Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей»

Виконав: студент 2-го курсу, групи 1БС-22м
спеціальності 125 «Кібербезпека»
_____ Денис ВАСІЛЕВСЬКИЙ
Керівник : к.т.н., доц., доц. каф. ЗІ
_____ Вадим МАЛІНОВСЬКИЙ
«18» 12 2023 р.
Опонент: д.т.н., проф., проф. каф. ПЗ
_____ Людмила ЛІЩИНСЬКА
«18» 12 2023 р.

Допущено до захисту

Завідувач кафедри ЗІ
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«18» 12 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
Володимир ЛУЖЕЦЬКИЙ
«13» 09 **2023 року**

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Василевському Денису Анатолійовичу

1. Тема роботи: «Метод підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей»;
керівник роботи: Маліновський Вадми Ігорович , к.т.н., доц. каф. ЗІ,
затверджені наказом ректора ВНТУ від 18 вересня 2023 року, протокол № 247.
2. Строк подання студентом роботи 13 грудня 2023 р.
3. Вихідні дані до роботи:
   - тип системи і методу: інформаційна система контролю доступу (ІС СКУД); із багатопараметричним методом ідентифікації, із кількістю параметрів N>2;
   - тип кінцевих пристроїв: IoT-пристроїв із IP-інтерфейсом;
   - тип вхідних даних: цифрові дані, що надходять у ІС СКУД;
   - тип реалізації : структурна , апаратна та програмна реалізація методів.

   Необхідно розробити та\або вдосконалити:
   - метод захисту інформації в ІС СКУД ;
   - модель захисту інформації та структурні схеми в ІС СКУД .

   Необхідно провести експериментальне дослідження розроблених рішень.
4. Зміст текстової частини: Вступ. 1. Науково-технічне обґрунтування доцільності досліджень та аналіз технологій ІС СКУД, а також методів і підходів захисту даних ІС СКУД. Аналіз технологій і параметрів інтерфейсів в ІС СКУД. 2. Проведення удосконалення методів і моделі, а також структур ІС СКУД із метою підвищення рівня інформаційної безпеки. 3. Експериментальні дослідження та програмна реалізації окремих рішень досліджень. Моделювання та розрахунки параметрів ІС СКУД 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Модель ІС безпеки ір-контролера в СКУД

(плакат А4). Мережева модель роботи ІС СКУД на основі вдосконален методу(плакат А4). Структурна схема інтерфейсу ІС СКУД (плакат А Структурна схема системи ІС СКУД із ір-контролером (плакат А4). Моде безпеки ІС СКУД, що ілюструє принцип багатопараметричної ідентифікації параметрам (плакат А4). Структура ІС СКУД із 2-х рівневим кіберзахистом IoT приладами (плакат А4). Модель ІС захисту СКУД (плакат А4). Ілюстра методу підвищення інформаційного захисту в ІС СКУД (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Вадим МАЛІНОВСЬКИЙ, к.т.н., доц. каф. ЗІ	1505.2023	
2	Вадим МАЛІНОВСЬКИЙ, к.т.н., доц. каф. ЗІ	19.05.2023	
3	Вадим МАЛІНОВСЬКИЙ, к.т.н., доц. каф. ЗІ	12.09.1.23	
4	Ольга РАТУШНЯК, к.т.н., доц. каф. ЕПВМ		

7. Дата видачі завдання 1 вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Приміт
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обгрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обгрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Денис ВАСІЛЕВСЬКИЙ

Керівник роботи _____ Вадим МАЛІНОВСЬКИЙ

УДК 004.056

Василевський Д.А Метод доступу на основі пристроїв робота зі спеціальності 125 інформаційних і комунікаційн

На укр. мові. Бібліогр: 3

В магістерській кваліф моделі підвищення рівня ін основі пристроїв Інтернету інноваційними і передбача підвищення безпеки ш ідентифікації та/або ауте зокрема передбачають гну етапи захисту даних та вигляді унікального циф суб'єкта доступу. Це інформаційної системи пристроїв Інтернету підлаштовуємість. Пре вдосконалення існуючи для досягнення мети.

Ілюстративна ча

В економічному

Ключові слова речей, захист інформ

АНОТАЦІЯ

УДК 004.056

Василевський Д.А Метод підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. – Вінниця: ВНТУ, 2023. – 102 с.

На укр. vові. Бібліогр: 33 назв; рис.: 37; табл. 1.

В магістерській кваліфікаційній роботі представлено розробку методу і моделі підвищення рівня інформаційного захисту систем контролю доступу на основі пристроїв Інтернету речей. Запропоновані в роботі метод і модель є інноваційними і передбачають вдосконалення вже існуючих підходів і методів підвищення безпеки шляхом модифікації підходів мультифакторного ідентифікації та/або аутентифікації за декількома (багатьма) параметрами, зокрема передбачають гнучку стадію вибору кількості параметрів та додаткові етапи захисту даних та вибір і обробку самих параметрів ідентифікації у вигляді унікального цифрового зліпка, що може унікально ідентифікувати суб'єкта доступу. Це в сукупності дозволяє підвищити рівень захисту інформаційної системи комплексу контролю доступу (ІС СКУД) на основі пристроїв Інтернету речей та запровадити необхідну гнучкість і підлаштовуємість. Представлені в МКР рішення є новими і передбачають вдосконалення існуючих підходів та використання їх у сукупності із іншими для досягнення мети.

Ілюстративна частина складається з 8 плакатів.

В економічному розділі оцінено витрати на роботу.

Ключові слова: система контролю доступу на основі пристроїв Інтернету речей, захист інформаційної системи, ідентифікація, аунтентифікація.

ABSTRACT

Vasilevsky D.A. Method of increasing the level of protection of the access control system based on Internet of Things devices. Master's qualification work in the specialty 125 - Cybersecurity, educational program - Security of information and communication systems. – Vinnytsia: VNTU, 2023. – 102 p.

In Ukrainian language. Bibliography: 33 titles; Figures: 37; Table 1.

The master's qualification work presents the development of a method and model for increasing the level of information security of access control systems based on Internet of Things devices. The method and model proposed in the work are innovative and provide for the improvement of existing approaches and methods to improve security by modifying approaches to multifactor identification and/or authentication by several (many) parameters, in particular, provide for a flexible stage of selecting the number of parameters and additional stages of data protection and the selection and processing of the identification parameters themselves in the form of a unique digital impression that can uniquely identify the access subject. All of this together makes it possible to increase the level of protection of the access control information system (ACIS) based on IoT devices and introduce the necessary flexibility and adaptability. The solutions presented in the ICR are new and involve improving existing approaches and using them in conjunction with others to achieve the goal.

The illustrative part consists of 8 posters.

The economic section estimates the costs of the work.

Keywords: access control system based on IoT devices, information system protection, identification, authentication.

ЗМІСТ

ВСТУП

Актуальність теми. В сучасні часи, в роки широкої автоматизації та інформатизації часто постає практичне і теоретичне зевдання забезпечення фізичного контролю доступу до окремих технологічних зон на промислових комерційних і державних об’єктах, за рахунок використання систем контролю доступу (СКУД) на базі автоматизованих інформаційних систем та пристроїв автоматики. Такі системи забезпечують персоніфікований контрольований доступ суб’єктів (працівників та іншого персоналу) в окремі технологічні зони об’єкта по контрольованим правам доступу і із фіксації такої події. Це дозволяє організувати автоматичний чи автоматизований процес доступу на об’єкт із фіксацією подій доступу та моніторингом подій і самих об’єктів доступу на відео, значно підвищує безпеку і робить процеси несанкціонованого доступу, інциденти викрадення майна, інформації та інших цінностей, несанкціонованого фізичного доступу до них на об’єктах практично неможливим, або значно ускладненим, що в сукупності значно підвищує безпеку підприємств та організацій, на яких запроваджені СКУД [1, 3].

Впровадження інформаційних систем контролю доступу – ІС СКУД на сучасних підприємствах – значна і тривала тенденція, яка як показує практика значно підвищує безпеку і економічну ефективність організацій і підприємств.

Але існує проблема – навіть сучасні системи контролю доступу СКУД та їх інформаційні системи – ІС СКУД на базі пристроїв IoT (Інтернету речей) – не можуть забезпечити належний рівень інформаційної безпеки і кібербезпеки, що може значно вплинути на стабільність процесів оброблення і передавання інформації і роботи самих функціональних сервісів ІС СКУД [1, 2].

Тому, потрібно і необхідно вживати заходів для підвищення безпеки систем контролю доступу, вживати заходів захисту їх інформаційних мереж [2], систем й інтерфейсв СКУД та інших складових інформаційної системи IoT.

Для рішення проблеми покращення інформаційного захисту СКУД передбачається вдосконалення існуючих методу та моделі інформаційного захисту СКУД із IoT-пристроями на базі багатопараметричної ідентифікації

та/або автонтифікації для захисту інформації в ІС СКУД на базі IoT в організаціях та установах.

Метою є підвищення рівня захищеності інформаційної системи контролю доступу на базі пристроїв Інтернету речей.

Предметом є метод підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей.

Об'єктом є процес інформаційного захисту системи контролю доступу на основі пристроїв Інтернете речей в організаціях.

Для досягнення мети та завдань роботи передбачається використання удосконалених методу, моделі та алгоритму кіберзахисту ІС СКУД на базі IoT пристроїв із комплексним підходом до захисту інформації в каналах, та використання багатопараметричної ідентифікації та\або автонтифікації.

Апробація результаів наукової роботи підтверджується тим, що окремі результати МКР були опубліковані автором у роботі [13].

Наукова новизна одержаних результатів полягає у тому що:

– вдосконалено метод захисту інформації в ІС СКУД, що дозволило підвищити рівень захисту інформаційної системи контролю доступу і роботу із вищою стабільністю та підвищеним захистом від атак несанкціонованої ідентифікації та/або автонтифікації.

– вдосконалено модель безпеки даних та математичну модель ІС СКУД, що дозволяє впровадити комплексаний моніторинг подій в ІС СКУД та інтерфейсах СКУД, що на відміну від відомої включає підходи багатопараметричного контролю та дозволяє враховувати супутні параметри та інші чинники, які можуть впливати на безпеку ІС СКУД.

Практичне значення одержаних результатів полягає у тому що :

– вдосконалено алгоритмічну і структуру організацію інформаційної системи захисту СКУД, яка на відміну від відомої включає додаткові блоки – багатопараметричної ідентифікації та шифрування в системі, блоки фільтрації подій та містить спеціальні блоки моніторингу параметрів на вході і на виході ІС СКУД;

– модифіковано алгоритм процесу роботи СКУД, схему інтерфейсу СКУД і

структурну схему самої системи ІС СКУД. Розроблено окремий програмний модуль для моделювання і дослідження процесу багататопараметричної ідентифікації в ІС СКУД. Це дозволило розширити функціональні можливості, зменшити число комунікацій в ІС СКУД, та проводити формування унікальних об’єднаних сигналів багатопараметричної ідентифікації, що ідентифікують об’єкт доступу і можуть бути використані для підвищення захищеності ІС СКУД.

1 АНАЛІЗ СУЧАНИХ ТЕХНОЛОГІЙ СКУД НА БАЗІ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Принципи і проблематика кіберзахисту системи контролю доступу

Програмне забезпечення та інформаційна система (ІС) сучасних СКУД дозволяє вирішувати завдання контролю доступу і фіксації робочого часу співробітників в різних зонах на технологічних об'єктах – комерційних і державних. Інформаційна система комплексу СКУД має інтегровані комплексні функції високоінтелектуальної обробки даних (на базі ПЗ високого рівня), клієнт-серверну архітектуру, в т.ч. інтеграцію функціоналу ІС СКУД із системою відеоспостереження (СВС), функції розпізнавання облич, функції біометричного контролю, контролю інших параметрів (наркотичного та алкогольного сп'яніння, чи температури тіла) і загального стану здоров'я або окремих показників. Також в більшості відомих СКУД є функції доступу по ID-картам та іншим параметрам [2]. Програмний модуль ПЗ сучасних СКУД [4] забезпечує ідентифікацію та фіксацію перебування в різних зонах співробітників, контроль доступу, реєстрацію робочого часу до різних частин і в зонах технологічних об'єктів – «СКУД технологічного об'єкту» [2, 4] В різних зонах об'єкту забезпечуються різні функції доступу. В основних зонах – забезпечується комплексний контроль по багатьом параметрам: по ланці «Ідентифікація по ID-карті - Розпізнавання і верифікація/ідентифікація облич – температурний/алкометричний чи біометричний контроль». А у другорядних зонах – по одному параметру,наприклад, доступ тільки по персональній ID-картці із чіпом RFID , або дотсуп по пін-коду(PIN-code) . Загальний процес показаний на рис. 1.1.

Відповідна така ІС СКУД (рис.1.3) може забезпечити контроль доступу із різними параметрами і достатньо широким функціоналом в різних зонах технологічного об'єкта на підприємстві із реалізацією функцій дистанційного доступу і роботи зон різних суб'єктів (персоналу і відвідувачів).

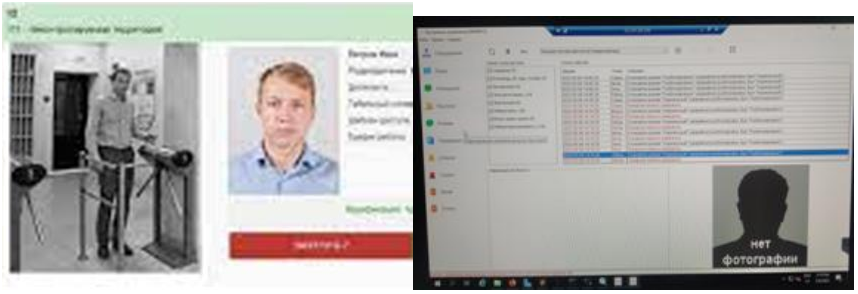


Рисунок 1.1 – Загальні принципи роботи СКУД на базі IoT [4]

Так , сама система СКУД може мати вигляд і структуру із забезпеченням багатофункціональності, як це показано на рис.1.2 та рис.1.3.

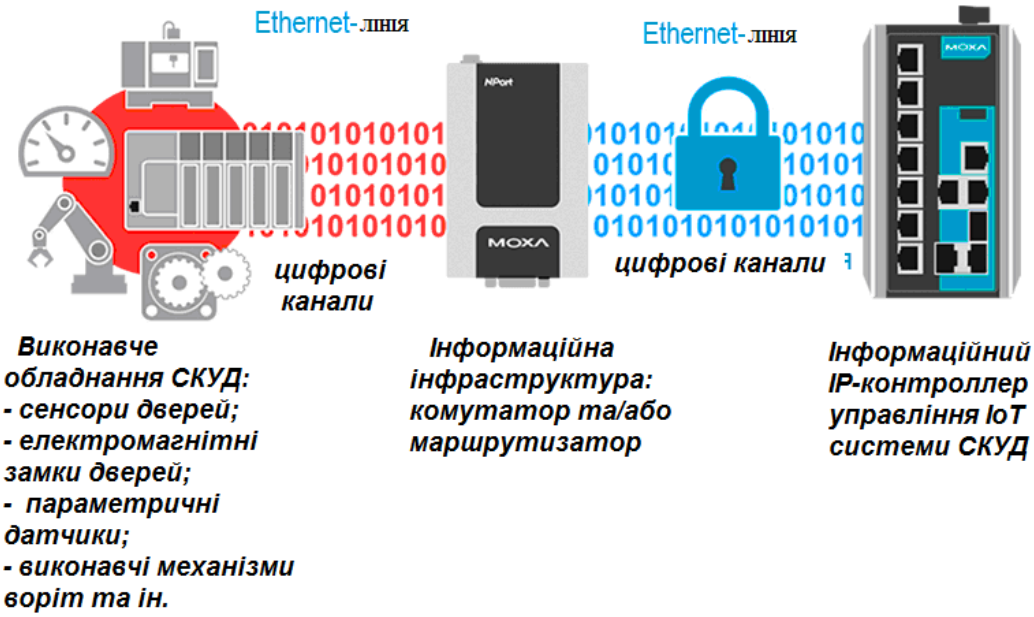


Рисунок 1.2 – Загальні складові в структурі СКУД і склад системи СКУД

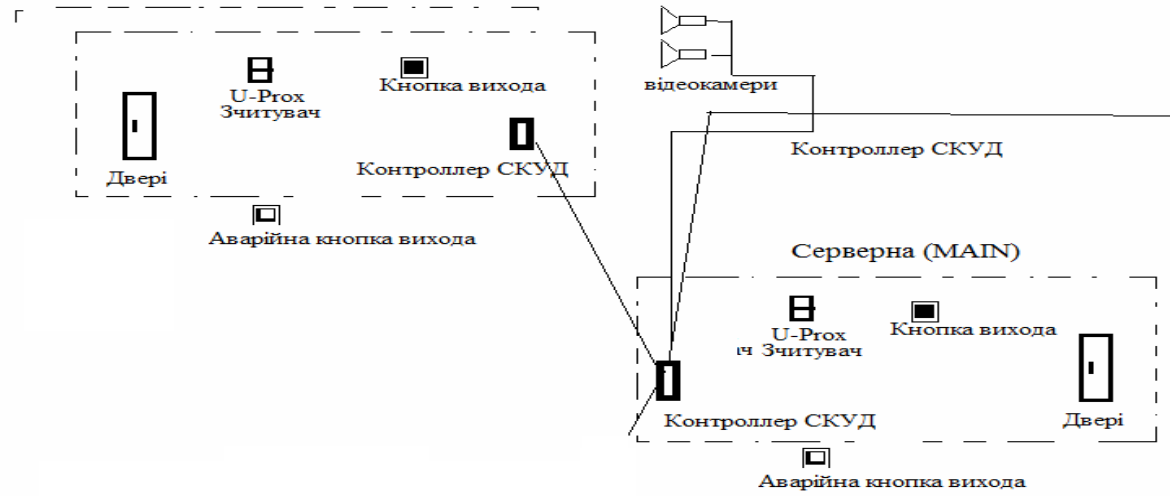


Рисунок 1.3 – Загальна структура ІС СКУД на базі IoT IP-контролерів

На рис. 1.4 показана типова схема промислової інфомраційної мережі системи СКУД із різним обладнанням.

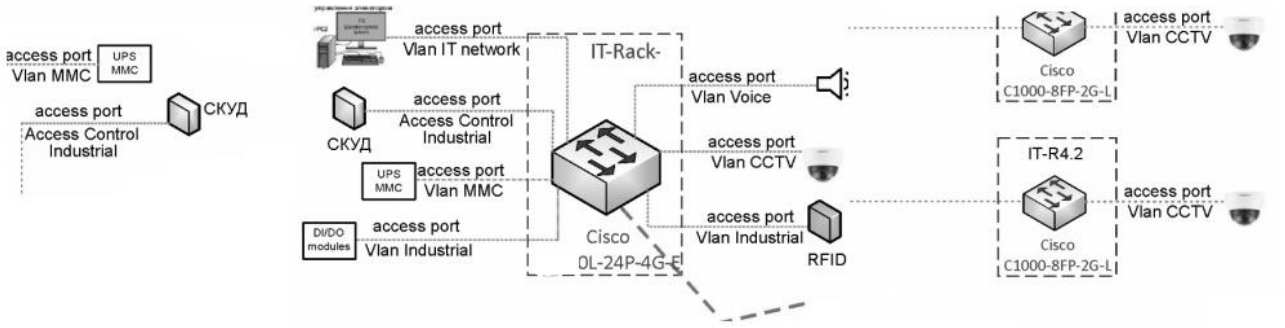


Рисунок 1.4 – Загальна структура інформаційної мережі СКУД на базі IoT IP-контролерів і різних виконавчих механізмів для контролю доступу в різних зонах принципи і структура СКУД

Система і саме ПЗ СКУД (рис.1.3 – рис.1.4) організовує надання доступу і оброблення до засобів контролю доступу – контролерів доступу відеоінформації (контролери і електромагнітні замки, камери СВС і інше обл.) оперативно-диспетчерські пульти, замки, турнікет та температурний контроль.

1.2 Будова програмного забезпечення і функціонал сучасних інформаційних технологій ІС СКУД

Загальна інформаційна будова базі ІС СКУД є складною, разом із IoT IP-контролерів, які керують різними виконавчими механізмами для контролю доступу в різних зонах підприємства в структурі СКУД . Вид ПЗ показано на рис. 1.6.

Програмне забезпечення СКУД [4](модуль ПЗ високого рівня, наприклад, Srhinx) у комплексі із обладнанням СКУД (контролери, системи та інше) дозволяє вирішувати основні завдання контролю і управління доступом у повному функціоналі із максимально прийнятними і актуальними на сьогодні характеристиками до систем контролю доступу.

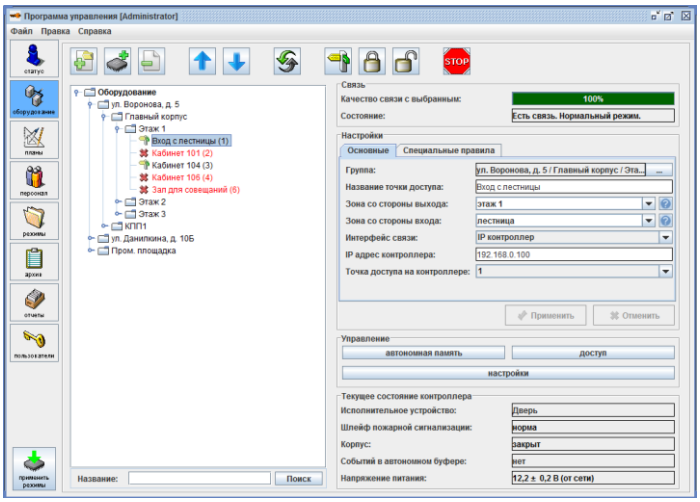


Рисунок 1.6 – Зовнішній вигляд інтерфейсу ПЗ управління системою СКУД і промисловими IoT IP-контролерами доступу [4]

Якщо функцій безкоштовного програмного забезпечення недостатньо, то можна придбати стандартне ПО Srhinx. Також можливо оновлення ПЗ [4] до стандартної версії (покупка стандартної версії), при цьому всі зроблені налаштування і дані зберігаються. В рамках безкоштовного ПЗ Prox та ПЗ Srhinx (рис.1.6, рис.1.7) обслуговується тільки одна точка доступу (один турнікет, одні двері, одні ворота або одна точка фіксації приходу / відходу співробітників). Кількість ідентифікаторів – від 1 до декілька тисяч. Дане ПЗ також використовується в проєкті як основа контролю та системи «IP-камери – шлагбаун- алкотестер». Зовнішній вигляд ПЗ показано на рис.1.7.

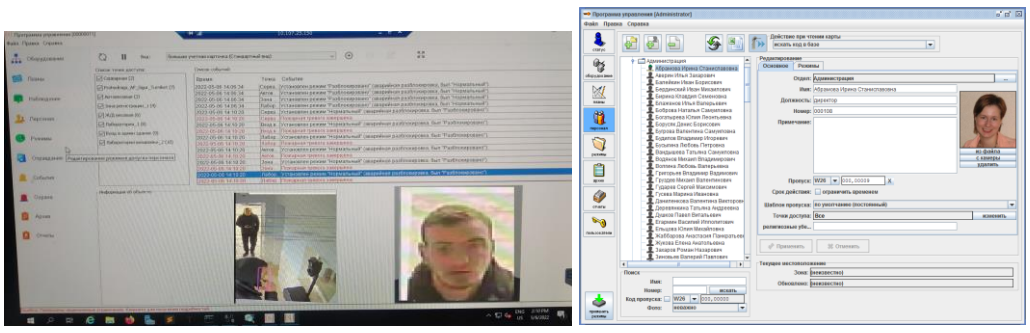


Рисунок 1.7 – Зовнішній вигляд ПЗ управління СКУД і промисловими IoT IP-контролерами при фіксації заходу суб’єкта на об’єкт [4]

Таке ПЗ дозволяє вести журналу обліку подій доступу і різних суміжних

систем доступу для контролю доступу персоналу на об’єкт і вести облік і авторизований доступ. Також дозволяється вести повний контроль і журнал подій.

