Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська кваліфікаційна робота на тему:
«Захищена система відеоспостереження для закладів охорони здоров'я»

Виконав: студент 4курсу групи 1БС-21б
спеціальності 125 Кібербезпека
_____ В'ячеслав ДЕЙБУК
Керівник: к. т. н., доцент каф. ЗІ
_____ Вадим МАЛІНОВСЬКИЙ
«17» червня 2025 р.
Рецензент: к. т. н. доцент каф. ПЗ
_____ Галина ЧЕРНОВОЛИК
«17» червня 2025 р.

Допущено до захисту
Завідувач кафедри ЗІ д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«17» червня 2025 р.

Вінниця ВНТУ – 2025 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти 1 (бакалаврський)
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
«21» березня 2025 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Дейбуку В'ячеславу Олександровичу

1. Тема роботи: «Захищена система відеоспостереження для закладів охорони здоров'я», керівник роботи: Маліновський Вадим Ігоревич, к.т.н., доцент кафедри ЗІ, затверджена наказом вищого навчального закладу від 20 березня 2025 р. №97.

2. Строк подання студентом роботи 17 червня 2025.

3. Вихідні дані до роботи: тип системи відеоспостереження – захищена; Вихідні дані до роботи: тип системи відеоспостереження – захищена; протоколи відеоспостереження: RTSP; OnVif; IP; IPSec; UDP; система має відповідати вимогам і стандартам систем і приладів для СВС та для медичних установ; тип топології мережі СВС: універсальна деревоподібна; тип шифрування у каналах СВС: AES 128/256; можливість інтеграції із іншими інформаційними мережами і Інтернет – так; тип архітектури ПЗ СВС: клієнт-серверна, розподілена.

Зміст текстової частини: вступ; 1. Аналітичний огляд технологій кіберзахисту для систем відеоспостереження у секторі охорони здоров'я; 2. Розробка структур захищеної СВС для сектору охорони здоров'я; 3. Структурна і алгоритмічна організація СВС для сектору охорони здоров'я; 4. Програмна реалізація засобів моніторингу у системах відеоспостереження для сектору охорони здоров'я. висновки; список використаних джерел; додатки.

4. Перелік ілюстративного матеріалу: 1.)Загальна структурна схема захищеної СВС; 2.) Структура СВС із мережевими екранами; 3.) Структурна схема СВС із системою камер; 3.) Схема застосування технологій захисту у СВС; 4.) Блок-схеми алгоритмів роботи засобу визначення кібератак та кіберзахисту у СВС; 5.)Засоби кіберзахисту і визначення кібератак у структурі СВС; 6.)Розроблена структурна модель кіберзахисту СВС для сектору охорони здоров'я; 7.)Результати роботи ПЗ модуля моніторингу стану камер СВС.

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Маліновський В.І. к.т.н., доцент каф. ЗІ	24.05.25	10.06.25
2	Маліновський В.І. к.т.н., доцент каф. ЗІ	26.05.25	10.06.25
3	Маліновський В.І. к.т.н., доцент каф. ЗІ	22.05.25	10.06.25
4	Маліновський В.І. к.т.н., доцент каф. ЗІ	28.05.25	10.06.25

6. Дата видачі завдання 21 березня 2025 р.

7. **КАЛЕНДАРНИЙ ПЛАН**

	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз методів кіберзахисту СВС для медичного сектору	24.03.25 – 30.03.25	Вик.
2	Розробка структури та алгоритмів роботи захищеної системи відеоспостереження	31.03.25 – 13.04.25	Вик.
3	Розробка основних модулів програмного застосунку для моніторингу процесів СВС	31.04.25 – 16.05.25	Вик.
4	Тестування роботи ПЗ і СВС	14.04.25 – 04.05.25	Вик.
5	Аналіз виконання БКР, висновки	05.05.25– 14.05.25	Вик.
6	Оформлення пояснювальної записки	19.0525- 26.05.25	Вик.
7	Попередній захист БКР	27.0525- 30.05.25	Вик.
8	Виправлення зауважень, перевірка на плагіат, підготовка ілюстративної частини	31.0525- 10.06.25	Вик.
9	Представлення БКР до захисту	11.06.25- 17.06.25	Вик.

Студент _____ В’ячеслав ДЕЙБУК

Керівник роботи _____ Вадим МАЛІНОВСЬКИЙ

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота складається з 61 сторінок формату А4, на яких є 16 рисунків, 11 таблиць, список використаних джерел містить 30 найменування.

Бакалаврська кваліфікаційна робота присвячена розробці захищеної системи відеоспостереження для медичних закладів, в яких потрібна висока інформаційна захищеність і конфіденційність відеоканалів та суміжних інформаційних систем обробки даних. В роботі представлена система, що базується на передових та дієвих технологіях захисту інформації, містить засіб моніторингу і виявлення кібератак на системи відеоспостереження, та дозволяє підвищити загальний рівень кібербезпеки систем відеоспостереження в закладах охорони здоров’я. У сучасному кіберпросторі і в умовах значних загроз інформаційної та кібербезпеки, стає критично важливим стійкий і високий захист систем відеоспостереження в різноманітних місцях. В роботі запропоновано модель і структуру захищеної системи відеоспостереження, що має високий рівень захисту і стійкості до атак та зовнішніх факторів впливу та може запобігти втратам і порушенням захищеності і конфіденційних критичних даних та запобігти несанкціонованого доступу до приватної інформації в закладах охорони здоров'я .

Ключові слова: кібербезпека, відеоспостереження, система відеонагляду (СВН), система відеоспостереження (СВС), кібератаки, кіберзахист, мережевий трафік, системи відео спостереження (СВС), системи відео нагляду(СВН), відмова в обслуговуванні (Denial of Service, DoS), несанкціонований доступ (НСД), моніторинг, трафік даних, відеопотік.

ABSTRACT

The bachelor's thesis consists of 61 pages of A4 format, on which there are 16 figures, 11 tables, the list of used sources contains 30 names.

The bachelor's thesis is devoted to the development of a secure video surveillance system for medical institutions, which require high information security and confidentiality of video channels and related information data processing systems. The work presents a system based on advanced and effective information protection technologies, contains a means of monitoring and detecting cyber attacks on video surveillance systems, and allows you to increase the overall level of cybersecurity of video surveillance systems in healthcare institutions. In modern cyberspace and in conditions of significant information and cyber threats, stable and high protection of video surveillance systems in various locations becomes critically important. The work proposes a model and structure of a secure video surveillance system that has a high level of protection and resistance to attacks and external factors of influence and can prevent losses and violations of security and confidential critical data and prevent unauthorized access to private information in healthcare institutions.

Keywords: cybersecurity, video surveillance, video surveillance system (VSS), video surveillance system (VSS), cyberattacks, cyberdefense, network traffic, video surveillance systems (VSS), video surveillance systems (VSS), denial of service (Denial of Service, DoS), unauthorized access (UNA), monitoring, data traffic, video stream.

