивірус для Windows. Він виявив 100% зразків шкідливого програмного забезпечення, які я використовував для тестування. Ви також отримуєте VPN, інструменти оптимізації та багато іншого. Хоча він не такий багатофункціональний, як найкращі антивіруси для Windows, він все одно досить хороший.

Intego – найкращий антивірус для macOS у 2026 році (також є досить надійна версія для Windows). Він пропонує чудовий захист від шкідливого програмного забезпечення на базі Mac, значно покращує та вдосконалює вже вбудовані інструменти безпеки та оптимізації пристроїв Apple, а також постачається з 30-денною гарантією повернення грошей без ризику, тож ви зможете переконатися, чи пропонує він найкращий захист для вас.

Panda Dome – найкращий варіант за гнучким ціноутворенням

Panda пропонує розширений антивірусний сканер, простий у використанні інтерфейс та гнучке ціноутворення. Його сканер шкідливих програм добре показав себе під час тестування. Було небагато хибних спрацьовувань, і хоча сканер виявив лише 95% шкідливих програм, захист у режимі реального часу все ж зміг заблокувати кожную загрозу, яку я намагався додати на свій комп'ютер. На жаль, кількість хибних прапорців була значно вищою, ніж у Norton та Bitdefender, а повне сканування тривало до 3,5 годин.

Переваги:

- Сканер зовнішніх пристроїв.
- Рятувальний комплект.
- Захист від програм-вимагачів.

Недоліки:

- Обмежений VPN на більшості планів.
- Захист веб-сторінок не дуже хороший.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

Panda постачається з багатьма додатковими функціями, зокрема:

- Веб-захист.
- Інструменти оптимізації.
- VPN.
- Брандмауер.
- Батьківський контроль.
- Менеджер паролів.
- Моніторинг темної мережі.
- Шифрувальник файлів.
- Rescue Kit (безкоштовний завантажувальний антивірус).

Додаткові функції не такі обширні чи вичерпні, як у Norton. Інструменти оптимізації ефективні – швидке одномінульне сканування очистило мою систему від 1,2 ГБ непотрібних даних, а автоматичне оновлення – зручна функція.

Однак деякі додаткові інструменти не досконалі. Наприклад, VPN має обмежені ліміти даних і не дозволяє вибирати сервер, якщо ви не оберете найдорожчий план. Аналогічно, функція автоматичного заповнення менеджера паролів працює добре, але їй бракує багатьох функцій, які зазвичай є в окремих менеджерах паролів.

Мені дуже подобається, що Panda пропонує так багато планів, дозволяючи вам вибрати саме ті функції та ліцензії, які вам потрібні. Є навіть непоганий безкоштовний план. Panda Free включає захист від вірусів у режимі реального часу для Windows, сканер програм для Android, Rescue Kit та VPN (обмежено 1 сервером та 150 МБ на день). Просто будьте готові до регулярних сповіщень про необхідність оновлення, якщо ви оберете цей план.

«Essential», найбазовіший платний план (660 грн./рік), додає брандмауер, ручні перевірки наявності темного веб-вузла та багато іншого. «Advanced» коштує 790 грн./рік і додає захист від програм-вимагачів, тоді як «Complete» (1180 грн./рік) надає вам менеджер паролів та різні інструменти оптимізації. «Panda Dome Premium» додає VPN з необмеженим трафіком, автоматизований

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

моніторинг темного веб-вузла та надає цілодобову підтримку клієнтів за 1830 грн. Усі плани мають 30-денну гарантію повернення грошей і дозволяють вам вибрати, скільки пристроїв ви хочете захистити.

Panda пропонує гнучкі плани та багато додаткових функцій, включаючи розширений захист від програм-вимагачів, Rescue Kit для порятунку заражених шкідливим програмним забезпеченням ПК, менеджер паролів, батьківський контроль, а також шифрувальник і шредер файлів. Усі преміум-плани Panda підкріплені 30-денною гарантією повернення грошей.

Avast – чудово підходить для початківців (з гарним безкоштовним планом)

Avast пропонує чудовий захист від шкідливого програмного забезпечення, зручний інтерфейс для початківців та надійний безкоштовний план. Його сканер досяг ідеального 100% рівня виявлення в моїх тестах, блокуючи всі віруси, програми-вимагачі, шпигунські програми тощо. Захист у режимі реального часу був таким же потужним, запобігаючи загрозам, перш ніж вони встигли виконатися. Однак повне сканування тривало близько 1 години, і я помітив незначні уповільнення під час виконання ресурсомістких завдань.

Переваги:

- Ідеальне виявлення шкідливих програм.
- Чудова безкоштовна версія.
- Інтуїтивно зрозумілі програми.

Недоліки:

- Обмежені функції VPN.
- Базовий моніторинг порушень.

Avast постачається з багатьма додатковими функціями, зокрема:

- Веб-захист.
- Брандмауер.
- VPN (з обмеженнями даних).
- Інструменти оптимізації.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

- Моніторинг витоків даних.
- Захист від крадіжки особистих даних (лише для США).
- Рятувальний диск.
- Безпечний браузер.
- Щит веб-камери.
- Пісочниця.

Додаткові функції непогані як на ціну, хоча й не такі досконалі, як у Norton. VPN забезпечує хорошу швидкість, але обмежує дані 5 ГБ/тиждень на тарифних планах нижчого рівня та не має роздільного тунелювання на комп'ютері. Інструменти оптимізації ефективно видаляли непотрібні дані та оновлювали драйвери в моїх тестах, швидко звільняючи місце.

Менеджер паролів Avast генерує, зберігає та автоматично заповнює паролі безпечно, хоча йому бракує розширених функцій, таких як спільний доступ до паролів, що є в усіх провідних автономних менеджерах паролів. Хоча Avast пропонує батьківський контроль, це абсолютно окремий продукт, який не входить до жодного з антивірусних планів.

Моніторинг порушень охоплює до 5 електронних листів (або 30 у сімейних планах), з корисними сповіщеннями та чіткими інструкціями щодо вирішення проблем. Проте, ця функція все ще дуже проста порівняно з Norton Privacy Monitor, яка також перевіряє пов'язану інформацію, таку як ваша фізична адреса, дата народження, теги гравця тощо.

Тарифні плани Avast дещо заплутані, але доступні. Безкоштовний Avast One Basic включає сканування ядра, веб-захист та обмежений VPN. Premium Security (1740 гривень/рік) додає розширений брандмауер, захист веб-камери та охоплює до 10 пристроїв. Avast One Gold (3650 гривень/рік) включає VPN з необмеженим трафіком, повну оптимізацію та підтримує до 30 пристроїв, тоді як Avast One Platinum (5220 гривень/рік (лише для США) пропонує страхування від крадіжки особистих даних на суму до 2 мільйонів доларів. Усі платні плани мають 30-денну гарантію повернення грошей.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

Avast забезпечує потужний антивірусний захист зі зручним дизайном, чудовим безкоштовним рівнем та корисними додатковими функціями, такими як VPN, інструменти оптимізації, моніторинг порушень та менеджер паролів. Батьківський контроль доступний для окремої покупки. Ви можете спробувати Avast без ризику з 30-денною гарантією повернення грошей.

Avira Prime – найкращий для оптимізації системи

Avira має один із найпотужніших антивірусних движків – він постійно демонстрував 100% рівень виявлення під час усіх моїх тестів, і це так добре, що технологія захисту від шкідливого програмного забезпечення Avira була ліцензована кільком конкурентам, включаючи TotalAV. Вона працює на більшості операційних систем, включаючи ChromeOS.

Переваги:

- Відмінне виявлення шкідливих програм.
- Дуже хороші системні інструменти.
- Підсилювач гри.

Недоліки:

- Ліміт VPN 1 ГБ/місяць (більшість тарифних планів).
- Немає батьківського контролю.

Avira Prime також має багато справді хороших додаткових функцій, таких як:

- Оптимізація конфіденційності.
- Оптимізація системи.
- VPN.
- Менеджер паролів.

Інструменти оптимізації системи Avira є одними з найкращих на ринку. Хоча багато антивірусів містять інструменти налаштування, розроблені для забезпечення безперебійної роботи вашого пристрою та звільнення місця на жорсткому диску, Avira постачається з одними з найсучасніших інструментів налаштування та очищення, що входять до комплекту антивіруса, зокрема:

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

– Оптимізатор запуску. Зекономив цілих 2 хвилини від часу запуску мого ПК!

– Game Booster. Автоматично розподіляє системні ресурси та зупиняє фонові процеси для покращення продуктивності системи.

– Очисник непотрібних файлів. Видаляє дублікати, невикористовувані файли та деякі кешовані файли.

Avira Prime – особливо хороший антивірус, якщо у вас старий або повільний ПК, на якому часто мало місця на жорсткому диску. Його інструмент оптимізації одним клацанням миші зміг видалити набагато більше сміття, ніж багато конкурентів, а Game Booster насправді мав помітний ефект у моїх тестах. Також є пошук дублікатів файлів, оптимізоване оновлення драйверів тощо. А оскільки антивірусний движок Avira повністю працює в хмарі, він не уповільнюватиме ваші пристрої, як це роблять багато інших конкурентів.

За ціною 2610 гривень на рік Avira Prime – це гарна пропозиція, але вона дорожча за деякі найкращі антивірусні пакети. Avira має дешевші плани, зокрема Internet Security (1530 гривень на рік), але Prime – єдиний пакет, який включає розширену оптимізацію системи, VPN з необмеженим трафіком та преміум-мобільні додатки.

Безкоштовна версія Avira є одним із найкращих безкоштовних антивірусів на ринку – якщо ви не хочете витратити гроші прямо зараз, Avira Free може захистити ваш пристрій за допомогою захисту в режимі реального часу, захисту від програм-вимагачів і навіть безкоштовної версії VPN від Avira.

Avira захищає користувачів за допомогою легкого хмарного сканера, а також пропонує чудові інструменти для оптимізації системи. Він також має VPN, менеджер паролів і покриття до 5 пристроїв на всіх операційних системах. Ви можете випробувати Avira без ризику з 60-денною гарантією повернення грошей.

Malwarebytes – найкращий засіб для базового захисту

Malwarebytes – це простий, легкий у використанні антивірус, який пропонує хороший захист від вірусів для всіх операційних систем і пристроїв,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

включаючи Chromebook.

Переваги:

- Гарний захист від експлойтів.
- VPN з необмеженим трафіком.
- Безпечний браузер.

Недоліки:

- Немає окремого брандмауера.
- Блокувальник реклами не може блокувати відео.
- Захист у режимі реального часу має проблеми з програмами-вимагачами.

Під час моїх тестів розширений сканер шкідливих програм Malwarebytes виявив близько 95% тестового шкідливого програмного забезпечення, що досить добре (але не так добре, як у провідних конкурентів, таких як Norton).

Malwarebytes також пропонує VPN з необмеженим обсягом даних, серверами в 36 країнах і пристойною швидкістю. Однак VPN від Malwarebytes не є найкращим вибором для потокового передавання відео або завантаження торрентів (якщо ви шукаєте хороший VPN для потокового передавання відео та завантаження торрентів, я рекомендую ExpressVPN).

Тим не менш, я великий шанувальник веб-захисту Malwarebytes, який успішно виявляв і блокував більшість фішингових сайтів, які я намагався відвідати під час тестування, а також рекламу, трекери та інші потенційні шахрайські програми. Блокувальник реклами мав проблеми з відеорекламою, але мені подобається, що розширення надає запис про все, що воно блокує.