Взаємодія сервера з контролером ІС СКУД (рис.1.7): програмне забезпечення та інформаційні технології СКУД дозволяє здійснювати спостереження за станом елементів системи. Тонка налаштування параметрів контролера організація зонального контролю, окремим випадком якого є припинення повторних проходів (antipassback) ручне управління пристроями: блокування, розблокування, дозвіл одноразового проходу та інше [3].

Архів і звіти: програмне забезпечення ІС СКУД SC; U-Prox[4] і система зберігає всю інформацію про зареєстровані події (проходи, заборони доступу, дії операторів) починаючи з моменту її першого запуску без тимчасових обмежень. Кількість подій в системі – необмежено. Також є можливість видалення обраних подій при необхідності.

Існує два способи роботи з масивом подій: оперативний доступ без генерації звітустворення докладного звіту. Програмне забезпечення ІС СКУД SC; U-Prox[4]. Для зручного відображення списку подій (показано на рис.1.8) при оперативному доступі можливе застосування фільтра з наступними особливостями: довільна вибірка подій за часом (за тиждень, місяць, квартал і т.д.) вибір об'єктів доступу вибір типів подій для відображення (проходи, зломи і ін.) сортування за типом або часу відео супровід будь-якого обраного події зі списку (при інтеграції з системами відеоспостереження).

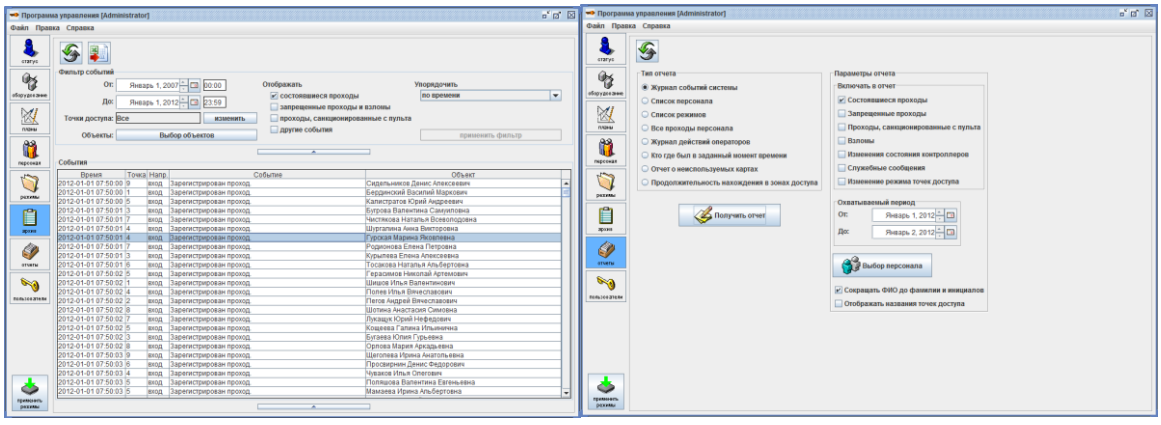


Рисунок 1.8 – Зовнішній вигляд інтерфейсу ПЗ Srhinx управління ІС СКУД [4]

Так керування промисловими механізмами здійснюється в ІС СКУД шляхом керування і взаємодії контролерів IoT із виконавчими ПЗ –модулями, які здійснюють обробку сигналів і опрацювання команд керування і сигналів із сенсорів згідно внутрішніх алгоритмів ПЗ. На рис. 1.9. –показаний інтерфейс ПЗ із консолью керування персоналом і налаштування профілів персоналу .

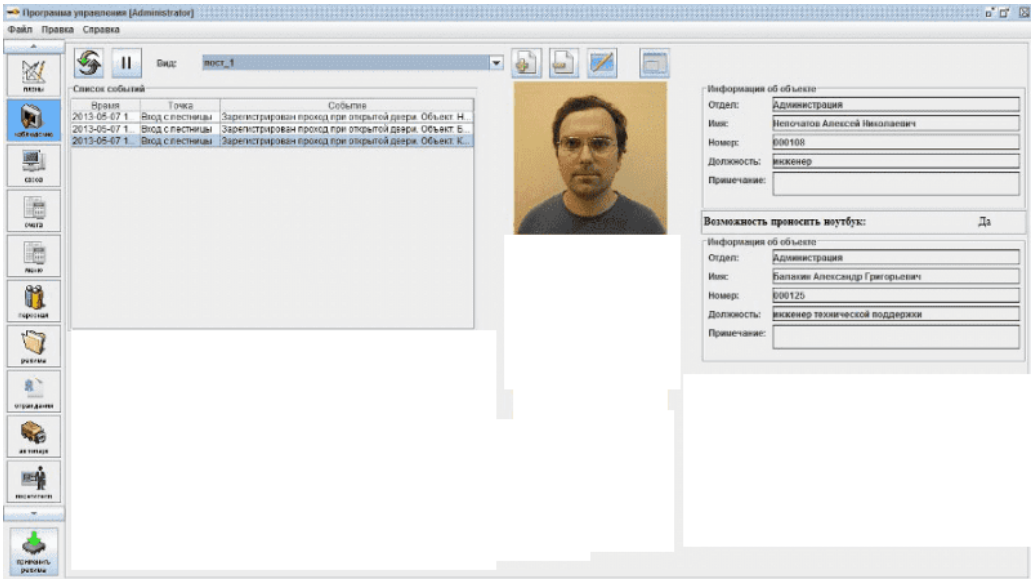


Рисунок 1.9 – Зовнішній інтерфейсу ПЗ ІС СКУД: консоль керування

Система і ПЗ забезпечує достатньо гнучкі налаштування і високоефективний контроль доступу та фіксацію перебування профілів в різних зонах, контроль робочого часу і контролю за персоналом, відеоспостетреження за персоналом і виконанням його функціональних обов’язків, що значно оптимізує процес і підвищує безпеку підприємства (рис. 1.10) [4].

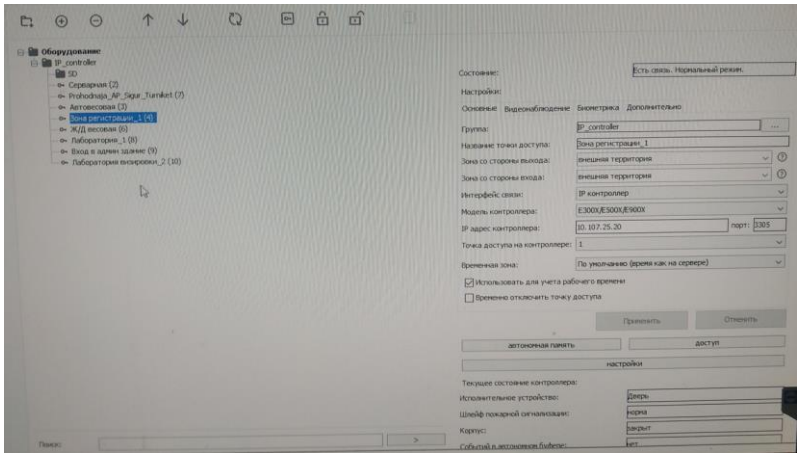


Рисунок 1.10 – Консоль налаштування зон доступа профілю персоналу в ПЗ

Консоль керування профілями персоналу і зонами доступу дозволяє налаштовувати систему максимально ефективно і гнучко, адаптуючи профіль під кожного співробітника окремо, і приписуючи кожному профілю свої права і свої обов’язки і зони.

Взаємодія сервера ІС СКУД із АРМ(ами) : реалізується через структуровану кабельну систему (СКС) на базі коммунікацій і сучасних маршрутизаторів Cisco Systems серії 2600S(Vlan) [5, 7] і дозволяє передачі пакетів даних відеопотоків із відеокамер до сервера СВС, а із сервера на АРМ операторів системи. Схема кластеру ІС СКУД показана на рис. 1.11.

Контроль і налаштування параметрів системи і організація зонального контролю ІС СКУД реалізується розподіленою обробкою системи і сервера СКУД [4, 8] в режимі 24/7. Взагалі практика використання технології Vlan є достатньо ефективним і дієвим механізмом підвищення безпеки комунікаційного обладнання ІС СКУД та інших інформаційних систем.

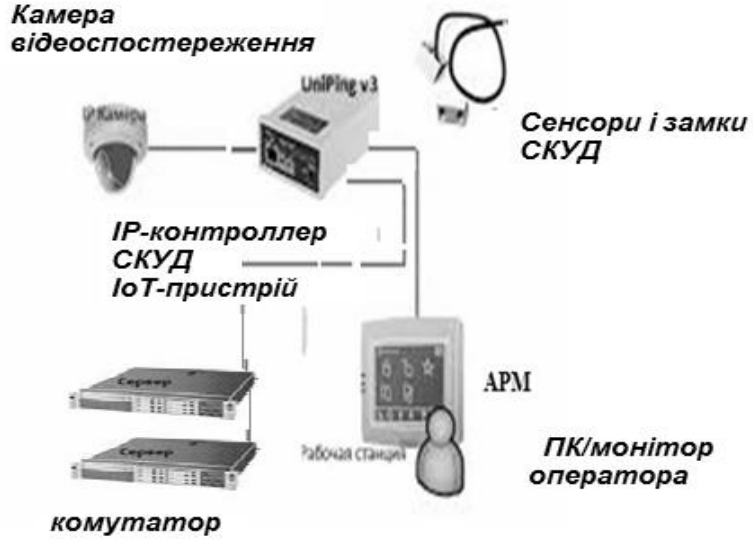


Рисунок 1.11 – Схема інформаційного кластеру мережі СКУД на базі контролера IoT із консолю контролю зон доступа СКУД

Також є можливість збереження отриманого списку в форматі MS Excel (XML/JML). ПЗ ІС СКУД може формувати наступні типи звітів: журнал подій системи список персоналу список режимів всі проходи персоналу журнал дій

операторів місцезнаходження об'єктів доступу в заданий момент, звіт про невикористовуваних картах тривалість перебування в зонах доступу. Для кожного з типів існує гнучка налаштування параметрів. Необхідний звіт генерується в форматі MS Excel[4, 14]. При цьому додаток, асоційоване з даним типом файлів, буде автоматично його відкривати (таким додатком може бути, наприклад, MS Excel, OpenOffice Calc або будь-яке інше програмне забезпечення, що дозволяє відкривати файли типу * .xls). Функції оперативної вибірки і створення звітів доступні в будь-який момент часу.).

Інтеграція: Система ІС СКУД SC; U-Prox дозволяє здійснювати взаємодію із різними системами відеоспостереження та контролю [15].

Інтеграція забезпечує: суміщення архівів (перехід за подією в відеоархів)використання розпізнаних автомобільних номерів для контролю доступу передачі подій в відео систему живе відео на графічних планах.

Сервер ІС СКУД SC; U-Prox може одночасно взаємодіяти з будь-якою кількістю серверів відеоспостереження різних типів. Інтеграція системи ІС СКУД SC; U-Prox реалізована і на стороні системи «Інтелект». Це зокрема означає, що засобами програмного забезпечення «Інтелект» в повній мірі можна керувати ІС СКУД SC; U-Prox. Саме ПЗ ІС СКУД SC; U-Prox також інтегрована з Onview-сумісними джерелами живого відео. Це дозволяє, наприклад, отримувати відео з будь-якої Onview сумісної IP-камери безпосередньо. Інтеграція з Active Directory дозволяє блокувати обліковий запис в домені, якщо оператор знаходиться в заборонених йому для роботи зонах доступу, заздалегідь визначених в системі. Система ІС СКУД SC; U-Prox інтегрована також з низкою інших систем:«система реєстрації, СВС «TRAS»,«1С » (рис.1.12) [4].

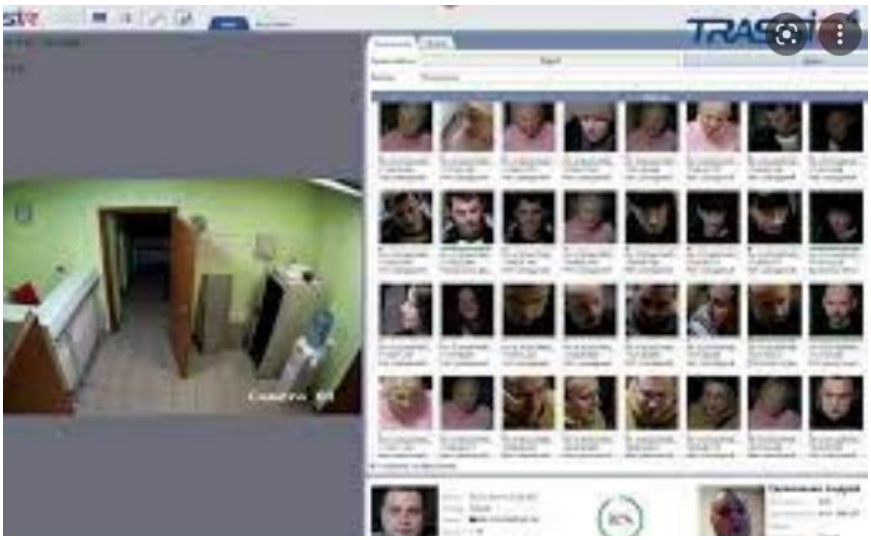


Рисунок 1.12 – Зовнішній вигляд консолі та інтерфейсу ПЗ СКУД із функцією відеоспостереженні контролю доступу в зоні N на базі контролера IoT в зоні

Багатозадачний режим роботи SIGUR виконує всі операції (моніторинг, контроль проходів, запис подій, перегляд подій, налаштування, комплексний доступ , роботу і взаємодію компонент СКУД по мережі, а також взаємодія з інтегрованими системами безпеки –СВС. Також задіюються функції відео нагляду і ведеться відповідне легування і реєстрація подій (рис.1.13, 1.14).

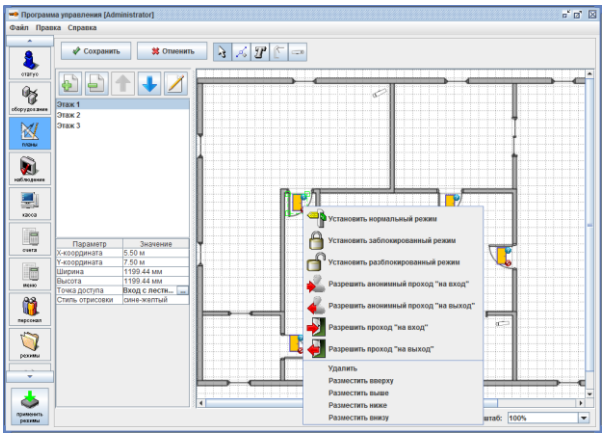


Рисунок 1.13 – Зовнішній вигляд зон доступу в консолі та інтерфейсу ПЗ СКУД в зоні N на базі контролера IoT [4]

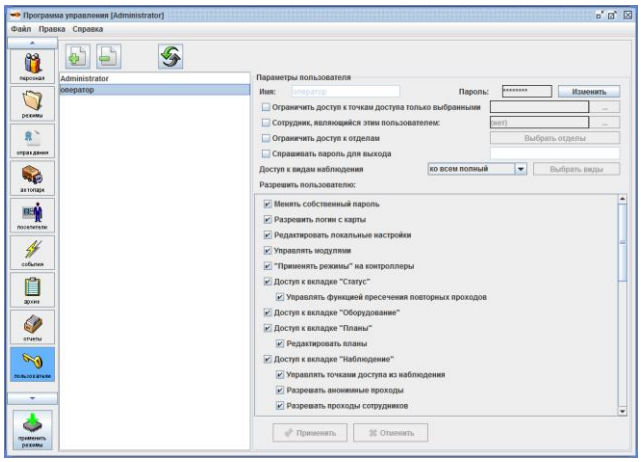


Рисунок 1.14 – Налаштування параметрів зон доступу в консолі та інтерфейсу ПЗ СКУД в зоні N на базі контролера IoT

Поверхові графічні плани (карти територій): Безкоштовне програмне забезпечення ПЗ СКУД кількість графічних планів необмеженонаявність інструментів для графічного редагування (малювання ліній, багатокутників, додавання тексту та ін.) можливість використовувати вже наявне зображення для завдання фонурозміщення на графічному плані інтерактивних елементів: точки доступу, зони доступу, камери відеоспостереження. Дані інтерактивні елементи відображають стан відповідних компонент системи і дозволяють ними управляти (розблокування точки доступу, перегляд відео з камер та ін.).

Організація робочих місць: програмне забезпечення ПЗ СКУД для АРМ і сама система дозволяє створити будь-яку кількість одночасно працюючих клієнтських (рис. 1.15).

Сучасні інформаційні технології та інформаційна система СКУД і Програмне забезпечення ПЗ є перспективним інструментом для здійснення комплексного високоінтелектуального контролю доступу співробітників в різни зони об’єкта підприємства, генерації та фіксації подій і співробітників. Впроваджена на різних технологічних об’єктах і компаніях система СКУД дозволяє вирішити основні завдання інтелектуального спостереження і контролю доступу співробітників .

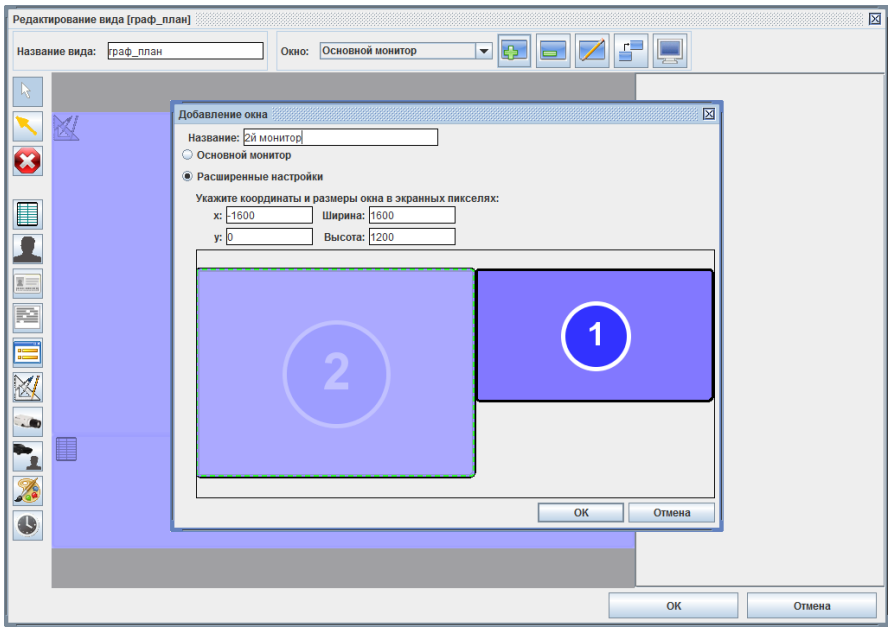


Рисунок 1.15 – Налаштування параметрів АРМ в зонах доступу в консолі та інтерфейсу ПЗ СКУД в зоні N на базі контролера IoT [4]

1.3 Аналіз відомих технологій і методів захисту інформаційних систем СКУД

Функцій програмного забезпечення СКУД ПЗ Shrinx достатньо для здійснення завдань спостереження, вискоінтелектуального контролю доступу в різних зонах і у різних необхідних місцях об’єкту разом із передачею даних і можливістю відтворення зображень на моніторах операторів АРМ.

Модуль СКУД ПЗ і система U-Prox – це комплексна сучасна автоматизована система, контролю доступу, із функціями штучного інтелекту, інтелектуальної обробки даних і потоків та зберігання відеоінформації[4, 7, 8].

Для захисту СКУД можна запропонувати: використання диференційних і багатоетапних підходів і механізмів захисту пристроїв самої ІС та IoT на всіх рівнях із використанням групових параметрів. Основна мета - зменшення рівня ймовірності ризиків різних кіберзагроз в ІС СКУД [2, 4, 5]. Також потрібна розробка нових прогресивних підходів, методів та моделі захисту на кращих світових практиках .

Традиційні і відомі підходи і методи захисту, які можуть використовуються для захисту СКУД і інформаційних систем, мають свої недоліки для ІС СКУД [2, 4, 8], хоча можуть забезпечити надійний захист, але інколи – недостатній, за рахунок того, що є прогалини в захисті.

Загалом, досягти максимального рівня захисту в СКУД і в їх пристроях IoT можливо тільки із використанням складного комплексного підходу використання окремих компонентів у абстрактному комплексному підході захисту системи СКУД.

Забезпечити повну безпеку функціоналу і захист передачі даних в ІМ СКУД та їх захищену обробку подій для СКУД і IP-контролера IoT пристроїв, а також даних користувачів в їх складі дуже важко сьогодні, враховуючи різний функціональний розвиток спеціалізованого хакерського ПЗ і ПЗ спеціального спрямування.

Забезпечення безпеки функціоналу ІТ СКУД на базі в IoT, на базі концепції цілісності, доступності та конфіденційності даних (CIA) [1, 7, 16]– є однією із головних задач при розробці і проєктування систем. Нові моделі і методи повинні базуватись на комплексному поєднані функціоналу віртуалізації даних, перевірка їх компонентами системи захисту IPS в окремих ізольованих програмних контейнерах для окремих потоків і процесів інформації із змішаним додаткових функціоналом[5]. Також для підвищення рівня безпеки в ІТ СКУД повинні бути створені додаткові етапи перевірки і контролю сторонніх інформаційних потоків із зовнішніх джерел. Захист можна забезпечити надійним вдосконаленим шифруванням у поєднанні із розпаралелюванням обчислювального процесу із розмежуванням прав доступу на різних рівнях обчислень і віртуальних обчислювальних середовищах(оболонок) ІС СКУД.

На рис. 1.16 показана узагальнена схема захисту інформації в СКУД.

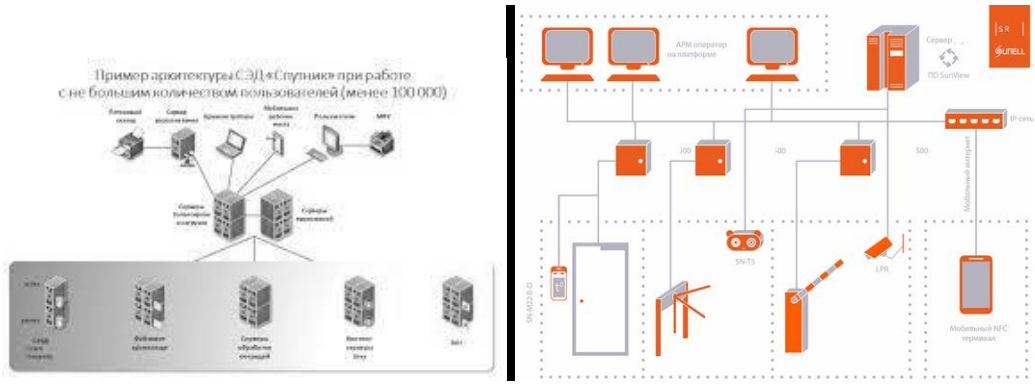


Рисунок 1.16 – Узагальнена схема організації захисту ІМ СКУД [4, 8]

Підвищення безпеки СКУД на базі IoT пристроїв. Із зростанням популярності смарт-пристроїв і сервісів IoT і в т.ч. і в СКУД, збільшується інтенсивність кіберзагроз в IoT та ІМ СКУД. По даним 50-60% всіх кіберзагроз та в т.ч. хакерських атак спрямовані на IoT-пристрої, в ІС СКУД це також має місце. Основними цілями для атак в IoT системах є канали інтерфейсів СКУД, середовища передачі пакетів даних, ядро IoT і компоненти вводу-виводу IoT-пристроїв та ІС СКУД, програмні модулі і компоненти ПЗ, ПЗ ядра ОС пристроїв IoT та сервісне ПЗ ІТ ІС СКУД систем. Це все може призвести до серйозних порушень безпеки.

