

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

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

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи кібербезпеки призначеної
для реалізації Security Operation Center”

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

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнов С.А.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність 125 "Кібербезпека"
Освітньо-професійна (освітньо-наукова) програма "Кібербезпека"

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

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

Берлін Ірині Сергіївні

(прізвище, ім'я, по батькові)

1. Тема роботи Програмне забезпечення системи кібербезпеки
призначеної для реалізації Security Operation Center

2. Керівник роботи Смірнов Сергій Анатолійович, канд. техн. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 129-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту 23.05.2026 р.

4. Мета та завдання випускної кваліфікаційної роботи: Метою роботи є розробка програмного забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center

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

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи кібербезпеки в промислову експлуатацію.

6. Висновки

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

Структурна схема системи кібербезпеки 1 аркуш

Функціональна схема системи кібербезпеки 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

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

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнов С.А.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Берлін І.С.
(прізвище та ініціали)

АНОТАЦІЯ

Берлін І.С. Програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки призначеної для реалізації Security Operation Center.

Метою розробки є програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center.

Результат роботи – програмна реалізація системи кібербезпеки призначеної для реалізації Security Operation Center.

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

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

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

Програму розроблено в середовищі Python.

Ключові слова: кібербезпека, Security Operation Center

ABSTRACT

Berlin I.S. Software for a cybersecurity system designed for the implementation of a Security Operation Center. 125 Cybersecurity. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed that is designed for a cybersecurity system designed for the implementation of a Security Operation Center.

The purpose of the development is software for a cybersecurity system designed for the implementation of a Security Operation Center.

The result of the work is a software implementation of a cybersecurity system designed for the implementation of a Security Operation Center.

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

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

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

The program was developed in the Python environment.

Keywords: cybersecurity, Security Operation Center

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	4
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	6
1.1 Призначення системи.....	6
1.2 Область застосування.....	7
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	9
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	9
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	24
2.3 Розгорнута постановка завдання	25
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	27
3.1 Опис функціонування системи	27
3.2 Розробка структурної схеми.....	32
3.3 Розробка функціональної схеми	38
3.4 Розробка діаграми процесів.....	50
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	52
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	52
4.2 Захист розробленого програмного забезпечення.....	64
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	69
6 ОСНОВНІ ВИСНОВКИ.....	76
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	78

					ВКРБ-125.26.0021.00.00.ПЗ			
Вим	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center	Літ.	Аркуш	Аркушів
Розроб.	Берлін І.С.					Б	1	87
Перев.	Смірнов С.А.							
Н.контр.	Коваленко А.С.					ЦНТУ КБ-22-2		
Затв.	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ALARA – As Low As Reasonably Achievable – настільки низько, наскільки це можливо – принцип прийнятного ризику

FMEA – Failure Modes and Effects Analysis – аналіз видів і наслідків відмов

HCR – Human Cognitive Reliability – Надійність людини як функція його здібностей

HEP – Human Error Probability – Імовірність помилки людини

IRRAS – Integrated Reliability and Risk Analysis System – інтегральна надійність та аналіз ризику систем – пакет прикладних програм

NUREG – Nuclear Regulatory – Стандарт США (керівництво) в атомній промисловості

NRC – Nuclear Regulatory Commission – Комісія з ядерного регулювання США

OHSAS – Occupational Health and Safety Assessment Series – Система менеджменту охорони здоров'я та безпеки персоналу

RRR – Risk Reduction Ratio – коефіцієнт зменшення ризику

RRI – Risk Reduction Interval – інтервал зменшення ризику

THERP – Technique for Human Error Rate Prediction – Методика аналізу помилок людини в техніці (США)

ABNB – аналіз видів і наслідків відмов

Security Operation Center, AC – атомна станція

АП – аварійна послідовність

БД – база даних

БП – базисна подія

ВП – вихідна подія

ГНД – галузевий нормативний документ

ДВ – дерево відмов

ДП – дерево подій

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		2

ЗІЗ – засоби індивідуального захисту
 ІАБ – імовірнісний аналіз безпеки
 ІБ – інформаційна безпека
 ІП – ініціююча подія
 ІТ – інформаційні технології
 КС – кінцевий стан
 ЛЧ – людський чинник
 МП – мінімальні перерізи
 НД – нормативний документ
 НС – надзвичайна ситуація
 НП – небажана подія
 НВ – небезпечний випадок
 ОП – охорона праці
 ОПН – об’єкт підвищеної небезпеки
 ПНО – потенційно небезпечний об’єкт
 ПЛАС – план ліквідації аварійних станів
 ПП – прикладна програма
 ППР – планово-попереджальний ремонт
 ПТЕ – правила технічної експлуатації
 РОП – ризик орієнтований підхід
 СБ – система безпеки
 СТП – стандарт підприємства
 СУОП – система управління охороною праці підприємства
 ТО – технічне обслуговування
 ФБ – функція безпеки

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

ВСТУП

Актуальність теми. Класичне визначення Security Operations Center (SOC) передбачає систему, в основі якої лежать рішення класу SIEM. Ці інструменти агрегують та зберігають логи з різного обладнання й програмного забезпечення для подальшого аналізу та оперативного виявлення інцидентів безпеки. Потреба організацій у таких рішеннях виникла, коли адміністратори й оператори інформаційної безпеки перестали справлятися зі зростаючим обсягом даних і ускладненням IT-інфраструктури: обсяг генеруємих логів став перевищувати можливості людини вручну все це проаналізувати. Крім того, застосування рішень від різних виробників в IT-інфраструктурі зажадало безлічі окремих систем моніторингу (по одній для продукту кожного вендору), і адміністратори найчастіше повинні були відслідковувати інциденти в десятках консолей. У підсумку назріла необхідність у зборі й зберіганні лог-файлів в одному місці для їхньої централізованого аналізу, кореляції й виявлення інцидентів. Результатом стало активне впровадження SOC на базі SIEM-рішень.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center.

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

- Огляд існуючих систем призначеної для реалізації Security Operation Center.
- Дослідження системи кібербезпеки призначеної для реалізації Security Operation Center.
- Програмна реалізація системи кібербезпеки призначеної для реалізації Security Operation Center.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі призначеної для реалізації Security Operation Center.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

КБПЗ_2026

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

При використанні існуючих SIEM-систем аналітики ІБ потрапили в непросту ситуацію: з одного боку, вони не мають всю повноту інформації, необхідної для виявлення інцидентів і одержання всеосяжної картини, з іншого боку, вони не можуть одержати відсутні дані внаслідок обмеження продуктивності SIEM-пристроїв. Приміром, аналітик легко може виявити, що спрацювала сигнатура на IPS, однак визначити результат її впливу вже набагато складніше.

Таким чином, SOC на базі традиційних SIEM-рішень продовжує залишатися необхідною ланкою в системі інформаційної безпеки компанії, але вже недостатньо ефективним.

Нове покоління – нові можливості

Вирішити існуючі проблеми покликані SIEM-системи нового покоління, що використовують технології глибокого аналізу пакетів (Deep Packet Inspection) і працюючі з «великими даними» і інформацією, обсяг якої на кілька порядків перевищує обсяги аналізованих і збережених у цей час даних, а також більше різноманітною й більше динамічною в порівнянні з тими даними, що збираються сьогодні. Такі системи забезпечують повний запис всіх мережових пакетів в організації, і це в сполученні з логами й іншими джерелами даних дозволяє проводити більше глибокий аналіз. Новий підхід при пошуку аномалій і інцидентів у цих системах можна сформулювати так: послідовно видаляти зі стogu сіно (добре відомі фактори), поки не залишаться одні голки (негативні фактори). Традиційний же підхід полягав у пошуку голок у стозі сіна (даних), тобто у виявленні відомих аномалій за конкретними правилами, установленим аналітиками ІБ.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

1.2 Область застосування

Нові SIEM-системи, що збирають і аналізують значно більшу кількість інформації, дозволяють істотно розширити можливості одержання даних у ряді областей.

Виявлення шкідливих програм. З кожним роком виявити атаки стає усе складніше, оскільки вони маскуються під легітимний трафік і залишаються непоміченими. Використання технології запису всіх мережевих пакетів (а не тільки лог-файлів) дозволяє збирати й відновлювати файли, а потім автоматизувати більшу частину аналізу, необхідного для виявлення явних ознак зловмисних дій.

Виявлення слідів активності атакуючого в ІТ-інфраструктурі. Виявившись у мережі організації, зловмисники найчастіше переміщаються між вузлами з метою збору відомостей, необхідних для розвитку атаки. Оскільки кінцеві вузли часто не входять у зону моніторингу, повний запис всіх мережевих пакетів стає одним з найважливіших засобів для виявлення пересування нападаючих, а також ступені їхнього впливу на ІТ-ресурси компанії.

Надання доказів незаконної активності. SIEM-системи, здатні до захвата мережевих пакетів і запису сесій, здатні відновити повну активність зловмисника й визначити витік даних. Оскільки багато сучасних атак залишаються непоміченими до безпосереднього завдання збитків, то аналітикам ІБ потрібен метод для його оцінки, і відновлення атаки часто є найбільш ефективним способом проведення розслідування й підрахунку збитку.

Додавання функціонала захвата пакетів і відновлення сесій у наступному поколінні SIEM-рішень важливо для аналітиків, оскільки дозволяє перейти на зовсім новий рівень вивчення й пріоритизації погроз. Приміром, традиційні SIEM-системи можуть повідомити аналітика, що було зафіксоване з'єднання якогось комп'ютера із сервером зловмисника, але не зможуть відповістити на запитання, що було при цьому передане. Захват пакетів і відтворення сесій у

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

сполученні зі збором лог-файлів і іншою інформацією може дати аналітикам розуміння того, які дані були виявлені й скомпрометовані зловмисником. Таким чином, аналітики крім самого факту проникнення можуть оцінити ступінь впливу на бізнес і репутацію компанії.

Збір такої величезної кількості даних жадає від нового покоління SIEM-рішень кардинального збільшення швидкості обробки й обсягів збереженої інформації. Це досягається за рахунок застосування розподіленої багаторівневої архітектури зберігання й аналізу даних, що дозволяє нормалізувати й обробляти більші неструктуровані набори даних на дуже високій швидкості.

На закінчення відзначимо, що SOC, побудований на традиційних SIEM-системах, продовжує залишатися ефективним засобом виявлення аномалій за конкретними правилами, установленим співробітниками служби ІБ. Однак на зміну йому починають приходити нові покоління SIEM-рішень, що оперують зі значно більшими обсягами інформації, що дозволяє аналітикам знайти погрози й аномалії, про які вони навіть не підозрювали. У такий спосіб організаціям забезпечується поінформованість і підтримка в прийнятті рішень, необхідні для нейтралізації сучасних погроз.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

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

Огляд Group-IB TDS – системи раннього попередження погроз

Серед співробітників служб інформаційної безпеки компаній зовсім різних масштабів часто доводиться чути теза про те, що цілеспрямовані атаки, та й взагалі будь-які серйозні кіберзагрози, – це не про нас.

Мол, ми ж не Пентагон, ЦРУ або Верховна Рада, а всього лише одне з підприємств величезної країни, кому ми потрібні, тому для запобігання звичайних заражень нам досить традиційних засобів захисту інформації.

Тим часом, реальна ситуація з кіберзлочинністю у світі після 2000-х чітко демонструє неефективність класичного підходу до забезпечення безпеки, пов'язаного з використанням традиційних методів захисту.

За даними Group-IB, одне тільки угруповання Cobalt викрала близько 1 млрд євро в 100 банків в 40 країнах миру, навіть незважаючи на те, що фінансова галузь завжди дуже тремтливо ставиться до безпеки.

Відповідно до визначення, цільові атаки – це будь-який напад кіберзлочинців на конкретну обрану ними ціль із використанням програмних або програмно-технічних засобів.

Вони протиставляються масовим атакам за допомогою вірусів або інших шкідливих програм, у яких жертва вибирається по доступності.

Сьогодні явно домінує мотивація одержання фінансової наживи як основна для зловмисників (самовираження, політичні амбіції, протестні акції й просто розваги зовсім відійшли на другий план), крім того, хакери навіть при масових атаках не гидують застосовувати найсучасніші техніки при обході

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

захисних рубежів, такі як машинне навчання й штучний інтелект. У цьому зв'язку поняття сильно розминаються, а розхожа приказка «якщо вас ще не зламали, ви про це, швидше за все, просто не знаєте» не здається смішною.

Відповідаючи на виклики, пов'язані із все більшим поширенням складних кіберзагроз, виробники захисних рішень змушені розвивати інтелектуальну складову своїх продуктів.

Саме тому особливий інтерес представляє герой сьогоднішнього огляду – TDS, оскільки, на відміну від багатьох інших anti-APT-вендорів, Group-IB при реалізації системи відштовхується від накопичених сильних консалтингових і експертних компетенцій.

Для тестування нам був наданий вилучений доступ до стенда з розгорнутою й налаштованою системою TDS, а також організована лабораторна міні-інфраструктура, щоб ми змогли на практиці оцінити принцип роботи й всі можливості продукту.

Архітектура й функціональні можливості

Комплексне рішення Group-IB Threat Detection System (TDS) призначено для виявлення сучасних високотехнологічних атак на ранній стадії.

Воно визначає зараження, які пропускають стандартні засоби захисту: антивіруси, межмережеві екрани, системи запобігання вторгнень.

По заявах вендору, застосування TDS істотно знижує ризики, допомагаючи вчасно виявити й запобігти розкраданням, фінансові шахрайства, спроби шпигунства, витік конфіденційної інформації й інші інциденти.

Саме по собі рішення є частиною власної екосистеми Threat Intelligence, однак може поставлятися й окремо.

В TDS використовуються дані кіберрозвідки, що збираються фахівцями Group-IB по усьому світі, про дії зловмисників, у тому числі інформація про появу нових шкідливих програм і адрес командних центрів, змінах відомих вірусів, різних тактиках атак, а також інформація, отримана в ході реагування на інциденти інформаційної безпеки й розслідувань кіберзлочинів лабораторією

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

комп'ютерної криміналістики Group-IB. У рішенні застосовуються наступні основні технічні підходи для виявлення погроз:

- сигнатурний аналіз трафіку;
- виявлення мережових аномалій методами машинного навчання;
- поведінковий аналіз файлів, що витягаються з каналу зв'язку й одержуваних від поштової системи й з інших джерел.

Архітектурно TDS складається із трьох елементів:

- Sensor.
- Polygon.
- SOC Group-IB.