Мені дуже подобається захист від експлойтів Malwarebytes. Він досить налаштовуваний і допомагає Malwarebytes бути ефективним проти експлойтів нульового дня, а також шкідливого програмного забезпечення. Malwarebytes також має кілька хороших засобів захисту від крадіжки особистих даних у своїх планах Identity. Є моніторинг соціальних мереж, моніторинг кредитної історії для клієнтів зі США та багато іншого.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

На жаль, Malwarebytes не має додаткових функцій. У нього немає брандмауера, а інструменти батьківського контролю та оптимізації обмежені. Тим не менш, це хороший вибір для користувачів, які шукають гідну антивірусну програму, яку можна встановити та забути про неї. Вартість Malwarebytes починається від 1740 гривень на рік.

Malwarebytes – це мінімалістична антивірусна програма, яка пропонує ефективне сканування на наявність шкідливих програм та веб-захист. Вона забезпечує надійний VPN, зручний інтерфейс та захист від крадіжки особистих даних (як додатковий компонент). Malwarebytes – це надійний вибір для тих, хто шукає базовий захист, і вона постачається з 60-денною гарантією повернення грошей.

Trend Micro – найкращий для безпечного перегляду веб-сторінок

Trend Micro має непоганий антивірусний механізм, хороші діагностичні інструменти та чудове розширення для веббраузера, яке блокує онлайн-шахрайство та небезпечні вебсайти.

Переваги:

- Захист від програм-вимагачів.
- Захист конфіденційності в соціальних мережах.
- Захист онлайн-банкінгу.

Недоліки:

- Немає окремого брандмауера.
- Інструменти оптимізації могли б бути кращими.

Антивірусний сканер отримав досить хороші результати в моєму тестуванні, виявивши більшість вірусів, троянів, програм-вимагачів та шпигунських програм у моїй системі, хоча він не набрав таких високих балів, як провідні конкуренти, такі як Norton. Trend Micro також пропонує кілька налаштувань сканування, що дозволяють користувачам налаштовувати захист від шкідливих програм.

Під час тестування Trend Micro виявив більше фішингових веб-сайтів, ніж

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

Chrome, Firefox або Safari. Крім того, він виявив шахрайські посилання, небезпечний контент, шкідливий код і навіть дезінформацію, а також заблокував рекламу та просканував мою історію переглядів на наявність будь-яких небезпечних сайтів, які я міг відвідати.

Починаючи з 1740 гривень на рік, Trend Micro пропонує кілька планів на вибір, але найкращим вибором є Trend Micro Premium Security Suite, який коштує 2180 гривень на рік. Найкомплексніший план, Premium Security Suite, коштує 2390 гривень на рік, охоплює до 10 пристроїв і додає різні засоби захисту від крадіжки особистих даних і повнофункціональний VPN.

Trend Micro пропонує потужний набір функцій захисту від шкідливих програм та інтернет-безпеки для користувачів Windows, Mac, Android, iOS та Chromebook. Він особливо добре захищає веб-сторінки, а його розширення для браузера допоможе вам уникнути шкідливих веб-сайтів, шахрайських посилань та підозрілого контенту. На всі плани Trend Micro надається 30-денна гарантія повернення грошей.

MacKeeper – інтуїтивно зрозумілий та багатофункціональний антивірус для Mac.

MacKeeper – одна з небагатьох антивірусних програм, спеціально розроблених для Mac. Вона має хороший захист від шкідливого програмного забезпечення, низку функцій безпеки та конфіденційності, що базуються на вбудованих засобах захисту Apple, та дуже інтуїтивно зрозумілий додаток для macOS.

Переваги:

- Гарний захист від шкідливих програм для Mac.
- Інструменти для очищення та оптимізації Mac.

Недоліки:

- Немає захисту від фітінгу.
- Без брандмауера.

Я протестував MacKeeper на своєму MacBook Pro (з чіпом M2), і він

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

виявив 99% файлів шкідливого програмного забезпечення, специфічних для Mac, що подібно до найкращих антивірусів для Mac, включаючи Intego та Norton. Його інструменти очищення та оптимізації Mac видалили понад 7 ГБ непотрібних файлів та дублікатів з мого MacBook Pro (мені також дуже подобається, що MacKeeper пропонує опцію видалення небажаних вкладень електронної пошти, чого я не бачив у жодному іншому антивірусі).

VPN від MacKeeper також дуже хороший – безпечний, швидкий і сумісний з більшістю стрімінгових сайтів. Єдине, що мені не подобається в цьому VPN, це відсутність прозорості щодо політики відмови від ведення журналів. Я хотів би, щоб MacKeeper надавав чіткішу інформацію про те, як він керує даними користувачів.

З іншого боку, MacKeeper не має захисту від фішингу, що є важливою функцією безпеки для антивіруса у 2026 році. Він також не має брандмауера чи батьківського контролю, які входять до комплекту Intego.

MacKeeper пропонує кілька планів, вартість яких починається від 2490 гривень на рік. Усі плани однакові; єдина різниця між ними полягає в тривалості підписки та кількості комп'ютерів Mac, на які поширюється підписка (1–3).

MacKeeper – це хороший антивірус лише для Mac – він має майже ідеальний рівень виявлення шкідливого програмного забезпечення, включає чудові інструменти очищення системи та пропонує безпечний і швидкий VPN з необмеженим обсягом даних. Однак йому бракує захисту від фішингу, брандмауера та батьківського контролю. MacKeeper пропонує кілька платних планів і підтримує річні підписки з 30-денною гарантією повернення грошей.

Методологія тестування: критерії порівняння та ранжування

Під час оцінювання продуктів я дотримувався нашої перевіреної методології. Я використовував реальні сценарії з критеріями, що включали перевірку безпеки, швидкості, простоти використання, цінності та підтримки клієнтів. Зокрема:

– Я протестував рівень виявлення шкідливих програм та можливості

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

сканування. Я провів десятки тестів на наявність шкідливих програм, тестів захисту в реальному часі, тестів продуктивності процесора тощо. Після завершення до цього списку потрапили лише продукти, які захищали від найсучасніших загроз шкідливого програмного забезпечення. Norton показав тут найкращі результати, але інші антивіруси у цьому списку також показали хороші результати.

– Я шукав високоякісні доповнення. Більшість антивірусів пропонують додаткові функції у своїх платних антивірусних пакетах, але деякі з них по суті марні. Я протестував кожну функцію, що входить до складу продуктів у цьому списку, щоб переконатися, що вони справді корисні та ефективні. Bitdefender має широкий спектр корисних функцій, але багато інших також.

– Я перевіряв швидкість та ефективність. Найкращі антивіруси легкі та працюють безперебійно – навіть на старіших або повільніших комп'ютерах. Я протестував та виміряв, наскільки швидко та ефективно працював кожен антивірус у цьому списку, і надав додаткові бали тим, які не спричинили жодного уповільнення.

– Я перевіряв підтримку кількох платформ. Найкращі антивіруси сумісні з більшістю операційних систем, включаючи менш популярні, такі як ChromeOS або FireOS. Хоча не всі мої найкращі варіанти підтримують усі платформи, більшість антивірусів, які я протестував, бездоганно працювали на кількох операційних системах.

– Я оцінив цінність кожного продукту. Антивірусне програмне забезпечення може бути великою інвестицією. Я врахував усі відповідні фактори, такі як захист веб-сторінок та перегляду веб-сторінок, а також кількість пристроїв, які охоплюються. Усі ці найкращі антивіруси пропонують чудову цінність.

Як вибрати найкращий антивірус для вашої операційної системи

Вибір найкращого антивіруса для вашої операційної системи вимагає певного планування. Щоб переконатися, що ви обрали той, який вам підходить,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

вам слід:

– Крок 1. Визначте конкретні потреби вашої операційної системи. Усім операційним системам потрібен антивірус для захисту від загроз, але не кожен антивірус працює на всіх пристроях. Знайдіть антивірус, який підтримує платформу, яку ви використовуєте. Крім того, варто розглянути продукти з надійним досвідом захисту вашого конкретного пристрою (Norton чудово працює на Windows, тоді як Intego орієнтований на користувачів Mac).

– Крок 2. Перевірте, чи має антивірус усі потрібні вам функції. Найкращі антивірусні програми пропонують різні функції, окрім базового виявлення вірусів, але кожен антивірус пропонує дещо інший набір інструментів. Подумайте, для чого ви найчастіше використовуєте свій комп'ютер, щоб визначити, які функції для вас найважливіші.

– Крок 3. Порівняйте ціну з іншими антивірусами на ринку. Ціни на антивіруси можуть значно відрізнятись залежно не лише від функцій, але й від тривалості підписки. Порівняння цін допоможе вам отримати найкращу пропозицію, не переплачуючи за функції, які вам можуть не знадобитися.

Ось наш кураторський список найкращих антивірусів для різних операційних систем та пристроїв:

– Найкращі антивіруси для Windows. Ринок величезний, але після ретельних досліджень, тестування та порівняння я рекомендую Norton як найкращий вибір для Windows.

– Найкращі антивіруси для Mac. На жаль, оскільки більшість антивірусів зосереджені на Windows, багато з них пропонують лише базові версії свого програмного забезпечення для Windows для користувачів Mac. Однак кілька антивірусів для macOS забезпечують хороший захист від шкідливого програмного забезпечення, покращують вбудований захист Apple та прості у використанні на пристроях Mac. Нашим найкращим вибором для macOS є Intego.

– Найкращі антивіруси для Android. Хоча антивірусів для Android не бракує, більшість із них недостатньо хороші, щоб повністю захистити ваш

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

пристрій. Ми визначили кілька програм, які забезпечують чудовий захист від шкідливих програм та веб-захисту, а також додаткові функції, які можуть ще більше захистити вашу онлайн-активність. Ми рекомендуємо Norton або TotalAV як найкращий антивірус для Android.

– Найкращі антивіруси для iOS. Хоча це правда, що пристрої iOS не можуть підхоплювати віруси, вони вразливі до широкого спектру інших онлайн-загроз, включаючи фішингові шахрайства, шпигунське програмне забезпечення, рекламне ПЗ та крадіжку особистих даних. Найкращі антивіруси для iOS можуть захистити ваш пристрій і дані від цих загроз. Наш антивірус №1 для iOS – це Norton.

– Найкращі антивіруси для ChromeOS. Chromebook мають унікальні функції безпеки, але все ще вразливі до онлайн-загроз. Я рекомендую користувачам Chromebook придбати антивірус, але вам потрібно вибирати ретельно, оскільки більшість антивірусів погано працюють на ChromeOS.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – відповідно до загального визначення є високорівнева мова програмування загального призначення, який орієнтований на підвищення продуктивності та читання коду.

Мова Python підтримує структурне, об'єктно-орієнтоване, функціональне й аспектно-орієнтоване програмування. Основні архітектурні риси даної мови – динамічна типізація, автоматичне керування пам'яттю, абсолютна інтроспекція, механізм обробки винятків, підтримка багатопотокових обчислень, високорівневі 24 структури даних. Підтримується розбиття програми на модулі, які в свою чергу, можуть бути об'єднанні в пакет.

За роки існування, в python було створено безліч спеціалізованих бібліотек. Для аналізу даних використовують такі:

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

psutil (python system and process utilities) – є крос-платформовою бібліотекою для отримання інформації про запущені процеси і використання системи (процесор, пам'ять, диски, мережа) в Python.

Модуль реалізує багато команд командного рядка, такі як: ps, top, lsof, netstat, ifconfig, who, df, kill, free, nice, ionice, iostat, iotop, uptime, pidof, tty, taskset, rmap.