Також, було проаналізовано основні методи захисту інформації в ІС СКУД, які наведені у таблиці 1.2. Саме ці методи є основними і потребують детального вивчення та вдосконалення.

Таблиця 1.2. – Основні відомі методи захисту інформації в ІС СКУД

п\п	Клас безпеки	*Відомі методи і підходи захисту*	***Недоліки та переваги***	***Складність (макс10); частота використання***	***Ступінь запровадження на практиці***
1	*A	Обмеженнгя фіз./інф. доступу	(-)Не завжди реалізує мий; (+) простий, дешевий та ефективний)	складність 2 ; часто,	часто. практ.впровадж.
2	*B	Сегментація мережі VLAN	(-) висока складність та вартість; (+) проситий та ефективний)	складність 8 ; рідко,	відносно рідко, практ. впровадж

3	*A	Автонтифікація за 2-м і більше факторам («!» 6 неНЕ параметрам), наприклад відео +ID	(-)Висока вартість, складність та потреба у використання додаткового обладнання; Не завжди реалізує мий; (+) висока ефективність	складність 10 ; Помірно рідко,	Рідко, практично впроваджується
4	*A	Шифрування при передачі даних в каналах ІС СКУД	(-)Висока вартість, складність та потреба у додатковому обладн.; (+) висока ефективність	складність 9 ; рідко,	Рідко, практично НЕ впроваджується
5	*B	Ізоляція системи і каналів	(-)Не завжди реалізує мий, складність в маштабі всієї ІС СКУД; (+) простий, та ефективний);	складність 4-5 ; часто,	Помірно часто: впроваджується
6	*B	Обфускація каналів і параметрів	(-)Висока вартість, складність та потреба у використання додаткового обладнання; Не завжди реалізує мий; (+) відносно підвищена ефективність	складність 4-5 ; рідко,	Рідко, практично НЕ впроваджується
7	*A	Комплексний захист Інноваційний підхід	(-) (інколи висока вартість та складність); (+)висока ефективність	складність –(5-7:орієнт.*) ; Рідко (*),	--, - *(Помірено рідко. але із оптимізацією – планується часто)

Проведений аналіз показує, що найбільш придатні і найбільш застосовувані методи захисту і ІТ СКУД – це ідентифікація та авторизація.

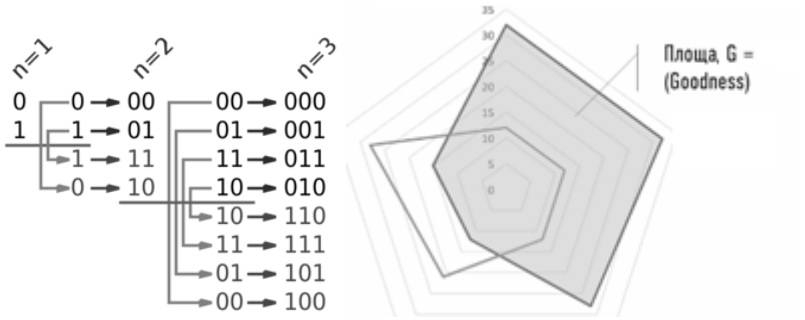
2 УДОСКОНАЛЕННЯ МЕТОДУ І МОДЕЛІ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА БАЗІ ПРИСТРОЇВ ІОТ

2.1 Удосконалення методу підвищення інформаційної безпеки ІС СКУД на основі підходів багато параметричної ідентифікації та\або автентифікації

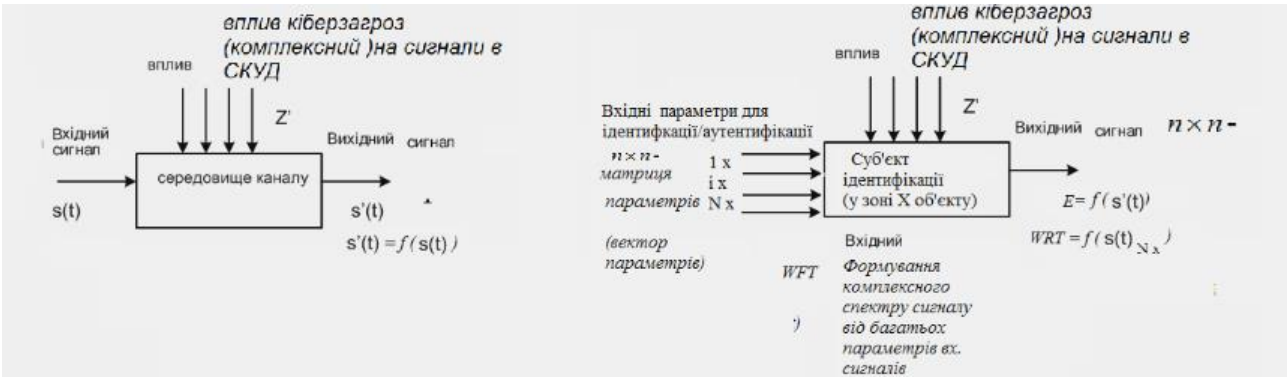
Сам метод багатопараметричної ідентифікації передбачає використання багатьох N_x – параметрів в системі автонтифікації або іденитфікації об'єкта (в данному випадку субєкта) доступу . Причому кількість параметрів може бути змінена в процесі і гнучко адаптована до умов, в залежності від змінних вхідних вимог і необхідного (бажаного) рівня безпеки [7, 12-16]. Тобто є можливість вибору N_x , самим методом, в залежності від рівня захисту і складності обєкта, тобто:

$$
\begin{aligned}
&N_x = f(t, k_j, S_w, g(h));\\
&N_{SUMx} = \overline{A}_i \sum_{i=1}^{n} \overline{f}_i\,(t_i, k_{ji}, S_{wi}, g_i(h, t_i))) + B_u(t_i);\\
&0 \le t_i \le T;\ t_i \ge \tau > 0.
\end{aligned}
\qquad (2.1)
$$

де, $f(t, k_j, S_w, g(h))$ - функція залежності вибору кількості параметрів ідентифікації та/або автонтифікації, від показників; t- час системи; k_j – умовний рівень захищеності системи; S_w- рівень необхідного захисту системи, або рівень безпеки, який потрібно досягти; $g(h)$- функція складності та умовних вхідних одиниць параметрів системи і об'єкта (суб'єкта доступу); N_{SUMx} – сумарна кількість параметрів ідентифікації в системі ІС СКУД, в залежності від кількості n - точок автонтифікації та ідентифікації в ІС СКУД , яка задається від миттєвих і локальних зхначень параметрів функції зележності вибору параметрів ідентифікації та автонтифікації в ІС СКУД (рис. 2.1).



Вибір параметрів Nx



- метод передбачає моніторинг в системі енергетичного характеристичного спектру E багатьох сигналів N x Si(t) при багатопараметричній ідентифікації ;
- їх подальшого контролю в певних допустимих межах 0<E<Epor;
- створенню і фіксації\обробки інциденту при перевищенні E≥Epor ;
- моніторингу інших метрик сигналів QoS в каналах та інтерфейсах ІС СКУД та пристроях IoT , QoS ≥QoSpor .

Рисунок 2.1 – Особливості реалізації моделі і методу багатопараметричної ідентифікації в ІС СКУД

Сам алгоритм і функція керування системою диференціальних систем з запізненням, яка має наступний вигляд [10]:

$$f(t) = Af(t-\tau_i) + bu(t) = \overline{A}_i \sum_{i=1}^{n} \overline{f}_i (t_i - \tau_{\Delta i}) + \sum_{i=1}^{n} \overline{bu}_i (t_i), \quad t \geq t_0,\ \tau > 0. \qquad (2.2)$$

Ця модель також зазначена як ефективна і дієва для задач автоматизованого керування процесами на фондових ринках. Де ступінь ризику і ціна помилки є високою.

Можна показати, що дана модель (2.1) буде ефективною і для задач автоматизованого управління інформаційними процессами у системах із високими ризиками і високою відповідальністю за помилку. До таких систем належиться системи безпеки і в т.ч. й ІС СКУД. Втрати інформації при

передаванні пакетів даних можна описати по теорії Шеннона [5, 17]:

$$H(Y|X) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i) \times P(y_j|x_i) \times \log_2 P(y_i|x_j) \qquad (2.3)$$

де, $P(x_i)$ – імовірності виникнення втрат інформації в системі реалізації багатопараметриченої ідентифікації. Саме графічне представлення показане на рис. 2.2.

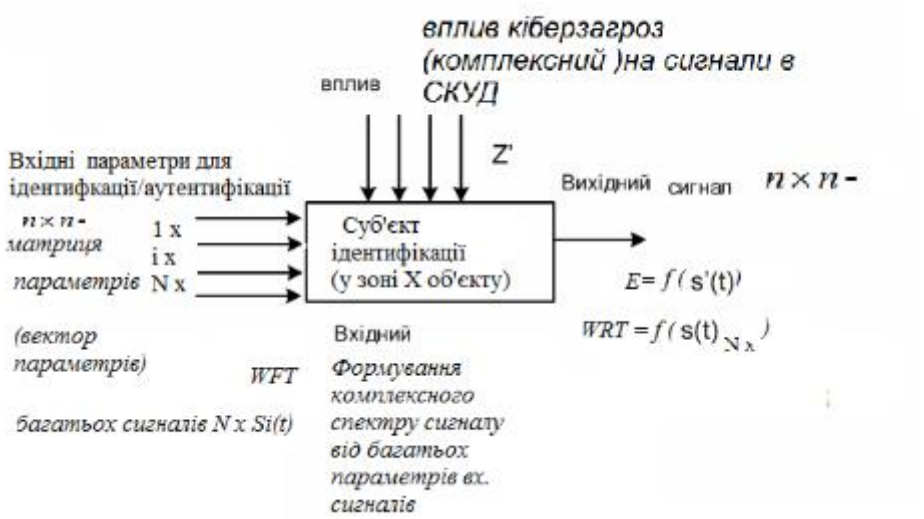


Рисунок 2.2 – Особливості реалізації і підхід в моделі і методі ІС СКУД із використанням формування спектрального відбитку («зліпку» спектру сигналів)

Параметри інтерфейсів і каналів зв’язку в ІС СКУД можуть бути визначені співвідношенням Шеннона-Найквіста.

Сигнал і швидкість в каналах та інтерфейсах ІС СКУД із врахуванням шифрування і захисту даних буде мати вигляд [5, 7, 21]:

$$C = \Delta F \cdot \log_2\left(1 + \frac{P_s}{P_n}\right) = \Delta F \cdot \log_2\left(1 + \frac{P_s}{N_0 F}\right) \qquad (2.4)$$

Сам метод передбачає декілька стадій і виглядає так:

елементами $\bar{g}_{ij}$ є його енергія E [12]:

$$E| = \sum_{i=1}^{n}\sum_{j=1}^{n} \bar{g}_{ij}^{2} = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} P(u,v)\,, \qquad (2.7)$$

де $P(u,v),\ u,v = \overline{0,n-1}$, — енергетичний спектр сигналу .

Таким чином, як одна з числових характеристик інформаційно-технологічної системи може розглядатися енергія сигналу $\bar{G}$.

В середині системи повпнні досягатись середні праметричні критерії , тобто 0<Pr < Ppor NE, де Ppor NE – порогові значення появи нелінійних зміни критеріїв.

- Виконання завадостійкового кодування/передавання інформації в інформаційному тракті СКУД і шифрування передачі;
- Використання багатопараметроичної автонтифвкації та\або ідентифікації за рахунок введення та поєдання багатьох параметрів і обєднання їх у унікальний ідентифікуючий сигнал частотної смуги сигналу *W* по швидкості передавання у об‘єднаних інтерфейсах СКУД (рис. 2.3) шляхом застосування модифікованого методу WRT для інтерфейсу CREL в СКУД.

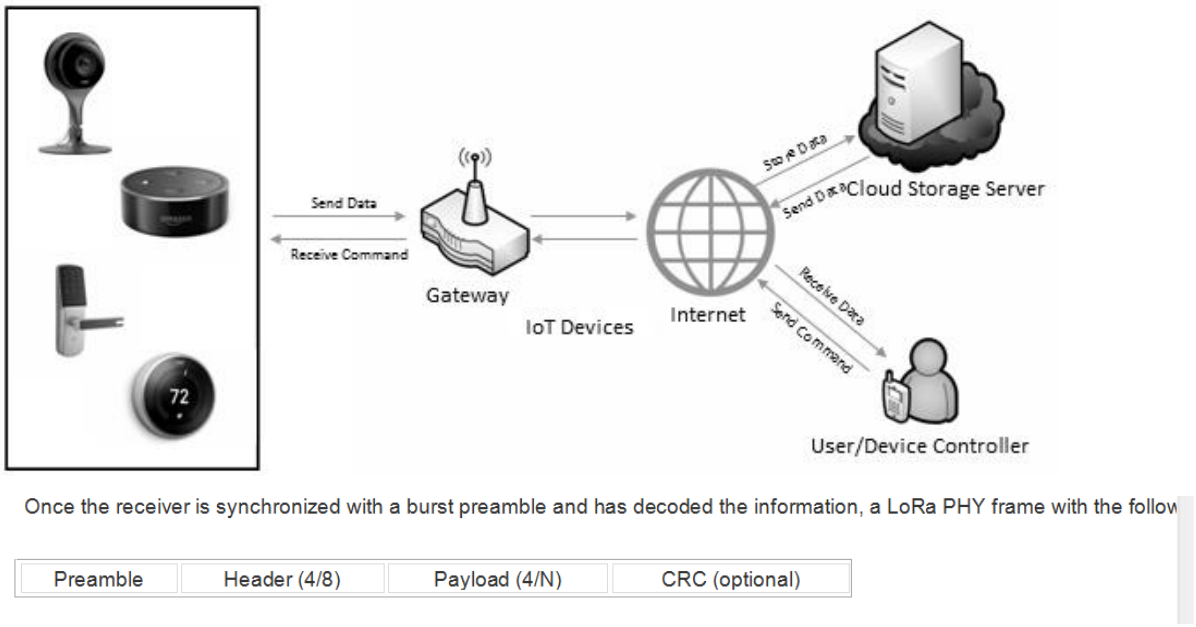


Рисунок 2.3 – Приклад логічної структури системи захисту ІС СКУД

На базі структури ІС СКУД (рис.2.3) показано використанням додаткових параметрів: відео розпізнавання FaceId в сукупності із іншими параметрами системи ІС СКУД в самому оптимізованому методі захисту інформаційних даних.

Сам метод багатопараметричної ідентифікації і відмінності показані на рисунку 2.4.

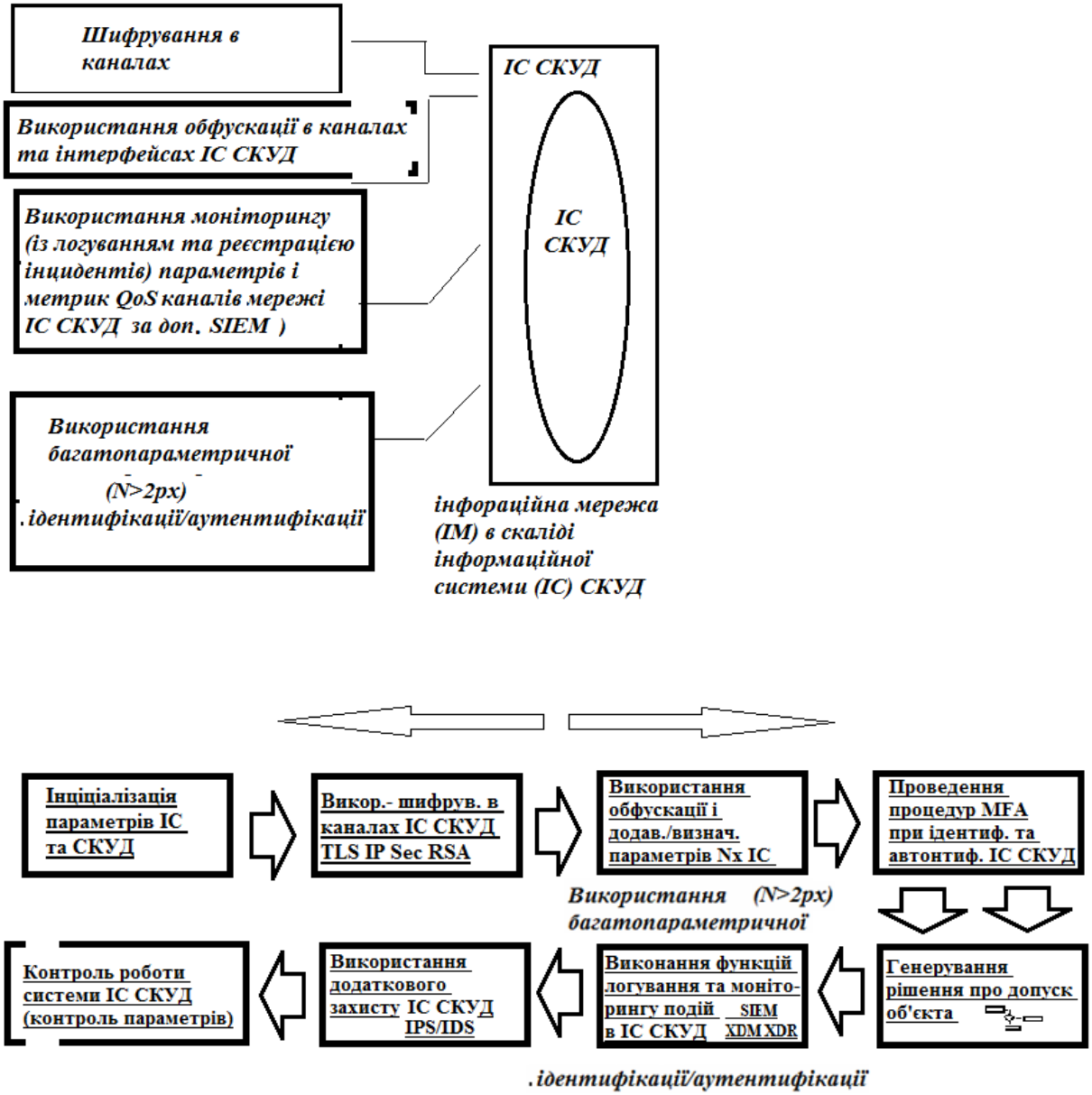


Рисунок 2.4 – Метод багатопараметричної ідентифікації та\або автонтифікації для захисту даних в ІС СКУД і його стадії

Метод багатопараметричної ідентифікації передбачає декілька стадій і включає як традиційні відомі етапи. Які ґрунтується на MFA (MultiFactor Authentication) – багатофакторної авторизації та ідентифікації , так і нові стадії. Які передбачають вибір кількості факторів. В залежності від умов, інші підходи захисту інформації в інформаційних мережах ІС СКУД. Сам процес вибору параметрів описаний в (2.1) та деталізується залежностіми (2.2), що передбачає вибір мінімум Nx>2 кількості параметрів Nx = 2 .. n; n є N_{SUMx}. Окремі стадії

методу показані на рис. 2.5 та рис. 2.6 на рис. 2.7 – рис. 2.8 показані принципи і окремі положення методу.

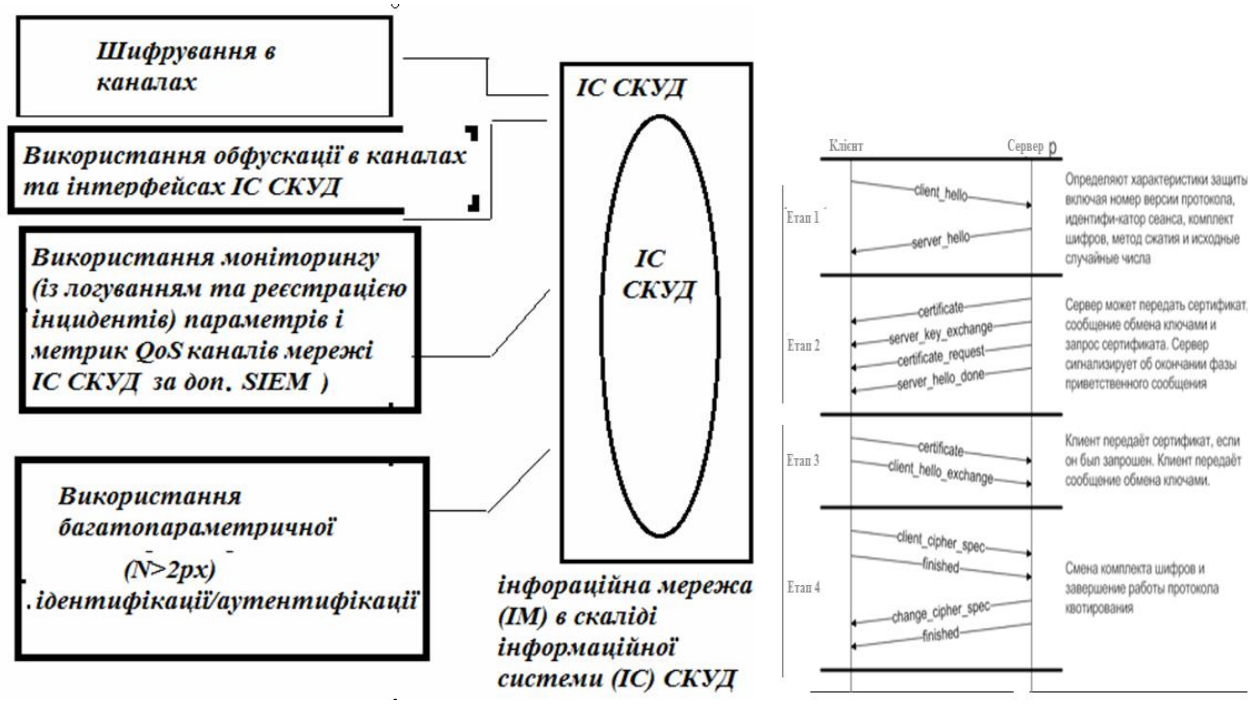
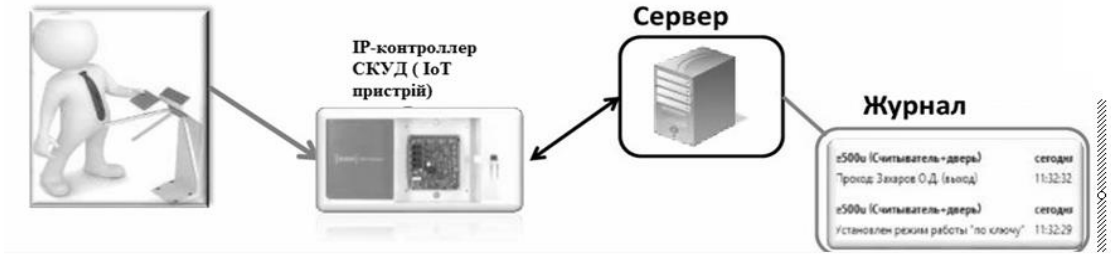


Рисунок 2.5 – Окремі стадії методу багатопараметричної ідентифікації та\або автонтифікації для захисту даних в ІС СКУД і стадії захищеного обміну



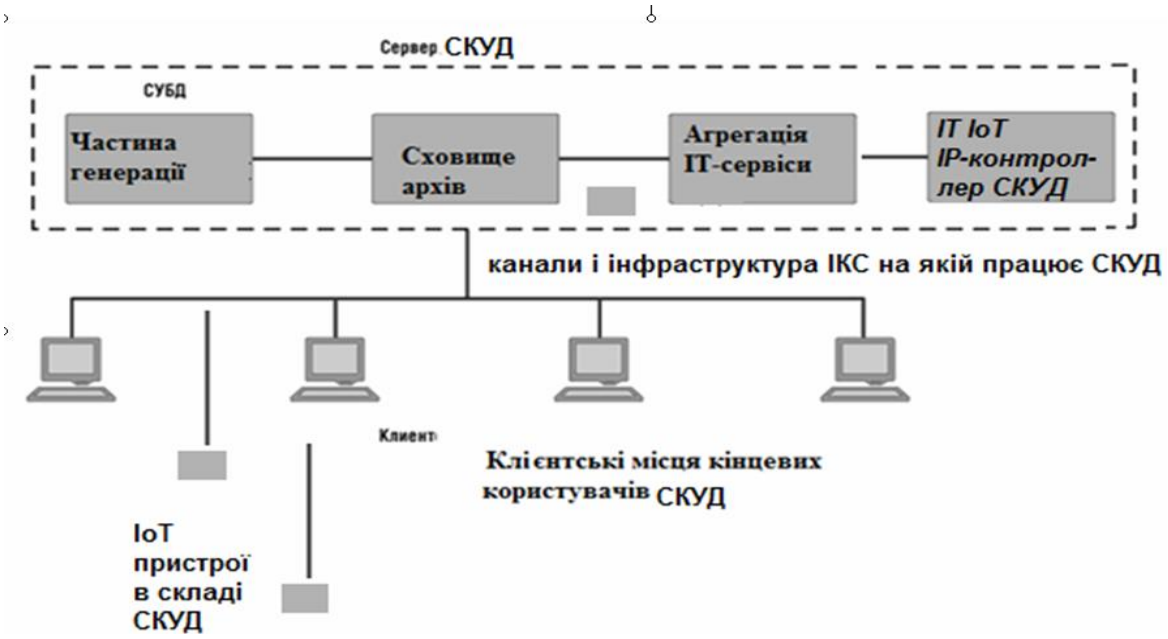


Рисунок 2.6 – Принципи і окремі положення методу та впровадження у структуру ІМ ІС СКУД із розподіленою обробкою і передачею даних по ІКС СКУД , яка інтегрується в інфраструктуру підприємства

Рисунок 2.7 – Сервіси відеоспостереження і розпізнавання облич (2-й ID фактор) в складі функціоналу сучасних СКУД

Вирішення завдання підвищення інформаційної безпеки ІС СКУД можливе завдяки використання вдосконаленого методу багатопараметричної автонтифікації\ідентифікціх, зокрема із використанням багатопараметричної ідентифікації/автонтифікації (із кількістю осн. параметрів N>2x). Засади до створення первинного алгоритму на базі методу показані на рис. 2.8.