TDS Sensor

TDS Sensor призначений для аналізу вхідних і вихідних пакетів даних.

Він дозволяє виявити небажану й небезпечну мережеву взаємодію, передані шкідливі об'єкти, шпигунські програми, засоби вилученого керування, спроби використання уразливостей, загальні аномалії в мережі компанії й незвичайне поведіння пристроїв.

Для роботи Sensor використовує власні сигнатури й поведінкові правила зі спеціально розробленої й підтримуваної системи даних про погрози, заснованої на 15-літньому досвіді розслідування кіберзлочинів співробітниками Group-IB.

При цьому, крім ведення власної бази, Group-IB одержує самі актуальні індикатори компрометації (IOC) у рамках партнерського обміну даними із центрами моніторингу погроз по усьому світі.

До таким, наприклад, ставляться: організації з офіційним статусом CERT (Group-IB також є такою), Інтерпол і Європол, різні співтовариства й об'єднання.

Виявлення погроз за допомогою Sensor здійснюється, нагадаємо, на основі власної бази сигнатур, що у поточній версії ніяк не можна поправити вручну або вибірково відключити.

По запевненню розроблювачів, це пов'язане з тим, що втручання неспеціаліста у вузькій сфері threat hunting і без досвіду тонкого налаштування

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

й формального опису сигнатур може привести до серйозного падіння ефективності роботи всієї системи.

Однак архітектурно механізм імпорту з використанням YARA-правил у рішенні закладене, його використання буде дозволено в наступних релізах і очікується вже цього року.

Для оцінки шкідливості файлів необхідно, виходячи з технологічних можливостей і оцінки застосовності, вибрати один із трьох способів мережевої інтеграції Sensor:

1. Пасивний збір файлів із трафіку. Необхідно подати копію внутрішнього трафіку (до NAT і/або Proxu), наприклад, по SPAN. Дозволяє не перебудовувати мережеву інфраструктуру й реалізується мінімальною кількістю налаштувань. Мінус полягає в тому, що при виборі даного способу існує ризик втрати файлів через негарантовану передачу всіх пакетів. При великому навантаженні можливі втрати пакетів даних, часом в обсязі 6-10% від загального числа.

2. ICAP-інтеграція. Необхідно окремо налаштувати перенапрямок трафіку із проксі або інших серверів. Плюсом є куди більше висока надійність у плані гарантованої перевірки всіх файлів.

3. Web-API (у ручному режимі, з деякими обмеженнями). З метою персональної інтеграції з деякими рішеннями клієнта може бути використаний відкрита Web-API. Спосіб є самим ресурсозатратним і явно не годиться при розгортанні пілотних проектів. Цей варіант розрахований на великі впровадження на складній інфраструктурі.

Крім того, для поведінкового аналізу вкладень до листів, Sensor повинен бути інтегрований з поштовою системою підприємства одним з наступних способів:

1. Пасивний збір листів із трафіку. Як ми вже відзначали вище, трафік, одержуваний по SPAN, може бути неповним, що істотно підвищує ймовірність ненадходження на Sensor прикладеного до листа файлу. Саме тому для поштової інтеграції звичайно використовується один їх двох інших механізмів.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

2. Одержання листів по POP3/IMAP. Припускає створення на поштовому сервері окремого ящика для схованого копіювання всіх вхідних листів у нього. Далі Sensor по POP3 або IMAP автоматично забирає всю пошту з його, а потім очищає вже проаналізовані листи за собою.

3. Одержання листів по SMTP. Найбільш популярний спосіб, полягає в налаштуванні правила дзеркалювання листів по 25 порту, вимагає окремого налаштування встаткування замовника.

Крім перерахованого, існує спосіб аналізу файлів при підключенні системи в inline-режимі.

У випадку з поштовою інтеграцією встановлюється два Sensor, між якими піднімається VRRP-Канал для відказостійкості.

На поштовому сервері IP цих пристроїв вказуються як MTA (Mail Transfer Agent).

Для аналізу файлів в web-трафіку при такій інсталяції використовується Proxu з ICAP, зконфігуровані не передавати файли в мережу, поки їх не перевірить комплекс TDS.

Sensor інтегрується із системою поведінкового аналізу TDS Polygon і настраюється на передачу інформації про виявлені інциденти в SOC Group-IB по безпечному каналі з додатковою можливістю відправлення подій по Syslog у будь-яку внутрішню корпоративну систему, наприклад в SIEM.

Локальний інтерфейс, доступний на Sensor, не відрізняється високим рівнем юзабіліті й більше підійде досвідченим, люблячим «поковиряться» (наприклад, Wireshark і іншими подібними інструментами) фахівцям з розслідування інцидентів ІБ.

Крім описаного, при виконаній попередній інтеграції з Polygon, локальний інтерфейс керування Sensor дозволить переглянути оброблені файли й листи з висновком про шкідливість, а також прийняти самостійне рішення про пропуск або не пропуск заблокованих елементів з карантину до робочих станцій користувачів.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

Докладніше про те, як працює режим блокування, піде мова в наступному розділі.

TDS Polygon

TDS Polygon використовується для поведінкового аналізу підозрілих об'єктів у безпечному середовищі (пісочниці), що витягаються з каналу зв'язку й одержуваних від поштової системи й з інших джерел.

Отримані по електронній пошті або завантажені з інтернету файли перевіряються на предмет шкідливої активності до влучення на комп'ютери користувачів.

Застосування технологій поведінкового аналізу дозволяє виявити раніше невідомі шкідливі програми без використання сигнатур, а також блокувати їхню доставку на кінцеві робочі станції.

Після одержання об'єктів на аналіз Polygon емулює їхній запуск і оцінює поведінку (середній час оцінки – 2,5 хвилини, воно може варіюватися залежно від типу файлу) у власній системі розгорнутих віртуальних машин (використовуються стандартні версії популярних операційних систем начебто Windows 7 x86/x64, із установленим офісним софтом).

Конфігурація й образи цих машин жорстко зашиті в продукт і не доступні до редагування користувачем системи.

Однак по запиті клієнтів техпідтримка Group-IB готова доповнити стандартну комплектацію Polygon бажаними операційними системами й налаштуваннями оточення, головною умовою тут є надання замовником ліцензій на все необхідне програмне забезпечення.

Цікавою фішкою Polygon є запис перших 6 секунд відео поведінки аналізованого об'єкта, начебто б його запускав користувач у себе на робочому місці.

Використовуючи вердикти по об'єктах, отримані в ході поведінкового аналізу від Polygon, систему TDS можна налаштувати в режимі блокування пошти.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

Ця функція буде особливо корисна тим компаніям, у яких безпека при одержанні листів ставиться вище, ніж їхня гарантована доставка до адресата.

Для реалізації необхідно інтегрувати Sensor у режимі MTA (Mail Transfer Agent) як SMTP-relay.

По запевненнях розроблювача, затримка в доставці листів при включенні такого режиму не перевищує 5 хвилин, а звичайним користувачам у випадку позитивного блокування не приходить ніяких повідомлень.

При цьому служба ІБ оперативно інформується про такі інциденти й ухвалює рішення щодо подальшому пропуску або блокуванні файлу, що потрапив у карантин.

SOC Group-IB

Центр моніторингу (Security Operations Center – SOC) складається із власної інфраструктури, розгорнутої в приватній хмарі, і команди фахівців Group-IB, які відслідковують і аналізують виявлені системою TDS події (TDS-SOC).

Експерти TDS-SOC негайно повідомляють фахівців з безпеки організації про критичні погрози по електронній пошті або телефону, а також дають рекомендації з їхнього усунення.

Підтримка працює цілодобово, цілий рік без вихідних, а самі зазначені послуги вже включені у вартість усього рішення й окремо не тарифікуються.

Зведення про виявлені погрози доступні у вигляді звітів за будь-який період часу.

Важливою особливістю всього рішення є те, що даний компонент украй важливий до застосування при впровадженні, тому що вся аналітична частина системи TDS зав'язана саме на нього.

Однак, по заявах розроблювачів, восени 2018 року планується випуск виконання з «відчужуванням SOC».

У перелік послуг TDS-SOC також входить сервіс моніторингу працездатності всього встаткування, експлуатованого в рамках системи TDS.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

Дивно, але за послуги SOC розроблювач не бере додаткової плати.

Більш докладно про пристрій компонента SOC поговоримо безпосередньо в ході тестування рішення трохи нижче.

Особливості впровадження системи

Система TDS може бути розгорнута в компанії й використовуватися в одному із трьох варіантів:

1. Sensor, Polygon установлюються усередині організації, SOC здійснює зовнішню експертну підтримку. Такий варіант впровадження TDS є найбільш оптимальним, оскільки забезпечує гарантовану безперебійну роботу всіх модулів системи.

2. Sensor установлюється усередині організації, Polygon – у хмарі Group-IB, SOC здійснює зовнішню експертну підтримку. Зазначений підхід можна рекомендувати при пілотних впровадженнях або в тій ситуації, коли установка Polygon (поставляється винятково у вигляді програмно-апаратного комплексу) на підприємстві вкрай утруднена або неможлива зовсім.

3. Sensor і Polygon установлюється усередині організації, SOC не підключається (такий варіант впровадження доступний уже з осені 2018). Головною особливістю TDS є технологічна концепція Group-IB, відповідно до якої більша частина функцій по керуванню й експлуатації всієї системи віддається в руки й на сторону експертів SOC. У такій структурі Sensor TDS є DPI-рішенням для аналізу всіх вхідних і вихідних пакетів даних, на якому передвстановлен набір сигнатур, за допомогою яких визначається зловлива активність, чорний список адрес контролерів бот-мереж, а також обновлювані щодня правила фільтрації. Якщо в компанії є SIEM-система, Sensor уміє відправляти події в неї, використовуючи syslog. Описаний варіант впровадження є єдиним, котрий дозволяє вести самостійну обробку подій безпеки без їхньої передачі в Group-IB. Для організацій з підвищеними вимогами до рівня ізоляції внутрішньої інфраструктури вендор пропонує розгорнути локальний центр відновлень (наприклад, в DMZ), у результаті чого Sensor буде повністю

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

ізолюваний від зовнішнього миру, при цьому базу сигнатур можна підтримувати в актуальному стані.

Установка й системні вимоги

Відповідно до загального підходу компанії Group-IB, при поставці системи TDS фахівці розроблювача або авторизованого партнера підключаються й допомагають на кожному з етапів впровадження й інтеграції з мережевою інфраструктурою, через що процес самостійної установки як такий практично відсутній.

Sensor може поставлятися як програмно-апаратний комплекс, так і у вигляді софту для установки на залізо або віртуальну машину клієнта.

Системні вимоги до сервера клієнта або віртуальній машині для установки софту Sensor:

- Процесор – 4 ядра.
- Оперативна пам'ять – 16 Гб.
- Жорсткий диск – 360 Гб.
- Мережеві порти – мінімум 2 шт.: для порту керування й для прийому дзеркалюемого трафіку.

У класичному, «нехмарному» виконанні Polygon поставляється замовникам тільки у вигляді програмно-апаратного комплексу.

У силу того, що керування й всі аналітичні можливості рішення цілком зосереджені в хмарі Group-IB, вимоги, пропоновані до робочого місця адміністратора, у край прості й формальні: будь-який пристрій із установленим браузером і доступ в інтернет.

Робота із продуктом

Після виконання необхідних процедур по інтеграції системи TDS у корпоративну інфраструктуру компанії-клієнтові виділяється обліковий запис від особистого кабінету на закритому порталі керування системою. Нагадаємо, що в рамках тестування продукту Group-IB надала нам доступ до підготовленого тестового середовища із уже розгорнутими компонентами TDS.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

Ситуаційний центр і керування повідомленнями

На головному екрані користувачеві доступне загальне інформаційне зведення по виявленим системою погрозам, стан сенсора, статистика по подіях і завантаження каналу.

Дизайн інтерфейсів виконаний у класичному стилі, призначення дашбордів і графіків інтуїтивно зрозуміло.

Всі елементи клікабельні й дозволяють одержати деталізовану інформацію.

Єдиний, мабуть, мінус у тім, що головний екран налаштовува_ не, поки елементи не можна забрати, додати або посувати, чим ми вже розпещені в багатьох інших продуктах.

Але й цю опцію розроблювач обіцяє додати вже цією осінню.

Зараз для вибору варіантів відображення набору подій передбачений вибір тимчасового інтервалу, а також 3 режими:

- Параноїдальний – виводяться абсолютно всі детекти.
- Збалансований – відображаються події середнього рівня й вище.
- Дзен-режим – показуються винятково критичні спрацювання.

З верхньої частини інтерфейсу завжди можна перейти до відображення й керування повідомленнями.

Саме цей розділ менеджмент-панелі є основним каналом оперативної комунікації між безпечниками компанії й фахівцями SOC Group-IB.

Тут заводяться й обробляються тікети, по кожному з яких доступна деталізація й коментарі учасників.

Виявлення погроз по сигнатурах

Для детального розбору зареєстрованою системою TDS шкідливої активності використовується розділ Події, у який можна також «провалитися» прямо з дашбордів на головному екрані.

Для зручності сприйняття всі події об'єднані в ланцюжки, зв'язані між собою в рамках одного кейса.

Саме зручне тут – це інтелектуальний рядок пошуку.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

Вона дозволяє швидко фільтрувати непотрібні дані, використовуючи простий і зрозумілий синтаксис, довідка по застосуванню якого також під рукою.

Відшукавши шкідливу активність, що цікавить, одержуємо повну розкладку по ній.

Якщо виведеної на екран докладної інформації про джерело й жертву виявилось недостатньо, можна скачати PCAP-Файл із записом трафіку в «сиром» виді й відтворити її для проведення більше детального розслідування (наприклад, за допомогою утиліти Wireshark).

Відзначимо, що інформація про те, що відбувається на конкретних хостах – цілях атаки, не приводиться, це прерогатива вже суміжних рішень, наприклад EDR (Endpoint Detection and Response).

Group-IB активно працює в цьому напрямку й обіцяє випустити пілотні версії рішення подібного класу вже цього року.

Не утомлюємося повторювати, що основні компетенції Group-IB пов'язані з областю Threat Intelligence і розслідуванням кіберзлочинів, саме тому знайомство з детальною інформацією з конкретної сигнатури, що спрацювала, для нас було самим довгоочікуваним.

Отже, крім словесного опису характеру шкідливого впливу, доступна інформація про функціональність, модулі, адреси керуючих центрів і навіть наведена деталізація по відомих деструктивних діях, таким як модифікація файлів або віток реєстру операційної системи.