ЗМІСТ

ВСТУП

У сучасних комерційних та державних установах системи відеоспостереження (СВС) мають велике значення і відіграють важливу роль для контролю стану безпеки та ситуації. Сучасні СВС забезпечують безпеку і моніторингу обстановки у секторі охорони здоров'я шляхом контролю ситуації із множини відеокамер: як всередині закладу, так і поза його межами. Вони встановлюються в офісах, в коридорах, медичних палатах, інших частиназх будівлі підприємства, а також у громадських місцях і на вулиці, підвищуючи рівень контролю [1]. Проте, разом із зростанням використання таких систем, збільшується і кількість кібератак на них [1-2], а також випадків їх компрометації, взламів, несанкціонованого використання інформації із них [3]. Існуючі вразливості та недосконалості у налаштуваннях цих систем, а також людський фактор і не врахування багатьох особливостей використання систем відеоспостереження в лікарнях роблять їх привабливими і доступними цілями для зловмисників і стороннііх осіб. Це може призвести до серйозних наслідків, таких як вторгнення в приватне життя, використання закритої медичної інформації, крадіжка конфіденційної інформації про пацієнтів, а також порушення громадського порядку, втручання в критичну інфраструктуру, до якої належать багато закладів охорони здоров'я.

Відомі випадки числених кібератак із використанням вразливостей СВС, таких як Botnet "Miraij"(із використанням частини камер СВН), взлам і НСД камер відеоспостередення в лікарнях, числені DDoS-атаки; експлуатація вразливостий в IP-камерах Dahua, Nest [2-6], та інших, які дозволяють несанкціонований доступ із зчитуванням відеопотоків, керування IP-камерами; прямий взлам камер СВС. Це створює загрозу вторгнення в приватне життя і процеси в медичному секторі; а також спряє використанню шкідливого програмного забезпечення, орієнтованого на системи СВС (наприклад, DarkComet RAT; IP Controll), що дозволяє віддалений контроль [2-7].

Дана робота є актуальною через збільшення числа кібератак на системи відеоспостереження в лікарнях в умовах розвитку цифрових технологій, діджіталізації та розвитку сучасного IT-сектору, а також в умовах значних інформаційних протистоянь. Передбачається впровадження надійних засобів кіберзахисту для забезпечення кібербезпеки СВС на базі довіри до джерел даних та принципів комплексного захисту інформації в СВС, що є важливим аспектом у сучасному секторі охорони здоров'я, який відноситься до критичної інфраструктури [5-10].

Метою бакалаврської кваліфікаційної роботи є підвищення рівня безпеки систем відеоспостереження для закладів охорони здоров'я .

Для досягнення мети планується розробити універсальну структуру, алгоритм та моделі і оцінки захисту системи відеоспостередення. Використання цих підходів дозволить захистити відеодані в системі СВС для сектору охорони здоров’я. Планується провести детальний аналіз існуючих кіберзагроз і типів втручань у СВС, їх оцінку, вивчення для ефективного захисту СВС у закладах охорони здоров’я. В результаті очікується створення універсальної захищеної структури СВС і алгоритму захисту СВС від кіребезагроз, що буде базуватись на багатьох підходах кіберзахисту. Це дозволить вчасно виявляти, попереджати і організовувати захист від можливих кібератак і вторгнень в секторі охорони здоров'я. Також це дозволить зменшити ймовірність кібератак та підвищити рівень кібербезпеки СВС при їх використанні.

Об’єктом бакалаврської кваліфікаційної роботи є процес інформаційного та кіберзахисту даних у промислових системах відеоспостереження у закладах охорони здоров'я на основі сучасних практичних технологій і методів кіберзахисту.

Предметом бакалаврської кваліфікаційної роботи є структури, моделі та алгоритми кіберзахисту у системах відеоспостереження у секторі охорони здоров'я.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз сучасних технологій відеоспостереждення СВС та стану

їх захищеності для закладів охорони здоров'я, аналіз структур СВС та програмного забезпечення для моніторингу даних в промислових системах;

- провести аналіз стану кібербезпеки та вразливостей систем відеоспостереження в медичному секторі, проаналізувати основні протоколи СВС: RTSP, IP, SMTP, UDP, OnVif. Проаналізувати можливості їх адаптації їх до сучасних викликів кібербезпеки та стійкість до кібератак у системах СВС;
- розробити нову або вдосконалити універсальну структуру захищеної СВС та алгоритм і модель кіберзахисту системи відеосопстереднння на базі комплексу факторів. Визначити допустимі основні алгоритми і рекомендації кібербезпеки для захисту даних у промислових СВС в секторі охорони здоров'я;
- розробити та розрахувати основні рекомендації для захисту систем відеоспостереження на базі структури кіберзахисту СВС у сфері охорони здоров’я;
- здійснити програмну реалізацію засобу моніторингу і тестування станів IP-камер в складі СВС та провести розрахунки окремих модулів захищеної СВС.

За результатами бакалаврської кваліфікаційної роботи опубліковано тези доповідей на науково-технічну конференцію «Молодь у науці 2025», ВНТУ, 2025 на тему: «Проблеми побудови захищених систем відеоспостереження у медичних закладах» [11].

1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ КІБЕРЗАХИСТУ ДЛЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ У СЕКТОРІ ОХОРОНИ ЗДОРОВ'Я

1.1. Основні засади і технології функціонування систем відеоспостереження в сфері охорони здоров’я

Значний та стрімкий технологічний розвиток дозволив реалізувати на практиці IP-відеоспостереження, в якості однієї із головних технологій безпеки у сучасному світі [1-10]. IP системи СВС на базі технології CCTV [7, 10] часто позиціонуються на ринку не тільки як дієвий засіб отримання важливої інформації на об'єктах, але й як інструмент безпеки співробітників та клієнтів. Сучасні системи відеоспостереження збирають та зберігають багато різноманітної відеоінформації, тому часто самі часто стають мішенями для кібератак, а також джерелами витоків великої кількості даних.

Електронні пристрої IP-відеокамер здійснюють фото- відео- фіксацію із передачею мультимедіа трафіку і організовують інформаційний зв’язок через мережу LAN Ethternet (802.3) і Internet через транспортні магістралі передаючі дані у різних географічних місцях. Інформаційні технології СВС застосовуються із метою захисту і моніторингу ситуацій в різних місцях, охорони громадського порядку в різних закладах, моніторингу безпеки.

Якщо раніше системи відеоконтролю переважно впроваджувалися лише у спеціальних обєктах, то сьогодні такі технології широко використовуються в громадах, в різних закладах, в тому числі в лікарнях. IP-відеокамери інтегрують органи державної влади, корпоративний сектор, медичні установи та особи.

IP-камера відеоспостереження знімає відео у форматах NLAV, MPEG4, XVID, DVD і транслює відеопотік IP/RTCP [7-10] у цифровому форматі з використанням мережевого протоколу IP, який забезпечує комутацію і маршрутизацію пакетів даних. Сучасна IP-відеокамера СВС має ПЗЗ-

фотоматрицю, оптичний адаптивний об'єктив, процесор CPU, суміжний сигнальний процесор, електрону систему кодування і стиснення інформації, операційну систему та мережевий інтерфейс. Найпоширенішою є практика віддаленого доступу до камер відеоспостереження із відеосервера/відеореєстратора, як показано на рис.1.1.