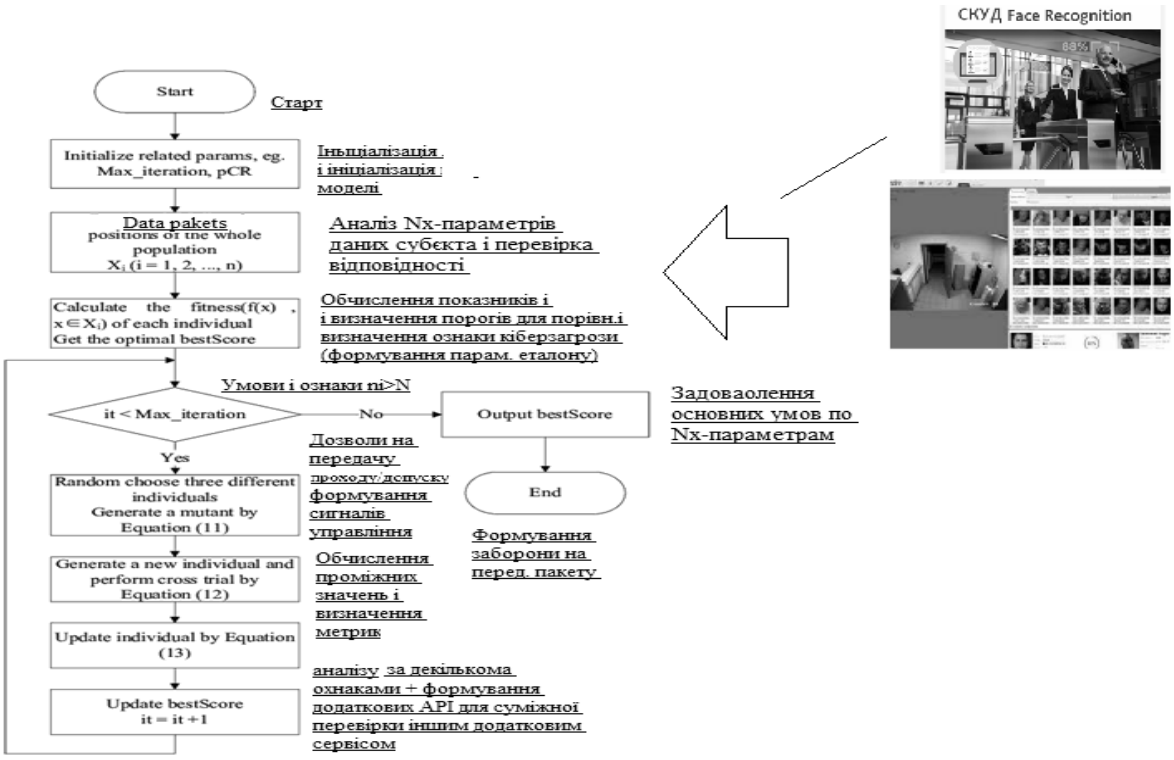


Рисунок 2.8 – Алгоритм роботи методу багато параметричної ідентифікації в ІС СКУД

Метод (рис.2.4) і алгоритм (рис.2.8) передбачають декілька стадій і включає як традиційні відомі етапи, які ґрунтується на MFA (MultiFactor Authentication) – багатофакторної авторизації та ідентифікації , так і нові стадії, які передбачають вибір кількості N-факторів (в залежності від умов захисту), інші підходи захисту інформації в інформаційних мережах ІС СКУД, що описані вище.

Алгоритм (рис.2.8) передбачає наступні стадії:

- ініціалізацію;
- визначення Nx-параметрів;
- кореляцію цих Nx-параметрів із еталонними значеннями;
- формування рішення про пропус/допуск(чи НЕ допуск суб’єкта в зону об’єкта);
- рекурсивний цикл і постійна аналітика;
- суміжні операції.

Наближене визначення параметрів показано на рис. 2.10.

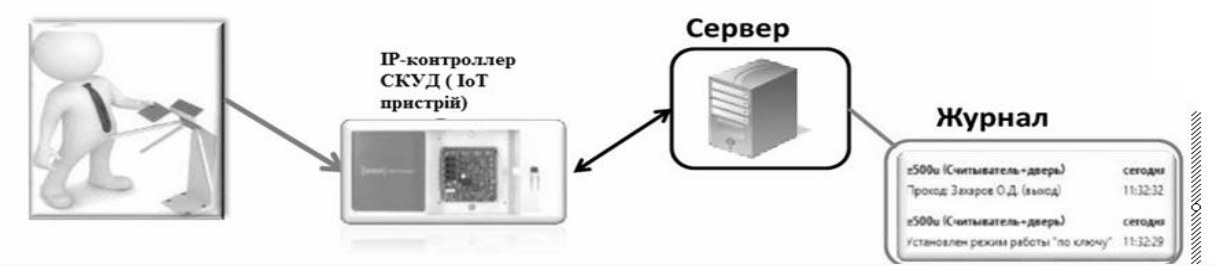


Рисунок 2.9 – Робота алгоритму і методу в складі ІС СКУД для допуску суб'єкта на об'єкта за 2-ма параметрами ID-картки (Nx=1) та FaceID(Nx=2)

В залежності від різних задача безпеки та необхідних рівнів інформаційної безпеки можна гнучко формувати параметри і кількість їх доступу в ті чи інші зони. В зонах із високими і вищими рівнями безпеки можливе використання більшої кількості параметрів Nx. І навпаки – в зону із меншим рівнем безпеки можна запускати із меншою кількістю параметрів Nx .

2.2 Удосконалення математичної моделі інформаційної безпеки ІС СКУД

В роботі [11] побудовано алгоритм функції керування системою диференціальних систем з запізненням, яка має вигляд диференційного рівняння [10]. В дослідженнях [10] також показано керування інформаційною безпекою в системі державного регулювання критичними процесами:

$$f(t) = Af(t-\tau_i) + bu(t) = \overline{A}_i \sum_{i=1}^{n} \overline{f}_i (t_i - \tau_{\Delta i}) + \sum_{i=1}^{n} \overline{bu}_i (t_i), \quad t \geq t_0,\ \tau > 0. \qquad (2.6)$$

Ця модель також зазначена як ефективна і дієва для задач автоматизованого керування процесами на фондових ринках. Де ступінь ризику і ціна помилки є високою.

Можна показати, що дана модель (2.6) буде ефективною і для задач автоматизованого управління інформаційними процессами у системах із високими ризиками і високою відповідальністю за помилку. До таких систем належиться системи безпеки ІС СКУД.

Придатність і обгрунтування вибору моделі (2.6) в якості прототипу для

розробки мат. Моделі опису процесів у ІС СКУД також пояснюєтья і обгрунтовується відносною простотою і точністю відпвдіді („accurancy response“) в цих системах і досить точне формування команд керування і відхилення векторів управління в цих системах.

Було зазначено, що система (2.6) відносно керована, якщо для довільної неперервно-диференційованої функції $\varphi(t)$, на проміжку часу d*t*, часу& d*t*& $t_0 - \tau \le t \le \tau_0$, таке, що система (2.6) має розв'язок $x_0(t)$, задовольняє граничним умовам: $x_0(t) = \varphi(t),\ t_0 - \tau \le t \le \tau_0,\ x_0(t_1) = x_1.$

При конструюванні функції управління системою (2.6) було введено матричну функцію, яка отримала назву запізнюючого експоненціалу і яка має такий вигляд [11]:

$$e_{\tau}^{At} = \begin{cases} \theta, & -\infty < t < -\tau; \\ 1, & -\tau \le t < 0; \\ 1 + A \cdot \dfrac{t}{1!} + A^2 \cdot \dfrac{(t-|\tau)^2}{2!} + \cdots + A^k \cdot \dfrac{(t-(k-1)\tau)^k}{k!}, & \\ & (k-1)\tau \le t < k\tau, \end{cases} \tag{2.7}$$

де θ – матриця нульових опорних значень; I – одинична опорна матриця.

За допомогою функції (2.6) розв'язок системи (2.7) було представлено у вигляді:

$$x(t) = \theta_{\tau}^{A\tau}\varphi(t0-\tau) + \int_{\tau_0-\tau}^{\tau 0} e_{\tau}^{A(t-\tau-s)}\varphi(s)ds + \int_{\tau_0}^{\tau} e_{\tau}^{A(t-\tau-s)}bu(s)ds. \tag{2.8}$$

$$x_0(t) = \varphi(t);\ t_0 - \tau_{\Delta i} \le t \le \tau_0.$$

із початковими умовами $x_0(t) = \varphi(t),\ t_0 - \tau \le t \le \tau_0$.

Функція керування, яка входить в третій додаток (2.9), має такий вигляд [11]:

$$u(s) = b^T e_{\tau}^{A(t-\tau-s)}\left(\int_{t_0}^{t1} e_{\tau}^{A(t-\tau-s)}bb^T e_{\tau}^{A^T(t1-\tau-s)}ds \times (x_1 - e_{\tau}^{A\,t_1}\varphi(t_0-\tau) - \right. \tag{2.10}$$

$$\left. -\int_{\tau_0-\tau}^{\tau} e_{\tau}^{A(t-\tau-s)}\varphi(s)bu(s)ds\right)$$

Із окремими уточненнями і врахування (2.1), її можна показати як:

$$F(f(t_i), t_i, \tau_i, u_i(t_i)) = A_i \times \sum_{i=1}^{n} \overline{f}_i(t_i - \tau_{\Delta i}) + \sum_{i=1}^{n} \overline{bu}_i(t_i), \quad t \geq t_0,\ \tau > 0. \qquad (2.11)$$

Модель (2.10) та (2.11) для n- рівневого обчислювального процесу в МК передбачає, що чіткі зв'язки між елементами системи МК (наприклад в пристрої IoT) існують тоді, коли зв'язки між окремими обчислювальними блоками і стадіями мікропрограми існують та чітко встановлені на

Із врахуванням цього формула (2.9) конкретизується і перепишеться у вигляді функції векторноо добутку [11]:

$$G = F(X_1 f_1, X_2 f_2, X_3 f_3, \ldots X_i f_i, \ldots X_n f_n,) \rightarrow Gmax(F(X_1 f_1,). \qquad (2.12)$$

В дослідженнях керування інформаційною безпекою в ІС СКУД в системі регулювання безпеки підприємства, в якості математичної моделі будемо використовувати представлення (2.9) і (2.10). Здійснюючи постійний моніторинг інформаційно-телекомунікаційних систем, які забезпечують функціонування ФР, необхідно виділяти, як окрему множину, сценаріїв атак, та їх кількість $x(t)$, які здійснюються в момент часу t. Початкова функція $\varphi(t)$/ формується постійно на відрізку часу $[t_0 - \tau;\ t_0]$, яка визначає кількість атак протягом часу t_0, який назвемо часом квантування. При цьому, система державного регулювання кібернетичною безпекою повинна здійснити відповідні заходи, при яких $x1 = 0$. В цьому випадку керуюча функція $u(s)$ здійснює стабілізацію функціонування інформаційних систем і відбиває атаки. Кількість майбутніх можливих атак на проміжку $[t_0;\ t_0 + \tau]$, визначається розв'язком представленням (2.9), яке в свою чергу є початковою функцією для прогнозування кількості атак на про міжку часу $[t_0 + \tau;\ t_0 + 2\tau]$.

Матриця елементів *ij n mA* $A = \|a_{ij}\|_{n \times m}$, яка входить в представлення (2.9) уявляє собою степінь незахищеності інформаційної системи, на яку здійснюється атака і єстохастичною. Елементи цієї матриці *aij* – це ймовірність незахищеності *i*-го об'єкта, $i = \overline{1, n}$ від j-го. сценарію атаки, $j = \overline{1, m}$.

Вектор – стовпчик b визначає ступінь захищеності i-го об’єкту від можливих кібератак в ІС СКУД. Допустимо, що $m = n$. Якщо рівність не виконується, то відповідна матриця доповнюється до квадратноїматриці нульовими елементами. Виходячи із цього, за допомогою представлення (2.9) і структурі функції керування (2.10), можна наближено зпрогнозувати кількість можливих кібератак на систему ІС СКУД і при цьому, аналізуючи їх сценарії, своєчасно їх нейтралізувати. При цьому, побудувавши фазові шаблони портретів у різних інтервалах часу можно аналізувати стійкість захисту системи ІС СКУД від кібератак. На рис. 2.11 представлена залежність кількості кібератак від часу на квантовваному відрізку. Кібератаки спостерігались протягом періоду Ті у моделі ІС СКУД під час пікових навантажень електронних сигналів. Крива, яка зображена на цьому рисунку є початковою функцією. $\varphi(t)$ при $0 \le t \le 1.$

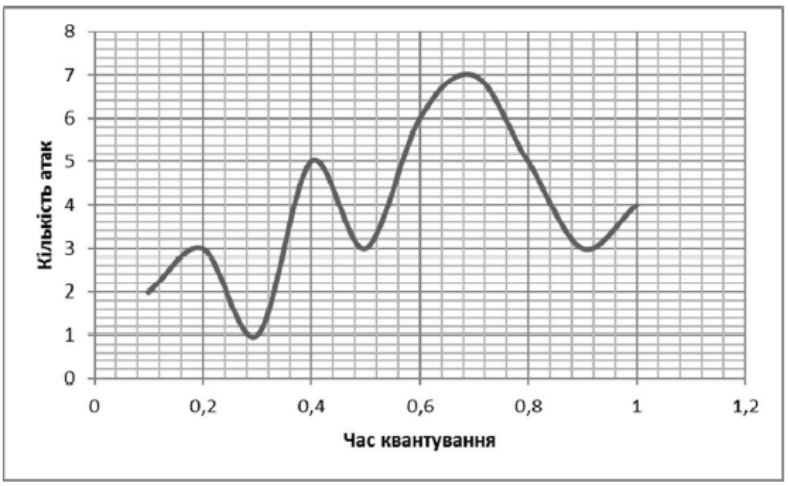


Рисунок 2.10 – Залежність кількості кібератак протягом однієї години

Ступінь незахищеності інформаційної системи при цьому була 0,01-0.015, а ступінь захищеності була 0.51-0,65.

Тому (рис. 2.10) та формула (2.6) в цьому випадку перетворюється в одномірну, тобто в наступне диференціальне рівняння:

$x(t) = 0.013x(t -) + 0.65u(t)$, $1 < t < 2$.

Завдання захисту і функції керування захистом в ІС СКУД полягає у зменшенні впливу кіберзахгроз (атак) протягом періоду часу Ті . У наступному

періоді часу система захисту Іс СКУД повинна продовжити працювати в стаціонарному режимі, навіть коли кіберзагрози (атаки) вже відбиті. Інакше кажучи, $x1(t) = 0$, тобто функція (2.10) здійснює стабілізацію моделі системи ІС СКУД , системи, яка описується рівнянням (2.11). З практичної точки зору, ПЗ [4] керування СКУД – це інфраструктурний сервіс (рис. 2.11). Між електронним сервісом ІС СКУД і Інтернет-мережею [7-15] повинно існувати інформаційно-телекомунікаційне середовище – інфраструктурний сервіс, який приймає на себе атаки, виконує захист шляхом шифркування та обфускації (наприклад, створенн пулу фейкових IP-адрес). Функції фіксуються ПЗ СКУД і подають інформацію в аналізатор сценаріїв атак і одночасно після їх відбиття за допомогою функції керування $u(s)$, дає дозвіл електронному сервісу на проведення окремих операції в ІТ ІС СКУД.

Рисунок 2.11 – Керування процесом захисту інформації в ІС СКУД

Цей процес (рис.2.11) відбувається неперервно в ІТ ІС СКУД. Аналізатор сценарію атак – це каркас в якому створюється база знань про сценарії атак і здійснюється формування нових функцій для протидії для інфраструктурного сервісу. Виходячи з вище викладеного, можна зробити висновок, що однією із складових стабілізації фондового ринку в є інформаційна безпека на торгах, тому ефективність торгів залежить від вміння системи захисту виявити і відбити атаку в поточний момент часу. За допомогою математичної теорії керування можна будувати моделі державного регулювання кібернетичною безпекою фондового ринку.

Створення систем захисту, як буфера між Інтернет–мережою і інформаційною системою дає можливість не тільки виявляти атаки, але аналізуючи їх сценарії, постійно модернізувати існуючі засоби захисту.

Розглядаючи динаміку атак [18-32], як динамічну систему із запізненням, ми постійно маємо можливість прогнозувати їх кількість, будуючи закон розподілу ймовірностей їх за допомогою систем диференціальних рівнянь з запізненням і водночас отримувати нову інформацію про розвиток новітніх сценаріївкібернетичних атак. Система захисту повинна бути керованою. Завжди необхідно володіти інформацією про те, що відбувається в інформаційній системі, а ще краще, отримати прогноз розвитку ситуації.

Підходи із використанням векторних моделей при моделюванні процесів інфоромаційної безпеки ІС СКУД. Також, додатково модель (2.10) інформаційної системи ІС СКУД на базі поєднання різних технології захисту інформації та водночас різних методик може бути доповнена математичною моделлю опису інформаційних процесів у СКУД на базі графової моделі. Дана модель описується марківськими процесами для інформаційних фнкцій та функціями складних векторних процесів за допомогоюграфів окремих функцій параметрів системи. Також враховубються додаткові дані (метадані) вкладеності взаємодії інформаційних процесів. Такі графи із Xn – вершинами у вигляді парної взаємодії описуються дискретними функціями типу [12]:

$$G\,(f_i) = (X_i,\ Y_i,\ n,\ I,\ t_i) \qquad (2.13)$$

де, X_i,- множина усіх вершин графу*; E={e1,e2,e3, …em}* –множина ребер графу.

Данам модель може досить чітко змоделювати роботу інформаційного процесу в системі ІС СКУД. А також врахвати вплив на нього декількох чинників кіберзагроз одразу. Або вплив декількох кіберзагроз із своїми чинниками кожна окремо. В графічному представленні така модель мала б декілька функціональних блоків і вузлів із векторними зв'язками між ними.

3 ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРАЦІЙНИХ СИСТЕМ СКУД ШЛЯХОМ ОРГАНІЗАЦІЯ МОДЕЛЕЙ І АЛГОРИТМІВ КІБЕРЗАХИСТУ

3.1 Розробка моделі загроз і захисту даних в ІС СКУД системах

Стандартні моделі захисту ІС СКУД для пакетів даних в їх каналах передбачають використання стандартних, але дієвих методів інформаційного захисту ІС СКУД, що не зовсім достатньо і часто потребує великих ресурсів, зокрема для: аналізу потенційних типів інформаційних загроз і сценаріїв кіберзагроз в інформаційних системах СКУД і формування правил ІБ для них із створенням дієвих механізмів і систем захисту інформації (і, зокрема, пакетів даних в каналах і ІС СКУД). Стандартна модель захисту інформаційної системи ІС СКУД із системою захисту передбачає створенні певного шаблону із підлаштовуваними параметрами (факторами впливу) на сам об’єкта інформційного захисту і його інфораційні процеси (тобто ІС СКУД).

Фаза 1 моделі. Повністю перелічити та провести аналіз усіх загроз і об'єктів системи ІС СКУД (а також дата-процесів), що підлягають захисту від впливів порушника *Oi*.

Фаза 2 моделі. Повністю перелічити та провести аналіз всіх можливих варіантів дій хакерів і порушників (в т.ч. кіберзагроз), тобто вказати всі потенційні загрози інформації: формується набір загроз інформаційної безпеки $З_Н$.

Фаза 3 моделі. Визначити у кількісному співвіднощшенні заходи кіберзахисту від відповідної загрози для кожного об'єкту. Кожна кіберзагроза, позначена у фазі 2, має свою ймовірність появи, яка визначається на даній фазі: результаті утворюється граф моделі захисту ІС СКУД, де ребро (t_i,O_j) означає, що загроза t_i дозволяє отримати доступ до об'єкта Пр O_j.

Фаза 4 моделі. Сформувати засоби комплексного захисту інформації в системі ІС СКУД. *Мета* засобів захисту інформації в ІС СКУД – створити бар'єр та захищене середовище для доступу до інформації ІС СКУД по кожному ребру графа. Так формується набір засобів забезпечення захисту

інформації *М*. Один і той же засіб безпеки може захищати декілька об'єктів і протистояти декільком кіберзагрозам одночасно.

Фаза 5. Визначити в кількісному вираженні міри можливості дії протистоянгнгя кіберзагрозам в системах ІС СКУД. Якщо ці заходи перевищують рівень загрози в ІС СКУД, то така система захисту ІС СКУД вважається достатньою.

Двоперіодний графовий рисунок перетворюється в триперіодний за рахунок появи додаткового набору параметрів M_i*,(M)*. Набір M_i, є деякою мірою і забезпечує опір для загрозливих дій порушників та кіберзагроз. При цьому в метаграфі ребро O_j (t_i,o_j) позначає незахищений інформаційних об'єкт в ІС СКУД. На даному етапі також визначають ступінь захищеності системи за рахунок зіставлення кожній дузі графа вагового кількісного коефіцієнта.