Як ми вже відзначали раніше, ніякі дані, пов'язані з IOC (індикаторами компрометації) погрози, користувачеві міняти не можна.

Аналіз мережевих аномалій

Принцип розбору детектованих системою TDS мережевих аномалій у цілому аналогічний роботі із сигнатурним аналізом і припускає роботу з такою ж зручним пошуковим рядком.

Алгоритми визначення шкідливої активності вибудовані відповідно до концепції DGA (Domain Generation Algorithms).

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

Цікаво, що по кожній виявленій потенційній погрозі відображається скорінг шкідливості, що у ході всього нашого тестування не помилявся, показуючи по всім спрацюванням імовірність, близьку до 100%.

Поведінковий аналіз файлів

Переходячи до розслідування, пов'язаному з поведінковим аналізом об'єктів модулем Polygon, опустимо опис уже звичної роботи з ланцюжками подій.

Вибираємо серед них файл, що цікавить, дивимось інформаційне зведення по ньому.

Відзначимо, що докладний звіт по кожному такий вредоносу можна вивантажити у вигляді гарного pdf-документа.

Цікаво, що ніколи не будучи антивірусним вендором, Group-IB тільки по поведінковому аналізу може збирати таку велику кількість реально корисної інформації й файлах, так ще й з 100% імовірністю визначати його шкідливість.

Для докладного вивчення крім загальної інформації доступний аж ніяк не маленький список поведінкових маркерів, ранжируваних по загальному ваговому внеску в підсумковий вердикт (особливо шкідливі, шкідливі, інші).

Всі піймані небезпечні об'єкти можна скачати для самостійного вивчення в лабораторних умовах.

Якщо вкладення прийшло по електронній пошті, система також розбирає структуру листа й дозволяє завантажити його цілком або витягтися окремо адреси й посилання.

Для одержання інформації про те, до яким потенційно небезпечним ресурсам спробував звернутися об'єкт, доступні відомості по його мережевій активності. Корисним також може стати вивчення дерева процесів, так чи інакше задіяних або знову створюваних шкідливим файлом.

По всіх зібраних доказах стає зрозумілої загальна картина й вся послідовність дій небезпечного об'єкта так, начебто б його запуслав у себе на робітник станції користувач.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

Якщо й цього виявиться недостатньо, можна подивитися 6-секундне відео про те, що відбувається з емулюємою системою після зараження.

Робота з базою знань і створення звітів. Покінчивши з виявленням погроз і провівши розслідування всіх що цікавлять шкідливих активностей, відзначимо ряд додаткових можливостей системи TDS.

Крім стандартних налаштувань користувачів і інших деталей, одна з таких – централізована база знань про погрози.

По кожній з відомих Group-IB масових атак, що нашуміли заражень, бот-мереж і інших зловливих активностей, доступно вичерпний опис, аналогів якому по ступені подробиці й глибини подачі матеріалу у світі, як нам здається, не так уже багато.

У ході тестування ми не змогли пройти мимо й ще раз ознайомилися з деякими голосними вірусними епідеміями.

Відзначимо, що крім довідкових даних приводяться конкретні рекомендації зі зниження ймовірності зараження, що включають як технічні міри, так і стратегію захисту.

Застава успішного й показового застосування будь-яких засобів захисту – продумана система побудови звітів.

Система TDS дозволяє вивантажувати технічне зведення по одному із чотирьох передвстановлених шаблонів у форматах pdf, csv, xlsx, які недоступні до редагування.

Окремо відзначимо, що експерти Group-IB у рамках обслуговування й надання модуля SOC по запиті готують спеціалізовані бізнес-звіти про стан інформаційної безпеки на підприємстві для керівництва (наприклад, на щоквартальній основі).

Технічна підтримка й додаткові сервіси

Крім уже описаного величезного пакета послуг (включаючи цілодобову техпідтримку) у рамках SOC, що входить у комплексну систему TDS, Group-IB пропонує своїм клієнтам широкий спектр додаткових сервісів.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

В основному вони пов'язані із традиційним для компанії бізнесом, таким як моніторинг атак, реагування на інциденти й розслідування кіберзлочинів.

Крім того, фахівці Group-IB можуть провести аудитів безпеки, організувати захист бренда в мережі, а також ICO- і блокчейн-проектів.

У рамках даного огляду окремо варто зупинитися на страховці від кіберризиків.

Купуючи TDS, клієнти Group-IB одержують те, про що все давно мріяли – можливість реального матеріального відшкодування у випадку, якщо реалізувалася та або інша погроза, а система не спрацювала.

Поліс надається партнером – великою міжнародною страховою компанією AIG (American International Group) і поширюється на ризики витоку корпоративних або персональних даних і порушень безпеки комп'ютерної системи, викликаних зараженням або ушкодженням інформації, у тому числі з використанням як шкідливих програм, так і методів соціальної інженерії (обман, підкуп співробітників і т.п.).

Обмовимося, що поліс покриває заздалегідь застережені страхові випадки, а саме:

- збитки, пов'язані з порушеннями даних і безпеки інформаційних систем;
- витрати, пов'язані з розслідуванням зроблених злочинів у комп'ютерній сфері;
- витрати, пов'язані з питаннями реагування на описані вище інциденти.

Ми ознайомилися з функціями, особливостями впровадження й протестували на практиці систему раннього попередження кіберзагроз TDS від Group-IB.

Поза всякими сумнівами, підходи до реалізації рішення міцно закріплять за ним славу «захисту від цілеспрямованих атак із хмарним інтерфейсом» і «SOC у комплекті». Вигідне використання своїх кращих компетенцій при розвитку й просуванні продукту виглядає щонайменше цікавим, а по факті – украй професійним стосовно замовника.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

Як продукт, Group-IB TDS дуже простий у використанні, має зрозумілий і зручний інтерфейс.

В умовах гострої недостатності фахівців вузьких компетенцій на ринку інформаційної безпеки допомога в експлуатації складного рішення для захисту від цілеспрямованих атак з боку професіоналів дуже актуальна.

TDS можна вважати скоріше сервісом із установлюваним додатковим устаткуванням на стороні клієнта, чим навпаки.

Важливим плюсом рішення є також те, що при відсутності автоматизованої реакції на інциденти система TDS надає максимально докладні рекомендації з нейтралізації виявлених погроз, що включають як технічні, так і організаційні методи протидії.

Оскільки структура самого бізнесу Group-IB побудована інакше, чим в інших вендорів аналогічних TDS рішень, важливим плюсом продукту є доступ продукту до самих різних джерел даних, агрегуються як on-site-способом (те, що збирається в ході аналізу трафіку й файлів на стороні клієнта), так і реагувань, що добуваються в ході, на інциденти інформаційної безпеки (Incident Response), розслідувань кіберзлочинів, комп'ютерної криміналістики, кіберрозвідки.

Незважаючи на давно, що з'явився на ринку клас, рішень по боротьбі із цілеспрямованими атаками й включення в процес іменитих (у тому числі вітчизняних) розроблювачів, ця тема по-справжньому поки так і не вистрілила.

Сьогодні ми переживаємо новий виток інтересу до таких систем, зв'язаний не стільки з «продажем страху», але й із двома основними технологічними факторами.

Перший – розвиток напрямку реагування (у тому числі в рамках EDR-рішень), обумовлене загальним розумінням, що з виявленими складними погрозами в підсумку потрібно щось робити, бажано давши при цьому реальний інструмент у руки користувачеві.

Другий – нарощування аналітичних можливостей і підвищення ступеня автоматизації, пов'язані з бажанням наблизитися до тій самій «однієї кнопки», що

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

і рішення буде приймати сама, і знешкоджувати атаки зі стовідсотковою точністю.

Таким чином, по обох пунктах у системи TDS від Group-IB існують чіткі перспективи для розвитку, і якщо із другим всі й так зрозуміло, те по першому ведеться робота у вірному напрямку – вендор обіцяє випустити повноцінне EDR-рішення, перша версія якого (поки в пасивному режимі) запланована вже на 2018 рік.

Переваги:

- Простота використання й зручність інтерфейсу.
- Безкоштовна обробка виявлених інцидентів фахівцями SOC Group-IB.
- Виявлення мережових атак по сигнатурах, виявлення мережових аномалій і мережева пісочниця в одному продукті.
- Моніторинг погроз і інфраструктури завжди в режимі 24/7/365.
- Повнота надаваних поведінкових звітів.
- Вичерпна деталізація по погрозах, векторам атак, зараженням.

Недоліки

- Немає можливості відключати, правити, додавати свої сигнатури.
- Відсутній компонент моніторингу робочих місць убудованого реагування (EDR).

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Python – це потужна мова програмування, яка проста у вивченні. Він має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис і динамічна типізація Python разом з його інтерпретованим характером роблять його ідеальною мовою для створення сценаріїв і швидкої розробки додатків у багатьох сферах на більшості платформ.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

Інтерпретатор Python і обширна стандартна бібліотека доступні у вихідному або двійковому вигляді для всіх основних платформ на веб-сайті Python <https://www.python.org/> і можуть вільно поширюватися. Цей же сайт також містить дистрибутиви та вказівники на багато безкоштовних сторонніх модулів Python, програм і інструментів, а також додаткову документацію.

Інтерпретатор Python легко розширюється за допомогою нових функцій і типів даних, реалізованих у C або C++ (або інших мовах, які можна викликати з C). Python також підходить як мова розширення для налаштовуваних програм.

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 кібербезпеки призначеної для реалізації Security Operation Center.

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

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

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

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

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

д) розробити рекомендації по організаційних та методичних заходах, які

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

забезпечать впровадження системи кібербезпеки в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

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

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

К6ПЗ_2026

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Як розставити пріоритети, із чого варто почати побудова SOC для досягнення конкретних результатів у короткий термін? На ці питання ми дамо відповіді в цій роботі.

Ми всі частіше чуємо від своїх замовників, що SOC у них ще не побудований, але завдання детектування інцидентів і реакції на них стоїть тут і зараз.

І виникають цілком закономірні питання: із чого варто почати, щоб реалізувати частина функцій у короткий термін, які є підводні камені і як їх обійти, які процеси варто впровадити в першу чергу?

Кіберзагрози більше не є поодинокими подіями чи рідкісними інцидентами. У 2026 році організації стикаються з постійними, автоматизованими та цілеспрямованими атаками, які розвиваються швидше, ніж традиційні засоби контролю безпеки. В результаті роль Центру операцій безпеки, широко відомого як SOC, докорінно змінилася.

Сучасний центр охорони здоров'я (SOC) – це вже не просто кімната, повна екранів, що відстежують сповіщення. Це стратегічна, заснована на аналітиці функція, призначена для виявлення, аналізу та реагування на загрози в режимі реального часу, одночасно підтримуючи безперервність бізнесу, дотримання вимог та управління корпоративними ризиками.

У цьому посібнику пояснюється, чим насправді займається сучасний SOC у 2026 році, як він працює та чому він став критично важливою функцією як для зростаючих, так і для великих підприємств.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

Традиційні центри безпеки (SOC) були розроблені на основі реактивних моделей безпеки. Оповіднення генерувалися, аналітики досліджували їх, а дії вживалися лише після того, як інцидент вже почався.

Такий підхід більше не є ефективним.

У 2026 році центри безпеки (SOC) працюють, використовуючи проактивні та засновані на аналітиці принципи безпеки. Вони зосереджені на ранньому виявленні, передбаченні загроз та постійному вдосконаленні, а не на простому обробці сповіщень. Автоматизація відіграє центральну роль, тоді як аналітики-люди зосереджуються на розслідуванні, оцінці та прийнятті рішень. Найголовніше, що сучасні SOC узгоджують операції безпеки з реальними бізнес-ризиками, а не працюють ізольовано.

Основні обов'язки сучасної SOC у 2026 році

Сучасний центр операцій безпеки виконує кілька взаємопов'язаних функцій, які разом утворюють безперервний життєвий цикл безпеки.

1 Безперервний моніторинг загроз

Зловмисники не діють за робочим графіком. Сучасна система захисту даних (SOC) забезпечує цілодобовий моніторинг кінцевих точок, мереж, хмарних платформ, додатків та систем ідентифікації.

Замість того, щоб реагувати на окремі сповіщення, команди SOC аналізують поведінкові моделі та аномалії з часом. Це дозволяє завчасно виявляти підозрілу активність, перш ніж вона переросте в повноцінний інцидент.

2 Розширене виявлення та аналіз загроз

Зловмисники у 2026 році регулярно обходять захист на основі сигнатур. Як результат, SOC покладаються на поведінкову аналітику, контекстну розвідку загроз та машинний аналіз.

Аналітики безпеки оцінюють намір атаки, масштаб та потенційний вплив на бізнес, замість того, щоб просто підтверджувати, чи є сповіщення шкідливим. Платформи та операційні моделі, що підтримуються такими рішеннями, як

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

ManageX, наголошують на точності та контексті, допомагаючи командам зменшити втому від сповіщень та зосередитися на значущих загрозах.

3 Реагування на інциденти та їх стримування

Виявлення без реагування пропонує обмежений захист. Сучасні центри захисту від несанкціонованих дій (SOC) розроблені для швидких та скоординованих дій.

Реагування на інциденти включає негайні дії щодо стримування, такі як ізоляція скомпрометованих облікових записів або кінцевих точок, з подальшим поглибленим розслідуванням та аналізом першопричин. Винесені висновки документуються та використовуються для покращення майбутніх процесів виявлення та реагування.

У 2026 році швидкість реагування безпосередньо впливає на час простою, витік даних, регуляторні наслідки та довіру до бренду.

4 Автоматизація та оркестрація безпеки

Автоматизація є важливою для управління масштабами сучасних кіберзагроз. Центри захисту даних (SOC) використовують платформи оркестрації для автоматизації повторюваних завдань, таких як сортування тривоги, збагачення та дії початкового реагування.

Автоматизація забезпечує узгодженість, зменшує людські помилки та дозволяє аналітикам зосередитися на складних розслідуваннях, а не на рутинних завданнях. Людський досвід залишається центральним, але автоматизація підвищує ефективність.

Зони охоплення SOC у 2026 році

Сучасна система керування охороною даних (SOC) забезпечує повну видимість усього цифрового середовища. Зазвичай охоплення включає кінцеві точки, такі як ноутбуки, сервери та мобільні пристрої, а також мережі, хмарні робочі навантаження, додатки, API та системи ідентифікації.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

Також ретельно відстежуються схеми переміщення даних та доступу. Така цілісна видимість дозволяє центрам захисту даних (SOC) виявляти багатоетапні атаки, які поширюються по різних середовищах.