Підтримує Linux, Windows, OSX, FreeBSD і Sun Solaris, як 32-бітові, так і 64-бітові архітектури, з версіями Python від 2.6 до 3.4 (користувачі Python 2.4 і 2.5 можуть використовувати 2.1.3 версію модуля).

Також підтримується PyPy.

psutil.cpu_percent (interval = None, percpu = False) – повертає число з крапкою, що представляє спільне використання процесора. interval – якщо більше 0.0, то повертає завантаження саме за вказаний інтервал, інакше за проміжок з імпорту модуля або останнього виклику методу percpu – якщо True, поверне список з даних для кожного CPU.

psutil.virtual_memory () – повертає іменований кортеж, статистика про використання системної пам'яті.

total – загальна кількість фізичної пам'яті;

available – доступна пам'ять для процесів;

percent – відсоток використання пам'яті, $(total - available) / total * 100$;

used – використовувана пам'ять;

free – вільна пам'ять.

Сума доступною і використовуваної може бути не дорівнює загальній пам'яті, в залежності від платформи.

psutil.swap_memory () – повертає іменований кортеж, статистика по файлу підкачки системи:

total – загальний розмір файлу підкачки;

used – використовуваний розмір файлу підкачки;

free – вільний розмір;

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

percent – відсоток заповнення, $(total - available) / total * 100$;

psutil.net_io_counters (pernic = False) – повертає іменований кортеж, статистика по вводу / виводу мережі;

bytes_sent – кількість відправлених байтів;

bytes_recv – кількість прийнятих байтів;

packets_sent – кількість відправлених байтів;

packets_recv – кількість прийнятих байтів;

errin – кількість помилок при прийманні;

errout – кількість помилок при відправці;

dropin – кількість прийшлих пакетів, які були відкинуті.

Бібліотека Pandas – це пакет для мови Python, який забезпечує швидку, гнучку і виразну структуру даних (яка називається DataFrame), розроблену для спрощення роботи зі структурованими (табличними, багатовимірними, потенційно неоднорідними) даними. Даний пакет є важливою складовою для практичного аналізу даних у реальному світі за допомогою мови програмування Python.

За допомогою пакета Statsmodel можна виконувати статистичні обчислення, які включають в себе описову статистику, логічний висновок, а також оцінку для різних статистичних моделей. Це сприяє ефективному статистичному дослідженню даних.

Matplotlib – бібліотека на мові програмування Python для візуалізації даних двовимірною 2D графікою (3D графіка також підтримується). Отримувані зображення можуть бути використані як ілюстрації в публікаціях. matplotlib написана і підтримується в основному Джоном Хантером і поширюється на умовах BSD-подібної ліцензії.

Інтерпретатор CPython – еталонна реалізація, яка підтримує більшість активних платформ, у тому числі Linux-системи (Debian, Ubuntu, Arch, Kali, CentOS, RedHat), Windows і OSX. Дана мова розповсюджується під вільною ліцензією Python Software Foundation License, яка дає можливість

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

використовувати її без обмежень в будь-яких застосунках, у тому числі в комерційних. Також існують реалізації під інтерпретатор JVM з можливістю компіляції, CLR, LLVM та інші незалежні реалізації. Проект PyPy використовує Just-in-Time компіляцію, яка значно збільшує швидкість виконання Python-застосунків. Мова програмування Python розвивається, нові версії з додаванням властивостей реалізуються приблизно один раз на два з половиною роки. Мова Python не стандартизована, але роль стандарту де-факто грає CPython, яка розробляється під прямим контролем автора мови. На даний момент Python займає одну з найвищих позицій у рейтингу мов програмування згідно з TIOBE.

Бібліотека NumPy – основний пакет наукових обчислень для Python. Переважно він створений з використанням C-розширень, що надає змогу значно пришвидшити обчислення при використанні даного пакету. Пакет містить модулі для швидкої роботи з N-вимірними масивами, складні функції, методи лінійної алгебри, швидке перетворення Фур'є, генерацію випадкових чисел. Крім очевидних наукових застосувань, пакет NumPy також може бути використаний як ефективний багатовимірний контейнер із загальними даними. Можна визначити довільні типи даних. Це дає змогу NumPy легко й швидко інтегруватися з найрізноманітнішими базами даних.

PyBrain – одна з кращих Python бібліотек для вивчення і реалізації великої кількості різноманітних алгоритмів пов'язаних з нейронними мережами. Являє собою вдалий приклад поєднання компактного синтаксису Python з гарною реалізацією великого набору різних алгоритмів з області машинного інтелекту.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

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 контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

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

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

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

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

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

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

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

За основу для створення системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи було взято антивірусну програму. Антивірусні програми використовують кілька методик виявлення шкідливих програм в різних їх поєднаннях. Основна з них – це сигнатурної детектування загроз.

Формуються геші файлів, наприклад SHA-1 або SHA-256, – при цьому під гешуванням в даному випадку розуміється перетворення вмісту файлу з використанням односпрямованої математичної функції (алгоритму криптографічного гешування), в результаті якого виходить унікальний набір шістнадцяткових символів. Односпрямованої така функція називається тому, що отримати з файлу геш дуже просто, а от відновити з гешу вихідний файл вже неможливо. Вірусна сигнатура влаштована трохи складніше: крім гешу, вона містить ще цілий ряд унікальних ознак файлу.

Сигнатури збираються в блок даних, званий вірусними базами.

Антивірусна програма досліджує файли і порівнює результати дослідження з сигнатурами, записаними в антивірусній базі. У разі збігу такий файл вважається шкідливим. Дана методика сама по собі має значний недолік: зловмиснику досить змінити структуру файлу на кілька байтів, і його сигнатура зміниться. До тих пір поки новий зразок шкідливий не потрапить в вірусну лабораторію і його сигнатура не буде доданий в бази, антивірус не зможе розпізнати і ліквідувати дану загрозу.

Крім сигнатурного детектування, більшість сучасних антивірусних програм використовують ті чи інші механізми поведінкового аналізу. Поведінковий аналіз можна віднести до різновиду імовірнісного аналізу – як це і впливає з назви

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

даного методу, антивірусна програма стежить за поведінкою додатків і, якщо воно здається їй підозрілим, блокує роботу потенційно небезпечної програми.

Один з безпечних методів дослідити поведінку програми – запустити його в так званій пісочниці (sandbox) – захищеному ізолюваному віртуальному контейнері, з якого програма не може отримати доступ до компонентів ОС і файлової системи. Якщо поведінка програми викликає у антивіруса підозри, наприклад вона виконує інжект, модифікує завантажувальний запис або змінює структуру виконуваного файлу, вона може бути визнана потенційно небезпечної або шкідливою.

Евристичний аналіз – різновид імовірнісного аналізу шкідливих програм, заснована на логічних алгоритмах, що дозволяють виявити і знешкодити потенційно небезпечне додаток. Евристичний аналіз приходить користувачам на допомогу в тих випадках, коли загрозу не вдається виявити за допомогою сигнатурного детектування.

Спрощуючи, основний принцип евристичного аналізу можна описати таким чином. Кожній функції, яку може реалізовувати програма в операційній системі, призначається якийсь умовний «рейтинг безпеки». Якісь дії програми можуть вважатися менш небезпечними, інші – більш. Якщо за сукупністю виконуваних додатком дій воно перевищує якийсь умовний «поріг безпеки», воно визнається потенційно шкідливим.

Наприклад, якщо програма працює у фоновому режимі, не має графічного інтерфейсу, послідовно опитує віддалені сервери, а потім намагається завантажити з них і запустити в системі якийсь додаток, воно з високою часткою ймовірності може виявитися троянцем-завантажувачем. Або утилітою оновлення браузера Google Chrome. У цьому, очевидно, і криється основна ахіллесова п'ята евристичного методу аналізу вірусних загроз – велика ймовірність «фолс-позитиву», помилкового спрацьовування.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

Інший метод евристичного аналізу – емуляція виконання програми. Антивірус завантажує підозріле додаток у власну буферну пам'ять, виконує розбір коду на інструкції і виконує їх по черзі, перевіряючи результат.

Евристичний аналіз застосовується з метою виявити і знешкодити загрози, ще невідомі антивірусу – тобто ті, сигнатури яких на поточний момент відсутні в вірусних базах. Звідси логічно випливає ще один недолік евристичних алгоритмів – навіть якщо невідому раніше загрозу вдається виявити, її далеко не завжди виходить відразу «вилікувати». У багатьох випадках користувачеві доводиться очікувати появи чергового оновлення вірусних баз, що містить алгоритми лікування конкретно для цієї шкідливої програми.

3.2 Розробка структурної схеми

При розробці структурної схеми програмного забезпечення для виявлення відхилень в роботі комп'ютера необхідно поставити перед собою задачу доволі чітко та просто описати загальну структуру створюваного програмного забезпечення.

Дана схема повинна включати у себе відображення зв'язків між блоками, що представляють собою схематичне зображення різних модулів системи.

Були виділені основні підсистеми, що будуть забезпечувати функціонування моделі у тому виді, як вона була запланована.

Структурна схема містить у собі наступні основні блоки:

- блок виводу інформації стосовно стану комп'ютера;
- основний блок програмного забезпечення.

Блок виводу інформації стосовно стану комп'ютера

Цей блок відповідає за вивід інформації про загальний стан комп'ютера. На екран виводиться наступна інформація:

- аналіз та виведення стану центрального процесора на екран користувача;
- відображення загальної кількості та кількості використаної RAM пам'яті за допомогою factory method;

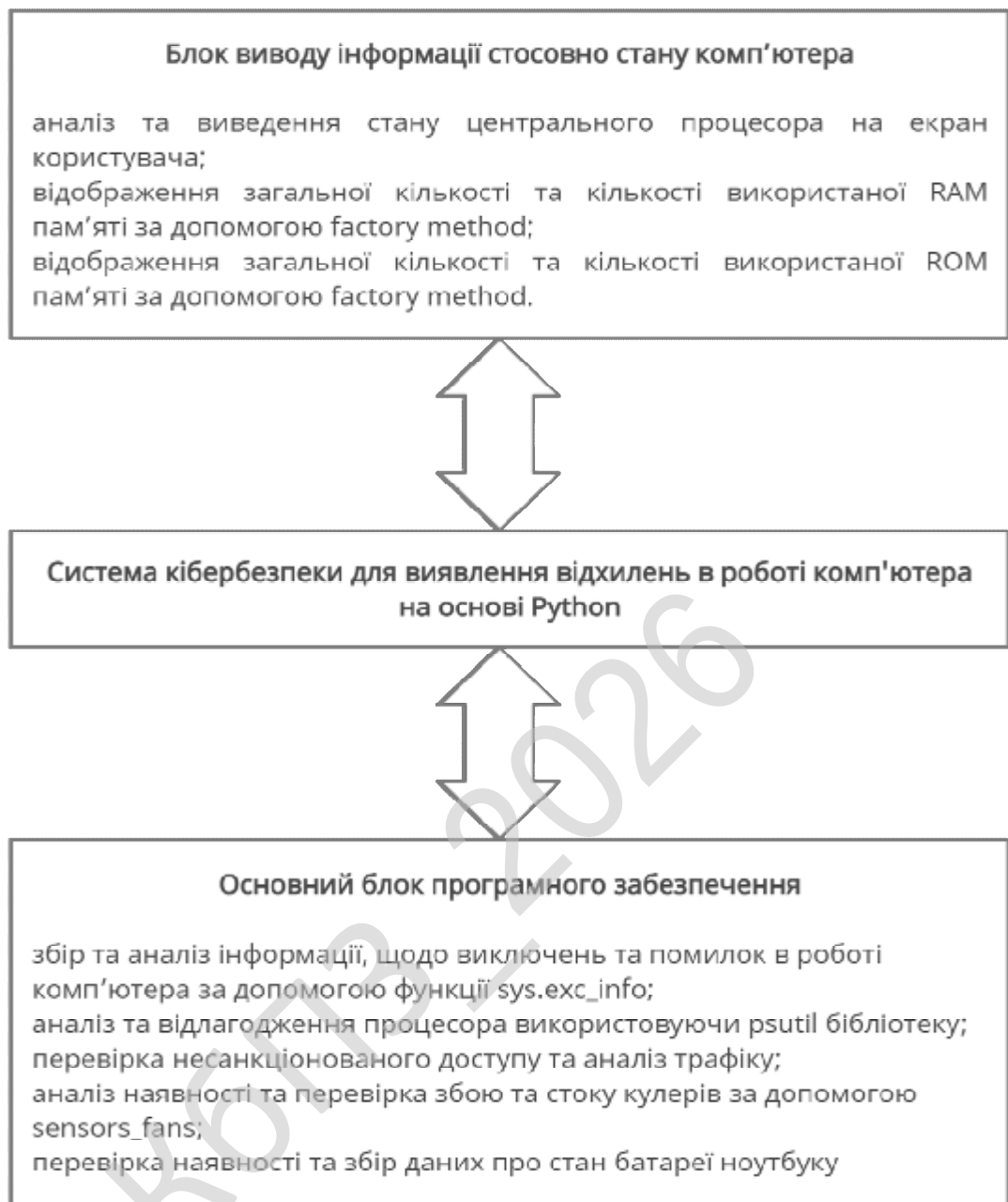


Рисунок 3.1 – Структурна схема системи

– відображення загальної кількості та кількості використаної ROM пам'яті за допомогою factory method.