Різновиди моделей ІБ ІС СКУД:

1. Модель системи на базі розмежування прав доступу до ресурсів ІС СКУД;

2. Модель системи захисту ІС СКУД на базі шифрування в каналах.

Ці дві моделі можуть описувати захист ресурсів із кількома користувачами. При цьому, якщо ІТ ресурси вимагають більшого рівня захисту, то доступ до них здійснюється лише за наявності у користувача прав. Ці 2 моделі безпеки ІС СКУД мають раяд особливостей при використанні на практиці.

1. На практиці часто досить складно визначити всі шляхи негативних дій по відношенню до системи ІС СКУД, що погіршує адекватність результатів моделі;

2. Відсутність визначення ребра (t_i,o_j) не означає, повний захист системи;

3. Не враховуються витрати на захист системи і отримуваний результат. Модель захисту ІС СКУД показана на рисунку 3.1.

Дана модель (рис.3.1) враховує комплексний фактор реалізації ризиків в каналах і інфомраційно-комунікаційних трактах реалізації передавання даних в системах, їх оцінку та шляхи нейтралізації. Об'єктивні показники моделі:

- *Канальні загрози інформаційній безпеці,* характеризуються ймовірністю реалізації атаки, пропорційно кількості комунікацій в ІС СКУД;
- *Вразливі точки* (точки реалізації загроз інформаційної системи або

системи запобігання загрозам (системи інформаційної безпеки);

- *Враховується ризики* – фактори кіберзагроз, що відображають можливі наслідки від атак і загрози в ІБ ІС СКУД: втрата, модифікація інформації та несанкціонований доступ до неї (зчитування та запис).

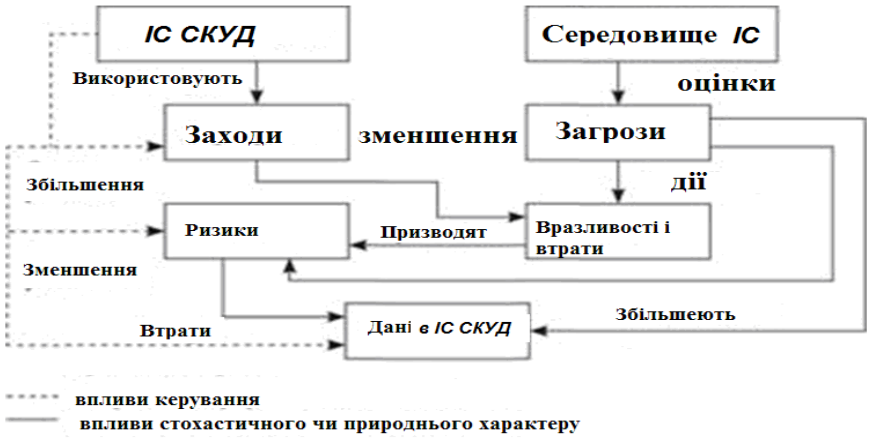


Рисунок 3.1 – Модель загроз і захисту даних в системах ІС СКУД із оцінками загроз

Також відомою є модель, що передбачає використання оцінки ризиків і запровадження заходів інформаційної протидії (рис. 3.1).

Для побудови збалансованої системи інформаційної безпеки ІС СКУД потрібно спочатку провести комплексний аналіз ризиків у сфері інформаційної безпеки пакетів даних на базі системи захисту інфомраційних даних. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки ІС СКУД із дієвим захистом потрібно будувати так, щоб досягти заданого рівня ризику.

3.2 Методика захисту пакетів даних в ІС СКУД із використаннм вдосконаленої моделі захисту

Модель і методика кіберзахисту в ІС СКУД дозволяє проаналізувати та оцінити вплив факторів на ІС, оцінити вимоги по інформаційній безпеки, аналіз функцій і послуг в ІТ ІС СКУД. Досягти високрих рівнів захисту можна при вирішенні основних задч безпеки ІТ ІС СКУД:

- оцінка ризиків по всім комунікаціям в системах і комплексна оцінка фактору безпечності даних;
- віднесення і класифікація інформації до категорії ступеня захисту і дооступу);
- прогнозування і своєчасне виявлення кіберзагроз для ресурсів ІС СКУД;
- створення умов функціонування з найменшою вірогідністю кіберзагроз;
- створення механізму і умов оперативного реагування на кіберзагрози;
- створення умов для максимально можливої локалізації наслідків кіберзагроз;
- уникнення зайвих витрат на заходи безпеки в ІТ ІС СКУД;
- здійсненні захисту на всіх стадіях життєвих фаз моделі ІБ ІС СКУД;
- забезпечення роботу ІБ ІС в короткі терміни та оцінка ефективності захисту.

Побудова моделі інформаційної безпеки та технології захисту ІС СКУД при розгляді та аналізі параметрів моделі ІБ систем ІС СКУД та вибір ункій захисту потребує врахуввання взаємозв'язків між ресурсами ІС СКУД. Наприклад, реалізації сценарію кібератак і втрати чи витоку даних із ІС. Також сценарію виходу із ладу якогось вузла ІС СКУД, що може призвести до втрати даних або виходу з ладу функціоналу СКУД чи іншого критичного елемента ІС СКУД. Ці взаємозв'язки визначають основу побудови моделі безпеки ІС для організації надійної інформаційної безпеки. Ця модель, відповідно до пропонованої методики може підвищити рівень інформаційного захисту і ІБ СКУД і за умов суміжного використання із методом ІБ забпезпечити високий рівень інформаційного захисту ІС ІТ СКУД: як для виділених ресурсів, так і для локальних. Модель ІБ дозволяє оцінити і виробити заходи протидії потенційним ризикам і кіберзагрозам безпки в ІС СКУД, зменшити втрати даних, помилки невірної ідентифікації, що визначають різні порушення функціоналу безпеки в процесах компанії та призводять до негативних наслідків. Також модель ІБ може проводити відповідні оцінки і розробку заходів протидій потенційним ризикам. Також ждозволяє врахувати

взаємозв'язки інформаційних ресурсів в ІС СКУД, які визначають загрози безпеці та оцінюють вірогідність їх реалізації.

3.3 Аналітична оцінка кіберзагрози в системах ІС СКУД

Для успішного застосування і оцінки захисту в ІС СКУД інформаційних блоків і пакетів пропонується використати математичні моделі оцінки і захисту від загроз (модель безпеки даних в ІС СКУД).

Окремі кіберзагрози в ІС СКУД, наприклад прямі мережеві втручання та SQL|XSS-ін'єкції, чи ін'єкції шкідливого коду чи функціоналу ШПЗ в ІС СКУД можно формалізуються розширеною моделлю втручання:

$$G(x,y,f) = g_0(t,x,e) \exp[-\alpha(t)\, q_k(x)\, I\, k\,], \qquad (3.1)$$

де, $q_k(x)$ – характеристики дії загроз; I- інтенсивність загроз ; k - коефіцієнт характеру виникнення загроз.

Значення коефіцієнтів $k=10^{-4} – 10^{-6}$ вважався задовільним, то в наш час завдяки розвитку технологій вважається прийнятним $k=10^{-6}$. Тому будь-яка система повинна бути розроблена із запасом надійності і передбачати деякий «запас безпеки», щоб передбачати різкі зміни умов впливу кіберзагрози на основі компоненти I та k . В СКУД вище інформаційні процеси і їх характер (в ІС СКУД), зокрема – загасання (спад) прояву і збільшення(стрибки) захисту при різних умовах явищах, зокрема при збільшенні інтенсивності інформаційних потоків (і загроз в т.ч.) можливе при збільшенні коефіцієнту загроз $-\alpha(\lambda)$ при збільшенні їх інтенсивності λ самих загроз , яка можна досить високих значень в екстремальних умовах і при критичному впровадження. Це передбачено в моделі загроз. Це можна отримати при моделюванні (3.1) і показати на рис.3.2.

Ця модель оцінки формули(3.2) і результата (рис.3.2) може бути взята за основу при оцінці інформаційних загроз і може використовуватись при розробки зовнішніх заходів захисту для систем ІС СКУД, які послідовно підключаються і функціонують в складі основної структури ІТ СКУД.

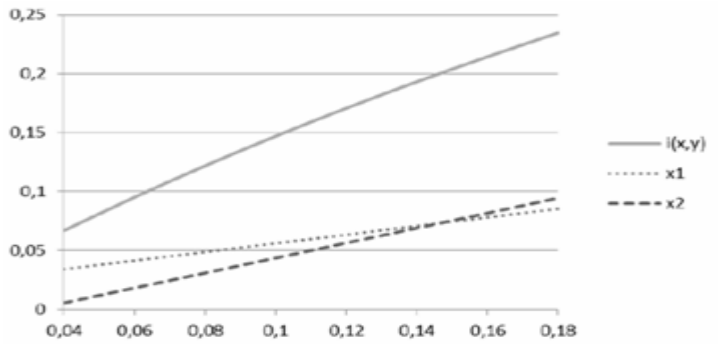


Рисунок 3.2 – Узагальнена характеристика зхзагроз в ІС СКУД та інтенсивність інформаційних процесів

Аналіз і нейтралізація шкідливого коду в трафіку і пакетів даних і в складі ІС СКУД із своїм обчислювальним процесом, відбувається в режимі наближеного до реального часу. Використання підходів захисту даних в ІС СКУД і зокрема технологій захисту даних, використання захищених каналів СКУД на базі основних мережевих протоколів захисту дозволяє проводити підвищення рівнів захисту від загроз. Стабаліація інформаційних обчислювальних процесів, а також захист трафіку передбачає умовно максимальну мінімізацію кіберзагроз та ризиків їх появи $r_{сх}$:

$$E_{сх} \rightarrow [\max(\min Y_r) \; , Y_r \in M_r] ;$$

$$´Yr = \sum_{i}^{n} Yr_i \rightarrow N * Y_i s \qquad (3.2)$$

де Y_r – узагальнена ймовірність появи інформаціних ризиків в системі ІС СКУД ($Y_r \in M_r$) , де M_r – множина інформаційних ймовірностей загроз (мапа кіберзагроз).

Дана модель безпеки ІС СКУД забезпечує достатньо точну оцінку безпеки ІС СКУД і враховує основні впливи і параметри самої системи СКУД.

3.4 Структурна організація ІС СКУД на базі запропонованих підходів

Варто відзначити, що інформаційні дані в СКУД як і електронна система і ПЗ СКУД та їх ресурси даних – це послуги і суміжні ІТ сервіси, які надаються для забезпечення електронної взаємодії між різними відділами в складі системи безпеки підприємства.

Вразливості і загрози для пакетів даних теж мають місця в системах ІС СКУД та можуть мати серйозні наслідки для всіх бізнес-процесів підприємства і бути використані зловмисниками для компрометації і несанкціонованого потрапелення 3-х осіб на територію підприємства шкідливого трафіку і вторинного зламу ІКС систем ІС СКУД. Структури ІС СКУД на рис.3.3 та на рис.3.4.

Рисунок 3.3 –Структура ІС СКУД, яка інтегрована в ІТ інфрастуктуру

Також , відповідно до проведеного аналізу загроз для систем ІС СКУД, в процесі досліджень і аналізу виявлено, що можуть бути використані недосконалості та вразливості в ІС СКУД, які можуть в подальшому бути використані (рис.3.3).

Окремим місцем є інформаційні мережі і інфраструктура систем ІС СКУД, яка потребує окремої уваги з точки зори інформаційної безпеки самої ІС СКУД, оскільки це може стати джерелом втрат інформації. Структура інформаційної мережі та сервісів інформаційної технології ІС СКУД показана на рис. 3.4.

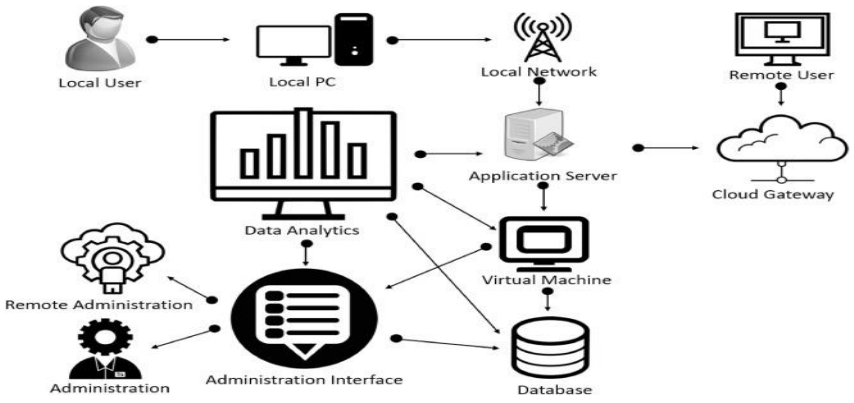


Рисунок 3.4 – Структура інформаційної мережі ІС СКУД із базовим захистом

Базова структура передбачає базовий захист ІС СКУД, але його часто не достатньо для повноцінного захисту і це потребує ретельного вивчення і застосування нових підходів захисту і в тому числі комплексних підходів на різних ділянках і вузлах ІС СКУД із використанням комплексної системи захисту інформації (КЗСІ) в ІС СКУД.

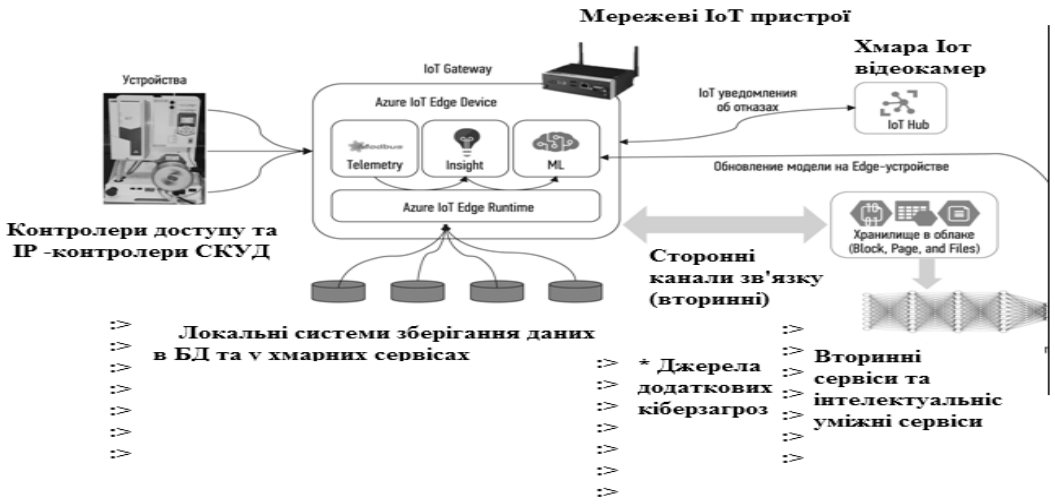


Рисунок 3.5 – Структурна модель обміну даними в СКУД на базі інтелектуальних сервісів

3.5 Оцінка вразливостей і джерел загроз для структур ІС СКУД

Аналіз структур (рис.3.3 - рис.3.5) показав, що існують вразливості та недоліки ІС СКУД, які можуть вплинути на стабільність інформаційної системи СКУД. Окремі із найпоширеніших вразливостей наступні :

1. Недостатня аутентифікація і контроль доступу в ІС СКУД.

2. Незахищений обмін пакетами даних і відсутність шифрування.

3. Вразливості ПЗ і схемотехніки в ІС СКУД.

5. Втрати даних у каналах СКУД IoT через (MiTM-атаки) і вузлах (MiTN).

6. Несанкціонований фізичний доступ до обладнання і вузлів ІТ СКУД.

7. Атаки через побічні канали і комунікації.

Ці уразливості потребують систематичного аналізу та оперативного реагування і закриття.Одним із надзвичайно важливих аспектів є регламентація електронного контроль доступу. Базові резюмуючі висновки по аналізу часитини вразливостей ІС СКУД (рис.3.6):

- базовий захист в існуючих для забезпечення високого рівня ІБ ІС СКУД;

- окремі вузлу і місця ІС СКУД є більш вразливими до атак і впливів;

- потрібні нові і додаткові методи і заходи захисту для високорівневої ІС;

- запровадження нових засобів і заходів захисту інформації для захисту ІС СКУд і ПЗ високого рівня, в тому числі виконання політик кібергігієни та кібербезпеки на місцях (рис.3.6).

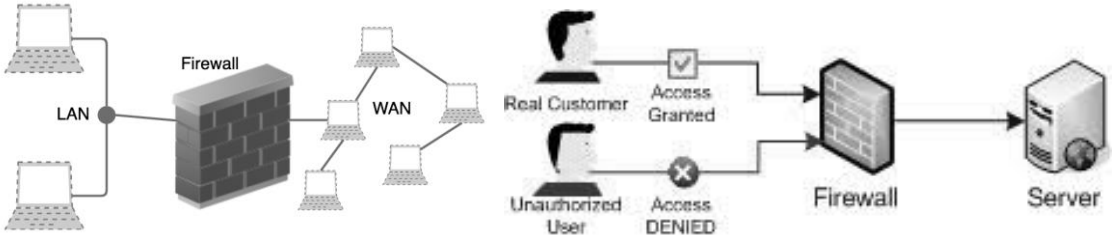


Рисунок 3.6 – Основні проблеми і загрози інформаційних втручань у мережі ІС СКУД по вторинним і основним каналам

Сучасні прилади і компоненти (програмні і апаратні) ІС СКУД досить широко охоплюють всі сфери сучасного життя від побутових систем ІС СКУД до персональних ПК і корпоративних систем ІС СКУД для використання професійних промислових функцій. Розвиток мережі Інтернет сприяє розвитку засобів ІС СКУД, які являють собою сукупність пристроїв і ПЗ, як

персональних пристроїв користувачів так і програмних систем для захисту електронних документів і інформації користувача, а також окремих вузлів і пристроїв із використанням Інтернет - каналів і інтерфейсів. Сучасні системи ІС СКУД є високоінтелектуальними ІС і містять засоби захисту і тракти зв'язку із іншими окремими ІС системами або програмами в їх складі. У сучасних ІС СКУД комплексна інформаційна безпека і ризики – значна проблема для передачі пакетів даних в мережах і каналах ІС СКУД.

Із зростанням популярності технології СКУД і суміжних систем, а також портативних мобільних пристроїв і смарт-пристроїв користувачів, і суміжних сервісів зростає й інтенсивність інформаційних загроз і через канали суміжних IoT пристроїв.

3.6 Адаптація нового методу і моделі більш захищеного обміну інформацією в системах ІС СКУД

Основні засади і тези фундаменту запропонованих підходів при розробці методу і моделі підвищеного інформаційного захисту ІС СКУД на базі пристроїв IoT :

– використання 2-х рівневого шифрування даних в ІМ ІС СКУД;

– використання багатофакторної (MFA) та багатопараметричної (MPA) ідентифікації (технологія MultiID) для суб'єктів доступу в ІС СКУД багатопараметричний контроль автонтифікації об'єктів із залученням мінімім 4-х параметрів і формуванням Multi Hash-ID *(HID) для кожного унікального параметру ідентифікації об'єкта електронних документів профілів у інформаційній системі СКУД і контроль проходження субєкта на різних етапах за допомогою технології MultiiD на кожному етапі його проходження на об'єкті, в системі ІС СКУД (на базі різних алгоритмів обчислення Геш-функцій MultiiD :

– Hash-функцій – Схема: A $-_{Hash}$ B $-_{Hash}$ –C;

– використання фізичної ізоляції і моніторингу цілісності ІС СКУД;

– використання регулярних бекапів даних на різних розподілених;

– використання шифрованного і поліпшеного і захищеної предасчі

пакетів даних в ІС СКУД;

– використання шифрування і доступу і захисту файлових систем ПК/серверів на розподілених джерелах сховища ІС СКУД;

– контроль дата процесів і дата –потоків (Data-flows) в СКУД за допомогою SIEM XDR;

– використання електронних ключів доступу операторів і адміністратора до ІС СКУД;

– виконання дотримання політик кібергігієни і кібербюезпеки;

– використання систем захисту даних IDS|IPS - моніторингу процесів SIEM в ІС СКУД і КСЗІ (Комплексних систем захисту інформації). Контроль документів і інформації в ІМ ІС СКУД, яка має вищий рівень цінності і секретності – запроваджуються більш високо рівневі заходи захисту, і навпаки – для інформації, яка має менший ступінь захисту – запроводжується менш високо рівневі заходи захисту ;

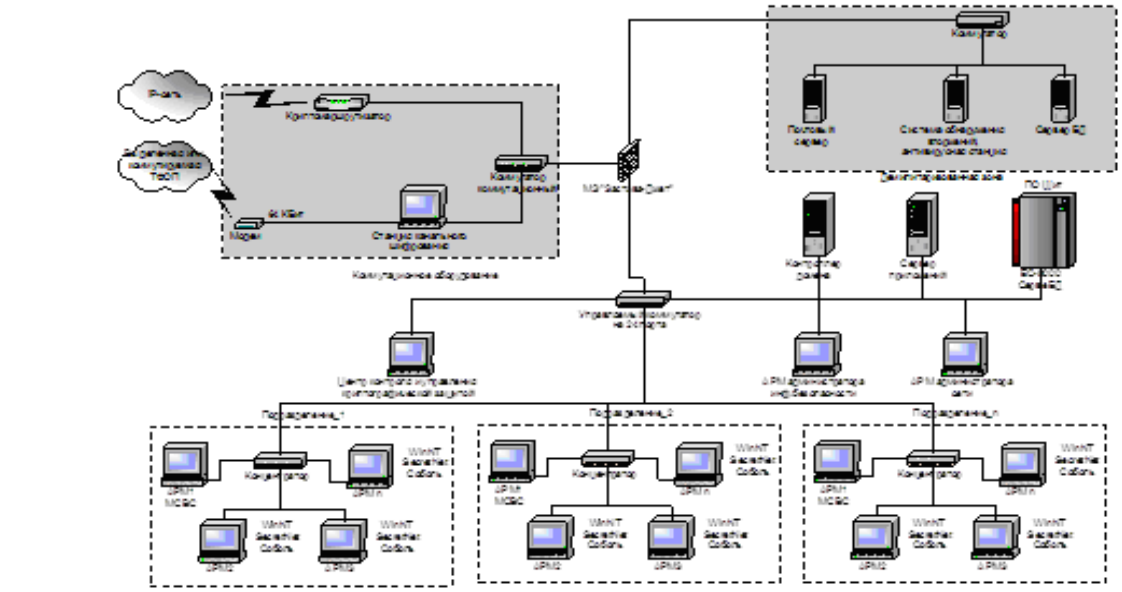
– використання підходу «диференційованої сегментації» мережі ІС СКУД за допомогою технології x-VLAN , що практично призводить до визначення оптимального рівня захисту ІС СКУД;

$$ESecL = ni \; x \; ki \; x \; Pi \; x \; IDLi \; x\text{-}VLAN \; / \; . \qquad (3.3)$$

де *ki* – коефіцієнт пропорційності захисту; *ni*– коефіцієнт пропорційності розмежування мереж і галудження на підмережі;c Level – загальний рівень захисту ланки системи ІС СКУД; Pi – питома технічна «вага/вартість інформації» в ІМ ІС СКУДі впровадження заходів і засобів захисту 1 –ї ланки системи ІС СКУД; IDLi – питомий рівень інформаційної захищеності при впровадженні заходів і засобів захисту 1 –ї ланки системи ІС СКУД.

Основна ідея і раціональне правило: вартість захисту ланки системи ІС СКУД повинна та бажано щоб була значно меншою за вартість її основного функціоналу Pi < Pi MAIN FUNC та вартість захисту ланки системи ІС СКУД повинна бути співмірною або дорівнювати повинна із вартістю її основного функціоналу Pi ≈ Pi MAIN FUNC. На рис. 3.7 показано структуру

функціональної схеми ІМ ІС СКУД. На рис. 3.8 показано структуру захищеної інформаційної мережі ІС СКУД із підвищеним рівнем захисту та додаткової підходами ІБ.