Роль розвідки загроз у сучасних системах управління операційною діяльністю (SOC)

Розвідка про загрози зараз є основою операцій SOC. Сучасні SOC постійно споживають розвідувальні дані з глобальних каналів, галузевих джерел та внутрішньої телеметрії.

Замість того, щоб реагувати лише на відомі індикатори, SOC використовують інтелект для передбачення поведінки зловмисника та нових моделей загроз. Фреймворки, що підтримуються такими платформами, як ManageX, інтегрують інтелект безпосередньо в робочі процеси виявлення та реагування, підвищуючи швидкість і точність.

Показники SOC, які мають значення у 2026 році

Ефективність SOC більше не вимірюється обсягом сповіщень чи кількістю заявок. Змістовні показники зосереджені на результатах.

До поширених показників належать середній час виявлення, середній час реагування, ефективність стримування, зменшення хибнопозитивних результатів та загальне покращення стану безпеки з часом. Ці показники допомагають організаціям зрозуміти, чи операції з безпеки дійсно знижують ризики.

SOC проти традиційних інструментів безпеки

Багато організацій досі покладаються на автономні інструменти безпеки без централізованих операцій. SOC надає принципово інші можливості.

Традиційні інструменти працюють ізольовано та генерують сповіщення. Центр захисту даних (SOC) інтегрує ці інструменти, співвідносить їхні дані та застосовує людський та автоматизований інтелект для забезпечення проактивного захисту. Результатом є перехід від тактичних реагувань до стратегічного управління ризиками.

Хмарно-орієнтовані та гібридні операції SOC

До 2026 року більшість організацій працюють у гібридних та мультихмарних середовищах. Центри захисту даних (SOC) повинні контролювати хмарні журнали, виявляти неправильні конфігурації, відстежувати зловживання ідентифікацією та захищати потоки даних між платформами.

Це вимагає спеціалізованих знань та постійної адаптації. Для багатьох організацій керовані або гібридні моделі SOC, що підтримуються такими платформами, як ManageX, забезпечують практичний спосіб досягнення цієї можливості без надмірних внутрішніх накладних витрат.

Підтримка SOC та дотримання вимог

Хоча SOC сам по собі не є рішенням для забезпечення відповідності, він відіграє вирішальну роль у підтримці нормативних вимог. SOC забезпечують безперервний моніторинг контролю, документування інцидентів та звітність, готову до аудиту.

Організації зі зрілими операціями SOC краще підготовлені до регуляторних перевірок, оскільки докази генеруються безперервно, а не ретроактивно.

Коли організації потрібен SOC

Організації зазвичай оцінюють можливості SOC, коли кількість інцидентів безпеки зростає, впровадження хмарних технологій прискорюється, зобов'язання щодо дотримання вимог розширюються або внутрішні команди перевантажуються.

Для багатьох компаній, що розвиваються, керований або гібридний підхід SOC пропонує захист на рівні підприємства без складнощів створення повноцінної власної операції.

Майбутнє державних операційних компаній після 2026 року

Забігаючи вперед, SOC продовжуватимуть розвиватися в напрямку прогностичних моделей безпеки, підтримки рішень за допомогою штучного інтелекту та глибшого узгодження з показниками бізнес-ризиків.

SOC дедалі більше функціонуватиме як центральна нервова система кібербезпеки, дозволяючи організаціям впевнено працювати в складних цифрових середовищах.

У 2026 році сучасний Центр операцій безпеки – це не просто перегляд панелей інструментів чи реагування на сповіщення. Він спрямований на захист бізнес-результатів, зниження ризиків та забезпечення безпечного зростання.

3.2 Розробка структурної схеми

Незважаючи на критичну важливість ізоляції мереж, у відкритому доступі бракує детальної експертної інформації з цієї теми. У даному розділі ми проаналізуємо найпоширеніші вразливості, виявлені під час наших попередніх аудитів. Сподіваємося, ці дані допоможуть пентестерам розширити власний інструментарій, а фахівцям з інформаційної безпеки — зрозуміти вектори атак, які зловмисники використовують для проникнення з корпоративного сегмента до технологічних мереж керування (OT/ICS).

Збір інформації

– Етап збору даних спрямований на пошук вразливої інформації, що стосується мережі керування технологічними процесами. Отримані відомості дозволяють зловмиснику детально вивчити структуру мережі та спланувати вектор атаки. Зокрема, це стосується:

– Даних про персонал: Технологи, оператори та профільний IT-персонал зазвичай мають доступ до конфіденційних сегментів. Аналіз Active Directory за посадовими ролями дозволяє ідентифікувати конкретні робочі станції та спільні

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

мережеві ресурси (SMB-шари). Такий підхід значно звужує коло пошуку, дозволяючи хакеру зосередити зусилля лише на критично важливих хостах.

– Мережева та проєктна документація. Ці дані дозволяють зловмиснику детально вивчити архітектуру системи керування, ідентифікувати критичні хости та визначити IP-адреси для подальшої розвідки. У найгіршому сценарії документація надає повну карту технологічних процесів, вказуючи на пріоритетні цілі для атаки. Після компрометації корпоративних файлових серверів або репозиторіїв (наприклад, SharePoint), пошук зазвичай фокусується на файлах форматів VSD (Visio), PDF та DOC/DOCX у директоріях, що стосуються інженерних та виробничих підрозділів.

– Технічна документація АСУ ТП. Ці матеріали часто містять описи регламентів віддаленого доступу, інструкції з авторизації на виробничих хостах та детальний перелік активних технологій. Нерідко в таких документах зберігаються критично важливі конфіденційні дані (наприклад, облікові записи), що є надзвичайно цінним при аналізі сегментації мережі. Подібні файли зазвичай виявляють у загальних IT-директоріях або в специфічних мережевих папках виробничих підрозділів.

– Конфігурації мережевого обладнання та резервні копії. Аналіз бекапів конфігураційних файлів міжмережевих екранів, маршрутизаторів та комутаторів дозволяє зловмиснику розробити оптимальну стратегію проникнення в технологічний сегмент. Вивчення цих налаштувань допомагає виявити хости в корпоративній мережі, яким дозволено віддалений доступ через протоколи RDP, VNC та SSH. Крім того, з резервних копій систем керування можна вилучити хеші паролів та іншу критичну інформацію. Зазвичай такі дані виявляють у системах IT-моніторингу, сховищах засобів резервного копіювання або на спільних мережевих ресурсах IT-департаменту.

Ідентифікація місця проникнення

Для адміністрування таких систем зазвичай застосовуються протоколи **віддаленого доступу**. Найпоширенішими точками входу є:

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

– Jump-сервер (jumpbox) або термінальний сервер. Зв'язок між корпоративним та технологічним сегментами мережі часто реалізується через проміжний хост (jump box). Найчастіше використовуються протоколи RDP, VNC та SSH, рідше — рішення для віртуалізації робочих столів, наприклад Citrix. У компаніях із високим рівнем зрілості інформаційної безпеки віддалений доступ обов'язково захищається механізмами багатофакторної автентифікації (MFA).

Офіційні регламенти віддаленого доступу до технологічної мережі зазвичай детально описані в документації. Крім того, виявити jump-сервери або термінальні вузли можна шляхом аналізу схем мережі та конфігурацій міжмережевих екранів. Для цього ідентифікуються хости, яким дозволено з'єднання з корпоративного сегмента через стандартні порти віддаленого керування. Додатковим ефективним методом є аудит робочих станцій профільного персоналу, що дозволяє точно визначити використовувані шлюзи та протоколи доступу.

– VPN-з'єднання. Окремим категоріям персоналу (переважно інженерам та операторам) може надаватися прямий VPN-доступ для віддаленого керування технологічними процесами. Як і у випадку з використанням jump-серверів, для захисту таких з'єднань рекомендується впровадження багатофакторної автентифікації (MFA).

Аналіз групових політик та VPN-клієнтів. Часто для авторизованих користувачів створюють спеціалізовані групи в Active Directory. Аудит членства та описів груп, до яких входять ключові інженери та технологи, дозволяє швидко ідентифікувати осіб із правами на VPN-доступ. Наступним кроком є дослідження їхніх робочих станцій на наявність встановлених VPN-клієнтів, мережевих інтерфейсів або активних сесій із технологічним сегментом. Такі комп'ютери фактично стають «містком» для проникнення в мережу керування.

– Dual-homed хости (вузли з двома інтерфейсами). У типовій архітектурі АСУ ТП деякі вузли можуть мати пряме підключення до обох сегментів мережі або працювати через специфічні правила міжмережевого екрана, що відкривають

доступ до технологічного середовища. Зазвичай це сервери архівації даних (Historians), які збирають інформацію для аналізу ефективності виробництва. Компрометація таких серверів часто дозволяє обійти офіційні регламенти віддаленого доступу та потрапити в мережу керування напряму. Навіть за обмежених прав, аналіз активних сесій на цих вузлах допомагає зловмиснику визначити цільові діапазони IP-адрес у виробничому сегменті.

Найбільш ефективним методом виявлення серверів архівації (Historians) є аналіз проєктної документації та схем мережі. Варто звертати увагу на специфічні імена хостів, які часто містять префікси або скорочення на кшталт «HI», «HIS» або «HIST». Хоча через відсутність єдиних галузевих стандартів сканування портів може бути ускладненим, поширені системи (наприклад, OSIsoft PI) легко ідентифікуються за стандартними для цього ПЗ портами. Якщо вендор системи керування вже відомий, подальший пошук точок входу в корпоративному сегменті базується на вивченні офіційної документації виробника щодо мережевих портів.

Ще одним дієвим методом виявлення dual-homed хостів (вузлів із кількома інтерфейсами) є аудит корпоративного сегмента через віддалене виконання команд (наприклад, за допомогою WMI або PsExec). Це дозволяє отримати дані про активні мережеві з'єднання, налаштування інтерфейсів та таблиці маршрутизації. Попри те, що такий підхід генерує значний мережевий трафік («шум») і потребує обробки великих масивів даних, він чітко вказує на вузли, що мають доступ до технологічної мережі. Попередня фільтрація результатів за відомими IP-діапазонами АСУ ТП значно спрощує аналіз.

Доступ до сегрегованої мережі

Після ідентифікації потенційних точок входу до мережі АСУ ТП наступним етапом є аналіз кожного вузла на наявність типових уразливостей. Мета цього кроку — оцінка можливості несанкціонованого проникнення в технологічний сегмент. Нижче наведено перелік найпоширеніших проблем, виявлених під час попередніх експертиз безпеки різних мереж.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

– Слабкі парольні політики. Використання ненадійних паролів залишається критичною вразливістю для мереж АСУ ТП. Основна складність полягає у низькій мотивації інженерів та операторів дотримуватися правил кібергігієни. Часто користувачі застосовують однакові облікові дані як для корпоративного, так і для технологічного сегментів, помилково вважаючи ризик атаки мінімальним. У разі компрометації корпоративної мережі та викрадення паролів ключових співробітників, зловмисники можуть безперешкодно отримати доступ до систем керування виробництвом через раніше ідентифіковані точки входу.

Використання дефолтних та слабких паролів. Часто в мережах АСУ ТП залишаються активними стандартні заводські налаштування автентифікації. Власники систем не змінюють їх, щоб уникнути потенційних збоїв через відхилення від еталонної конфігурації виробника. Поширеною практикою є використання ідентичних логінів і паролів (наприклад, operator:operator, manager:manager) або комбінацій, що містять назву бренду (наприклад, Administrator:siemens).

Відсутність політик блокування облікових записів. Ситуація ускладнюється тим, що в мережах АСУ ТП часто не налаштовують блокування акаунтів після невдалих спроб входу. Це робиться для запобігання випадковим зупинкам критичних процесів через помилки персоналу. Проте такий підхід дозволяє зловмисникам безперешкодно проводити атаки методом перебору (brute-force). У поєднанні зі слабкими або дубльованими паролями, відсутність обмежень на кількість спроб входу робить підбір облікових даних надзвичайно ефективним методом проникнення.

– Зберігання паролів у незашифрованому вигляді. Облікові дані для керування технологічними процесами часто фіксуються безпосередньо в документації. Під час аудиту сегментації мережі на етапі збору інформації необхідно ретельно дослідити всі репозиторії, де зберігаються технічні описи та

інструкції. Будь-які знайдені документи мають бути проаналізовані на наявність паролів, що можуть бути використані для доступу через виявлені точки входу.

– Інтеграція корпоративного домену в мережу керування. Наявність у корпоративній мережі dual-homed хостів або робочих станцій із VPN-доступом, приєднаних до Active Directory, створює серйозні ризики. Зловмисники можуть отримати доступ до цих вузлів безпосередньо через привілейовані доменні акаунти (наприклад, адміністратора домену). Навіть за наявності обмежень доступу для певних груп, компрометація корпоративного сегмента дозволяє легко ідентифікувати потрібних користувачів та вилучити їхні паролі з пам'яті.

– Вразливі мережеві сервіси. Точки входу часто містять додаткові служби (бази даних, вебзастосунки), вразливі до типових атак. Кожен хост із доступом до мережі АСУ ТП має бути просканований на наявність неврахованих сервісів. У разі їх виявлення проводиться аналіз на предмет помилок конфігурації або відомих уразливостей, що можуть призвести до повної компрометації вузла.

Під час проведення пентесту ICS-інфраструктури негайно повідомляйте про критичні ризики, якщо виявлено такі факти:

– Наявність промислового трафіку (Modbus/DNP3) у загальному корпоративному сегменті.

– Доступ із корпоративної мережі до HMI-інтерфейсів із правами на зміну параметрів (запис).

– Виникнення критичних збоїв у роботі промислових контролерів або реакторів під час мережевого сканування інструментами на кшталт Nmap.

Безпека промислових систем (ICS) є критично важливою для інфраструктури, проте в цій галузі досі спостерігається суттєвий дефіцит практичних знань та експертних матеріалів.

Виходячи з усього перерахованого вище, сформована структурна схема системи, яка зображена на рисунку 3.1.