При виявленні відхилень в цих показниках, буде виведено повідомлення на екран користувача, в якому буде рекомендовано вибрати “Аналіз та відлагодження процесору”.

Основний блок програмного забезпечення

Отже, необхідно організувати основні дії антивірусу. Основна програма антивірусу складається із запропонування та вибору підпрограми, кожна з яких відповідає за певний функціонал. Програмне забезпечення містить такі підпрограми:

- збір та аналіз інформації, щодо виключень та помилок в роботі комп'ютера за допомогою функції `sys.exc_info`;
- аналіз та відлагодження процесора використовуючи `psutil` бібліотеку;
- перевірка несанкціонованого доступу та аналіз трафіку;
- аналіз наявності та перевірка збою та стоку кулерів за допомогою `sensors_fans`;
- перевірка наявності та збір даних про стан батареї ноутбуку.

3.3 Розробка функціональної схеми

Функціональна схема розробленої системи зображена на рисунку 3.2. Функціональна схема розроблена для прикладу реалізації програмного забезпечення для виявлення відхилень в роботі комп'ютера.

Функціональні схеми застосовуватися у програмуванні для візуалізації алгоритмів і спрощення обчислення їх складності, у цій сфері форма створення – довільна. За такою схемою можна визначити, як здійснюються перетворення і які для цього необхідні функціональні елементи. Кожен функціональний елемент містить лише ті входи і виходи, які необхідні для його коректної роботи. Дана схема розробляється на основі структурної схеми для кожного блоку, в результаті з окремих функціональних елементів складається загальна функціональна схема об'єкту. На основі функціональної та структурної схем розробляється принципова схема.

Функціональними схемами користуються для вивчення принципу роботи виробів (у нашому випадку програмного забезпечення), а також при їх налагодженні, контролі чи ремонті. На такій схемі зображують всі функціональні

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

частини виробу та основні зв'язки між ними. Функціональні частини на схемі зображують у вигляді умовних графічних позначень згідно з вимогами державних стандартів. Дозволяється окремі функціональні частини, на яких немає умовних графічних позначень, зображувати у вигляді прямокутників, а також розкривати до рівня принципів схем.

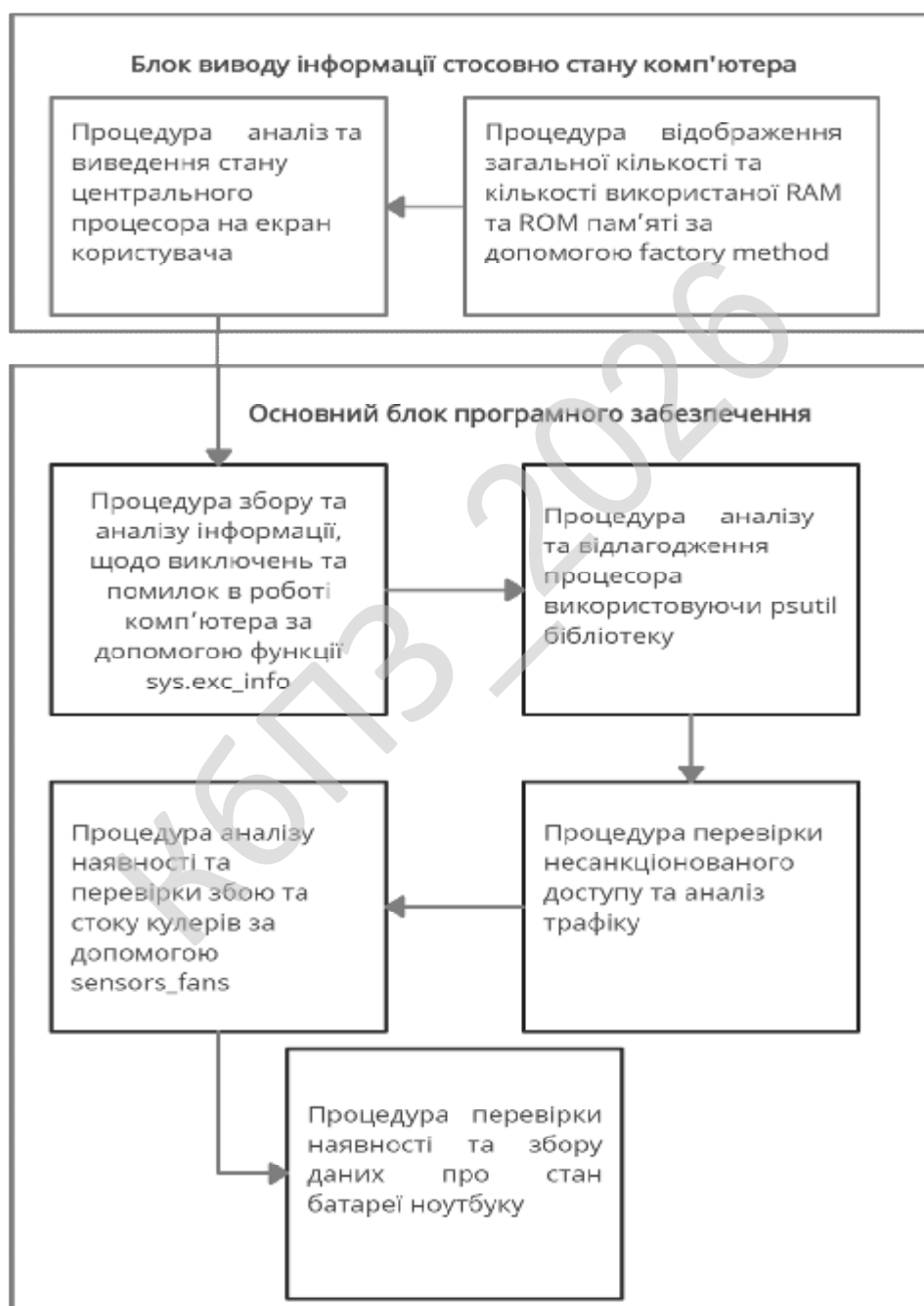


Рисунок 3.2 – Функціональна схема системи

Дозволяється об'єднувати функціональні частини в функціональні групи, які виділяють на схемі штрих-пунктирними лініями. Кожній виділеній групі присвоюють назву або умовне позначення.

На схемі повинно бути вказано:

- для кожної функціональної частини, зображеної прямокутником, її назва або умовне позначення, вписане у прямокутник;
- для кожної функціональної частини або елемента, зображеного умовним графічним позначенням позиційне позначення.

Якщо функціональна схема використовується разом з принциповою, то позиційне позначення елементів та функціональних частин на цих документах повинні бути однаковими. Перелік елементів в цьому випадку для функціональної схеми не складають, оскільки користуються даними принципової схеми.

Якщо функціональна схема розробляється самостійно (без принципової), то позиційне позначення елементів і функціональних частин вказують за загальними правилами і розробляють перелік елементів.

На функціональних схемах рекомендується вказувати поряд з графічним позначенням чи на вільному полі схеми технічні характеристики функціональних частин, діаграми, параметри сигналів тощо.

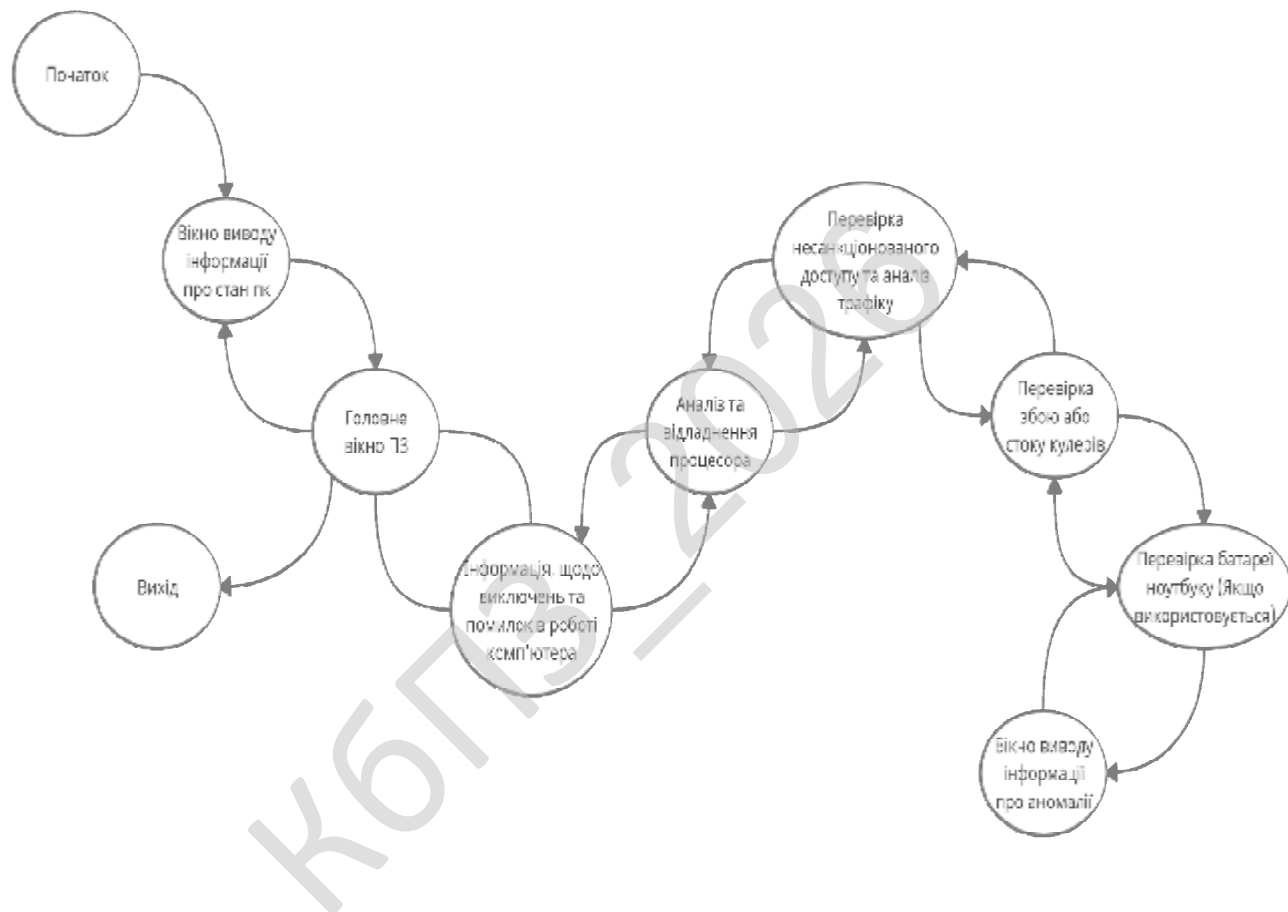
3.4 Розробка діаграми процесів

Основа побудови 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).