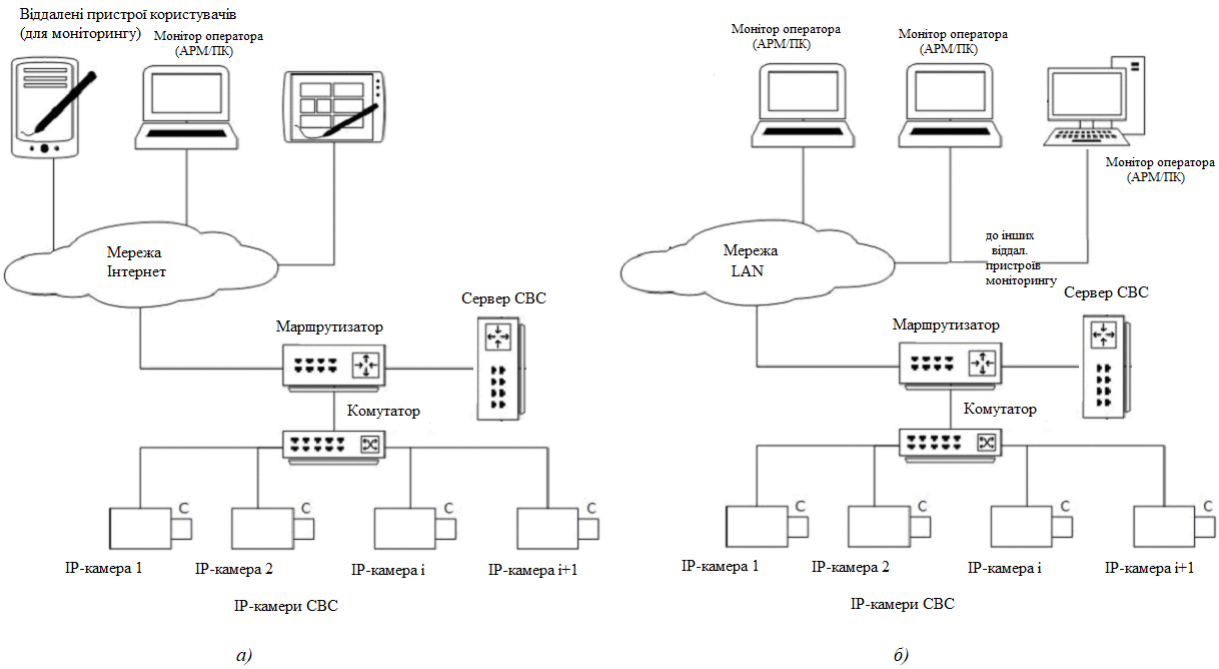


Рисунок 1.1 – Структура цифрової системи відеоспостереження [4, 6-9]:

а) географічно-віддалена WEB-система СВС— із доступом по Інтернет;

б) локальна закрита СВС — із доступом по локальній мережі LAN

За своїм функціональним призначенням і способом обробки інформації системи відеоспостереження поділяють на :

- СВС із записом і контролем у режимі реального часу, що транслює відеопотоки високої швидкості і якості із відеокамер у реальному часі.

- СВС із можливістю збереженням відеоінформації від камер із затримкою і фіксацією локальних окремих подій у певному місці та циклі. Такі СВС можуть накопичувати, зберігати відеодані протягом необхідного часу. Переваги цього методу роботи у тому, що відеофайлами можна управляти:

переглядати, редагувати, збільшувати зображення, робити уривки відео тощо. Системи 2-го типу застосовуються в установах із організацією охорони території та контролю стану і режиму роботи та робочого часу.

- Системи із застосуванням смарт-функцій і автоматизованого контролю (наприклад, за допомогою нейромереж, контролера, сервера чи ПЗ контролю високого рівня). Базовий принцип систем відеоспостереженян формування відео потоків від камер СВС (рис.1.2).

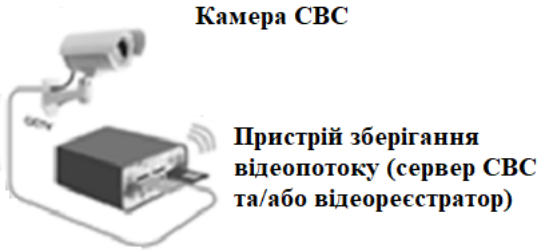


Рисунок 1.2 –Базова структура елементарної СВС на базі 1-ї відеокамери [3, 4]

Звісно структура (рис. 1.2) масштабується і пропорційно збільшється відповідно до кількості камер СВС. В реальних системах і в реальних умовах використовуються СВС на 32х, 64х, 128х і більше кількості каналів із відповідним числом камер відеоспостереження і підтримкою такої ж кількості каналів на сервері СВС.

1.2 Аналіз проблем безпеки в системах відеоспостереження

Із точки зору безпеки СВС бувають: із зовнішнім WEB-доступом; закриті локальній системи із доступом по LAN (локальній ЛВС); комбіновані закриті, що працюють у закритій локальній мережі, але мають доступ і контрольований доступ до Інтернет чи іншими інформаційними мережами через один або два інтерфейси.

Із точки зору кібербезпеки, найбільш захищені - це СВС 2-го типу, оскільки є ізольованими і сегментованими. Існує ще й 3-й тип систем є порівняно захищеним, але меньш від 2-го, оскільки має виходи і зв'язки із іншими мережами (в т.ч. Інтернет), які контролюються. Хоча і контрольовані, але існуючі зв'язки створюють ризики кібератак і мережевого несанкціннованого доступу до

елементів СВС в закритому периметрі. 1-й тип СВС - це самий незахищений і сильно підвержений впливу кібератакам і НСД із боку зловмисників. Саме такий тип часто використовується в сучасних лікарнях (рис.1.3).