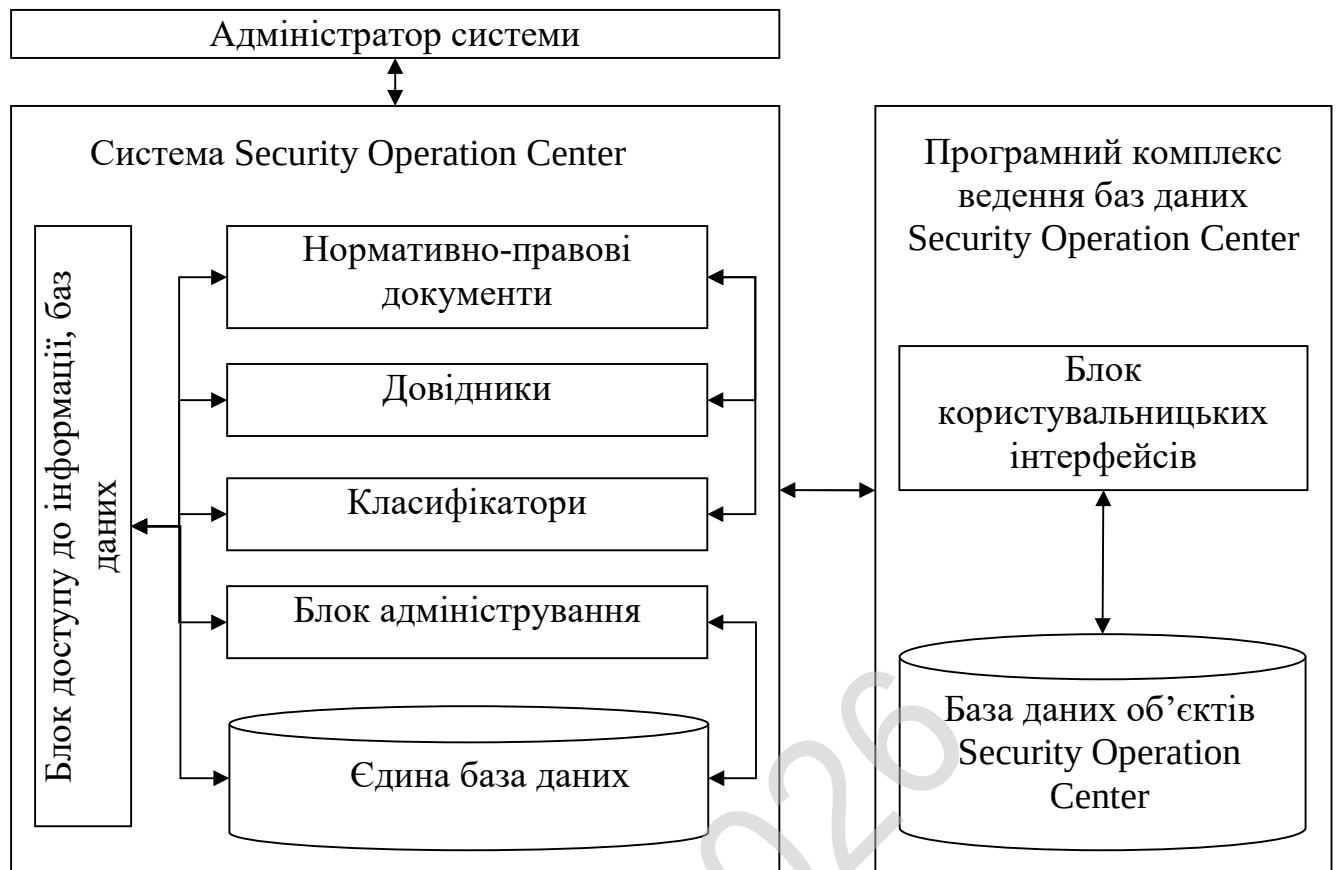


Рисунок 3.1 – Структурна схема системи

3.3 Розробка функціональної схеми

Для управління системою оператору необхідна інформація, яка б дозволяла:

- швидко оцінити загальний стан об'єкту, тобто в стані нормальної експлуатації, в умовах очікуваної експлуатаційної події чи в аварійному стані і переконатися, що виконуються запроектовані автоматичні дії по забезпеченню безпеки;

- визначити відповідні дії, які необхідно розпочати оператору.

Для виконання ролі оператора системи Security Operation Center людині потрібна інформація з параметрів окремих систем об'єкту й устаткування.

Функціональна схема системи зображена на рисунку 3.2

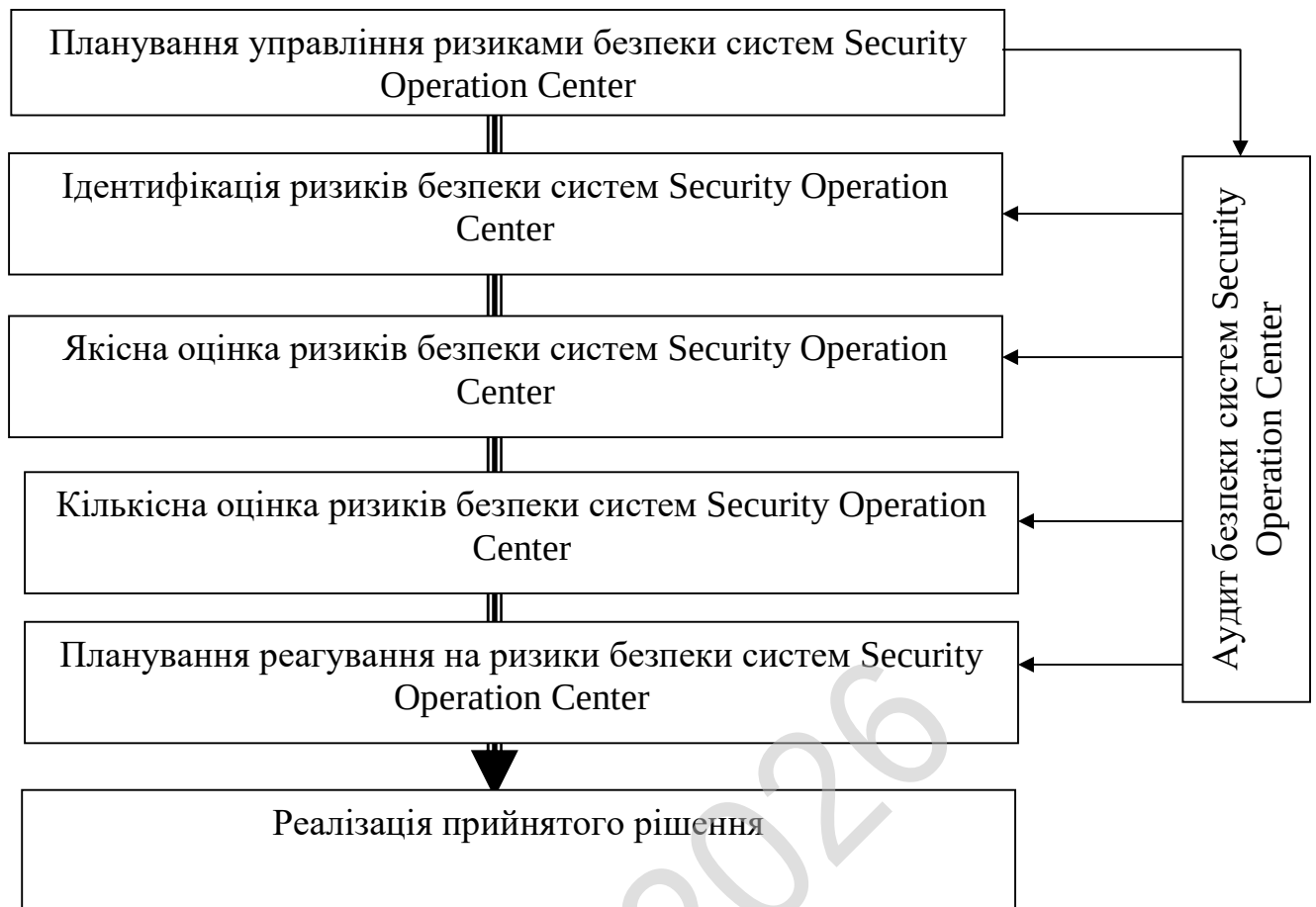


Рисунок 3.2 – Функціональна схема системи

Необхідно, щоб проєкт сприяв успішному виконанню оператором своїх дій у межах наявного часу, в умовах передбачуваного навколишнього фізичного середовища і психологічного навантаження. Бажано звести до мінімуму необхідність у негайному втручанні оператора. У проєкті варто врахувати той факт, що таке втручання прийнятне тільки в тому випадку, коли проєктувальник може довести, що оператор має досить часу для прийняття рішення і відповідних заходів; що необхідна інформація, на основі якої оператор повинен приймати своє рішення, представлена в дохідливій і чіткій формі і що фізичні параметри навколишнього середовища в приміщенні пульту управління та на додаткових пультах управління об'єктом після даної події є прийнятними.

Процедура системного аналізу помилок

Процедура системного аналізу помилок людини має загальні кроки для різних методик [4].

Ця процедура відома в англійській аббревіатурі як SHARP – Systematic Human Action Reliability Procedure. Процедура включає сім кроків і два етапи, на яких приймаються рішення. Два перших кроки виконуються системними аналітиками, два подальших – фахівцями з аналізу людського чинника, останні три кроки процедури виконуються спільними зусиллями.

Розглянемо процедуру виконання кожного кроку.

– Крок 1 – Визначення дій людини, включаючи дії по ремонту, роботу по програмах, дії по локалізації аварій, тобто всіх дій з помилками персоналу, які погіршують або поліпшують ситуацію.

– Крок 2 – Скрінінг – відбір важливих подій, помилок, що мають ключове значення для імовірності аварійної ситуації (наприклад, плавлення активної зони).

– Крок 3 – Розділення – виділяються всі дії оператора, що вимагають більш детального аналізу, тобто задача розбивається на більш дрібні, характерними складовими яких будуть:

1. Здатність зрозуміти, що треба робити (для аналітиків), розділення дій по операціях;

– Нездатність визначити систему.

– Нездатність виконати дії.

2. Включення кроків в модель ІАБ;

3. Необхідність (можливість) побудови додаткових аварійних послідовностей, якщо визначилися інші помилки операторів.

– Крок 4 – Уявлення – повне **представлення** всіх помилок і їх аналіз з докладними діями.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

– Крок 5 – Визначення **взаємного впливу** елементарних дій (операцій), впливи на наступні етапи;

– Крок 6 – Розрахунки – визначаються **кількісні** значення ймовірностей помилок;

– Крок 7 – Документування.

Обсяг робіт на кожному кроці залежить від типу методики, що використовується.

Визначення базових значень ймовірностей помилок людини

Помилки під час експлуатації частіше складають помилкові дії: або не передбачені, або передбачені в експлуатаційних процедурах, чи процедурах технічного обслуговування; рідше – невиконання окремих дій, що вимагаються. Прикладами є неправильний вибір засобів управління, передача неправильних команд чи інформації, зміна послідовності виконання задач і занадто раннє чи занадто пізнє виконання задач. Такі помилки можуть виникнути в результаті помилок при прийнятті рішень операторами: невірно витлумачених чи нечітких процедур; помилкові показання контрольно-вимірювальних приладів; неправильне розуміння чи просто помилка оператора. Для визначення надійності системи ці можливі помилки потрібно враховувати в проекті.

Значення імовірності помилки у випадку наявності адекватних процедур та їх застосування при виконанні складних робіт зменшується у 50 разів.

Представляє інтерес також таблиця обліку залежності ймовірностей помилки від змін обставин: змін в складі бригади, що виконує роботу, розділення дій за часом і місцем, наявність чи відсутність вказівок на виконання роботи (підказки) і комбінацій названих обставин. Врахування всіх обставин проводиться по нижченаведеному алгоритму. Значення імовірності помилки без врахування змін обставин (НЕР) дорівнює N , в залежності від їх комбінацій – номери для типів помилкових дій людини, приймає значення:

– 1 (одиниця) у разі повних змін;

– $(1+N)/2$, у разі високих (великих) змін;

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

- $(1+6N)/7$, у разі помірних змін;
- $(1+19N)/20$, у разі низьких (малих) змін;
- N , у разі нульових змін.

Ця таблиця відноситься до методики ASP, що широко використовується для аналізу помилок людини-оператора. При цьому, обставини сильно змінюють імовірність помилки. Наприклад, якщо базова ймовірність $N = 0.1$, то в залежності від змінених обставин імовірність помилки буде: 0,1; 0,145; 0,23; 0,55; і 1,0 відповідно до різного ступеню залежності.

Побудова дерева помилок персоналу

Дерева аналізу надійності людини вперше були введені в методиці THERP[46]. Події в такому дереві позначаються у вигляді відрізків прямих ліній, розташованих під кутом один до одного.

Відрізки, розташовані **праворуч**, зображають **неуспішні** дії (відмови), які позначаються великими літерами латинського алфавіту, відрізки зліва – **успішні дії**, позначаються малими буквами латинського алфавіту. Поруч з позначенням, звичайно можуть бути пояснюючі надписи й значення ймовірності відповідної події. Дії по відновленню функцій систем позначаються горизонтальними пунктирними лініями.

Відрізки показують послідовність дій. Початок послідовності дій знаходиться вгорі. Кожне дерево, в залежності від числа гілок, має різне число послідовностей. Послідовністю тут будемо називати дії, або їх сукупність, що приводять до якогось результату (на кінець гілки). Так дерево, представлене на рисунку 3.10 містить такі послідовності: *abc*, **A**, **aB**, *abCD*, *abCd*.

Чисельні значення ймовірностей неспіху проставляються поруч з подіями. Зазначимо, що успіх і відмова є взаємно доповнюючими подіями.

При побудові дерева надійності людини також як і при побудові дерева відмов систем, важливе значення мають всі допущення, припущення і межі. Всі вони повинні бути чітко описані.

Аналіз загального ризику з врахуванням помилок персоналу

При оцінці ризику від промислових об'єктів (Security Operation Center) необхідно враховувати дії людини, тобто повинен використовуватися комплексний підхід: системний аналіз надійності обладнання, аналіз надійності людини і, в результаті, аналіз загального ризику:

Відмова системи = відмова обладнання + помилка людини.

Наведена формула дещо спрощена, оскільки є взаємодії, які можуть поліпшити або погіршити ситуацію. Розуміти її треба так: оператор остання лінія захисту (в глибоко ешелонованому захисті).

Цілі моделювання подій, пов'язаних з помилками людини:

- представити помилки і їх механізми;
- якісно представляти роль чинників, що впливають на поставлену задачу;
- кількісно описати помилку, що дозволить зробити аналіз чутливості;
- виробити стратегію запобігання помилкам або відновлення функцій оператором.