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

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



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

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень.

Було створено блок-схеми роботи системи. Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схема це представлення задачі для її аналізу або розв'язування за допомогою спеціальних символів (геометричних образів), які позначають такі елементи, як операції, потік, дані тощо.

Блок вхідних та вихідних даних прийнято позначати паралелограмом, блок обчислень (обробки) даних – прямокутником, блок прийняття рішень – ромбом, еліпсом – початок та кінець алгоритму.

У інформаційних технологіях функціональна схема складається з функціональних блоків, які являють собою конструктивно відособлені частини (елементи або пристрої) автоматичних систем, які виконують певні функції. Функціональні блоки на схемі позначають прямокутниками, всередині яких надписують їх найменування відповідно до функцій, що виконуються. Зв'язки між функціональними блоками (внутрішні впливи) позначаються лініями зі стрілками, які вказують напрям впливів.

Функціональні схеми можуть виконуватися в укрупненому і розгорненому вигляді. У першому випадку на схемі зображають найважливіші блоки системи і зв'язки між ними.

У другому варіанті схема відображається більш детально, що полегшує її читання та ілюструє принцип роботи.

Основні елементи схем алгоритму це термінатор, процес, рішення, зумовлений процес (підпрограма), дані та з'єднувач. Термінатор це елемент відображає вхід із зовнішнього середовища або вихід з неї (найчастіше застосування – початок і кінець програми). Всередині фігури записується відповідна дія.

Процес це виконання однієї або кількох операцій, обробка даних будь-якого виду (зміна значення даних, форми подання, розташування). Всередині фігури записують безпосередньо самі операції. Рішення це показує рішення або функцію перемикального типу з одним входом і двома або більше альтернативними виходами, з яких тільки один може бути обраний після обчислення умов, визначених всередині цього елемента.

Вхід в елемент позначається лінією, що входить зазвичай у верхню вершину елемента. Якщо виходів два чи три то зазвичай кожен вихід позначається лінією, що виходить з решти вершин (бічних і нижній). Якщо виходів більше трьох, то їх слід показувати однією лінією, що виходить з вершини (частіше нижній) елемента, яка потім розгалужується.

Відповідні результати обчислень можуть записуватися поруч з лініями, що відображають ці шляхи. Зумовлений процес (підпрограма) це символ відображає виконання процесу, що складається з однієї або кількох операцій, що визначені в іншому місці програми (у підпрограмі, модулі). Всередині символу записується назва процесу і передані в нього дані. Дані це перетворення у форму, придатну для обробки (введення) або відображення результатів обробки (виведення). Цей символ не визначає носія даних (для вказівки типу носія даних використовуються специфічні символи). З'єднувач це символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми.

Використовується для обриву лінії та продовження її в іншому місці (приклад: поділ блок-схеми, що не поміщається на листі). Відповідні сполучні символи повинні мати одне (при тому унікальне) позначення.

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 алгоритм роботи відображення інформації, щодо виключень та помилок в роботі комп'ютера, на рисунку 4.3 зображено алгоритм роботи аналізу та відлагодження процесора, на рисунку 4.4 зображено алгоритм перевірки несанкціонованого доступу та аналізу трафіку, на рисунку 4.5 зображено алгоритм перевірки збою або стоку кулерів, на рисунку 4.6 зображено алгоритм перевірки батареї ноутбуку(якщо використовується).

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.

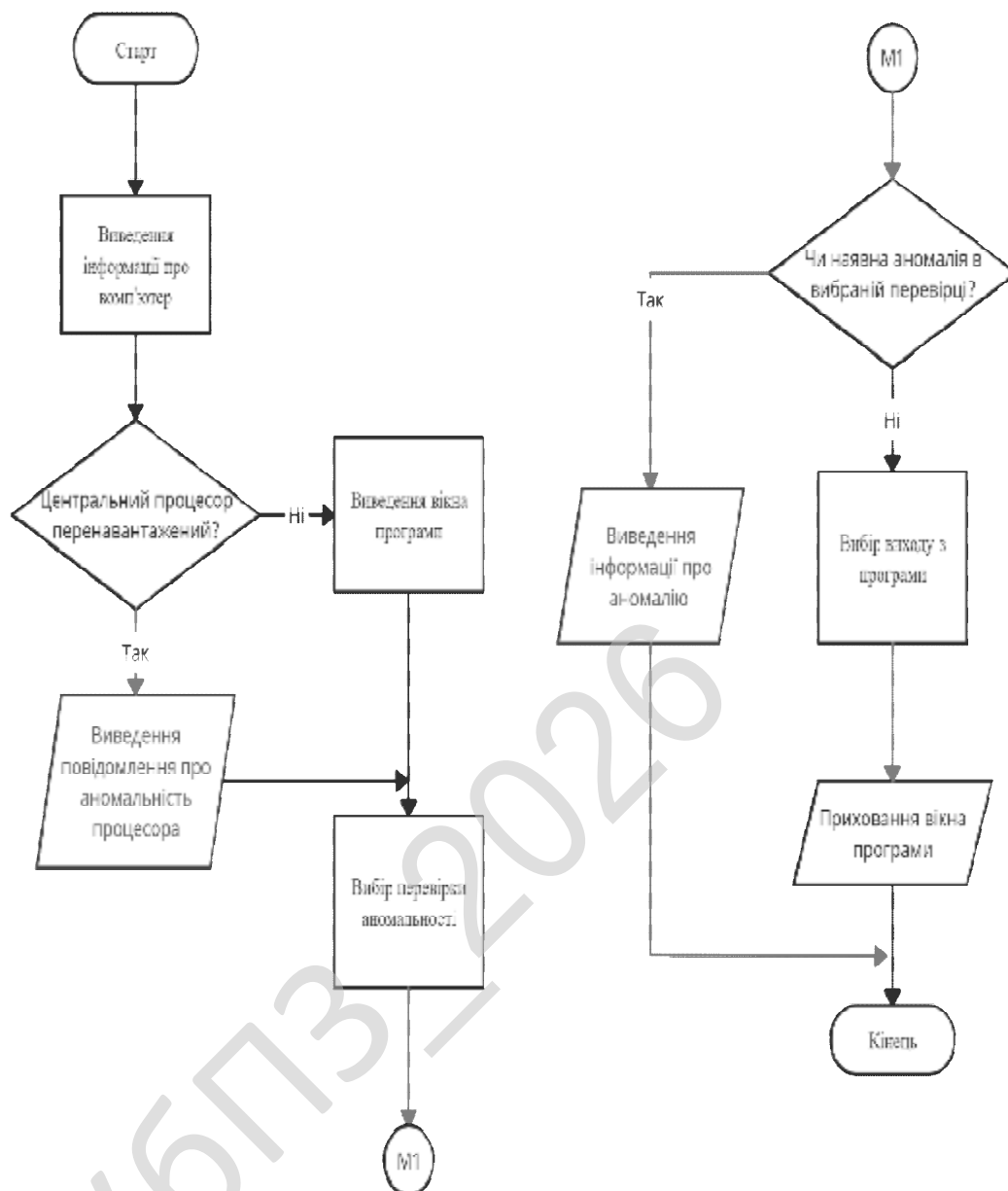


Рисунок 4.1 – Блок-схема основної програми

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

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

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

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

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

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

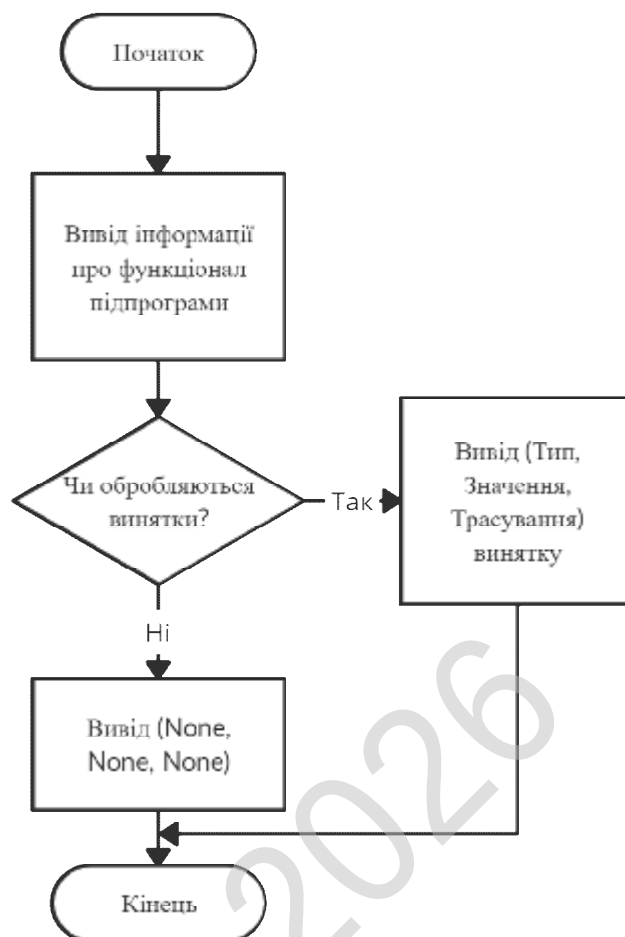


Рисунок 4.2 – Блок-схема підпрограми для виводу інформації, щодо виключень та помилок в роботі комп'ютера

Дана підпрограма повертає кортеж із трьох значень, які дають інформацію про виняток, який обробляється в даний час. Повернута інформація є специфічною як для поточного потоку, так і для поточного кадру стека. Якщо поточний фрейм стека не обробляє виняток, інформація береться з кадру стека, що викликає, або його абонента, і так далі, поки не буде знайдено фрейм стека, який обробляє виняток. Тут "обробка винятку" визначається як "виконання пропозиції за винятком". Для будь-якого кадру стека доступна лише інформація про виняток, який обробляється в даний час.

Якщо де-небудь у стеку не обробляється жоден виняток, повертається кортеж, що містить три значення None. В іншому випадку повертаються значення

(тип, значення, відстеження). Їх значення полягає у: тип отримує тип обробленого винятку (підклас BaseException); значення отримує екземпляр винятку (екземпляр типу виключення); traceback отримує об'єкт traceback, який інкапсулює стек викликів у точці, де спочатку сталося виняток.