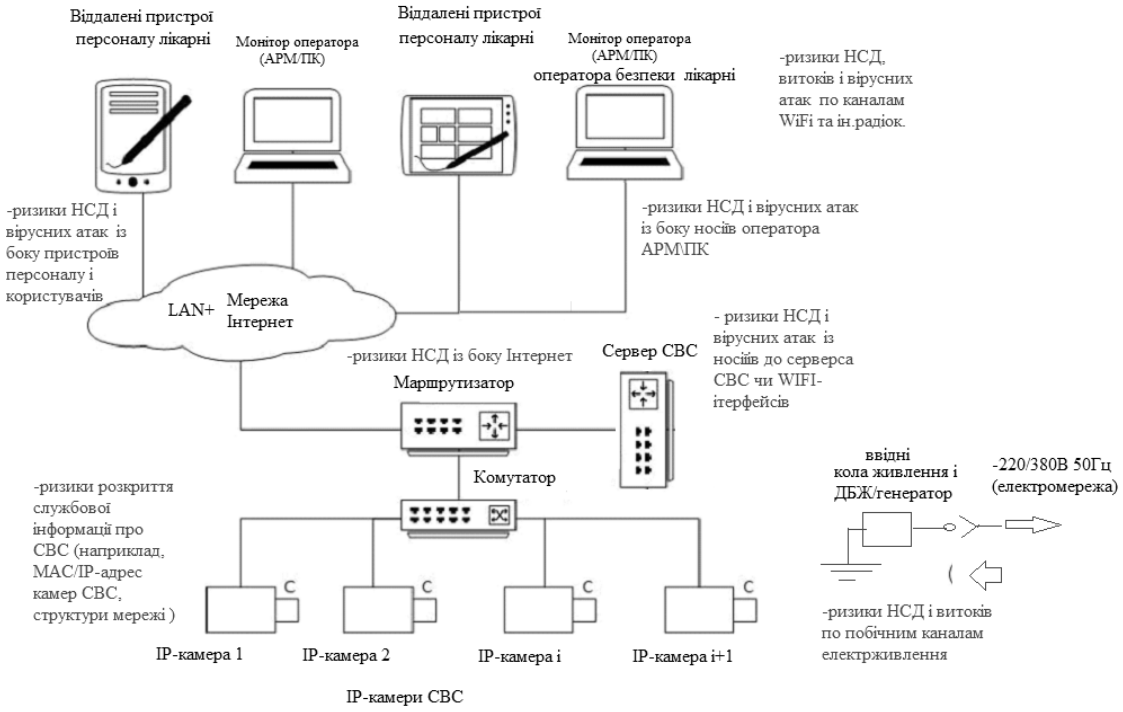


Рисунок 1.3 – Іллюстрація структури СВС незахищеного типу

Аналізуючи незахищені структури СВС (рис.1.3), можна побачити, що є ряд кіберзагроз із можливістю втрати даних, несанкціонованого доступу (НСД) до СВС і витоків даних через різні канали (в т.ч. побічні) в СВС. Як показує проведений аналіз і практика, найбільші ризики складаюить наявні канали звязку із мережею Інтернет (відсоток кіберзагроз близько 70-80%).

Разом із тим, при сучасному програмному та апаратному оснащенні, вони здатні вирішувати завдання відеоспостереження більш широко і достатньо ефективнго. Потрібно тільки забезпечити їх надійну кібербезпеку і стабільність.

1.3 Аналіз методів організації надійного кіберзахисту СВС

Системи відеоспостереження на базі IP-камер стали невід'ємною частиною сучасної інфраструктури безпеки, яка використовується в різних

сферах на багатьох об'єктах від приватної до критичної інфраструктури [5-7]. Для забезпечення високого стану кібербезпеки і стабільного кіберзахисту СВС, необхідно мати умовне уявлення про ризики кібербезепки [6] і можливі кібератаки в них, а також мати мапу типових вразливостей (CWE) для СВС .

Основні ризики кіберзагроз в мережах СВС можуть бути використані для організації кібератак і шкідливих втручань в канали і саму СВС. На основі проведеного аналізу вони можуть бути представлені у табл. 1.1.

Під час установлення заходів і підходів безпеки і аналізу ризиків СВС (табл. 1.1) і камер для і цифрового відеореєстратора (відеосервера) необхідно зважати на той факт, що більшість ризиків є високими і цілком реальними в системах СВС і можуть практично втілитись на практиці та цілком проявитись у вигляді практичних атак, як на рівні апаратного так і програмного забезпечення. Це проявляється у вигляді зламів обладнаня СВС, НСД і виводу із ладу відеокамер, всієї системи СВС, отримання несанкціонованого доступу (НСД) до зображнь і налаштувань камер СВС і т.п.

Таблиця 1.1 – Аналіз ризиків кіберзагроз для СВС

Ризик	**Принцип і різновид**	**Опис**
Несанкціонований доступ до СВС	Прямий НСД до мережі СВС	Прямий доступ до СВС через відкриті доступні можливості мережі і архітектурні особливості
	Використання відкритих портів/сокетів	Використання доступу через відкриті ресурси і віртуальні логічні і фізичні порти локальних мереж СВС без ізоляції різнородного трафіку.
	Доступ по побічним каналам і BackDoor	Використання побічних каналів, бекдор (BackDoor) в ПЗ та апаратурі СВС, невірні конфігурації ПЗ і обладнання, що відкриває дистанційнийдоступ по основним і побічним каналам через BackDoor
Порушення автонтифікації	Автентифікація та авторизація пристроїв в мережі СВС	Використання порушення багатофакторної аутентифікації та управління доступом. Відсутність Oauth/2FA/MFA у поєднанні із TLS/SSL для шифрування трафіку.
Порушення безпека даних: кібердані та інформційні дані	Відсутність захисту і шифрування при зберіганні	Відсутність використання шифрування та інших методів захисту (наприклад контолю доступу і парольного доступу до консолі зберігання) для збереження відеоданих.
	Видалення, модифікування копіювання	Відсутність регулярного резервування даних.

Продовження таблиці 1.1.

Вірусні загрози	Дія ШПЗ та шкідливих скриптів та команд СВС із видаленням, модифік. копіювання	Відсутність захисту в системах СВС для виявлення і блокування шкідливої і підозрілої активності.
Організаційні загрози і заходи	Політики безпеки	Відсутність впровадження політик і адмін. правил кібербезпеки СВС.
	Навчання персоналу і людський фактор	Відсутність навчання персоналу і тренінгів для співробітників щодо кібербезпеки.
	Інформаційна безпека сервісної інформації	Незахищене поводження і обробка сервісної інформції СВС(наприклад, IP-адрес, портів, функцій, моделей обладнання, структури даних СВС). Відсутність розробка та тестування планів реагування на кіберінциденти.
Мережеві загрози та вразливості СВС	Доступ через канали мережі і WiFi канали Наявність включе-ного і невикористовуємого інформаційного функціоналу обладн.	Виконання незахищеного доступу до обладнання СВС із використанням вразливостей, незакритих каналів і радіокнаалів (наприклад, WiFi/ Ehternet). Відсутність мережевих екранів і контролю обладнання СВС і його трафіку даних. Відсутність належних налаштувань пристроїв
Фізична безпека пристроїв СВС	Відсутність контролю фіз. доступу до обладнання СВС	Відсутність належдного обмеження фізичного доступу до серверів і комутаційного обладн. Відсутність вандалостійких заходів
Вторинні фактори загроз	Відсутність тривалих ліцензій, підтримки, зап.частин, відстутн. стабільного енергозабезпечення і резервного живлення.	Відсутність підходів забезпечення стабільності і компенсації вторинних негативних ризиків. Використання в СВС у системі охорони здоровя недосконалого обладнання, неякісних компонентів та інше. (наприклад, відстуність зап.частин, відсутність вандалостікого і фізичного захисту компонентів СВС та мережі.

Тому серед мір безпеки повинні бути і заходи тестування таких систем в секторі охорони здоров'я, які дозволяють автоматично моніторити стан обладнання СВС і сканувати стан камер на предмет наявності уразливостей. Для забезпечення надійного та стабільного кіберзахисту систем відеоспостереження (СВС) в лікарнях України слід дотримуватися певних принципів, детально викладених у табл.1.2.