Основні базисні події, пов'язані з помилками операторів, можуть вводитися в моделі ІАБ на рівні систем – в дерева відмов, або на рівні послідовностей – в дерева подій. Введення в дерева відмов основних базисних подій, пов'язаних з помилками операторів, має деякі переваги:

- отримані при детальному моделюванні відомості враховуються спочатку і використовуються для подальшого аналізу;
- не використовуються консервативні оцінки;
- консервативний відбір для дерев відмов і оцінки базисних подій, пов'язаних з помилками операторів, призводить до того, що завищений рівень людських помилок суперечить повному аналізу. Це сприяє виконанню детального моделювання і кількісних оцінок.

Імовірність відмови системи в цьому випадку визначається з урахуванням можливої помилки оператора, що має всі кількісні характеристики і свій закон розподілу ймовірностей.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

У деревах подій врахування людського чинника (HF) може відбуватися як проміжні події із заданими ймовірностями відновлення систем, що відмовили. У випадку складної залежності проміжні події можуть вводитися окремими деревами аналізу надійності людини. Ці дерева можуть мати звичайну форму, або спеціальну, яка розглянута вище.

Отже, в моделях ІАБ дії (помилки) оператора можуть враховуватися в таких варіантах:

- дії зроблені неправильно;
- дії, що призводять до відмов;
- як успішні й аварійні послідовності;
- як дії по відновленню оператором функцій систем, що відмовили;
- при аналізі взаємозалежності і взаємного впливу окремих подій (THERP);
- як типи різних помилок.

В цілому використання методики THERP цілком виправдано для моделювання помилок оператора. Методика проста, зрозуміла й однозначна. Для широкого її застосування необхідно навести зв'язок імовірності помилки оператора від його навченості, досвіду та стану діючої системи управління охороною праці на підприємствах різних галузей України, тобто адаптації методики до конкретних умов.

Застосування імовірнісних моделей для визначення ризику виробництва

Ризик виробництва розуміємо як змінну що характеризує стан безпеки виробництва і дорівнює добутку імовірності небажаної події на величину її наслідків.

Побудова структурно-логічних моделей процесів охорони праці

Якщо маємо випадковий процес дій людини в процесі виробництва, шляхом його дослідження, вивчення й аналізу можливо встановити залежності кінцевих подій від причин та базисних подій, що його складають, а звідсіля і

розробка моделей будь-яких НВ на базі наведених вище алгоритмів, визначення (побудова) структурно-логічної моделі НВ як системи інформаційного, природного або соціального характеру. Поняття “Система” розуміємо в загальному визначенні, як множину об’єктів разом із відносинами між об’єктами і їх атрибутами (визначення А. Хола). При цьому, на відміну від систем безпеки Security Operation Center, не завжди існують матеріальні зв’язки між елементами в вигляді трубопроводів або електричних з’єднань. Частіше в системах, що пропонується розглядати, зв’язки між елементами існують тільки в логічному виді. В цьому полягає різниця між системами Security Operation Center і системами що пропонується розглядати. Відношення системи до того чи іншого типу буде, очевидно, залежати від факторів та обставин, які пов’язані з джерелом небезпек, їх впливу на розвиток та наслідки небажаних подій. Ці фактори та обставини повинні бути проаналізовані фахівцями галузі, відібрані для складання й опису моделі ці з них, що складають замкнуту систему. Важливим етапом цієї роботи буде визначення базисних подій, при цьому обов’язкове дотримання всіх вище приведених вимог щодо базисної події. Фактори та обставини, які будуть прийматися за базисні події, повинні розглядатися як деякі захисні бар’єри, що перешкоджають появі та розвитку небажаної події. Базисна подія у цьому випадку розглядається як відмова захисного бар’єру, людська помилка, чи несприятлива умова для функціонування визначених захисних бар’єрів системи. Подія відмови, як і для технічних систем, не вимагає подальшої розробки, не може бути більше деталізована чи уточнена.

Побудова імовірнісних моделей (ДВ) в цьому випадку, аналіз системи, отримання МП, розрахунок імовірності небажаної події – все це задачі ІАБ, їх вирішення можливо за допомогою коду IRRAS.

Використання ДВ в задачах розрахунку ризиків безпеки систем Security Operation Center

На основі ДВ досить просто будувати моделі складних технічних систем. Якщо система, ризик якої визначається, сама складається з декількох систем,

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

здатних впливати на наслідки, доцільно вводити моделі дерев подій, що зв'язують роботу систем єдиною логікою. Можливе застосування методу аналізу ДВ і не для технічних систем. Як базисні події в такому випадку мають бути узяті такі події, що впливають на ризик (наслідки) і не можуть бути більш спрощені, при цьому імовірності чи інші їхні імовірнісні характеристики можуть бути знайдені якими-небудь методами. При цьому алгоритм і правила побудови й розрахунку ДВ змінюються відповідно до наведеного нижче алгоритму.

Основні кроки аналізу ризику за допомогою структурно-логічних моделей для будь яких систем:

- Визначити і коротко характеризувати небажану подію, що можлива як підсумкові дії небезпечного або шкідливого чинника.
- Визначити і коротко охарактеризувати початкову подію, що обумовлює дію шкідливого чинника.
- Визначити базисні (незалежні) події, що можуть впливати на процес дії небезпечного чинника за час від початкової події до небажаної події.
- Зробити оцінку інтервалу часу від початкової події до небажаної події.
- Визначити чинники й обставини, що можуть впливати на хід подій за час від початкової події до небажаної події.
- Оцінити зв'язок базисних подій (чинників) і обставин за час від початкової події до небажаної події.
- Визначити можливі міри й засоби запобігання дії шкідливого або небезпечного чинника, і ввести їх у модель базисними подіями.
- Визначити можливе втручання людини в процес і можливі помилки при цьому, і врахувати їх у імовірнісної моделі.
- Зробити оцінку ймовірностей приведених базисних подій.
- Побудувати дерево відмов, визначити ступінь ризику під час дії небезпечного чинника, і можливі шляхи запобігання небажаної події.

При побудові дерева надійності людини також як і при побудові дерева відмов систем, важливе значення мають всі допущення, припущення і межі визначеної системи.

Управління ризиками. Загальна схема

Мету управління ризиком при здійсненні будь-якої діяльності можна визначити як забезпечення безпеки персоналу і навколишнього природного середовища, шляхом встановлення і підтримки прийнятного рівня ризику, при використанні оптимальним чином з максимальною ефективністю наявних матеріальних ресурсів.

Управління ризиками – це діяльність, пов'язана з ідентифікацією, аналізом ризиків безпеки систем Security Operation Center і прийняттям рішень, спрямованих на мінімізацію негативних наслідків настання вихідних подій (явищ) і/чи зменшення імовірності їхньої реалізації до прийнятних значень. У загальному випадку процес управління ризиками при здійсненні діяльності на об'єкті включає виконання шести процедур (рисунок 3.2).

Планування управління ризиками – це процес прийняття рішень по застосуванню і плануванню управління ризиками для конкретної діяльності. Цей процес може містити в собі:

- Організацію на підприємстві спеціального підрозділу (групи управління ризиками), відповідального за оцінку і управління.
- Вибір методики оцінки ризиків безпеки систем Security Operation Center.
- Визначення джерел даних для ідентифікації ризику.
- Визначення тимчасового інтервалу для аналізу ситуації.

Дуже важливим буде визначення припустимих (прийнятних) рівнів ризику, які повинні вибиратися на основі чинного законодавства.

Ідентифікація ризиків безпеки систем Security Operation Center визначає, які ризики можуть вплинути на діяльність, що розглядається. Характеристики цих ризиків безпеки систем Security Operation Center повинні бути оформлені документально. Ідентифікація ризиків безпеки систем Security Operation Center

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

повинна проводитися регулярно протягом усієї діяльності об'єкта. Спеціалізований підрозділ повинний залучати до робіт по ідентифікації ризиків безпеки систем Security Operation Center всіх учасників процесу: проєктантів, експлуатаційників, фахівців інших підрозділів і незалежних експертів. Ідентифікація ризиків безпеки систем Security Operation Center повинна організовуватися як ітераційний процес. Перші розрахунки потенційного ризику виконують проєктанти. У процесі діяльності об'єкту, з урахуванням досвіду експлуатації, уточнюються дані по надійності систем і устаткування, процедурам управління, помилкам персоналу і робиться перерахунок ризиків безпеки систем Security Operation Center для об'єкту. Для формування об'єктивної оцінки в завершальній стадії процесу оцінки можуть брати участь незалежні експерти. Приклад ідентифікації ризиків безпеки систем Security Operation Center, для радіаційних ризиків безпеки систем Security Operation Center викладений у галузевому нормативному документі НРБУ-97/Д-2000.

Якісна оцінка ризиків безпеки систем Security Operation Center – це процес якісного аналізу результатів ідентифікації, а також визначення ризиків безпеки систем Security Operation Center, що вносять найбільший внесок у загальний ризик і які потребують вживання заходів по їхньому зниженню.

Як уже було показано раніше, останній етап якісного аналізу систем полягає в представленні умов невиконання функцій системи у вигляді так званої множини мінімальних перерізів [37]. Набір мінімальних перерізів системи однозначно визначений її деревом відмов і може бути отриманий при використанні спеціальних алгоритмів вибору мінімальних перерізів. Кількісні дані по базисних подіях впливають на важливість самого мінімального перерізу – його відсотковий вклад в імовірність відмов системи.

Якісна оцінка визначає ступінь важливості ризику і складових його подій. Доцільно створити банк даних ризиків безпеки систем Security Operation Center усієї діяльності на об'єкті, заснований на систематизованих даних, у тому числі даних по впливу ризиків безпеки систем Security Operation Center на персонал. На

цьому етапі можливо визначення чинників найбільшого впливу, що створить передумови управління.

Кількісна оцінка ризиків безпеки систем Security Operation Center визначає значення імовірності виникнення ризиків безпеки систем Security Operation Center і впливу їхніх наслідків на діяльність, що допомагає приймати оптимальні рішення й уникати невизначеності (у змісті управління) при цьому. Кількісна оцінка ризиків безпеки систем Security Operation Center передбачає виконання попередніх процесів, це завершальний етап задачі визначення ризиків безпеки систем Security Operation Center.

Планування реагування на ризики – це розробка методів і технологій зниження негативних наслідків ризиків безпеки систем Security Operation Center. Якісне, науково обґрунтоване планування можливе за умови виконання всіх попередніх етапів процесу відповідно до рисунка 3.2. Стратегія планування повинна відповідати типам ризиків безпеки систем Security Operation Center, їх величині і значимості, наявності ресурсів і тимчасових параметрів. У найбільш небезпечних випадках, можливо потрібно кілька варіантів реагування на ризики. Планування повинне здійснюватися у відповідності зі спеціальною методикою, що враховує специфіку об'єкту, чинні на ньому правила й інструкції.

Реалізація прийнятого рішення проводиться з врахуванням даних моніторингу і контролю параметрів, що проводяться з метою перевірки дотримання вимог встановлених норм. Моніторинг і контроль повинні здійснюватися спеціалізованим підрозділом об'єкту. При цьому повинні постійно контролюватися процес ідентифікації ризиків безпеки систем Security Operation Center, виконання плану реагування на ризики, оцінка ефективності заходів для зниження ризиків безпеки систем Security Operation Center, величина залишкового ризику і його прийнятність.

Якісний контроль виконання діяльності подає інформацію, що сприяє прийняттю ефективних рішень по запобіганню нових ризиків безпеки систем Security Operation Center чи зм'якшення наслідків. Контроль може ініціювати

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

вибір альтернативних стратегій, прийняття коректив, перепланування проекту для досягнення базового плану.

Для цілей моніторингу і перевірки дотримання норм забезпечується належне устаткування і впроваджуються відповідні процедури перевірки. Зазначене устаткування належним чином обслуговується і випробовується, а також калібрується з належною періодичністю на основі еталонів, що відповідають національним чи міжнародним еталонам.

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

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

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей.

Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

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

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

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

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

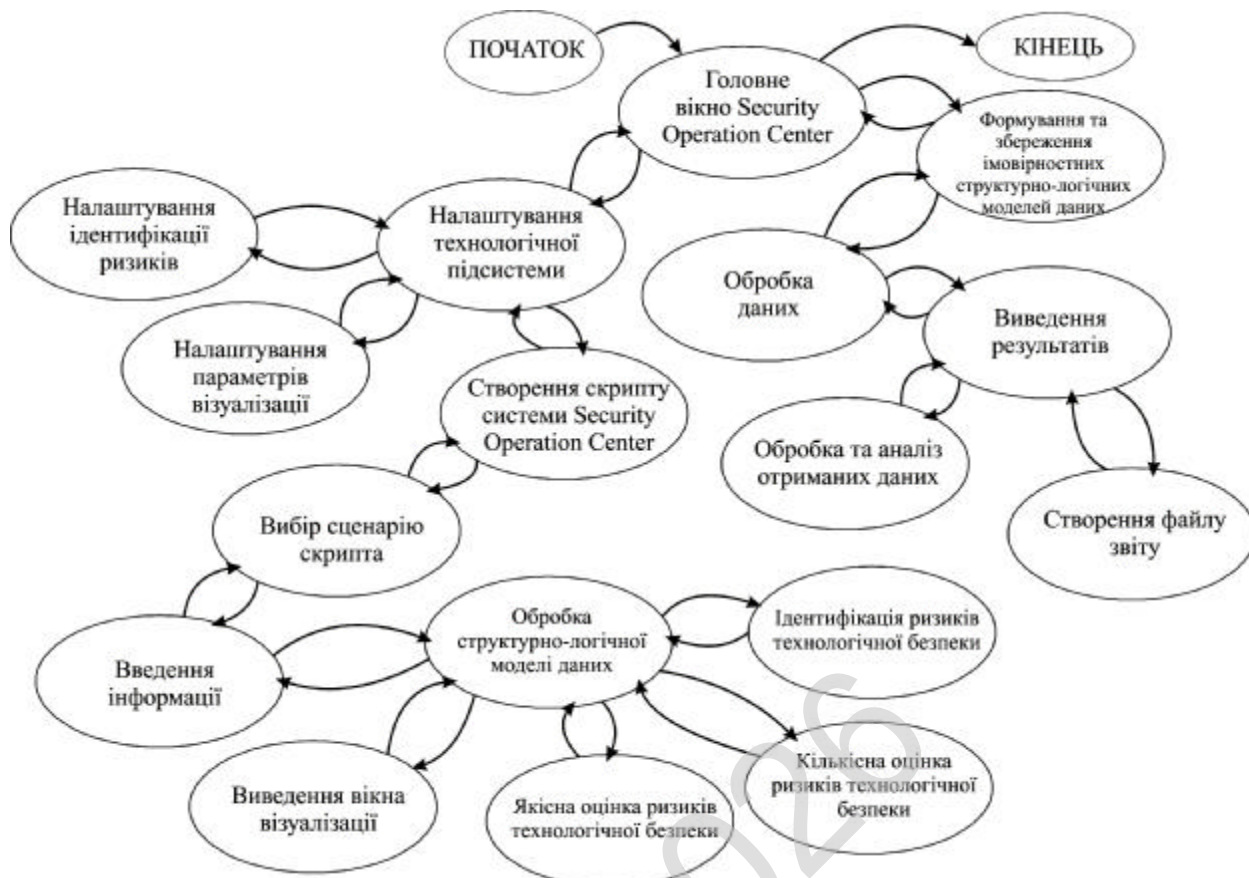


Рисунок 3.3 – Діаграма взаємодії процесів

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

Діаграми потоків даних містять чотири типи елементів:

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).