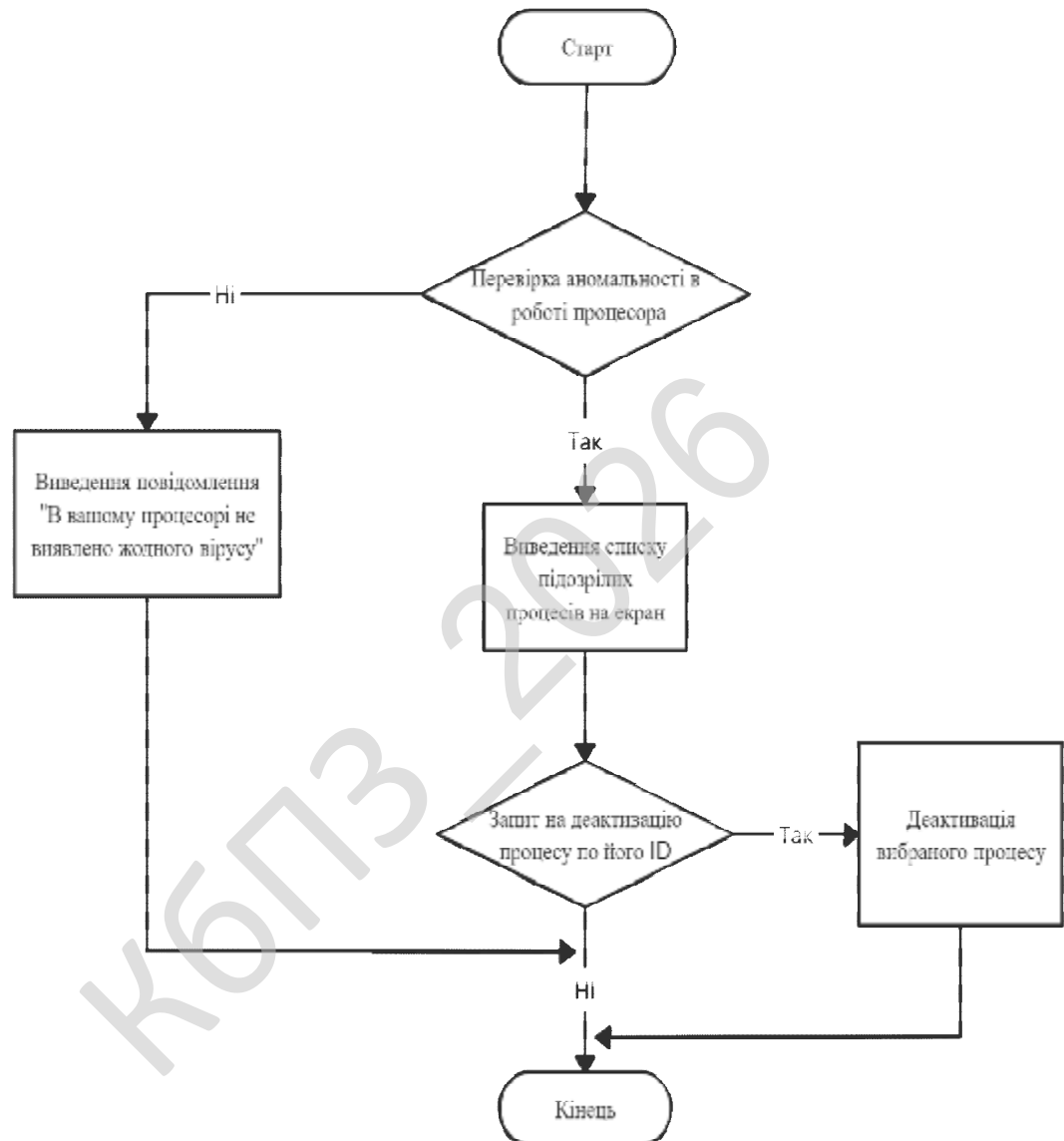


Рисунок 4.3 – Блок-схема підпрограми для аналізу та відлагодження процесора

Дана підпрограма виконує повернення частоти процесора як іменованого, включаючи поточну, мінімальну та максимальну частоти, виражені в МГц. У

Linux поточна частота повідомляє значення в реальному часі, а на всіх інших платформах воно представляє номінальне "фіксоване" значення. Якщо `pcrcpu` має значення `True` і система підтримує пошук частоти на CPU (лише для Linux), для кожного процесора повертається список частот, якщо ні, то повертається список з одним елементом. Якщо `min` і `max` неможливо визначити, вони встановлюються на 0.

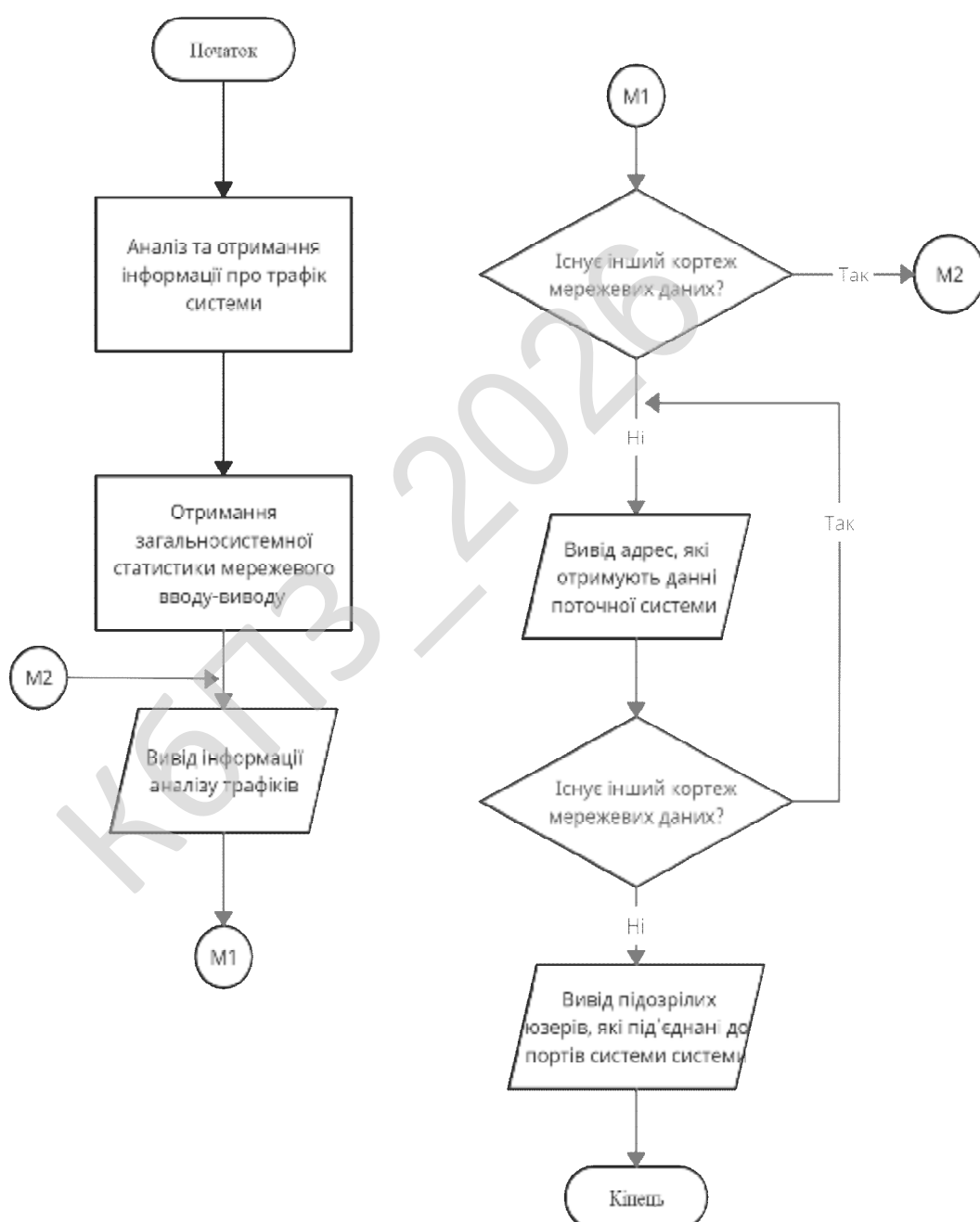


Рисунок 4.4 – Блок-схема підпрограми для аналізу та відлагодження процесора

Дана підпрограма повертає загальносистемні статистичні дані вводу-виводу у вигляді названого набору, що включає такі атрибути:

- bytes_sent: кількість надісланих байтів;
- bytes_recv: кількість отриманих байтів;
- packets_sent: кількість відправлених пакетів;
- packets_recv: кількість отриманих пакетів;
- errin: загальна кількість помилок під час отримання;
- errout: загальна кількість помилок під час надсилання;
- dropin: загальна кількість вхідних пакетів, які були скинуті;
- dropout: загальна кількість вихідних пакетів, які були скинуті (завжди 0

на macOS та BSD).

Якщо pernic має значення True, повертайте ту саму інформацію для кожного мережевого інтерфейсу, встановленого в системі, як словник з іменами мережевого інтерфейсу в якості ключів і названий кортеж, описаний вище як значення. У деяких системах, таких як Linux, у дуже зайнятій або довгоживучій системі числа, повернуті ядром, можуть переповнюватися і переноситися (перезапустити з нуля). Якщо параметр nowrap має значення True, psutil виявлятиме та коригуватиме ці числа у викликах функцій та додаватиме «старе значення» до «нове значення», так що повернені номери завжди будуть збільшуватися або залишатись тими самими, але ніколи не зменшуватись. net_io_counters.cache_clear () може бути використаний для анулювання кеш-пам'яті Nowrap. На машинах без мережевих інтерфейсів ця функція повертає None або {}, якщо pernic має значення True.

Також, підпрограма, повертає інформацію про кожну мережеву карту (мережеву карту інтерфейсу), встановлену в системі, як словник, ключі якого – імена мережевої карти, а значення – іменовані кортеж із наступними полями:

- isup: bool, що вказує, чи працює і чи працює мережева карта (мається на увазі підключений кабель Ethernet або Wi-Fi);
- duplex: тип дуплексного зв'язку; це може бути NIC_DUPLEX_FULL,

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

NIC_DUPLEX_HALF або NIC_DUPLEX_UNKNOWN;

- speed: швидкість NIC, виражена в мегабітах (МБ), якщо її неможливо визначити (наприклад, "localhost"), вона буде встановлена на 0;
- mtu: максимальна одиниця передачі NIC, виражена в байтах.