Таблиця 1.2 – Аналіз заходів і технологій кіберзахисту СВС у лікарнях

Категорія	Підхід і метод	Опис
Мережева безпека СВС	Сегментація і контроль мережі VLAN	Розділення мережі на сегменти для ізоляції різних видів трафіку. Використання віртуальних локальних мереж VLAN і ізольованих сегментів $VLAN_{SEC}$ для підмережі СВС
	Налаштування і зміна ппараметрів мережі	Використання динамічних параметрів і віртуалізації локальних мереж і VLAN. Використання ізоляції трафіку і сокетів від камер СВС. Використання ізольованих підходів
	Шифрування та зазхист даних	Використання TLS/SSL для шифрування трафіку між камерами та серверами.
Безпека пристроїв СВС	Автентифікація та авторизація	Використання багатофакторної автентифікації (Oauth/2FA/MFA) та управління доступом.
Безпека даних в СВС	Шифрування при зберіганні відеоданих	Шифрування для збереження відеоданих.
	Резервне копіювання	Регулярне створення резервних копій даних.
Моніторинг пристроїв СВС	Моніторинг у реальному часі	Використання систем IDS/IPS для виявлення підозрілої активності.
Організаційні заходи	Політики безпеки	Розробка та впровадження політик кібербезпеки.
	Навчання персоналу	Регулярні тренінги для співробітників щодо кібербезпеки.
	Плани реагування на інциденти	Розробка та тестування планів реагування на кіберінциденти.
Оцінка ризиків та вразливостей	Тестування на проникнення	Виконання пенетруючих тестів для виявлення вразливостей.
Фізична безпека пристроїв СВС	Контроль доступу до обладнання	Обмеження фізичного доступу до серверів і комутаційного обладнання.
Парольна і фізична безпека	Системи охорони переметру замки і ізольовані шафи Системи парольної безпеки	Використання систем охорони фізичного для захисту фізичних компонентів мережі. Антивандальні заходи і т.п. Наявність заходів і технологій контролю надійності паролів на обладнання СВС. Наявність засобів обмеження кількості спроб введенню паролів. Інші заходи.

Ці заходи і технології захисту представлення основних аспектів кіберзахисту систем відеоспостереження є основними в захищених системах передачі інформації, повинні бути використані при побудові захищених систем СВС та їх струкктур із застосуванням принципів надійного і стабільного кіберзахисту систем відеоспостереження, із закриттям вразливостей і недосконалостей існуючих систем різними способи використання. Орієнтована класична і незахищена структура СВС на базі відомих технологій СВС показана на рис.1.4.

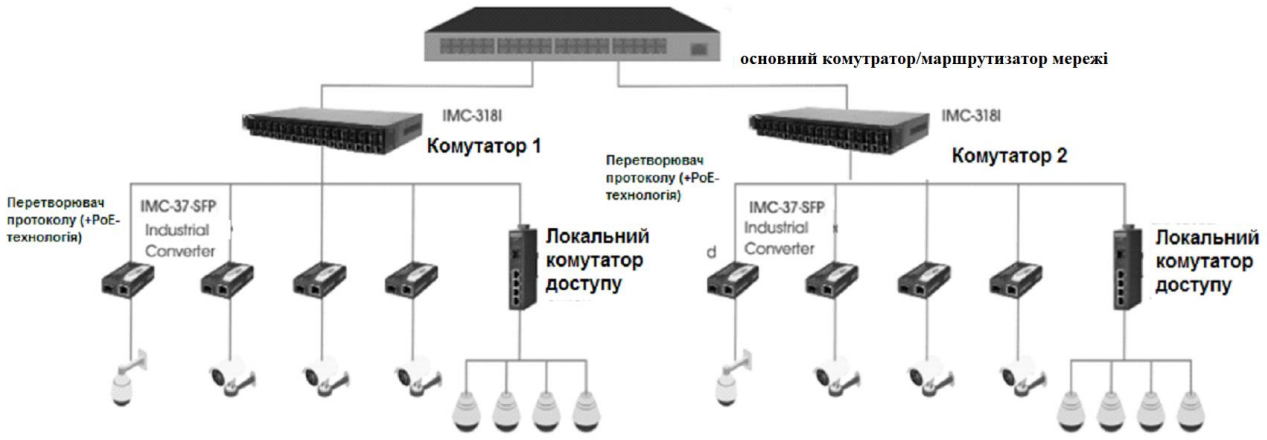


Рисунок 1.4 – Цифрова система СВС на базі багатьох камер для сектору охорони здоров'я [5 - 9]

Більшість класичних структурних схем відомих СВС (на прикладі рис.1.4) в лікарнях і медичних установах включають IP-камери відеоспостереження, відеореєстратор чи повнофункціональний відеосервер із масивом зберігання, мережеву інфраструктуру для передачі сигналів від камер до відеосерверу. До складу мережевої інфраструктри можуть входити проміжні ПК/АРМ операторів інші сервери, мережеві комутатори, маршрутизатори, інше мережеве обладнання, тощо. Але більшість існуючих систем СВС, як показує практика, не містять суміжних та/або проміжних пристроїв контролю трафіку чи пристроїв безпеки, що значно впливає на рівень безпеки. На основі проведеного в БКР аналізу було встановлено, що 6 із 10 систем СВС (80%)не містять мережевих екранів (ІВС), 5 із 10 існуючих СВС (50%) не містять цільового суміжного контролера безпеки чи суміжного сервісу безпеки типу End Point / IoT AV-Product, 9 із 10 існуючих СВС (90%) не містять засобів блокування стеження і відслідковування. Майже всі 10 (>90-95%) мають хоча б один ризик безпеки із табл.1.1. і не мають хоча б принаймні 3-х одночасно використаних заходів чи підходів, наведених в таблиці 1.2. Це призводить до значних ризиків кібербезпеки і до ефективного провадження кіберзагроз та проблем захисту СВС в секторі охорони здоров'я.

Наявність прогалин в безпеці СВС створює значні ризики до атак і зламу СВС в лікарнях в умовах інформаційної та гібридної війни для систем, що мають доступ до кіберпростору. Тому завдання забезпечення надійного захисту - полягає у розробленні ряду заходів захисту і комплексної моделі захисту СВС для сектору охорони здоров'я. Результати аналізу СВС у лікарнях у м. Вінниця(Україна) наведені у табл. 1.3.

Таблиця 1.3 – Аналіз СВС у секторі охорони здоров'я м. Вінниця

Назва лікарні	**тип і марта обладнная СВС**	**Опис проблем і ризиків безпеки(узагальнений)**
Вінницька клінічна лікарня №2	Hikvision СВН	Можливий НСД; мережеві загрози; фізична незахищеність; відсутність сегментації мережі доступ до АРМ/ПК; вірусні загрози
	Dahua	Можливий НСД; відсутність сегментації мережі доступ до АРМ/ПК
Вінницька міська клінічна лікарня (поліклініка)	Hikvisoon СВН	Можливий НСД; мережеві загрози; вірусні загрози
Вінницька районна лікарня	Dahua	Можливий НСД; мережеві, вірусні загрози
	KJS (China Vendor)	Можливий НСД; вірусні загрози
Військовий госпіталь	Hikvisoon, Dahua	Можливий НСД; відсутність сегментації мережі доступ до АРМ/ПК
інші	Партизан	Можливий НСД; мережеві загрози
	Nest	Можливий НСД; мережеві загрози
	-	-

Для традиційних технологій захисту в СВС в секторі охорони здоров'я (табл.1.3) можуть входити [2]:

- використання ізоляції каналів та базі комутаторів і маршрутизаторів по технології VLAN;

- використання IDS /IPS на базі мережевого обладнання і сервера;

- використання мережевого екрану(FireWall) апаратного або програмного ;

- використання VPN /VPS на базі мережевого обладнання;

- використання VLAN та сегментації на базі комутаторів мережі;

- використання прогресивних технологій захисту мереж СВС.