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.

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

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

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

Основні характеристики СКБД

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

Можливості СКБД

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

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

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

Основні компоненти середовища СКБД

1. Апаратне забезпечення.

2. Програмне забезпечення.

3. Дані.

4. Процедури – інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.

5. Користувачі: адміністратори даних (керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних); розробники БД; прикладні програмісти; кінцеві користувачі.

Архітектура СКБД

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

Рівні:

1. Зовнішній – представлення БД з точки зору користувача.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

2. Концептуальний – узагальнене представлення БД, описує які дані зберігаються в БД і зв'язки між ними. Підтримує зовнішні представлення, підтримується внутрішнім рівнем.

3. Внутрішній – фізичне представлення БД в комп'ютері.

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

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

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 роботу підпрограми.

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

Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування.

Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий стандарт, що використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю.

UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

Було використано наступні підходи UML: діаграма прецедентів (діаграми поведінки типу); Діаграма класів; Діаграма розгортання.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

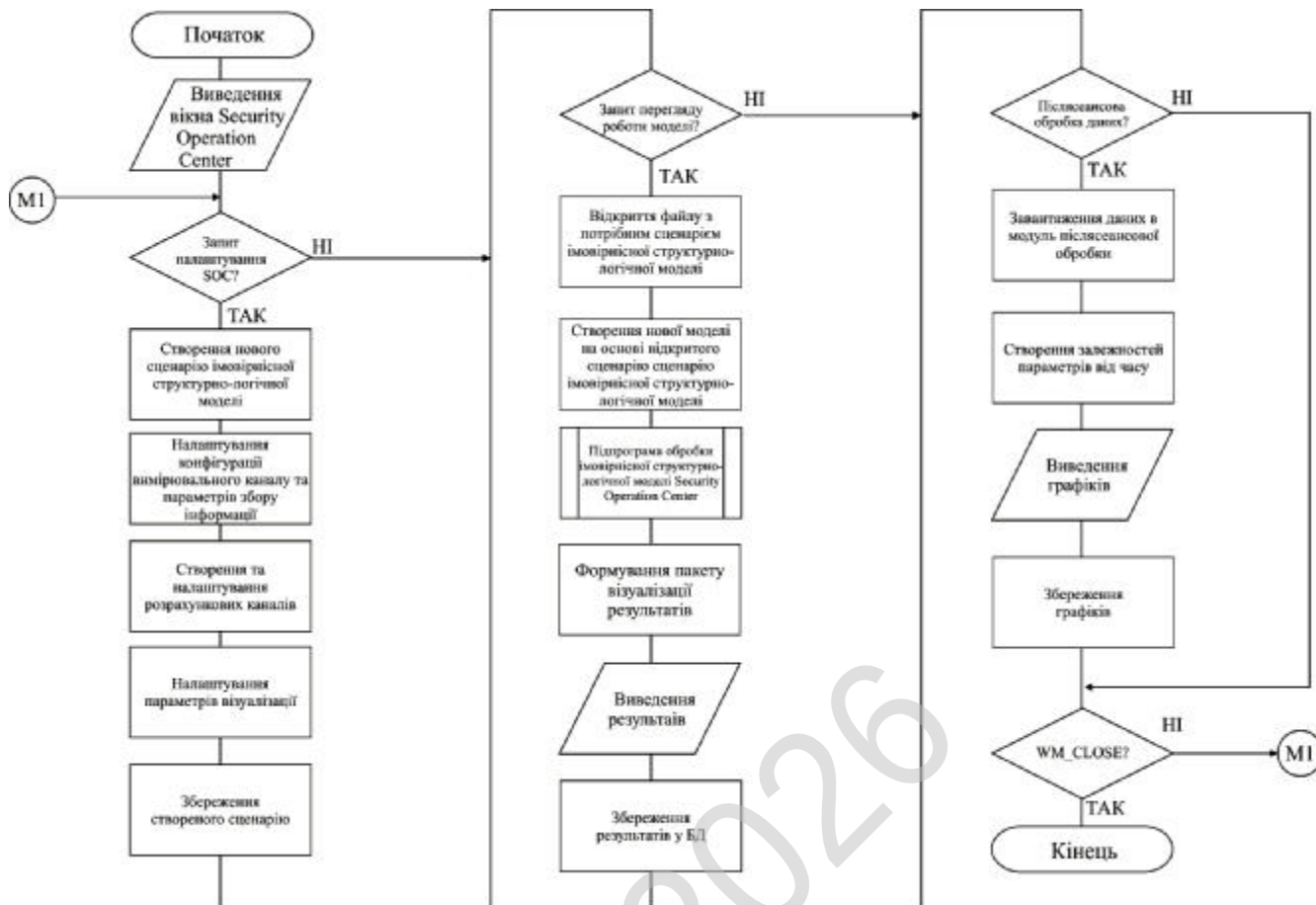


Рисунок 4.1 – Блок-схема основної програми

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.

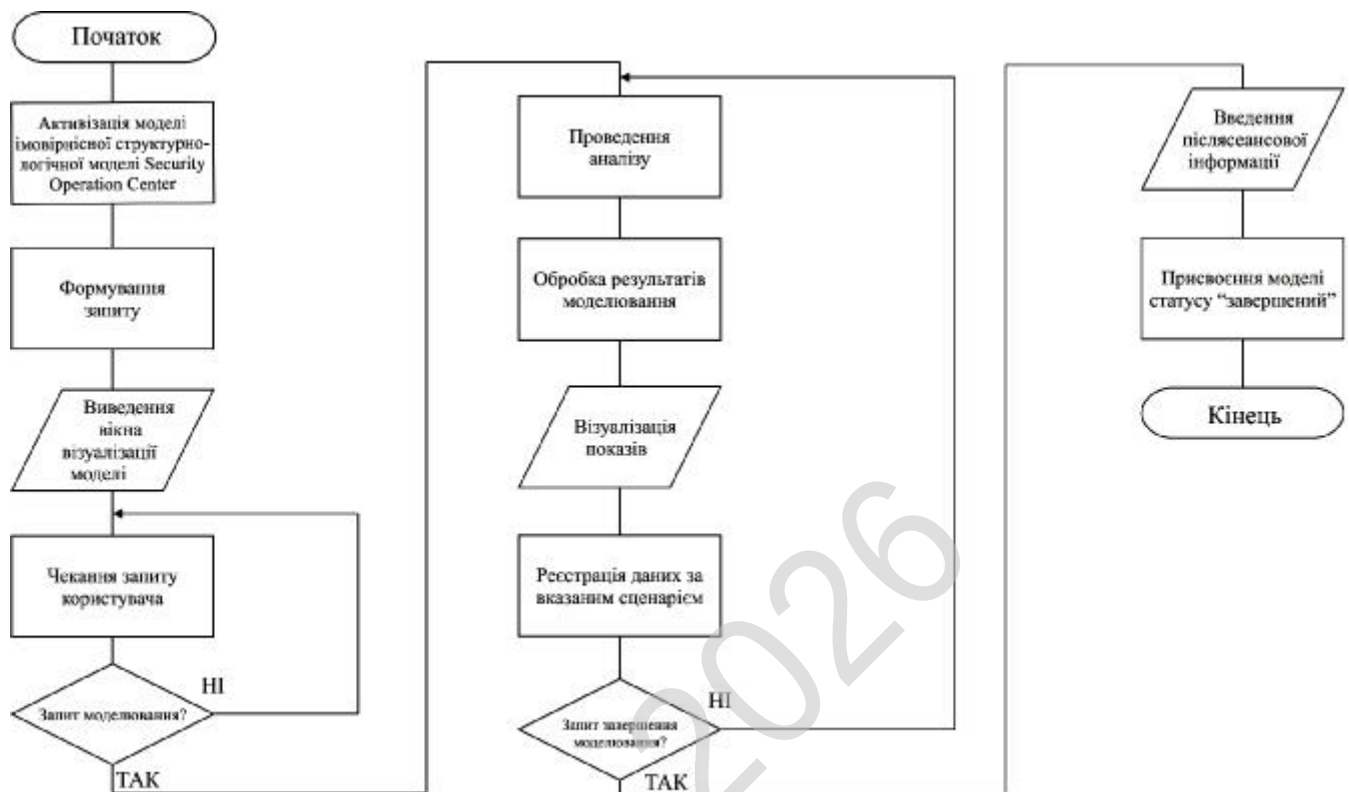


Рисунок 4.2 – Блок-схема роботи підпрограми

Архітектура системи

Програмне забезпечення системи кібербезпеки для реалізації Security Operation Center працює як локальна SOC платформа для збору, аналізу та реагування на події безпеки. Система приймає журнали подій від серверів, робочих станцій, мережевих пристроїв і прикладних сервісів, визначає підозрілі дії та формує інциденти для подальшої перевірки аналітиком.

Система має модульну архітектуру. Модуль збору подій приймає записи журналів у форматі JSON. Модуль нормалізації приводить події до єдиної структури. Модуль аналізу ризику перевіряє події за правилами. Модуль інцидентів створює записи про загрози. Модуль збереження даних використовує SQLite. Модуль звітності показує кількість подій, інцидентів і рівень критичності.

Основні функції

1. Збір подій безпеки з файлу журналу
2. Нормалізація IP адреси, користувача, типу події та часу
3. Виявлення невдалих входів, підозрілих IP адрес і критичних дій
4. Розрахунок рівня ризику для кожної події
5. Створення інцидентів SOC
6. Збереження подій та інцидентів у базі даних
7. Формування короткого звіту для аналітика

Основні модулі

1. EventCollector відповідає за читання журналів
2. RiskAnalyzer виконує оцінювання загроз
3. IncidentManager створює інциденти
4. SOCDatabase зберігає результати аналізу
5. SOCReport формує підсумкову інформацію

Розглянемо основну частину вихідного коду де можна побачити основні підходи та функціонал.

```
import json
import sqlite3
from datetime import datetime
from pathlib import Path

DB_NAME = "soc_center.db"
LOG_FILE = "security_events.jsonl"

#Модуль збереження подій та інцидентів SOC
class SOCDatabase:
    def __init__(self, db_name=DB_NAME):
        self.connection = sqlite3.connect(db_name)
        self.create_tables()
    def create_tables(self):
        cursor = self.connection.cursor()
        cursor.execute("""
            CREATE TABLE IF NOT EXISTS events (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
                event_time TEXT,
                source_ip TEXT,
```

```

        username TEXT,
        event_type TEXT,
        message TEXT,
        risk_score INTEGER
    )
    """
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS incidents (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            created_at TEXT,
            source_ip TEXT,
            username TEXT,
            severity TEXT,
            description TEXT,
            status TEXT
        )
    """)
    self.connection.commit()
    def save_event(self, event):
        cursor = self.connection.cursor()
        cursor.execute("""
            INSERT INTO events (
event_time, source_ip, username, event_type, message, risk_score
            )
            VALUES (?, ?, ?, ?, ?, ?)
        """, (
            event["event_time"],
            event["source_ip"],
            event["username"],
            event["event_type"],
            event["message"],
            event["risk_score"]
        ))
        self.connection.commit()
    def save_incident(self, incident):
        cursor = self.connection.cursor()
        cursor.execute("""
            INSERT INTO incidents (
created_at, source_ip, username, severity, description, status
            )
            VALUES (?, ?, ?, ?, ?, ?)
        """, (

```

```

        incident["created_at"],
        incident["source_ip"],
        incident["username"],
        incident["severity"],
        incident["description"],
        incident["status"]
    ))
    self.connection.commit()
def get_report(self):
    cursor = self.connection.cursor()
    cursor.execute("SELECT COUNT(*) FROM events")
    events_count = cursor.fetchone()[0]
    cursor.execute("SELECT COUNT(*) FROM incidents")
    incidents_count = cursor.fetchone()[0]
    cursor.execute("""
        SELECT severity, COUNT(*)
        FROM incidents
        GROUP BY severity
    """)
    severity_data = cursor.fetchall()
    return events_count, incidents_count, severity_data
def close(self):
    self.connection.close()
#Модуль збору та нормалізації журналів безпеки
class EventCollector:
    def __init__(self, file_path):
        self.file_path = Path(file_path)
    def load_events(self):
        events = []
        if not self.file_path.exists():
            return events

        with self.file_path.open("r", encoding="utf-8") as file:
            for line in file:
                try:
                    raw_event = json.loads(line.strip())
                    events.append(self.normalize_event(raw_event))
                except json.JSONDecodeError:
                    continue
        return events
    def normalize_event(self, raw_event):
        return {

```

```

    "event_time": raw_event.get("event_time", datetime.now().isoformat()),
    "source_ip": raw_event.get("source_ip", "0.0.0.0"),
    "username": raw_event.get("username", "unknown"),
    "event_type": raw_event.get("event_type", "unknown"),
    "message": raw_event.get("message", "")
}

#Модуль аналізу ризику подій
class RiskAnalyzer:
    def __init__(self):
self.suspicious_ips = {"10.10.10.13", "192.168.1.250", "172.16.5.99"}
        self.critical_events = {
            "privilege_escalation",
            "malware_detected",
            "data_exfiltration",
            "firewall_block"
        }
    def calculate_risk(self, event):
        score = 0
        if event["source_ip"] in self.suspicious_ips:
            score += 40
        if event["event_type"] == "failed_login":
            score += 25
        if event["event_type"] in self.critical_events:
            score += 60
        if "admin" in event["username"].lower():
            score += 15
        if "denied" in event["message"].lower():
            score += 10
        return min(score, 100)
    def define_severity(self, risk_score):
        if risk_score >= 80:
            return "critical"
        if risk_score >= 50:
            return "high"
        if risk_score >= 30:
            return "medium"
        return "low"

#Модуль створення інцидентів SOC
class IncidentManager:
    def create_incident(self, event, severity):
        if severity == "low":
            return None