Функціональна схема ІС СКУД

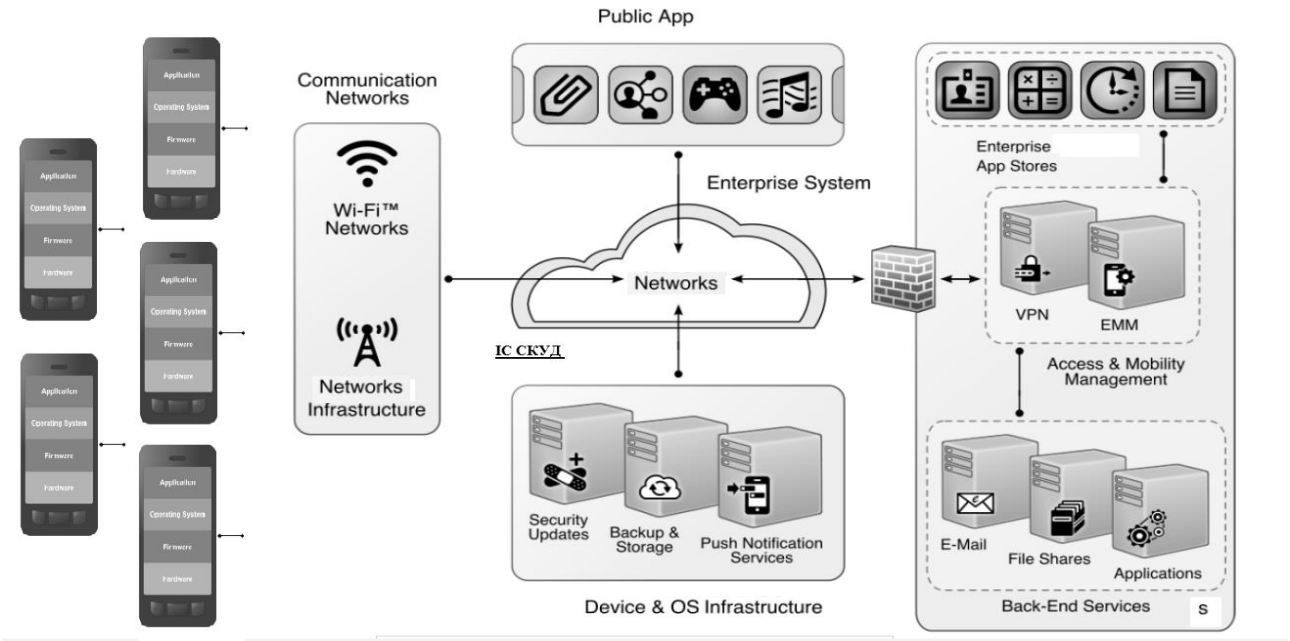


Рисунок 3.7 – Структура функціональної схеми ІМ ІС СКУД із підвищеним захистом і запропонованими підходами додаткового захисту на базі методу

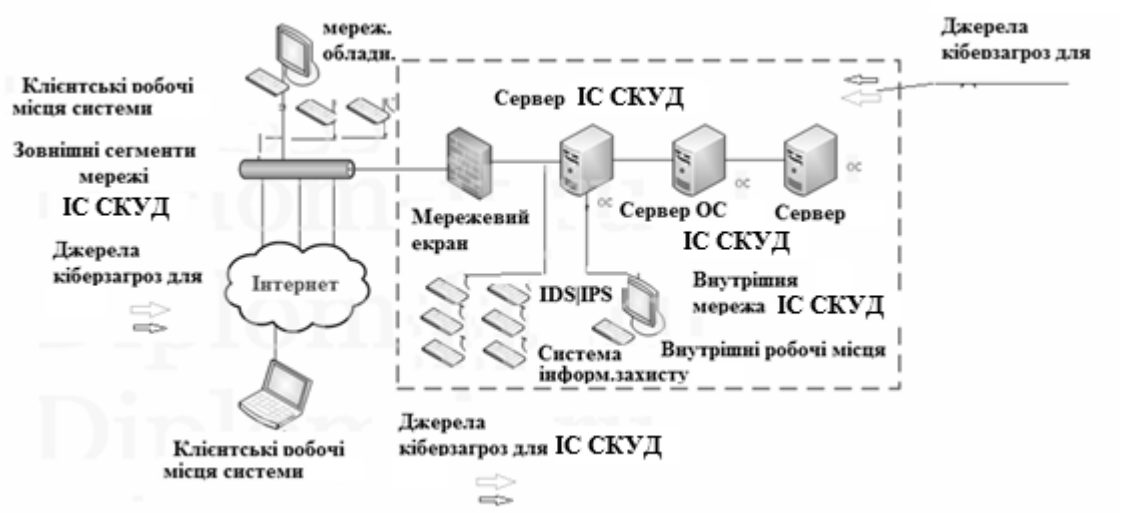


Рисунок 3.8 – Структура захищеної інформаційної мережі ІС СКУД із підвищеним рівнем захисту і підходами додаткової ІБ

Узагальнена структурна схема захищеної інформаційної мережі ІС СКУД (рис.3.8) ілюструє засади методу і моделі покращення захисту даних в ІС СКУД організації із використанням захищених ІМ для ІС СКУД

Для забезпечення безпечного контролю доступу за допомогою ІС СКУД і пакетів даних передачі і електронного сертифікати і апаратного ключа ІС СКУД (рис.3.7 – рис.3.9)даних в системах ІС СКУД в безпечних умовах, із контролем їх цілісності і додатковим рівнем ІБ, як показано на структурі (Рис. 3.9).

Так, принцип додаткового захисту полягає у:

– відправник із безпечністю отримує завізований і захищений режим передачі пакетів даних в ІС СКУД;

– в процесі підписання адресати отримують повідомлення з проміжними статусами документів: доставлено, погоджено чи відхилено із мітками часу і погоджено та підписано одним або двома сертифікатами (в залежності від необхідного рівня захисту ІС СКУД);

– дані передаються в захищених каналах ІМ в захищеній мережі ІС СКУД;

– здійснюється контроль параметрів ідентифікації суб’єктів в ІС СКУД за допомогою механізму унікальних Геш-функції для кожного

унікального параметра Nk>2 (не менше 2-х).

На рисунку 3.8 показано схему руху пакетів даних в захищеному режимі.

Покращена схема контролю ідентифікації багатьох пареметрів за допомогою накладання 2-го сертифікатів на електронні документи і проміжного контролю ціілістності (порівняно із відомою схемою), яка враховує накладання другого параметра (Kx=2 II) і проміжного контролю цілісності на проміжних етепах передачі інформаційних сигналів даних, які є і формують додатковий рівень захисту для більш важливих суб'єктів доступа і зон доступа, як це показано на рис. 3.9.

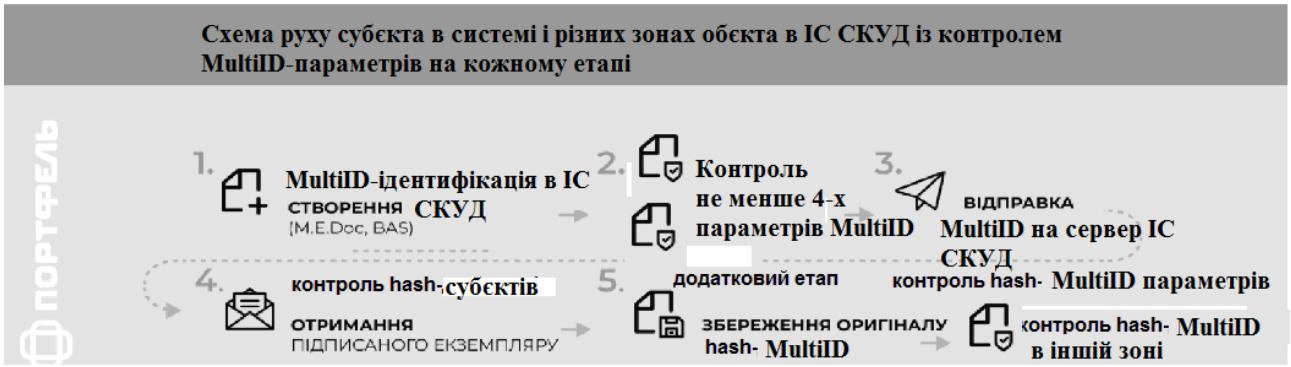


Рисунок 3.9 – Схема руху суб'єкта із контролем параметрів ідентифікації у різних зонах СКУД (в загальній схемі ІС СКУД за допомогою унікальних Геш-функції для кожного параметра

При великому обсязі даних організація отримує інструкцію щодо контролю профілів для роботи СКУД при електронного контролі доступу (ІС СКУД) та встановлює порядок використання електронного контролю доступу (ЕКД). Для більш важливих зон доступу може бути паралельно використано декілька параметрів (технологія MultiID) за допомогою алгоритма вибору ступеню захисту із мультиілдентифікацією за багатьома параметрами. Таким, чином кожен співробітник компанії і користовуач ІС СКУД повинен контролюватись за багатьма параметрами у ІС СКУД. Адміністратор і керуючий ІС СКУД і нормативами сам вазначати ступінь важливості і кількості параметрів контролю суб'єкта в ІС СКУД у різних зонах і приймати рішення про надання додаткового ступеню ідентифікації згідно технології MultiID (ID +)

(рис.3.10 – рис.3.12) і надання самогодоступу – для додаткового рівня захисту системи ІС СКУД системи отримати свої власні електронні ключі згідно з цією інструкцією. Тепер давайте розберемося, що таке 2-й електронний hash (ЕП2 чи КЕП 2), та яким чином формується multiID із MultiHash і профілю електронним сертифікатом в каналах і захистом додатковим алгоритмом (MultiID).

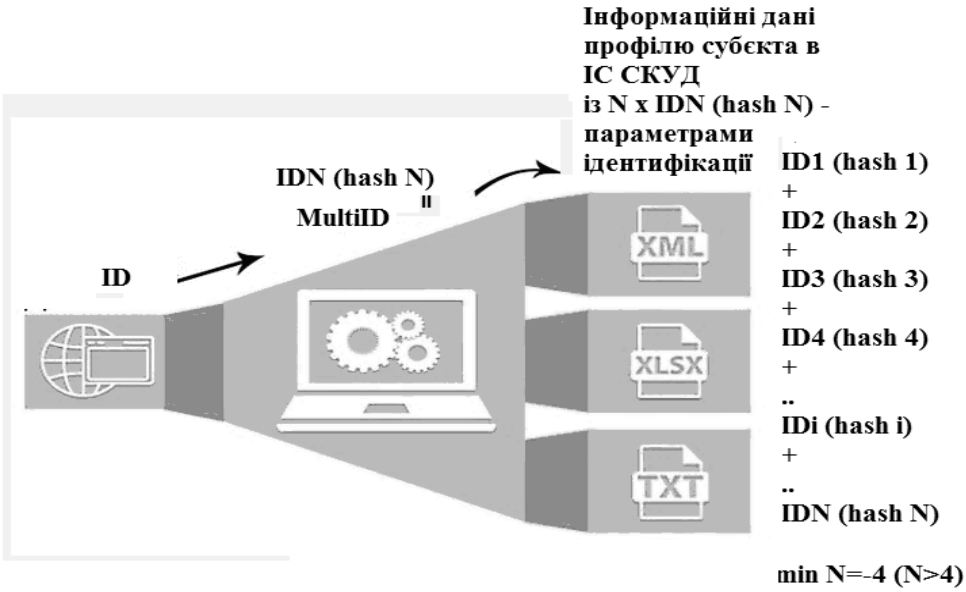


Рисунок 3.10 – Схема підписання і руху профілів даних суб'єктів за допомогою додаткового рівня захисту із запровадженням додаткових параметрів і генерації унікального Геш по згортці спектрів цих параметрів (MultiID f(g*{x hash [I + II + i + + N]}) із контролем Геш-функцій ідентифікаційних параметрів профілю суб'єкта у про файлі файлів в загальній схемі ІС СКУД

Дана технологія реалізує додатковий захист за допомогою (MultiID [I + II + i + + N] x hash із контролем декількох Геш-функцій ідентифікаційних параметрів профілю судєкта у про файлі файлів в загальній схемі ІС СКУД за допомогою додаткового захисту

Електронний контроль доступу в ІС СКУД реалізований за допомогою технології MultiID (ID +) пропонується використати як однин із варіантів додаткового захисту в ІС СКУД - як складова методу захисту , відомий

додатковий ідентифікаційні парамтери . що значно підвищує захист профілів від багатьох атак із підміною ID профілів суб'єктів доступу в ІС СКУД .

Особливо це актуально для більш важливих зон доступу в СКУД чи контролю найбільш ризикованих суб'єктів доступу в СКУД , де *hash*-функції формуються і складаються із мінімум 4-ох параметрів ідентифікації : 1-го відомого і 2-3-х секретних. Передбачається формування особистого ключа сертифіката та 2-го параметра для генерації *hash*-функції , які використовуються як пара параметрів (2). Секретний блок даних із самим ключем шифрування (секретним ключем) генерується на базі перетворень і предсатвляє захищений шифрований блок. Генерується аналогічно як і відкритий блок даних але за унікальна алгоритмом , що формує *hash*-послідовність із шифруванням на базі псевдо-випадкових символів. Сертифікат -го відкритого ключа 2 обчислюється на основі секретного ключа, але для вищої криптостійкості руху профілів даних суб'єктів за допомогою додаткового рівня захисту:

$$\text{Fsec (MultiID)} = \text{MultiID [Fsec [I] + Fsec [II] + Fsec [i] + + Fsec [N]] } x\ hash = = \sum_{i=4}^{N} \text{Fsec[i]}_i \rightarrow \text{Nhash} * \text{Fsec[i]}_i \quad (3.2)\ ;$$

$$\text{Fsec (MultiID)}_{\text{cx}} \rightarrow [\max(\min \text{Y}_\text{r}) \ , \text{Y}_\text{r} \in M_r]\ ;$$

$$\acute{}\,\text{Yr} = \sum_{i}^{n} \text{Yr}_i \rightarrow \text{N} * Y_\text{r}\text{s} \qquad (3.4)$$

де Fsec (MultiID) – узагальнена функція захисту від технології MultiID, яка зменшує ймовірність появи інфомраціних ризиків в системі $\text{p}_\text{r} \rightarrow \text{p min } (\text{p}_\text{r} \in m_r)$, де m_r – множина інформаційних ймовірностей загроз (мапа кіберзагроз).

Одинична функція захисту Fsec[i]_i ресурсу визначається функцією захисту при ідентифікації за допомогою тільки одного параметру і його Ґеш-функуції (MultiID [Fsec [I] *x hash*) обчислюється за допомогою 2-го іншого алгоритму. Зауважте, що неможливо отримати секретний ключ із самого сертифікату, як при використанні сертифікату 1 (традиційний захист) так і з використанням додаткового сертифікату 2 (додатковий захист), так і із їх комбінативним

поєднанням. Сертифікат відкритого ключа 1 і відкритого ключа 2 (рис.3.11 та рис.3.12)містить персональну інформацію та ID-власника (наприклад, ім'я, унікальний реєстраційний номер, видавця сертифіката та термін його дії) шифрується секретним та відкритим ключемами. Ці сертифікати визначаються алгоритмом шифрувння і можуть бути використані стандартні методи і шифри для генерації і передачі в захищеному вигліді в системі ІС СКУД. Розшифровка (дешифрування) відбувається на приймальні стороні пакета даних ідентифікації. Блок даних, в які входять унікальні параметри ідентифікаці на базі MPA і MultiID шифрується та дишифрується на кінцевих точках ідентифікації та обробки параметрів . В самі системі ІС СКУД ці блоки передаються в захищеному вигляді. Вміст цих блоків не змінюється в процесі передачі пакетів (наприклад. ЕПК І та ЕПК ІІ) каналами ІС СКУД . Замість цього можуть додаватись інші блоки даних, які можуть бути використані для обфускації для підвищення захисту інформації.

Процес отримання цього блоку складається із декількох етапів, показаних на рис.3.9, рис.3.10(вище). При модифікації даних змінюється й їх цифровий відбиток (signature та/або Геш-функція, *x hash*-функція), і тоді інформація про суб’єкт не пройде перевірку електронного цифрового відбитку *x hash*-ідентифікації (ЕЦБ). Таким чином, електронний цифровий відбиток (ЕЦБ), який ідентифікує субєкт разом із тим й захищає його від зміни третіми особами після накладання ЕЦП, а шифрування секретним ключем підтверджує авторство цього блоку даних. Сам процес руху і контролю даних ЕЦБ в структурі ІС СКУД показаний на рис.3.11.

Цифровий Геш (Геш-функція) ЕЦБ дозволяє контролювати цілісність даних на етапах проходження ідентифікації субєктів в СКУД (в ІС СКУД) між її вузлами. Тобто, якщо дані функції змінилась – субєкт не буде ідентифіковано або якщо вони пошкодились чи є інформаційні втручання в нього (допис іншої частини, спроба доступу, спроба запису вірусу, або додаткової частини та інше..) . Геш-функція (Hash-Functipon) – є індикатором цілістності і безпечності документа на шляху його руху в системах ІС СКУД.

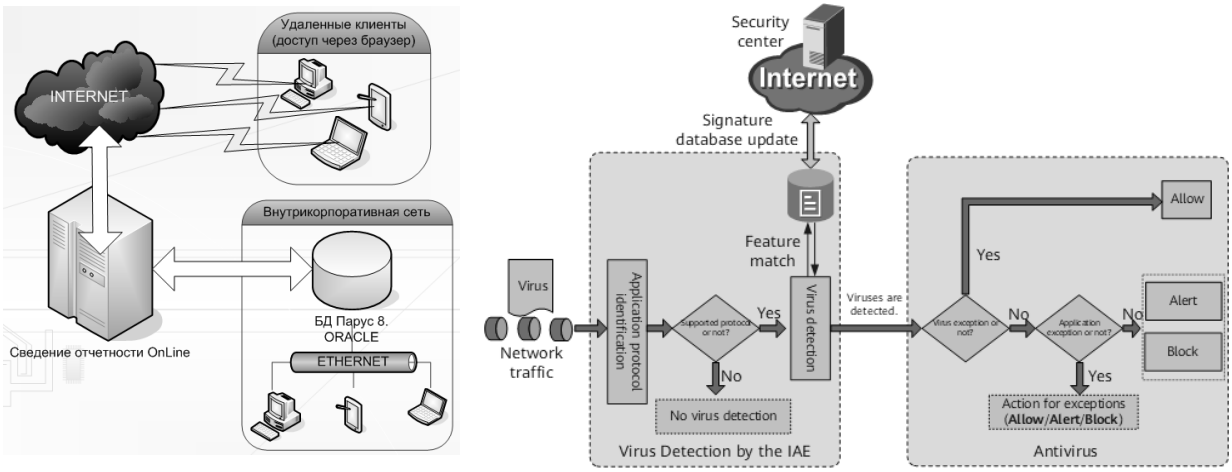


Рисунок 3.11– Процес руху і контролю даних ЕЦБ в структурі ті ІС СКУД системи із додатковим захистом даних на проміжних вузлах і точках

Досить серйозну небезпеку створюють інциденти та небезпечні файли в ІС СКУД, яку можуть проходити скомпрометований вузол мережі ІС СКУД, в якому файл чи ЕЦБ може бути викрадений чи пошкоджений або заражений вірусом. У простому варіанті на практиці і в більшості випадків – він пошкоджений. Це становить ризики для всієї системи ІС СКУД. Це становить досить серйозну загрозу для організацій і фізичних осіб, які експлуатують технології ІС СКУД, оскільки неправильне або недостатній рівень захисту інформації в ІС СКУД може призвести до витоку конфіденційних даних, порушення їх цілісності та доступності, порушення безпеки всієї ІС СКУД та інших її вузлів, а також спричинити ризик фальсифікації документів і становить небезпеку для інших вузлів ІС СКУД.

4 ЕКОНОМІЧНА ЧАСТИНА

Для успішного впровадження науково-технічної розробки надзвичайно важливо, щоб вона відповідала поточним вимогам науково-технічного прогресу і враховувала економічні аспекти. Оцінка економічної ефективності результатів науково-дослідної роботи є ключовою частиною цього процесу. Дослідження, яке представлене у магістерській роботі і присвячене розробці та вивченню "Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей", віднесено до науково-технічних проектів, спрямованих на введення на ринок. Рішення про комерціалізацію розробки може бути прийняте протягом виконання самої роботи, відкриваючи можливості для подальшого введення на ринок. Цей напрямок визначається як пріоритетний, оскільки розроблені результати можуть бути корисними для різних зацікавлених сторін і приносити економічні вигоди. Однак для успішної реалізації цього процесу вирішальним є залучення зацікавленого інвестора, який виявить інтерес до втілення даного проекту, і переконання його у доцільності інвестування у цю розробку. З метою досягнення цього завдання були визначені такі етапи виконання робіт:

1. Проведення комерційного аудиту науково-технічної розробки, включаючи визначення науково-технічного рівня та комерційного потенціалу.
2. Розрахунок витрат на реалізацію науково-технічної розробки.
3. Проведення розрахунку економічної ефективності впровадження та комерціалізації науково-технічної розробки для потенційного інвестора, а також обґрунтування економічної доцільності комерціалізації з точки зору інвестора.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» є підвищення рівні захищеності та рівня

інформаційної безпеки системи контролю доступу на базі пристроїв Інтернету речей (IoT) шляхом вдосконалення підходів, методу і моделі інформаційного захисту ІС СКУД із IoT пристроями.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1.

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі влас-тивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів

Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років

12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці. Для оцінки науково-технічного рівня і комерційного потенціалу розробки експертами було запрошено трьох незалежних експертів кафедри «Захисту інформації» Вінницького національного технічного університету: к. т. н., професор Кондратенко Наталія Романівна, к. т. н., доцент Дудатьєв Андрій Веніамінович, к. т. н., доцент Баришев Юрій Володимирович.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	Кондратенко Наталія Романівна	Дудатьєв Андрій Веніамінович	Баришев Юрій Володимирович.
	Бали, виставлені експертами:		
1. Технічна здійсненність концепції	4	3	4
2. Ринкові переваги (наявність аналогів)	3	4	4
3. Ринкові переваги (ціна продукту)	3	3	3
4. Ринкові переваги (технічні	2	3	3

властивості)			
5. Ринкові переваги (експлуатаційні витрати)	4	3	4
6. Ринкові перспективи (розмір ринку)	3	3	3
7. Ринкові перспективи (конкуренція)	1	2	2
8. Практична здійсненність (наявність фахівців)	4	3	4
9. Практична здійсненність (наявність фінансів)	3	4	3
10. Практична здійсненність (необхідність нових матеріалів)	4	4	4
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	4	4	4
Сума балів	$СБ_1=39$	$СБ_2=40$	$СБ_3=42$
Середньоарифметична сума балів $СБ_c$	$\overline{СБ} = \frac{\sum_1^3 СБ_i}{3} = \frac{39+40+42}{3} = 40.3$		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3.

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків	Науково-технічний рівень та комерційний потенціал розробки

41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» становить 40 балів, що, відповідно до таблиці 4.3 рівень комерційного потенціалу розробки високий, що свідчить про комерційну важливість проведення даних досліджень.

Магістерська кваліфікаційна робота «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок, тобто при цьому відбувається комерціалізація науково-технічної розробки. Цей напрямок є для нас пріоритетним, оскільки результатами розробки можуть користуватися не тільки самі розробники, а й інші споживачі, отримуючи при цьому суттєвий економічний ефект.