Всі відомі технології кіберзахисту СВС показують високу ефективність тільки за умов комплексного застосування, в силу різноманітності кіберзагроз в системах

відеоспостереження.Використання мережевих екранів (Firewall) можуть бути реалізовані на базі існуючих технологій: а) програмних рішень (ПЗ) в складі існуючого мережевого обладнання; апаратних рішень на базі апаратних пристроїв Firewall (наприклад, Cisco ASA 5505/5506/5525, Fortinet/Fortigate S70/80/90F/S).

Існують інші перспективні передові розробки в сфері методів захисту СВС на базі технологій Інтернету речей та систем захисту (IDS) і мережевих екранів (FW/NGFW) на базі штучного інтелекту (IDS). Такі системи здатні забезпечити кібермережевої інфраструктури СВС із технологіями Інтернету речей (IoT). Приклад такої системи показаний на рис.1.5.

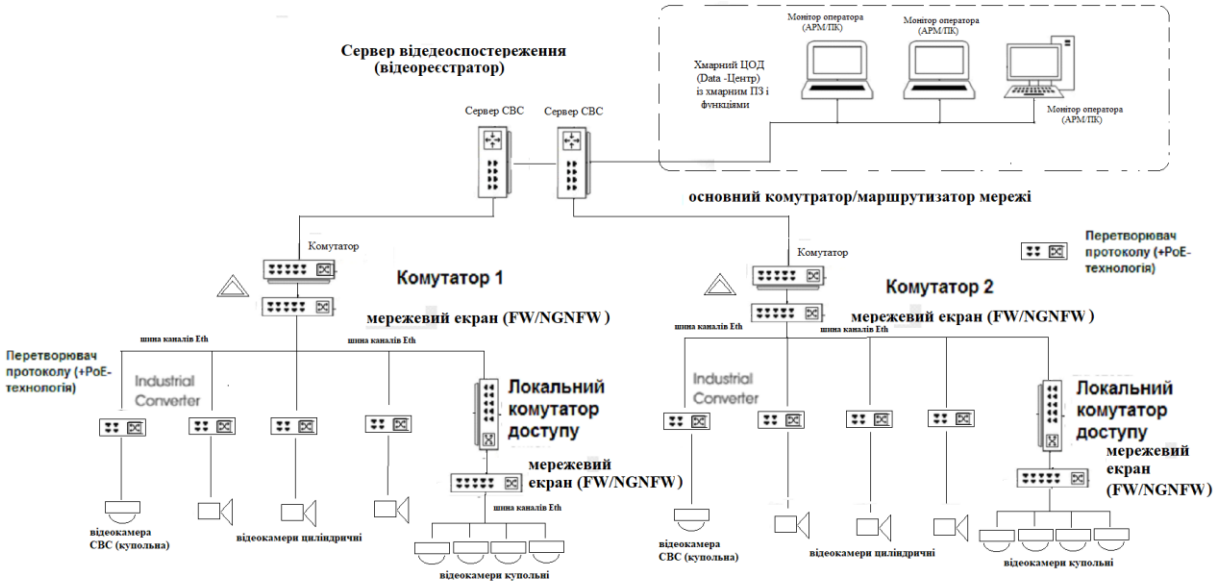


Рисунок 1.5 – Цифрова СВС із захистом мережевим екраном (FW/NGFW)

Аналіз структурної схеми (рис.1.5) показує, що вона є більш універсальнгою та функціонально гнучкою, використовує захищені кінцеві пристрої СВС із більшою безпекою пацієнтів в зонах спостередення, що робить процесс відображення гнучким, зручним та ефективним. Але, разом із тим це рішення включає додаткові фактории ризику кіберзагроз, що потребує нових підходів захисту та розширення відомих технологій захисту. Ще й на структуру, до складу якої входять захищені СВС із мережевим екраном (рис.1.5).

1.4 Завдання кібербезпеки мереж та відеокамер в складі СВС

Кібербезпека стає реальною проблемою для користувачів в медичному секторі, що використовує ІТ та СВС технології, інформаційно-комунікаційні системи із доступом до Інтернет [7-10] і відеоспостережеення зокрема, якщо не враховані багато факторів. Індустрія систем СВС розвивалася протягом тривалого часу, як і еволюціонувала і кібербезпека систем СВС. Перші СВС дозволяли зберігати інформацію локально, не використовували підключення до мережі Інтернет. Але сучасні СВС використовують можливості мережі і підключені IP-камери через мережу Інтернет, та пов'язані з ними інформаційні пристрої. Такі мережі СВС піддаються ризику зламу. Важливість та критичних даних, зібраних камерами СВС, особливо для сектору охорони здоров'я призвела до появи нового типу кіберзагроз - витоків критичної біомедичної та чутливої інформації.

Кібербезпека в сфері охорони здоров'я визнана серйозним ризиком, і ведика кількість організацій в сфері охорони здоров'я є незахищеними до великого числа кіберзагроз. Деякі пояснюють свої уразливості застарілими системами СВС чи обладнанням, або відсутністю безпеки СВС. Практика показує, що майже кожен пристрій СВС, майже ніколи не є захищеним від зламу на 100%.

Медичні організації часто вкладають не достатні кошти в розгортання технологій фізичної і кібербезпеки, а т.ч. СВС. Однак, все ж таки занадто мало інвестицій і зусиль витрачається на саму безпеку і кібербезпеку самих СВС в середині лікарень. Так, часто самі системи фізичної безпеки, якими є IP-камери у СВС, можуть бути із BackDoor(ом) чи із впровадженим ПЗ типу«Троянський кінь» або із відкритими портами чи не виключеним сервісним функціоналом від виробника, передаючі дані і розкриваючі відомості про саму ІТ-мережу СВС назовні. Це робить їх першою загрозою безпеки і легкою мішенню для зловмислників у сфері як державній, так і у комерційній в секторі охорони здоров'я .

Нові уразливості у ПЗ чи апаратурі СВС проявляються часто, і становлять значний ризик, тому повинні бути оперативно враховані і виявлені в процесі експлуатації СВС в сфері охорони здоров'я.

1.5 Шляхи підвищення інфораційного захисту систем СВС

Захист об’єктів в лікарнях, що відносяться до критичної інфраструктури, має першочергове пріоритетне значення для національної безпеки та регламентується низькою законодавчих та нормативних документів. Системи відеоспостереження на класичних об'єктах не регламентуються захистом спеціальними умовами, забезпечуючи функціонування в класичних умовах, із моніторингом та логуванням подій у них - як класичними і базовими засобами безпеки. Використовуючи передові практики кіберзахисту із аналітикою та алгоритмами машинного навчання і штучного інтелекту (AI), ці системи СВС можуть виконувати смарт-функції: наприклад, виявляти та ідентифікувати об’єкти, людей, техніку, події і моніторити свою поведінку в режимі реального часу. Наприклад, ПЗ і алгоритми AI можуть розрізняти нормальну і підозрілу активність в зонах безпки, НСД, перебування третіх осіб чи інформаційні вторгнення із генерацією миттєвих сповіщень і серверних логів для оперативного реагування персоналу служби безпеки.