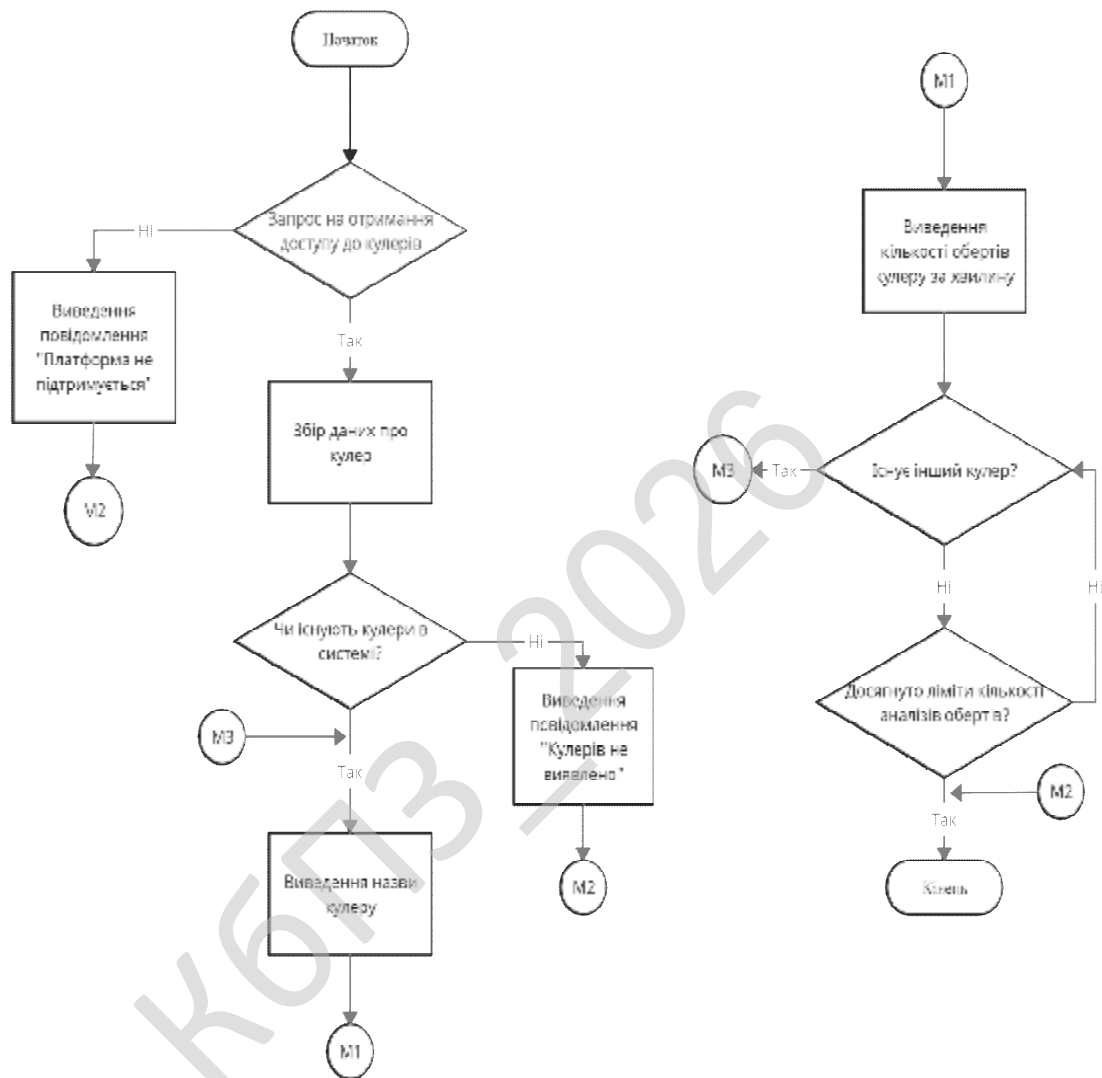


Рисунок 4.5 – Блок-схема підпрограми для перевірки збою або стоку кулерів

Дана підпрограма повертає швидкість апаратних вентиляторів. Кожен запис – це названий кортеж, що представляє певний вентилятор апаратного датчика. Швидкість вентилятора виражається в об / хв (обертів на хвилину). Якщо ОС не підтримує датчики, повертається порожній дикт.

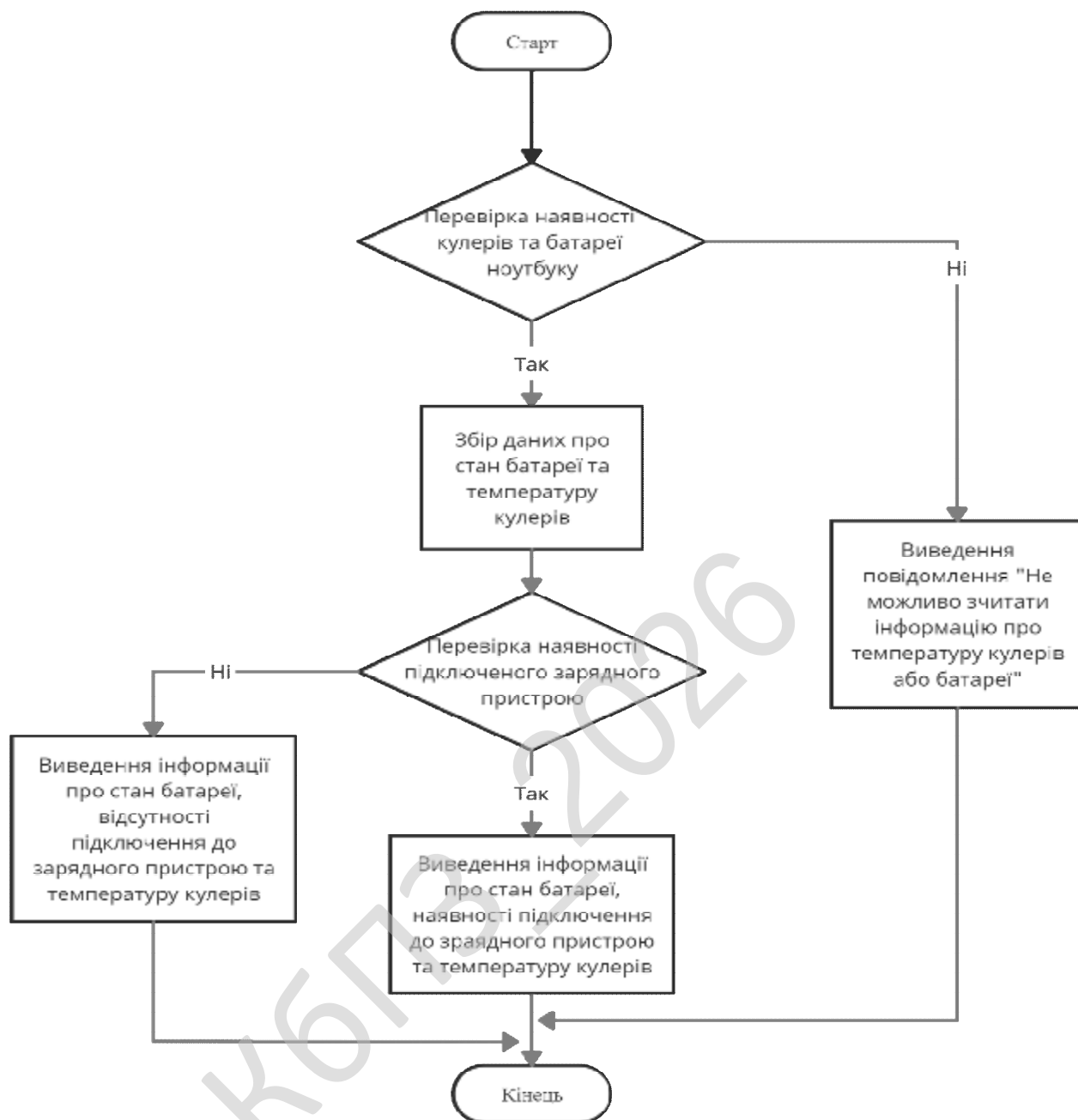


Рисунок 4.6 – Блок-схема підпрограми для перевірки батареї ноутбуку (якщо використовується)

Дана підпрограма повертає інформацію про температуру кулерів, стан батареї та наявність підключення до зарядного пристрою. Кожен запис – це названий набір, що представляє певний апаратний датчик температури. Усі температури виражені в Цельсії, якщо тільки за Фаренгейтом не встановлено значення True. Якщо ОС не підтримує датчики, повертається порожній дикт.

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм SHACAL-1, який заснований на перетвореннях алгоритму SHA-1. SHACAL-1 шифрує 160-бітний блок даних з використанням 512-бітного ключа шифрування. Допускається використання більше коротких ключів шифрування (не коротше 128 біт), які перед виконанням розширення ключа (процедура розширення ключа також успадкована від SHA-1 і буде описана нижче) повинні бути доповнені нульовими бітами для досягнення 512-бітного розміру.

В алгоритмі SHACAL-1 передбачено 80 раундів шифрування. Шифруєме повідомлення представляється у вигляді п'яти 32-бітних субблоків A , B , C , D і E , над якими в кожному раунді виконуються наступні дії:

$$A_{i+1} = K_i + (A_i \lll 5) + f_i(B_i, C_i, D_i) + E_i + M_i,$$

$$B_{i+1} = A_i,$$

$$C_{i+1} = B_i \lll 30,$$

$$D_{i+1} = C_i,$$

$$E_{i+1} = D_i,$$

де i – номер раунду ($i = 0 \dots 79$),

K_i – фрагмент розширеного ключа для i -го раунду,

f_i – функція для i -го раунду (див. нижче),

$\lll$ – операція побітового циклічного зрушення вліво,

M_i – константи, що модифікують, певні в такий спосіб:

Раунди	Значення константи
0...19	5A827999
20...39	6ED9EBA1
40...59	8F1BBCDC
60...79	CA62C1D6

Використовувані в раундах функції f_i визначені так:

Раунди	Функція
0...19	$f(x,y,z)=(x\&y) (x'\&z)$
20...39,60...79	$f(x,y,z)=x \oplus y \oplus z$
40...59	$f(x,y,z)=(x \oplus y) (x \oplus z) (y \oplus z)$

У таблиці символами $\&$, $|$ і $\oplus$ позначені, відповідно, побітові логічні операції «і», «або» й «або, що виключає» (XOR); x' позначає побітовий комплемент до x .

Шифртекстом є конкатенація вмісту змінних $A_{80}, B_{80}, C_{80}, D_{80}$ і E_{80} .

Процедура розширення ключа в алгоритмі SHACAL-1 також досить проста, вона виконується у два етапи:

Етап 1. 512-бітний вихідний ключ шифрування ділиться на 16 фрагментів по 32 біта $K_0...K_{15}...$

Етап 2. Інші фрагменти розширеного ключа $K_{16}...K_{79}$ обчислюються з перших 16 фрагментів у такий спосіб:

$$K_i = (K_{i-3} \oplus K_{i-8} \oplus K_{i-14} \oplus K_{i-16}) \lll 1.$$

Раунди розшифрування виконуються у зворотній послідовності; кожний з них має на увазі виконання наступних операцій:

$$A_i = B_{i+1},$$

$$B_i = C_{i+1} \lll 2,$$

$$C_i = D_{i+1},$$

$$D_i = E_{i+1},$$

$$E_i = K'_i + (B_{i+1} \lll 5)' + f'_i(C_{i+1} \lll 2, D_{i+1}, E_{i+1}) + A_{i+1} + M'_i + 4.$$

Тут запис $f(x)$ позначає побітовий комплемент результату виконання операції $f(x)$.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі система кібербезпеки IT-інфраструктури на об'єктах критичного застосування. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи: Функціональних кнопок ПЗ; Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші; Розділу обрання групи; Розділу виведення результату роботи системи.