Результатом магістерської роботи є процес підвищення рівня інформаційного захисту інформаційних систем (ІС) СКУД на базі IoT-пристроїв шляхом вдосконалення методу і моделі інформаційного захисту.

4.2 Визначення рівня конкурентоспроможності розробки

В процесі визначення економічної ефективності науково-технічної розробки також доцільно провести прогноз рівня її конкурентоспроможності за сукупністю параметрів, що підлягають оцінюванню.

В якості аналога для розробки було обрано аналог СКУД Sprinx CREL. Основними недоліками аналога є висока вартість та мала швидкодія, мала захищеність (інформаційна захищеність СКУД). Також до недоліків можна віднести високу експлуатаційну вартість і чисельні вразливості мережі ІС та ІКС СКУД..

У розробці дана проблема вирішується за рахунок використання багатофакторної та багато параметричної ідентифікації та автонтифвікації в ІС СКУД.

Одиничний параметричний індекс розраховуємо за формулою:

$$q_i = \frac{P_i}{P_{базі}}. \qquad (4.1)$$

де q_i – одиничний параметричний індекс, розрахований за i-м параметром;

P_i – значення i-го параметра виробу;

$P_{базі}$ – аналогічний параметр базового виробу-аналога, з яким проводиться порівняння.

Загальні технічні та економічні характеристики розробки представлено в таблиці 4.4.

Таблиця 4.4 – Основні техніко-економічні показники аналога та розробки, що проєктується

Показник	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (товар-конкурент)	Новий (інноваційне рішення)		
1	2	3	4	5
Кіберстійкість,	20	70-85	4	10%
Функціонал, кль.ф-цій	5-10	15-25	4	25%
Похибка, автонтифікації %	2-10	1-8	3	40%
Напрацювання на відмову, год	10000	10000-20000	4	15%
Якісний показинка	0,2	0,2-0.3	3	10%

Нормативні параметри оцінюємо показником, який отримує одне з двох значень: 1 – пристрій відповідає нормам і стандартам; 0 – не відповідає.

Груповий показник конкурентоспроможності за нормативними

параметрами розраховуємо як добуток частинних показників за кожним параметром за формулою:

$$I_{НП} = \prod_{i=1}^{n} q_i \,, \qquad (4.2)$$

де $I_{нп}$ – загальний показник конкурентоспроможності за нормативними параметрами;

q_i – одиничний (частинний) показник за i-м нормативним параметром;

n – кількість нормативних параметрів, які підлягають оцінюванню.

За нормативними параметрами розроблюваний пристрій відповідає вимогам ДСТУ, тому $I_{нп} = 1$.

Значення групового параметричного індексу за технічними параметрами визначаємо з урахуванням вагомості (частки) кожного параметра:

$$I_{ТП} = \sum_{i=1}^{n} q_i \cdot \alpha_i \,, \qquad (4.3)$$

де $I_{тп}$ – груповий параметричний індекс за технічними показниками (порівняно з виробом-аналогом);

q_i – одиничний параметричний показник i-го параметра;

α_i – вагомість i-го параметричного показника, $\sum_{i=1}^{n} \alpha_i = 1$;

n – кількість технічних параметрів, за якими оцінюється конкурентоспроможність.

Проведемо аналіз параметрів згідно даних таблиці 4.4.

$I_{тп} = 4 \cdot 0{,}1 + 4 \cdot 0{,}25 + 3 \cdot 0{,}4 + 4 \cdot 0{,}15 + 3 \cdot 0{,}1 = 3{,}5$.

Груповий параметричний індекс за економічними параметрами розраховуємо за формулою:

$$I_{ЕП} = \sum_{i=1}^{m} q_i \cdot \beta_i \,, \qquad (4.4)$$

де $I_{ЕП}$ – груповий параметричний індекс за економічними показниками;

q_i – економічний параметр i-го виду;

β_i – частка *i*-го економічного параметра, $\sum_{i=1}^{m} \beta_i = 1$;

m – кількість економічних параметрів, за якими здійснюється оцінювання.

Проведемо аналіз параметрів згідно даних таблиці .

$I_{ЕП}$=0,75 · 0,5 + 0,86 · 0,5 = 0,80.

На основі групових параметричних індексів за нормативними, технічними та економічними показниками розрахуємо інтегральний показник конкурентоспроможності за формулою:

$$K_{ІНТ} = I_{НП} \cdot \frac{I_{ТП}}{I_{ЕП}}, \qquad (4.5)$$

$K_{ІНТ} = 1 \cdot 3,5 / 0,80 = 4,4.$

Інтегральний показник конкурентоспроможності $К_{ІНТ} > 1$, отже розробка переважає відомі аналоги за своїми техніко-економічними показниками.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників.

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.6)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$З_о$ = 18000 · 5 / 21 = 4091 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	18000	818,2	5	4091
Інженер	15000	681,8	35	23864
Всього				27955

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i, \qquad (4.7)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \qquad (4.8)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6500 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б);

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1 \cdot 1{,}65 / (21 \cdot 8) = 65{,}8$ грн.

$З_{р1} = 65{,}8 \cdot 1 = 65{,}8$ грн.

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
1.Підготовчі	2	1	65,8	131,6
2.Монтажні	3	3	88,8	266,5
3.Складальні	2	5	111,9	223,7
4.Налагоджувальні	6	2	72,4	434,3
5.Випробувальні	3	4	59,8	179,5
Всього				1235,6

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \qquad (4.9)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (27955+1235,6) · 11 / 100% = 3210,92 грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \qquad (4.10)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (27955+1235,6+3210,92) · 22 / 100% = 7128,23 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{в\,j}, \qquad (4.11)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	180	1	180
ручка	15	1	15
Флешка	250	1	250
Всього			445
З врахуванням коефіцієнта транспортування			489,5

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему "Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей".

Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$К = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i \text{ грн.}, \quad (4.12)$$

де $Н_i$ – кількість комплектуючих i-го виду, шт.;

$Ц_i$ – ціна комплектуючих i-го виду, грн.;

$К_і$ – коефіцієнт транспортних витрат, $К_і$ = (1,1…1,15);

n – кількість видів комплектуючих.

Зроблені розрахунки бажано звести до таблиці:

Таблиця 4.8 – Витрати на комлектуючі

Найменування комплектувальних	Кількість	Ціна за штуку, грн.	Сума, грн.
Трансформатор	1	48	48
Електронні компоненти СКУд	16	5	80
Перемикачі	1	17,5	17,5
Считувачі	21	4	84
Моделі передачі даних	2	90	180
плати	38	4,5	171
Контроллера	12	45	540
Мікросхеми	2	50	100
Плас. Корпуси (полістерол)	1	40	40
Витратні матеріали	1	400	400
Всього з врахування коефіцієнт транспортних витрат			1826,55

4.3.5 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \qquad (4.13)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під

час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (25000 \cdot 1) / (2 \cdot 12) = 1041,67$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.9 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Комп'ютер	25000	2	1	1041,67
Робоче місце розробника ПЗ	210000	20	2	1750,00
Всього				2791,67

4.3.6 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \qquad (4.14)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е = 7,5$ грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$В_е = 0,25 \cdot 290,0 \cdot 7,5 \cdot 0,5 / 0,8 = 339,84$ грн.

4.3.7 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \qquad (4.15)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$В_{св}$ = (27955+1235,6) · 20 / 100% = 5838,03 грн.

4.3.8 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{H_{ів}}{100\%}, \qquad (4.16)$$

де $H_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (27955+1235,6) · 50 / 100% = 14595,08 грн.

4.3.9 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \qquad (4.17)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$В_{нзв}$ = (27955+1235,6) · 100 / 100% = 29190,16 грн.

Витрати на проведення науково-дослідної роботи на тему «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.18)$$

$В_{заг}$=27955+1235,6+3210,92+7128,23+489,5+1826,55+2791,67+339,84+5838,03 +14595,08 +29190,16 = 94600,14 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \qquad (4.19)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,5.

ЗВ = = 94600,14 / 0,5 = 189200,28 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» передбачають комерціалізацію протягом 3-х років реалізації на ринку.

В цьому випадку основу майбутнього економічного ефекту будуть формувати:

ΔN – збільшення кількості споживачів яким надається відповідна інформаційна послуга у періоди часу, що аналізуються;

N – кількість споживачів яким надавалась відповідна інформаційна послуга у році до впровадження результатів нової науково-технічної розробки, приймемо 1 особа

$Ц_б$ – вартість послуги у році до впровадження інформаційної системи, приймемо 50000,00 грн;

$\pm\Delta Ц_о$ – зміна вартості послуги від впровадження результатів, приймемо зростання на 1000,00 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для

кожного із 3-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \qquad (4.20)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2021 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0{,}8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =40%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ =(1·1000+50000·20)·0,83·0,4·(1-0,18/100%)=174413,86 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ =(1·1000+50000·(20+50))·0,83·0,4·(1-0,18/100%)=610850,61 грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3$ =(1·1000+50000·(20+50+60))·0,83·0,4·(1-0,18/100%)=1133579,7 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.21)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований

рівень інфляції в країні, τ=18%;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$ПП$ =174413,86 /(1+0,18)^1+610850,61 /(1+0,18)^2+1133579,7 /(1+0,18)^3= = 1228604,65 грн.

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \qquad (4.22)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 189200,28 грн.

$$PV = k_{інв} \cdot ЗВ = 2 \cdot 189200,28 = 378400,55 \text{ грн.}$$

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \qquad (4.23)$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 1228604,65 грн;

PV – теперішня вартість початкових інвестицій, 378400,55 грн.

$E_{абс} = ПП - PV$ = 1228604,65 - 378400,55 = 850204,09 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \qquad (4.24)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$T_{ж}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 3 роки.

$$E_{в} = \sqrt[Tж]{1+\frac{E_{абс}}{PV}} - 1 = (1+850204{,}09\ /378400{,}55)^{1/3} - 1 = 0{,}76.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \qquad (4.25)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,1;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,25.

$\tau_{мін}$ = 0,1+0,25 = 0,35 < 0,76 свідчить про те, що внутрішня економічна дохідність інвестицій $E_{в}$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Інформаційна технологія онтологічного моделювання бази знань з організації бібліотеки» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_{в}}, \qquad (4.26)$$

де $E_{в}$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,76 = 1,3 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже, згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей» становить 40 балів, що, свідчить про комерційну важливість проведення даних досліджень оскільки рівень комерційного потенціалу розробки високий.

При оцінюванні рівня конкурентоспроможності, згідно узагальненого коефіцієнту конкурентоспроможності розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 4,4 рази.

Також термін окупності становить 1,3роки, що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже, можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Методу підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей».

ВИСНОВКИ

В МКР представлено розробку підходів збільшення рівня інформаційної безпеки систем контролю доступу на базі пристроїв IoT шляхом впровадження вдосконаленого методу і моделі підвищення рівня інформаційної безпеки в ІС СКУД. Це в сукупності дозволяє підвищити захищеність функціонування всієї ІС та/або ІКС підприємства і його бізнес-процесів.

Запропоновані в роботі окремі підходи, метод та модель передбачають вдосконалення вже існуючих принципів безпеки в ІС шляхом використання підходів мультифакторної ідентифікації та/або аутентифікації за декількома (багатьма) параметрами. Зокрема передбачається гнучка стадія вибору кількості параметрів та додаткові етапи захисту даних та вибір і обробку самих параметрів ідентифікації у вигляді унікального «цифрового зліпка» на базі Геш-функції, що може унікально ідентифікувати суб'єкт доступу. Це у сукупності із іншими підходами дозволяє підвищити рівень захисту інформаційної системи комплексу контролю доступу ІС СКУД на основі пристроїв Інтернету речей. Представлені в МКР рішення є частково новими і передбачають вдосконалення існуючих підходів та використання їх у сукупності із іншими для досягнення мети.

Зокрема було удосконалено метод і модель захисту, що дозволяє краще захищати інформацію в ІС СКУД та при передаванні в інтерфейсах та каналах ІС СКУД, дозволяє передавати цифрові сигнали із вищою захищеністю та стабільністю .

В процесі роботи була модифікована математична модель роботи і оцінки впливу загроз, яка дозволяє більш точно враховувати параметри ідентифікації суб'єкту.

Розглянуто і модифіковано структуру і модель інформаційної системи ІС СКУД та інтерфейсів передачі даних, які виконують функції захисту і формування інформаційних подій в СКУД. Розроблені структури ІС СКУД дозволяють компенсувати вплив негативних складових кіберзагроз, проводити їх оцінку для підвищення рівня захисту даних в СКУД.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357с.

2. Маліновський В.І. Засіб захисту функціоналу і безпеки від несанкціонованого доступу і модифікації в пристроях Інтернету речей (IoT) // Маковійчук І.О., В.І. Маліновський // Матеріали L науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2021) : збірник доповідей. – Вінниця : ВНТУ, 2021. – ВНТУ: [Електронний ресурс]. – Режим доступу: URL: https://conferences.vntu.edu.ua/public/files/1/vntu_2021_netpub.pdf (Дата звернення 20.11.2023р.).

3. Маліновський В.І. Мінімізація факторів кіберзагроз і спеціалізовані підходи до інформаційного захисту мікропроцесорних систем індустріального Інтернету речей / В.І. Маліновський // Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп`ютерної інженерії. Факультет інформаційних технологій та комп`ютерної інженерії(ФІТКІ). –2022. 31.05.2022. – ВНТУ: [Електронний ресурс]. –: URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000 (Дата звернення 20.11.2023р.)

4. U-Prox – СКУД: [Електронний ресурс]: - Режим доступу URL:https://ott.net.ua/ua/systema-kontrolya-i-upravleniya-dostupom-u-prox (Дата звернення 20.11.2023р.)

5. Маліновський В.І. Аналіз ризиків кіберзагроз і захист даних в сучасних системах Інтернету речей (IoT) / В.І. Маліновський // Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії. Факультет інформаційних технологій та комп'ютерної інженерії(ФІТКІ). – 2022. 31.05.2022. – ВНТУ: [Електронний ресурс]. – Режим доступу: URL:https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki2022/paper/view/14999. (Дата звернення 20.11.2023р.).

6. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М.

В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.

7. Коробейнікова Т.І., Захарченко С.М. Технології захисту локальних мереж на основі обладнання CISCO. Львів : Вид-во Львів. політехніки, 2021. – 232 с.

8. Schiffman M., Rauch J. Modern Network Infrastructure Security. Pearson Education, Limited, 2020. –656 p.

9. Маліновський В.І. Аналіз загроз безпеки мікроконтролерів / В.І. Маліновський, Л.М. Куперштейн. // Інформаційні технології та компютерна інженерія. - 2022. - Вінниця: Універсум-Вінниця, ВНТУ – N3(55). – С. 21-32.

10. В. Шуклін. Математичне моделювання керування процесами інформаційної безпеки в системі державного регулювання кібернетичною безпекою фондового ринку / Г. В. Шуклін, О. В. Барабаш // *Системи управління, навігації та зв'язку. – 2018. – випуск №4(50). –СС.91-94. – ISSN 2073-7394.* – doi: 10.26906/SUNZ.2018.4.091 (Дата звернення 20.11.2023р.).

11. Маліновський В.І. Аналіз основних інформаційних загроз і впливів у сучасних мікроконтролерних системах / В.І. Маліновський, Л.М. Куперштейн, В.А. Каплун // "Оптико-електронні інфомраційно енергетичні технології . –№2 – 2022 –. С.23.-32.

12. Маліновський В.І. Підходи підвищення інформаційного захисту даних в каналах мережах IoT / В. І. Маліновський, Л.М. Куперштейн, В.І.Лукцічев - к.т.н., доц., Л. М. Куперштейн. – Збірник матеріалів Міжнародної Інтернет-конференції. – “Світ наукових досліджень." (випуск 20)"- 20-21 червня 2023. [Електронний ресурс]. – Режим доступу: URL: http://www.konferenciaonline.org.ua/ua/article/id-595/

13. В. І. Маліновський Моделі і принципи захисту інформаційних даних в системах безпеки пристроїв Інтернету речей //В. І. Маліновський, А.О. Димов, Д. А. Василевський – Збірник матеріалів Міжнародної Інтернет-конференції. “Світ наукових досліджень." (випуск 25)"- 14-15 грудня червня 2023. [Електронний ресурс]. – Режим доступу: URL: http://www.konferenciaonline.org.ua/ua/article/id-...

14. Маліновський В.І. Аналіз надійності функціонування сучасних пристроїв

і систем інтернету речей / Матеріали науково-технічної конференції «II International Scientific and Practical Conference “Modern research in World Science” : [Електронний ресурс]. – Режим доступу: URL: https://sci-conf.com.ua/wpcontent/uploads/2022/06/modern-research-in-world-science-12-14.06.22.pdf

15. Маліновський В.І. Сучасні кіберзагрози і захист даних в системах і пристроях Інтернету речей / Матеріали Міжнародної наукової Інтернет-конференції"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 69)"- 4-5 липня 2022. [Електронний ресурс]. – Режим доступу: URL: http://www.konferenciaonline.org.ua/ua/article/id-595/OM /

16. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах// А.В. Жилін, О. М. Шаповал, О. А. Успенський. Київ : «Політехніка», 2021. 213 с.

17. Бондарчук В.К., Куперштейн Л.М. Аналіз загроз та вразливостей веб-додатків Матеріали XLIX науково-технічної конференції підрозділів ВНТУ, Вінниця, 27-28 квітня 2020 р. / / В.К Бондарчук, Л.М Куперштейн :[Електронний ресурс]. – Режим доступу:
URL:: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29544/9265.pdf?sequence=3&isAllowed=y

18. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

19. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України. 2020. –256 с.

20. Закон України «Про інформацію» : *за станом на 1 січня 2019 р.* / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

21. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : *за станом на 1 січня 2019 р.* / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-

bin/laws/main.cgi?nreg=80%2F94-%E2%F0

22. ISO/IEC FIDIS 27005:2008, «Information technology — Security techniques-Information security risk management» ISO/IEC FIDIS 27005:2008

23. Kakareka, Almantas У. Vacca, John. *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. 2009. – p. 393. ISBN 978-0-12-374354-1.

24. Алексейчук І.С. Про технологію створення системи тестування / І.С. Алексейчук // Нові технології навчання: Науково-методичний збірник.

25. Кріспін Л. Гнучке тестування: практична інструкція : пер. з англ. / Л. Кріспін., Д. Грегорі – М.: «Вільямс [Електронний ресурс]. — Режим доступу: http://eprints.cdu.edu.ua/1482/1/testyvan.pdf .

26. What is REST? [Електронний ресурс]. — Режим доступу: http://www.restapitutorial.com/lessons/whatisrest.html. (дата звернення: 16.04.2023).

27. Markus Egger — MVVM Survival Guide for Enterprise Architectures in Silverlight and WPF [Електронний ресурс]. — Режим доступу: https://www.packtpub.com/application-development/mvvm-survival-guide enterprisearchitectures-silverlight-and-wpf. Martin Fowler — GUI Architectures. Часть 1 [Електронний ресурс]. — Режим доступу: https://bit.ly/2CvCk1e. (дата звернення: 09.05.2023).

28. Скотт Хокінс. Адміністрування веб-сервера Apache і керівництво по електронній комерції. [Електронний ресурс]. — Режим доступу https://muff.kiev.ua/files/books/Administririvanie.web-servera.Apache.pdf MySQL. Довідник. MySQL AB. — М: «Вільямс» (дата звернення: 28.05.2023).

29. Тестування програмного забезпечення [Електронний ресурс] – Режим доступу: https://kiev.lemon.school/uk/blog/osnovy-qa .

30. Маліновський В.І. Аналіз ризиків кіберзагроз і захист даних в сучасних системах Інтернету речей (IoT) / В.І. Маліновський // Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп'ютерної

інженерії. Факультет інформаційних технологій та комп'ютерної інженерії(ФІТКІ). – 2022. 31.05.2022. – ВНТУ: [Електронний ресурс]. – Режим доступу: URL:https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/14999.

31. Diogenes Y. Cybersecurity: strategies of attack and defense / Y. Diogenes, E. Ozkay. — M.: DMK Press, 2020. — 326 p.

32. Cory Beard, William Stallings Wireless Communication Networks and Systems. - Pearson Education, 2015. – 672 p.

ДОДАТКИ

84

ДОДАТОК А
ПРОТОКОЛ ПЕРЕВІРКИ
МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Метод підвищення рівня захисту системи контролю доступу на основі пристроїв Інтернету речей

Автор роботи: Василевський Денис Анатолійович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 88,8 %. Схожість – 11,2 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Денис Василевський
(підпис)

Керівник роботи _____ Вадим Маліновський
(підпис)

ДОДАТОК Б
Програмна реалізація моделі багатопараметричної ідентифікації в ІС СКУД

```
import java.util.Scanner;

public class DynamicIdentificationSystem {

    public static void main(String[] args) {
        int x = promptForX();
            int dotAfunctuion = promptFunctionrX();
        int numberOfParameters = calculateNumberOfParameters(x);
        String[] parameters = new String[numberOfParameters];

        for (int i = 0; i < numberOfParameters; i++) {
            parameters[i] = promptForParameter("Параметр " + (i + 1));
        }

        if (isValidParameters(parameters)) {
            System.out.println("Ідентифікація пройшла успішно.");
        } else {
            System.out.println("Ідентифікація не вдалася.");
        }
    }

    private static int promptForX() {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Введіть значення x: ");
        return scanner.nextInt();
    }

    private static int calculateNumberOfParameters(int x) {
        return x*N*dotAfunctuion;
    }

    private static String promptForParameter(String parameterName) {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Введіть " + parameterName + ": ");
        return scanner.nextLine();
    }

    private static boolean isValidParameters(String[] parameters) {
        return true;
    }
}
public class promptFunctionrX() {
SecurityLevelParameters = new SecurityLevelParameters;
```

```
System.out.print("Введіть значення параметрів безпеки: ");
SecurityLevelParameters[i] = promptForParameter("Параметри безпеки " + (i + 1));
promptFunctionrX() = new promptFunctionrX() ;
          promptFunctionrX() = 2;
if (isValidSecurityLevelParameters(SecurityLeveparameters)) {
if (isNotValidParameters(parameters)) {

for (int x = 0; i < SecurityLevelParameters; i++) {
          SecurityLevelParameters[i] = promptForSecurityLevelParameters("Параметр БЕЗПЕКИ " + (i
+ 1));

          System.out.println("Підвищення кількості параметрів безпеки при незадовільному рівні
безпеки при автоВизначення кількості параметрів ідентифікації.");
       } else {
          System.out.println("Кількість параметрів ідентифікації підвищилась.");
       }
    }

 }
public class DynamicIdentificationSystem {

    public static void main(String[] args) {
       int x = promptForX();
       int numberOfParameters = calculateNumberOfParameters(x);
       String[] parameters = new String[numberOfParameters];

       for (int i = 0; i < numberOfParameters; i++) {
          parameters[i] = promptForParameter("Параметр " + (i + 1));
       }

       if (isValidParameters(parameters)) {
          System.out.println("Ідентифікація пройшла успішно.");
       } else {
          System.out.println("Ідентифікація не вдалася.");
       }
    }

    private static int promptForX() {
       Scanner scanner = new Scanner(System.in);
       System.out.print("Введіть значення x: ");
       return scanner.nextInt();
    }

    private static int calculateNumberOfParameters(int x) {
       return x * 2;
}

    private static String promptForParameter(String parameterName) {
```

```
        Scanner scanner = new Scanner(System.in);
        System.out.print("Введіть " + parameterName + ": ");
        return scanner.nextLine();
    }

    private static boolean isValidParameters(String[] parameters) {
        return true;
    }
}


import java.util.Scanner;

public class IdentificationSystem {

    public static void main(String[] args) {
        int numberOfParameters = promptForNumberOfParameters();
        String[] parameters = new String[numberOfParameters];

        for (int i = 0; i < numberOfParameters; i++) {
            parameters[i] = promptForParameter("Параметр " + (i + 1));
        }


        if (isValidParameters(parameters)) {
            System.out.println("Ідентифікація пройшла успішно.");
        } else {
            System.out.println("Ідентифікація не вдалася.");
        }
    }

    private static int promptForNumberOfParameters() {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Введіть кількість параметрів N: ");
        return scanner.nextInt();
    }

    private static String promptForParameter(String parameterName) {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Введіть " + parameterName + ": ");
        return scanner.nextLine();
    }

    private static boolean isValidParameters(String[] parameters) {
        return true;
    }
}
```

ДОДАТОК В

Розробка удосконалених алгоритмів функціонування ІС СКУД для захисту даних

На основі аналізу був розроблений і систематизований основний та вдосконалений алгоритми функціонування ІС СКУД із підвищено.ю стабільність: рис.Г.1, рис.Г2

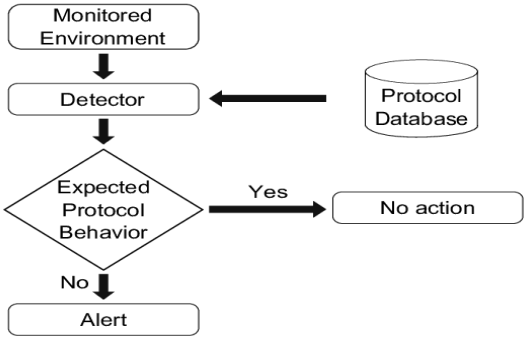


Рисунок Г.1 – Базовий алгоритм роботи СКУД

Згідно моделі комплексного інформаційного захисту ІС СКУД (рис.3.2 –рис. 3.11, див. розділ 3 МКР)на базі окремих структур і комплексних підходів передбачає використання покращених структур захищеної інформаційної мережі ІС СКУД із підвищеним рівнем захисту і запровадженням підходів і методів додаткового захисту із контролем цілісності. Сам алгоритм роботи системи безпеки ІС СКУД на базі вдосконаленого етоду і моделі покаханий на рис. Г.2.