Переваги рішень для відеоспостереження із активним кіберзахистом :

— Здатність автоматизувати процеси моніторингу та логування подій у СВС.

— Здатність активного і проактивного кіберзахисту у СВС.

— Підвищення інформаційного захисту суміжних систем СВС із автоматизацією процесів управління та контролю безпеки.

— Вчасне виявлення кіберінцидентів у СВС. Безпека систем із вдосконаленням функцій виявлення вторгнень і кіберінцидентів та алгоритмів із адаптацією до нових загроз і моделей поведінки.

— Інтеграція із сторонніми сервісами безпеки і хмарними сервісами і

системами. Це дозволить реалізувати додаткові функції безпеки і розширити функціонал захисту, (наприклад, інтеграція із такими системами як: контроль доступу, охоронна сигналізація, пожежна сигналізація, безпекові служби, безпека господарств, тощо).

Впровадження систем відеоспостереження із функціями безпеки дозволить значно покращити стан безпеки відеоспостередення в закладах охорони здоров'я. Але це вимагатиме інфраструктурних і фінансових вкладень із модифікацією архітектури систем безпеки. Такі заходи, як: впровадження захищених камер СВС; впровадження мережевих екранів та програмних і апаратних засобів безпеки; впровадження мікросхем і процесорів із «закритими» вразливостіями, закриття вразливостіей шлязом оновлення в програмному забезпеченні СВС; і використання можливостей захищеного зберігання даних із моніторином подій, що є важливими компонентами безпеки дозволить значно підвищити безпеку в системах СВС для сектору охорони здоров'я.

1.6 Аналіз відомих технологій та методів кіберзахисту СВС

Інформаційний і кіберзахист систем відеоспостереження в лікарнях стає все більш актуальним завдяки швидкому розвитку технологій безпеки. Нижче наведено основні відомі технологій та методи кіберзахисту систем СВС [2-14]:

- Прогресивне шифрування (AES/DES 128+) із кодуванням даних: що є критично важливим для забезпечення конфіденційності та цілісності інформації в рамках мережі СВС. Ключову роль відіграє вибір алгоритму шифрування ключа.
- Мультифакторна ідентифікація і аутентифікація в СВС: 2FA/MFA. Як метод є ефективним шляхом для забезпечення високої кібербезпеки кінцевих точок СВС. Використання сучасних методів 2FA/MFA для кінцевих користувачів і пристроїв СВС дає можливість та доцільність використання їх у системах СВС.
- Кіберзахист і захист від ШПЗ та шкідливих скриптів. Використання ПЗ для захисту від вірусів, ШПЗ, мережевих вторгнень у СВС є надійним рішенням кіберзахисту.

- Сегментування та контроль з'єднань у мережі СВС.

Забезпечення безпеки мережі СВС є основним компонентом захисту систем відеонагляду від кібератак. Важливо налаштувати мережеві екрани у СВС, VLAN і VPN, а також суміжні засоби мінімізації ризику НСД.

- Регулярне оновлення (UpDate) ПЗ СВС і софт-патчі безпеки для закриття вразливостей. Регулярні оновлення ПЗ, пристроїв СВС дозволяють виправляти недоліки безпеки і запобігти використанню експлойтів.

- Розмежування і контроль прав доступу до компонентів інформаційної системи СВС: правильно організовані права доступу дозволяють обмежити ризики кібератак і несанкціонованих доступів до СВС.

- Постійний моніторинг та логування із метою виявлення аномалій в ІКС СВС: використання систем моніторингу даних із системами фіксації подій.

Важливо мати процес автоматичного оновлення ПЗ від надійних та автонтифіковпаних ланцюгів постачання оновлень із системою моніторингу для вчасного усунення прогалин безпеки в СВС в медичному секторі. Це може значно підвищити оперативність реагування на кіберінцидент у СВС при сучасному виявлення порушення безпеки. Важливо використовувати високоефективні технології моніторингу і логування для виявлення кіберінцидентів та аномалій в СВС .Отже, кіберзахист систем відеонагляду в медичному секторі вимагає комплексних підходів і використання щонайменше 3-х методів. Також актуальний захист потребує постійного запровадження нових методів і засобів кіберзахисту із вдосконалення ПЗ та пристроїв і вдосконалення ПЗ і адаптації його до нових викликів кібербезеки і мережі Інтернет і кіберпросторі.

1.7 Аналіз основних кібезагроз на СВС у медичному секторі

Було преведено аналіз основних загроз на СВС в сфері охорони здоров'я для розробки рекомендацій щодо захисту СВС, які можуть бути прийняті для запобігання атакам (табл. 1.4).

Таблиця 1.4 – Існуючі кіберзагрози у СВС

Тип атаки	**Опис та методи**	**Наслідки**	**Загроза**
Ненадійні паролі та заводські облікові дані	Використання ПЗ і ботнеті для проведення атак на паролі методом bruite force камери, або використовуючи паролі по замовч. **Захист:** Зміни пароля, викор. менедж.паролів	Виведення з ладу великої кількості СВС камер, переривання роботи СВС, збої, масові підбір облікових даних	Більшість IP-камер поставляються з типовими логінами/паролями (наприклад, admin/admin.
Відкриті порти (RTSP, HTTP, Telnet, SSH)	Вразливість у прошивці камер Hikvision, що дозволяла виконання віддаленого коду . **Захист:** Обмеження доступу, фаєрвол, VPN, Zero Trust.	Зловмисник може отримати доступ до відео або захопити управління камерою.	Камери часто мають відкриті порти для адміністрування чи відеопотоку (наприклад, RTSP), які можна просканувати
Неоновлене ПЗ або вразливі прошивки камер СВС	Вразливість у прошивці камер Hikvision, що дозволяла виконання віддаленого коду . **Захист:** Регулярні оновлення прошивки, бажано з централізованого контролера.	Повний контроль над камерами, можливість шпіонажу; Несанкціонований доступ (НСД) до камер, викрадення даних. Камера з відомою вразливістю (наприклад, RCE або privilege escalation) може бути зламана автоматично.	Використання експлойтів для отримання доступу до камер. Виробники часто затримують випуски патчів або зовсім їх не надають.
Недостатньо зашифровані канали (RAT для СВС	Віддалене адміністрування через ШПЗ, встановлене на комп'ютери користувачів системи. **Захист:** Включення шифрування (HTTPS, RTCP, VPN).	Перехоплення або підміна відео, крадіжка облікових даних.Повний контроль над комп'ютерами і камерами, викрадення даних	Якщо RTCP-відеопотік або API-передача відбувається без TLS/SSL — можливо провести MITM-атаку. Встановлення шкідливого ПЗ через фішинг
Атаки через	Захист: Вимкнення UPnP, обмеження	Повний контроль над комп'ютерами і камерами, викр.даних	Протоколи ONVIF і UPnP
ONVIF, UPnP і P2P	ONVIF, контроль через ACL.	Віддалене підключення до камери без дозволу.	дозволяють автонастройку, але мають слабкі механізми автент.

Продовження таблиці 1.4

Ін'єкції через веб-інтерфейс (XSS, CSRF, Command Injection)		Можливі способи зламу камер. Зловмисник може контролювати всі функції камери, зчитувати відео, підключати інші пристрої.	Якщо у веб-інтерфейсі присутні вразливості, то можливо впровадити код або отримати права root.