```

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

```

        return {
            "created_at": datetime.now().isoformat(),
            "source_ip": event["source_ip"],
            "username": event["username"],
            "severity": severity,
            "description": f"SOC виявляє подію {event['event_type']} з ризиком
{event['risk_score']}",
            "status": "new"
        }
#Модуль запуску SOC обробки
class SOCApplication:
    def __init__(self):
        self.database = SOCDatabase()
        self.collector = EventCollector(LOG_FILE)
        self.analyzer = RiskAnalyzer()
        self.incident_manager = IncidentManager()
    def run(self):
        events = self.collector.load_events()
        for event in events:
            risk_score = self.analyzer.calculate_risk(event)
            event["risk_score"] = risk_score
            severity = self.analyzer.define_severity(risk_score)
            self.database.save_event(event)
        incident = self.incident_manager.create_incident(event, severity)
        if incident:
            self.database.save_incident(incident)
        self.print_report()
        self.database.close()
    def print_report(self):
        events_count, incidents_count, severity_data = self.database.get_report()
        print("Звіт Security Operation Center")
        print(f"Оброблено подій: {events_count}")
        print(f"Створено інцидентів: {incidents_count}")
        for severity, count in severity_data:
            print(f"Рівень {severity}: {count}")
#Приклад створення тестового журналу подій
def create_demo_log():
    demo_events = [
        {
            "event_time": datetime.now().isoformat(),
            "source_ip": "192.168.1.250",
            "username": "admin",

```

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

```

        "event_type": "failed_login",
        "message": "Access denied for administrator account"
    },
    {
        "event_time": datetime.now().isoformat(),
        "source_ip": "10.0.0.12",
        "username": "user01",
        "event_type": "normal_login",
        "message": "User login success"
    },
    {
        "event_time": datetime.now().isoformat(),
        "source_ip": "172.16.5.99",
        "username": "operator",
        "event_type": "malware_detected",
        "message": "Suspicious file is blocked"
    }
]
with open(LOG_FILE, "w", encoding="utf-8") as file:
    for event in demo_events:
        file.write(json.dumps(event, ensure_ascii=False) + "\n")
if __name__ == "__main__":
    create_demo_log()
    app = SOCAApplication()
    app.run()

```

4.2 Захист розробленого програмного забезпечення

Захист розробленого програмного забезпечення буде відбуватися за допомогою алгоритму UMAC (код автентифікації повідомлення на основі універсального гешування) – один з видів коду автентичності повідомлень (MAC).

Швидка «універсальна» функція використовується, для того, щоб гешувати вхідне повідомлення M у короткий рядок. До цього рядка потім застосовується функція XOR із псевдовипадковим значенням, у результаті чого ми одержуємо тег UMAC:

$$\text{Tag} = H_{K1}(M) \oplus F_{K2}(\text{Nonce})$$

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		64

де K_1 і K_2 – секретні випадкові ключі, які мають одержувач і відправник.

Звідси видно, що безпека UMAC залежить від того, яким випадковим способом відправник і одержувач вибрали таємну геш-функцію й псевдовипадкову послідовність. При цьому значення Nonce міняється кожний такт. Через використання Nonce, приймач і передавач повинні знати час відправлення повідомлення й принцип створення значення Nonce. Замість цього можна використовувати в якості Nonce будь-яке інше неповторюване значення, наприклад порядковий номер повідомлення. При цьому даний номер не зобов'язано бути секретним, головне щоб він не повторювався.

UMAC розрахований на використання 32-х, 64-х, 92-х, і 128-бітових тегів, залежно від необхідного рівня безпеки. UMAC звичайно використовується разом з алгоритмом шифрування AES.

Функція створення ключа й псевдовипадкової послідовності

Створення псевдовипадкових байтів необхідно для роботи UHASH і при створенні тегів

Вибір блокового шифру

Для своєї роботи UMAC використовує блоковий шифр, вибір якого визначають наступні константи:

- BLOCLEN – довжина, у байтах, блоку з яким працює блоковий шифр.
- KEYLEN – довжина, у байтах, ключа блокового шифру.

При цьому використовується функція

– ENCIPHER(K, P) – зашифрувати рядок P з BLOCLEN байтів, використовуючи ключ K .

Приклад: якщо використовується AES з 16-байтним ключем, то BLOCLEN буде рівним 16(тому що AES працює з 16-байтними блоками).

KDF – функція створення ключа

Ця функція генерує послідовність псевдовипадкових байтів, використовуваних для ключових геш-функцій.

Вхід:

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

- K – рядок довжиною KEYLEN байт. // Ключ блокового шифру.
- Index – ненегативне ціле число менше, чим 2^{64} .
- Numbytes – ненегативне ціле число менше, чим 2^{64} .

Вихід:

- Y – рядок довжини numbytes байт.

PDF: функція створення псевдовипадкового числа

Ця функція ухвалює ключ і даний час і повертає псевдовипадкове число для використання його в тегу покоління. За допомогою цієї функції можуть бути отримані числа довжиною 4, 8, 12 або 16 байт.

Вхід:

- K – рядок довжиною KEYLEN байт.
- Nonce – рядок довжиною від 1 до BLOCKLEN байт.
- Taglen – ціле число 4, 8, 12 або 16.

Вихід:

- Y – послідовність байтів довжини taglen.

Генерація UMAC-тегів

Генерація UMAC-тегів відбувається за допомогою UHASH функції при використанні Nonce значенні й отриманої до цього рядка. Їхня довжина може бути 4, 8, 12 або 16 байт.

Вхід:

- K – рядок довжиною KEYLEN байт.
- M – рядок довжиною менше 267 біт.
- Nonce – випадкове число від 1 до BLOCKLEN байт.
- Taglen – ціле 4, 8, 12 або 16.

Вихід:

- Тег, послідовність байтів довжиною taglen.

Алгоритм обчислення тегів:

Hashedmessage = UHASH(K, M, Taglen)

Pad = PDF(K, nonce, Taglen)

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

Tag = Pad xor Hashedmessage

UMAC-32 UMAC-64 UMAC-96 UMAC-128

Дані позначення містять у своїй назві певне значення довжини тегу:

- UMAC-32 (K, M, Nonce) = UMAC (K, M, Nonce, 4).
- UMAC-64 (K, M, Nonce) = UMAC (K, M, Nonce, 8).
- UMAC-96 (K, M, Nonce) = UMAC (K, M, Nonce, 12).
- UMAC-128 (K, M, Nonce) = UMAC (K, M, Nonce, 16).

Універсальна функція гешування(UHASH)

UHASH – універсальна функція гешування, серцевина алгоритму UMAC.

UHASH – функція працює в три етапи. Спочатку до вхідного повідомлення застосовується L1-HASH, потім до цього результату застосовується L2-HASH і, нарешті, до результату застосовується L3-HASH . Якщо при цьому довжина вхідного повідомлення не більш 1024 біт, то L2-HASH не використовується. Тому що функція L3-hash повертає тільки слово довжини 4 байта, те якщо потрібно одержати геш довжини більше 4 байт, здійснюється кілька ітерацій даної трирівневої схеми.

Універсальна функція

Нехай функція гешування вибирається із класу геш-функцій H, які відображають повідомлення в D, набір усіляких образів повідомлення. Цей клас називається універсальним, якщо для яких-небудь окремих пар повідомлень, існує на безлічі H/D функцій, функція, яка відображає їх в елемент D. Зміст цієї функції в тому, що якщо третя сторона прагне замінити одне повідомлення іншим, але при цьому вважає, що геш-функція була обрана абсолютно випадково, те ймовірність не виявлення підміни стороною, що ухвалює, прагне до 1/D.

L1-hash – перший етап

L1-hash розбиває повідомлення на шматки з 1024 байт і до кожного шматка застосовує алгоритм гешування називаний NH. Вихідний результат алгоритму NH в 128 раз менше вхідного.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

L2-hash – другий етап

L2-hash працює з виходом L1-hash, використовує поліноміальний алгоритм POLY. Другий етап гешування використовується, тільки якщо довжина вхідного повідомлення більше 16 мегабайт. Використання алгоритму POLY потрібно для того, щоб уникнути тимчасову атаку. На виході з алгоритму POLY виходить 16 байтне число.

L3-hash – третій етап

Цей етап потрібно для того щоб з вихідних 16 байтів алгоритму L2-hash одержати 4-байтне значення.

К6ПЗ-2026

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		68

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі програмне забезпечення системи кібербезпеки призначеної для реалізації Security Operation Center. 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.
- Верхнього меню: Файл; Сервіс; Структурно-логічна модель; Налаштування; Довідка.
- Розділу обрання групи.
- Розділу виведення результату роботи системи.

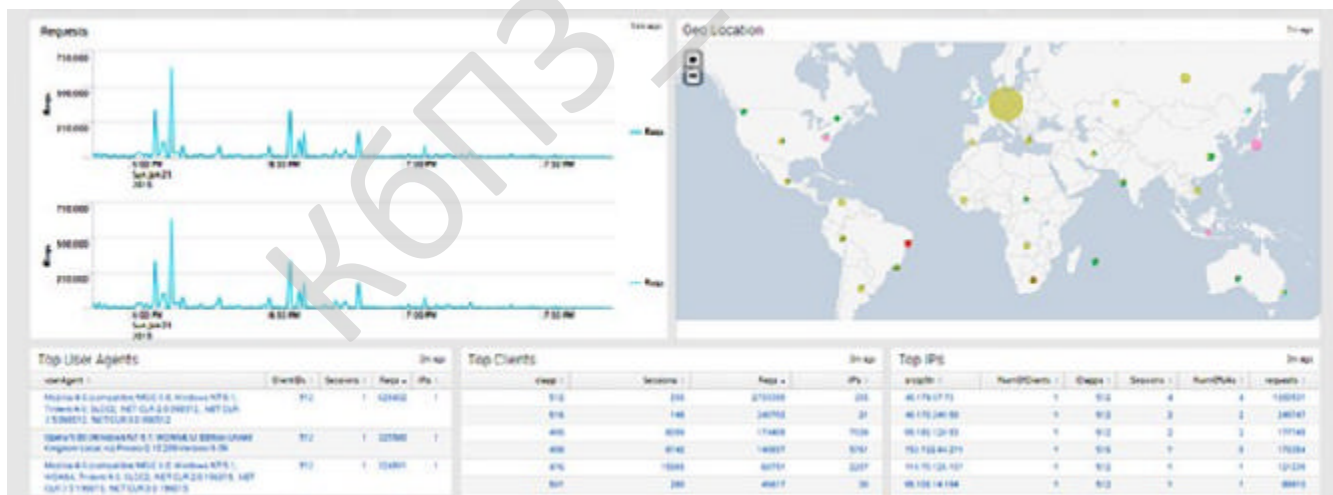


Рисунок 5.1 – Головне вікно ПЗ

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

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

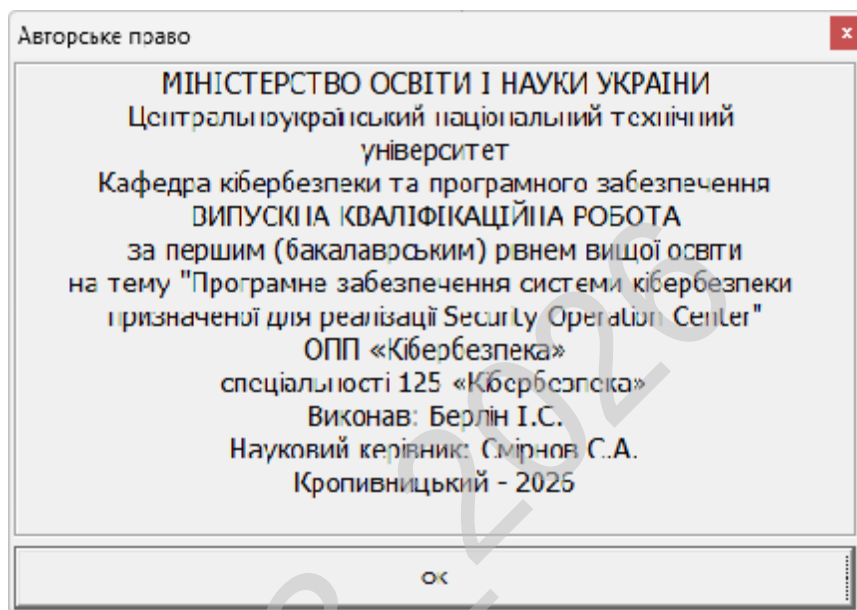


Рисунок 5.2 – Авторське право

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

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70

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.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження;

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

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в ІТ рішення за принципом найбільшої корисності для більшості учасників.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		71

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

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

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

Проводилась оцінка:

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

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

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

Проводилось тестування 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.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

– Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

– У програмі можуть бути пропущені деякі маршрути.

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

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

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

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

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

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

Проводилось тестування чорної скриньки.

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

Ці тести демонструють:

– Як виконуються функції програми.

– Як приймаються вихідні дані.

– Як виробляються результати.

– Як зберігається цілісність зовнішньої інформації.

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

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

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

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

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

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

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

Будь-який спосіб тестування «чорної скриньки» повинен:

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

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

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

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

Обрано умови розповсюдження – Shareware. Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження

комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії (тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

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

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

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

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

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки призначеної для реалізації Security Operation Center.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем призначеної для реалізації Security Operation Center.
- Досліджена система призначеної для реалізації Security Operation Center.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки призначеної для реалізації Security Operation Center.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання призначеної для реалізації Security Operation Center.

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

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

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для системи кібербезпеки призначеної для реалізації Security Operation Center. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід,

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		76

зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи кібербезпеки й включає програми, що реалізують її функції.

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

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм UMAC.

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

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.
2. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.
3. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
4. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
5. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
6. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
7. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
8. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
9. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
10. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
11. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
12. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

13. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

14. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

15. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

16. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

17. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

18. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

19. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security

Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

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

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

22. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.

23. 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.

24. 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.

25. 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.

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

27. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		80

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

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

29. 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.

30. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

31. 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.

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

33. 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.

					ВКРБ-125.26.0021.00.00.ПЗ	Арк. 81
Вим.	Арк.	№ докум.	Підпис	Дата		

34. 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.

35. 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.

36. 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,

37. 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.

38. 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.

39. 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.

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

					ВКРБ-125.26.0021.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		82

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

41. 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.

42. 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

43. 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.

44. 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.

45. 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.

46. 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.

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

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.

64. 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.

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

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

72. 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.

73. 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.