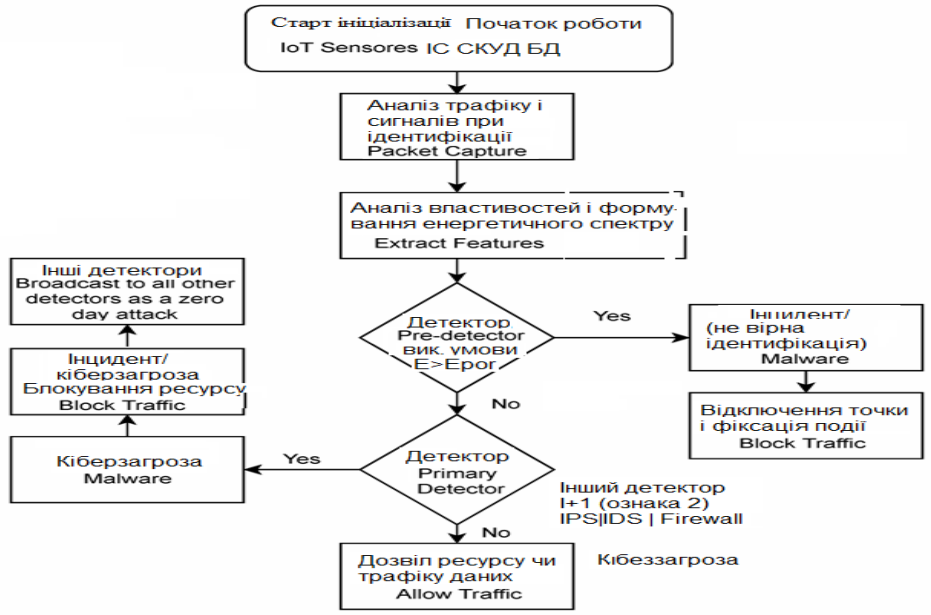
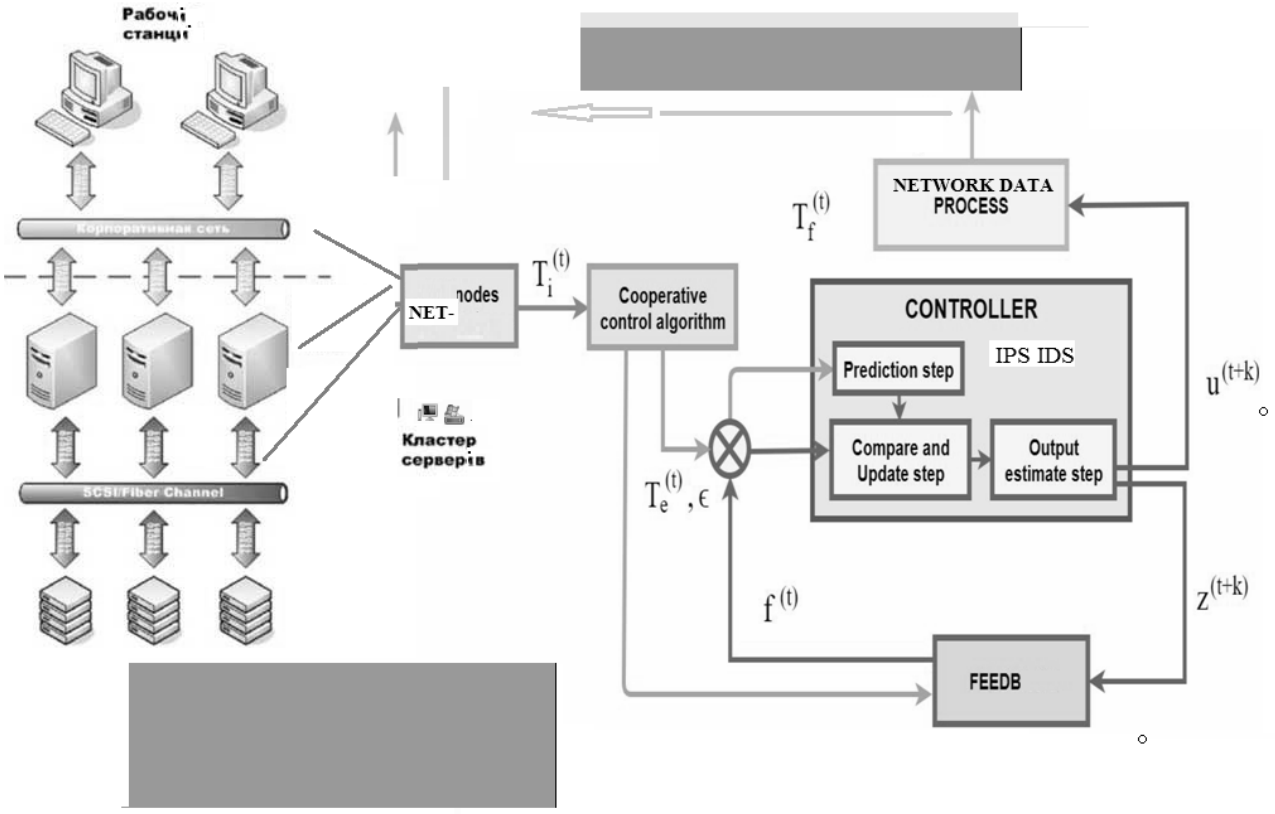


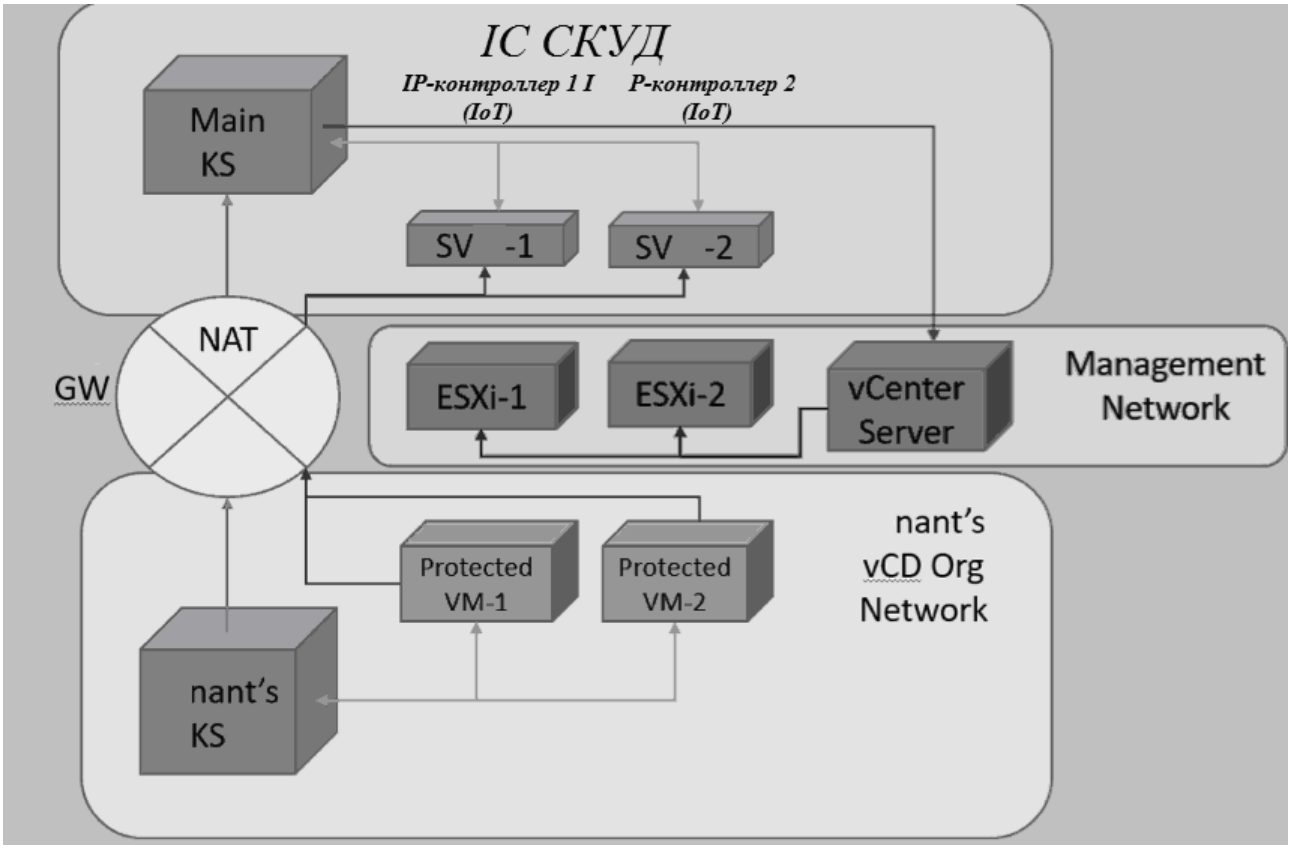
Рисунок Г.2 – Алгоритм роботи ІС СКУД із варахування додаткового захисту

ПЕРЕЛІК ІЛЮСТРАТИВНОГО МАТЕРІАЛУ

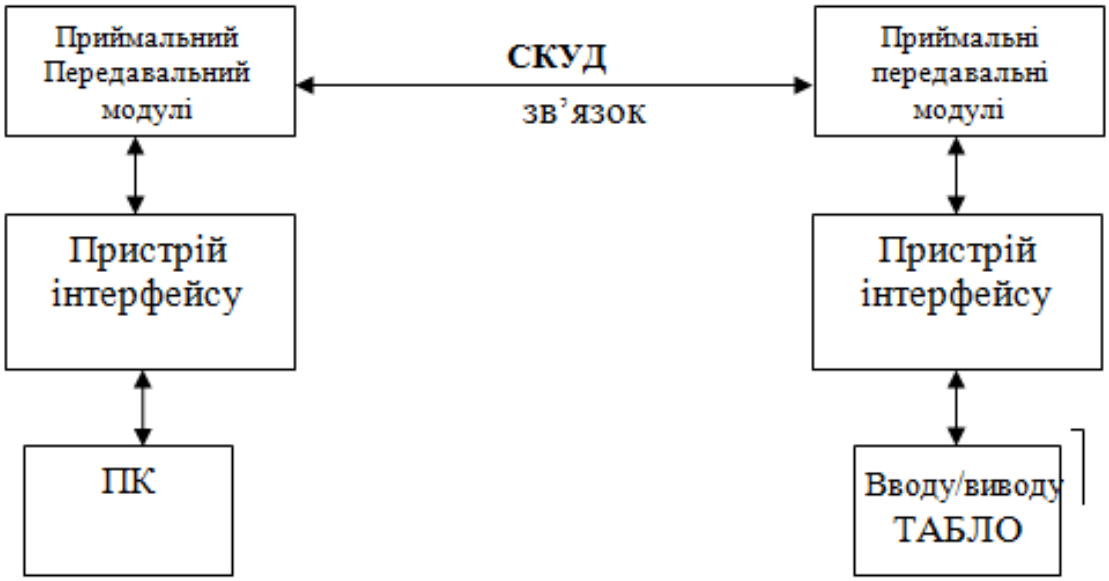
МОДЕЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ БЕЗПЕКИ IP-КОНТРОЛЕРА В СКУД



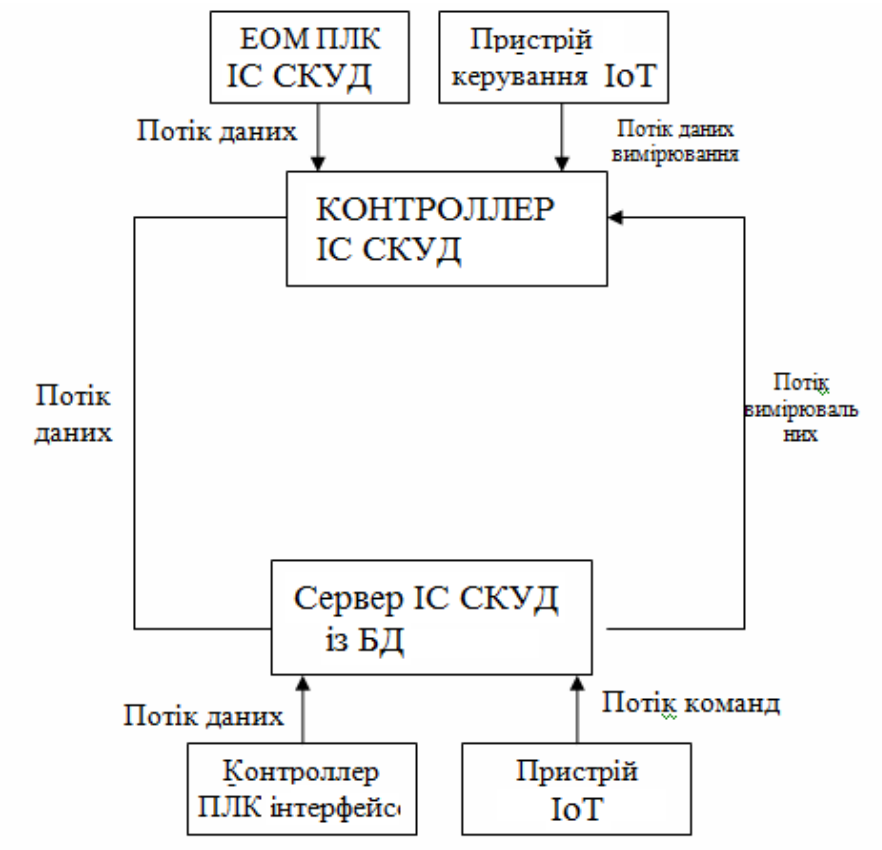
МЕРЕЖЕВА МОДЕЛЬ РОБОТИ ІС СКУД НА ОСНОВІ ВДОСКОНАЛЕНОГО МЕТОДУ



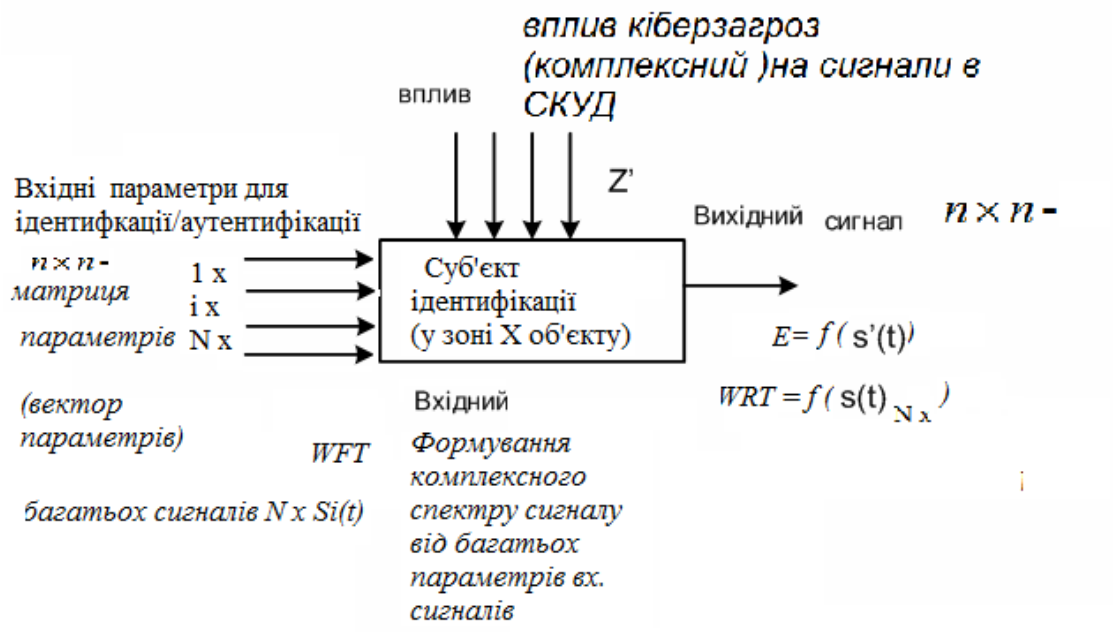
СТРУКТУРНА СХЕМА ІНТЕРФЕЙСУ ІС СКУД



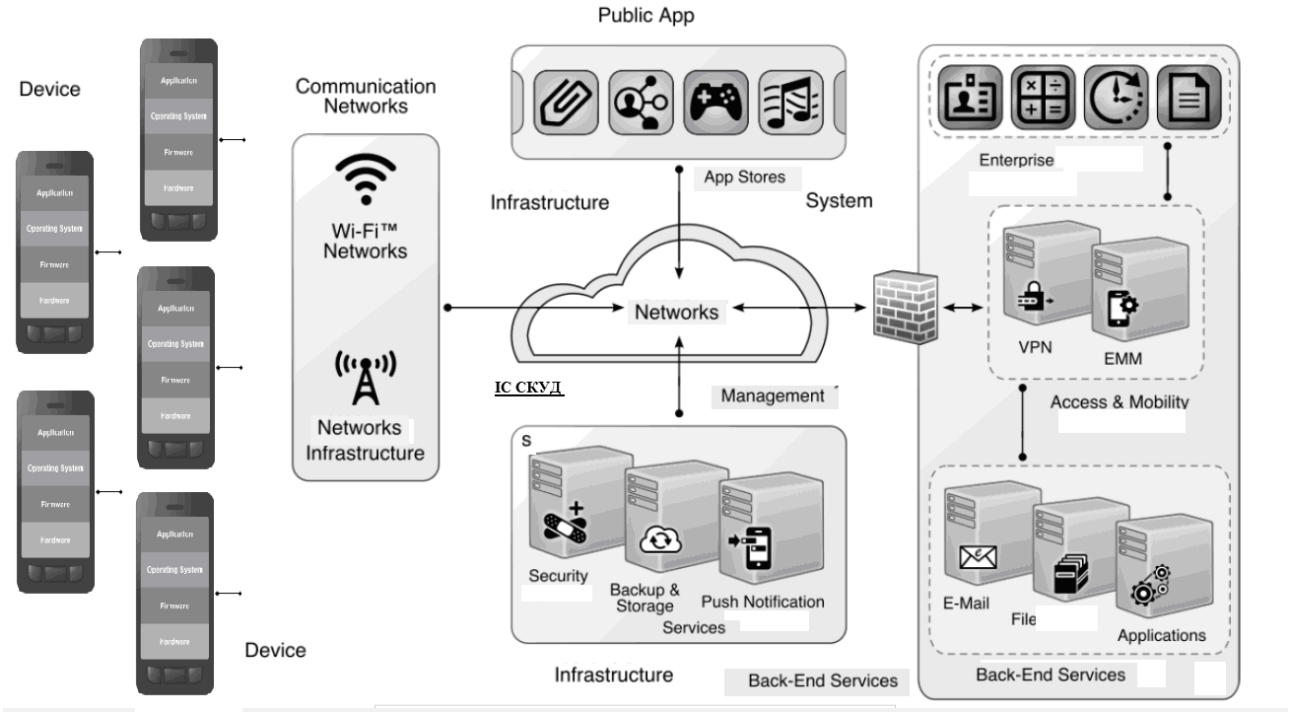
СТРУКТУРНА СХЕМА СИСТЕМИ ІС СКУД ІЗ ІР-КОНТРОЛЕРОМ



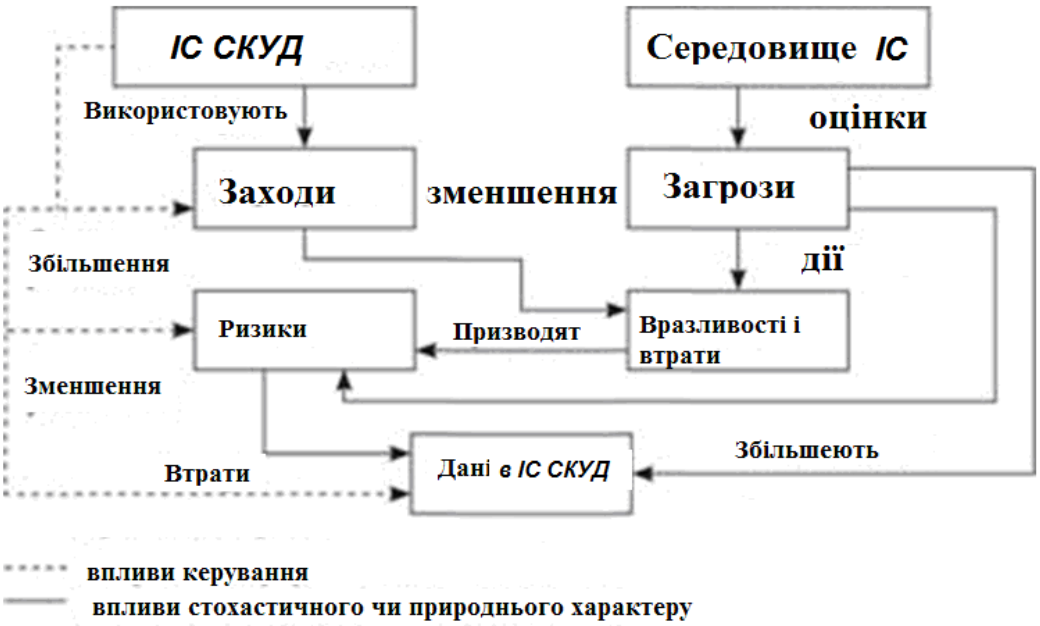
МОДЕЛЬ БЕЗПЕКИ ІС СКУД, ЩО ІЛЮСТРУЄ ПРИНЦИП БАГАТОПАРАМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ПО ПАРАМЕТРАМ



СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ СКУД ІЗ 2-Х РІВНЕВИМ КІБЕРЗАХИСТОМ, ІЗ І ІОТ ПРИЛАДАМИ



МОДЕЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАХИСТУ СКУД



ІЛЮСТРАЦІЯ МЕТОДУ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ СКУД