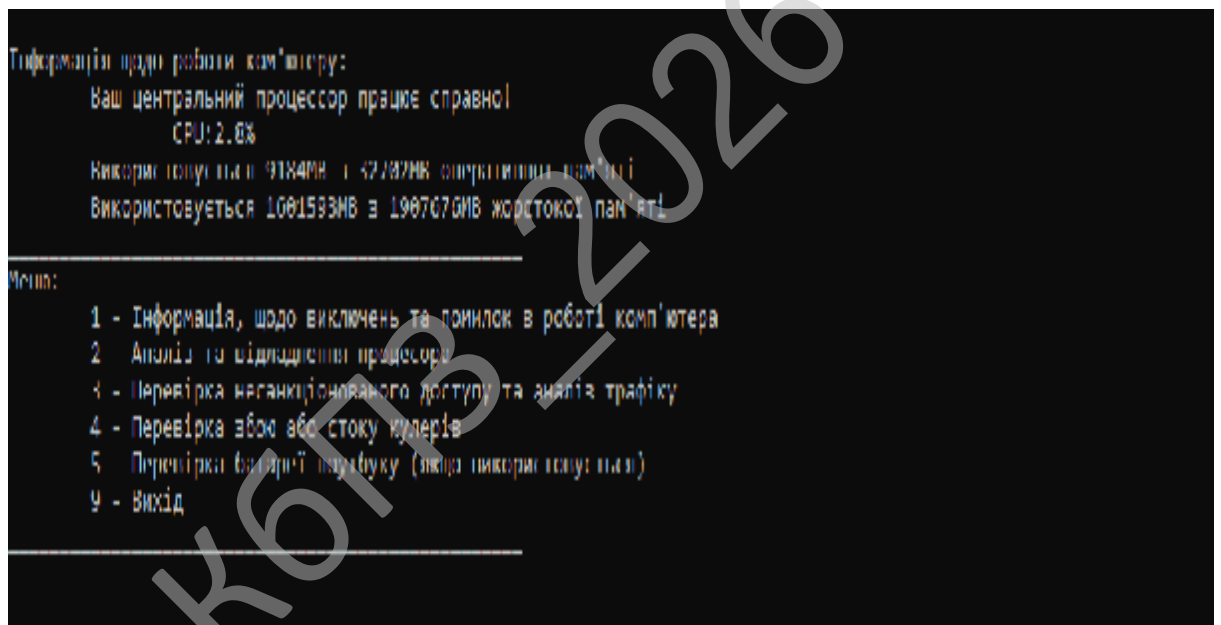


Рисунок 5.1 – Головне вікно ПЗ

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

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

помилки, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

На рисунку 5.2 зображено роботу підпрограми для виведення інформації, щодо виключень та помилок в роботі комп'ютера.

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 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.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

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

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

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 модулями (сервісами).

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.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

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

У цьому випадку формуються тестові варіанти, в яких:

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

Недоліки тестування "білої скриньки":

- Кількість незалежних маршрутів може бути дуже велика.
- Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

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

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

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

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

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

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

Проводилось тестування чорної скриньки.

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

Ці тести демонструють:

- Як виконуються функції програми.
- Як приймаються вихідні дані.
- Як виробляються результати.
- Як зберігається цілісність зовнішньої інформації.

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

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

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:

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

- Некоректних чи відсутніх функцій.
- Помилки інтерфейсу.
- Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
- Помилки характеристик (необхідна ємність пам'яті і т.д.).
- Помилки ініціалізації та завершення.

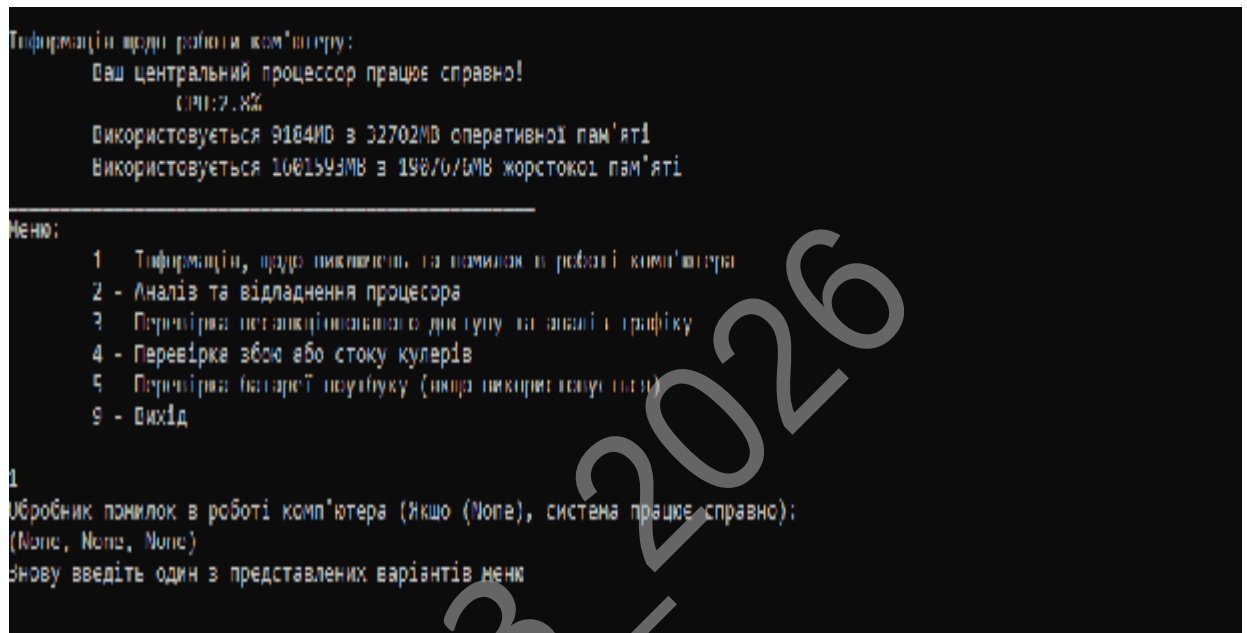


Рисунок 5.2 – Інформація, щодо виключень та помилок в роботі комп'ютера

На рисунку 5.3 зображено роботу підпрограми для аналізу та відлагодження процесора

```

Інформація щодо роботи комп'ютера:
Ваш центральний процесор працює справно!
CPU:1.8%
Використовується 8585МБ з 32768МБ оперативної пам'яті
Використовується 1601644МБ з 1907676МБ жорсткої пам'яті

Меню:
1 - Інформація, щодо виключень та помилок в роботі комп'ютера
2 - Аналіз та відлагодження процесора
3 - Перевірка несанкціонованого доступу та аналіз трафіку
4 - Перевірка збою або стоку кулерів
5 - Перевірка батареї ноутбуку (якщо використовується)
9 - Вихід

2
Аналіз процесора. Зачекайте...
Знову введіть один з представлених варіантів меню

```

Рисунок 5.3 – Аналіз та відлагодження процесора

На рисунку 5.4 зображено роботу підпрограми для перевірки несанкціонованого доступу та аналіз трафіку

```

3
Ethernet:
stats      : speed=100MB, duplex=full, mtu=1500, up=yes
вхідні дані : bytes=48.0G, pkts=38548505, errs=0, drops=0
вихідні дані : bytes=2.5G, pkts=16116101, errs=0, drops=0
MAC адреса  : 01-5D-64-51-80-D9
IPv4 адреса : 192.168.0.104
netmask     : 255.255.255.0
IPv6 адреса : fe80::1565:27d4:25ea:4303

Дивід усіх підозрілих підключень (Якщо пусто - підозрілих підключень не виявлено):
[suser(name='38099', terminal=None, host=None, started=1621063406.7477572, pid=None)]

Loopback Pseudo Interface 1:
stats      : speed=1073MB, duplex=full, mtu=1500, up=yes
вхідні дані : bytes=0.0B, pkts=0, errs=0, drops=0
вихідні дані : bytes=0.0B, pkts=0, errs=0, drops=0
IPv4 адреса : 127.0.0.1
netmask     : 255.0.0.0
IPv6 адреса : ::1

Дивід усіх підозрілих підключень (Якщо пусто - підозрілих підключень не виявлено):
[suser(name='38099', terminal=None, host=None, started=1621063406.7477572, pid=None)]

Знову введіть один з представлених варіантів меню

```

Рисунок 5.4 – Перевірка несанкціонованого доступу та аналіз трафіку

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

На рисунку 5.5 зображено роботу підпрограми для перевірки збою або стоку кулерів

```
Інформація щодо роботи комп'ютеру:
Наш центральний процесор працює нормально!
CPU: 2.6%
Використовується 10000000 з 32768000 оперативної пам'яті
Використовується 160161340 з 190767640 жорсткої пам'яті

Меню:
1 - Інформація, щодо виключень та помилок в роботі комп'ютера
2 - Аналіз та відладження процесора
3 - Перевірка неавтентифікованого доступу та аналіз трафіку
4 - Перевірка збою або стоку кулерів
5 - Перевірка батареї ноутбуку (якщо використовується)
9 - Вихід

4
Платформа не підтримується
```

Рисунок 5.5 – Перевірка збою або стоку кулерів

В підпрограмі для перевірки збою або стоку кулерів відбувається перевірка аномалій в роботі кулерів, якщо є до них доступ. Якщо підпрограма знаходить, що робота кулерів не співпадає з потребами процесора, то відбувається вивід кількості обертів кожного наявного кулера.

Якщо при роботі ноутбука або системного блоку з'явився шум, то в більшості випадків виною тому вентилятор. Його обороти повинні бути налаштовані так, щоб цей вузол якісно виконував роботу. Інакше кажучи, він повинен ефективно охолоджувати чіпсет або відеокарту. Однак при цьому робити це йому потрібно не на максимумі можливостей.

Проблема в тому, що автоматичне регулювання швидкості кулера не може постійно працювати коректно. Тоді користувачі налаштовують його параметри вручну. Вони знижують або збільшують кількість оборотів, щоб робота комп'ютера була більш комфортною.

На рисунку 5.6 зображено роботу підпрограми для перевірки батареї ноутбуку (якщо використовується)

Інформація щодо роботи комп'ютеру:
Ваш центральний процесор працює справно!
CPU: 0.8%
Використовується 9713мв з 16226мв оперативної пам'яті
Використовується 224825мв з 243570мв жорсткої пам'яті

Меню:

- 1 - Інформація, щодо виключень та помилок в роботі комп'ютеру
- 2 - Аналіз та відладання процесору
- 3 - Перевірка несанкціонованого доступу та аналіз трафіку
- 4 - Перевірка збою або стоку куллерів
- 5 - Перевірка батареї ноутбуку (якщо використовується)
- 9 - Вихід

5

Батарея:

заряд: 100.0%
статус: заряджений
зарядний пристрій: підключений

Знову введіть один з представлених варіантів меню

5

Батарея:

заряд: 99.0%
залишилось заряду: 1193040:28:15
статус: розряджається
зарядний пристрій: не підключений

Знову введіть один з представлених варіантів меню

Рисунок 5.6 – Перевірка батареї ноутбуку (якщо використовується)

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.
- Досліджена система моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.
- На основі отриманих результатів досліджень створена програмна реалізація системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи.

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

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

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

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

системи моніторингу та виявлення відхилень у роботі апаратно-програмних компонентів комп'ютерної системи. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

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

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм SHACAL-1.

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

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ док.ум.	Підпис	Дата		67

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

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

3. 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.

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

5. 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

6. 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.

7. 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.

8. 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, KL., Vuppalapati, 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.

9. 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.

10. 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 (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

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

12. 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.

13. 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.

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

14. 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,

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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

21. 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.*

22. 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.*

23. 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.*

24. 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.*

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

26. 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.*

27. 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.*

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, 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.*

44. 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.*

45. 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.*

46. 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.*

47. 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.*

48. 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.*

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

49. 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.

50. 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.

51. 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.

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

53. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». *CEUR Workshop Proceedings Volume 2732, 2020*, Pages 214-227.

54. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.

55. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. – Полтава, 2022. – 334 с.

56. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties».

International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

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

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

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

60. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)

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

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

63. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с

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

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

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

67. Смірнов О.А., Коваленко О.В., Кожанова А.С., Лєвошко О.Л., Константинова Л.В. Основи системного програмування. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. Коваленка О.В. – Кіровоград: КНТУ 2013. – 257с.

68. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. С.В. Кавуна. – Кіровоград: КНТУ 2012. – 442 с.

69. Смірнов О.А., Кузнецов О.О., Євсєєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова. – Кіровоград: КНТУ 2012. – 315 с.

70. Смірнов О.А., Мелешко Є.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

«Комп'ютерна інженерія». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2012. – 250 с.

71. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2012. – 454 с.

72. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Основи захисту інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2011. – 322 с.

К6ПЗ-2026

					ВКРБ-123.26.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78