Аналіз існуючих кібератак і загроз на СВС [2-9] показує, що системи відеоспостереження в медичному секторі є вразливими до деякних типів атак, включаючи брутфорс, атак через ONVIF, UPnP і P2PSQL-ін'єкції, DDoS-атаки, та атаки на ПЗ камер і сервера СВСю Можливі способи зламу камер та існуючі кіберзагрози приведені у табл. 1.5.

Таблиця 1.5 – Існуючі кібератаки у СВС

Метод	**Деталі**	**Наслідки**	**Загроза**
Brute-force R-Table	Підбір логіна/пароля через Telnet, SSH, або HTTP	Повний контроль над СВС, НСД	Парольний доступ
Exploit через відомі вразл.CVE на моделі	Shell-доступ	Повний контроль над СВС, НСД Шкідливе ПЗ у мережі.Камера стає частиною ботнету Віддалене прослух.	Використання вразливостей і несанкціонованого доступу
MITM-атака	Підміна відео або перехоплення	Викривлення даних Впров. у прошивку.	Створення бекдору
ARP/IP-атака	Прямий RSTM і SNMP -доступ	Повний контроль над СВС, НСД Викривлення даних Пошкодж. прошивки	Використання уразливостей і НСД Впровадження бекдору

Основний захист від таких атак (табл. 1.4) – використання сучасних програмно-апаратних засобів і окремого сервера кібербезпеки, а також спеціаліщованого ПЗ із програмними функуціями, згідно вимог до мережевої і

WEB кібербезпеки, згідно рекоментацій OWASP Top 10, NIST.

В роботі був проведений аналіз існуючих кіберзагроз у СВС для закладів охорони здоров’я (табл. 1.5) .

Аналіз методів та існуючих кібератак на СВС [4-7, 11] показує, що системи відеоспостереження в медичному секторі є вразливими до окремих типів атак.

Базові і найбільш розповсюджені вразливості включають використання паролів від виробників, вразливості в прошивці камер, недосконалості в ПЗ, відсутність шифрування та слабкий контроль доступу. Для захисту систем відеоспостереження необхідно застосовувати комплексний підхід [2, 11, 13], що включає регулярне оновлення ПЗ, використання сильних паролів, шифрування.

Витік конфіденційної біомедичної чи закритої інформації із СВС може бути піддається ризику витоку конфіденційної персональної інформації про пацієнтів, що є критичним. Це може стати суттєвою проблемою для таких об'єктів, як державні і приватні лікарні або закриті медичні заклади, у яких зберігається конфіденційна інформація. Використання програмних систем чи ПЗ для відстежування стало серьозним викликом для - камер відеоспостереження [12-23] за схемою використання і незаконного шпигунства чи стеження за особами. Це може включати відстеження приватних осіб, вторгнення у приватне життя.

Атаки на інфраструктуру і самі мережі СВС можуть стати серьозною загрозою для відеоданих. Використання методів і ПЗ для створення атак відмов в обслуговуванні сервісу (DDoS) може паралізувати ситему СВС і надання нею безпекових функцій в закладах охорони здоров'я. Також це може відбутись із витоком інформації через вразливості у мережевих пристроях.

2 РОЗРОБКА СТРУКТУР ЗАХИЩЕНОЇ СВС ДЛЯ МЕДИЧНОГО СЕКТОРУ

2.1 Принципи і структури інформаційного захисту систем СВС

Інформаційний захист систем відеоспостереження СВС є критично важливим для забезпечення конфіденційності, цілісності та доступності відеоданих та інфраструктури. Ось деякі способи і структури інформаційного захисту для систем СВН :

Шифрування даних [10]: використання шифрування даних під час їх передачі через мережу та зберігання є ефективним способом захисту конфіденційності відеоданих. Шифрування може бути застосоване як до всіх відеоданих, так і до окремих чутливих фрагментів, забезпечуючи захист від несанкціонованого доступу.

Аутентифікація та авторизація [24]: встановлення механізмів аутентифікації та авторизації дозволяє контролювати доступ до системи відеоспостереження. Він гарантує, що лише авторизовані користувачі мають доступ до відеоданих.

Фізичний захист відеокамер [12-16]: захист фізичної інфраструктури, такий як камери відеоспостереження [12-21], записуючі пристрої та сервери зберігання даних, від несанкціонованого доступу або втручання також є важливим аспектом захисту.

Моніторинг та аналіз активності: системи моніторингу та аналізу активності дозволяють виявляти ненормальну або підозрілу активність у системі відеоспостереження, що може вказувати на потенційні загрози або інциденти.

Резервне копіювання та відновлення даних: резервне копіювання відеоданих та можливість швидкого відновлення системи у випадку виникнення інцидентів дозволяють забезпечити доступність даних та продовжувати функціонування СВС.

Регулярні оновлення програмного забезпечення та застосування важливих патчів для всіх компонентів системи СВН допомагають уникнути використання вразливостей та забезпечити актуальний достатній рівень безпеку системи.

Освіта та навчання персоналу: навчання персоналу щодо кращих практик захисту інформації, виявлення фішингових атак та інших загроз, а також

процедур безпеки є ключовим аспектом успішного інформаційного захисту.

Ці стратегії та методи допомагають забезпечити повноту, конфіденційність та доступність відеоданих у системах відеоспостереження, що є критично важливим для їх ефективного функціонування та захисту від потенційних загроз.

2.2 Ключові проблеми кібербезпеки систем СВС так камер відеоспостереження

Недостатній інформаційний і кіберзахист у системах відеоспостереження може призвести до різних проблем кібербезпеки. Деякі ключові проблеми включають:

- витік конфіденційної інформації: Недостатня захищеність систем відеоспостереження може призвести до витоку конфіденційної інформації, такої як відеодані або доступність системи. Це може спричинити серйозні наслідки, такі як порушення приватності осіб, розголошення комерційної або конфіденційної інформації, а також ризик для безпеки об'єктів спостереження;

- несанкціонований доступ (НСД): Недостатній захист може відкрити двері для несанкціонованого доступу до системи відеоспостереження. Це може дозволити зловмисникам переглядати відеопотік, маніпулювати відеоданими або навіть отримати контроль над камерами для спостереження за об'єктами без дозволу.

Маніпулювання відеоданими: Зловмисники можуть спробувати вплинути на відеодані шляхом їх модифікації або видалення, що може призвести до розповсюдження фальшивих або маніпульованих зображень. Це може призвести до помилкових висновків або викривлення дійсності.

- відмова в обслуговуванні (DoS) атаки: Недостатньо захищені системи можуть бути піддані атакам з відмовою в обслуговуванні, спрямованим на перешкоджання нормальному функціонуванню. Наприклад, атаки DDoS можуть перевантажити IP-мережу або сервери, що призведе до втрати доступу;

- використання в якості вектора атаки: Недостатньо захищені камери відеоспостереження можуть бути використані як вектори атаки на інші системи

або мережі. Наприклад, компрометовані камери можуть бути використані для здійснення атак внутрішньої мережі або для викрадення інформації.

Ці проблеми підкреслюють важливість належного інформаційного захисту в системах відеоспостереження, який включає в себе використання шифрування, механізмів аутентифікації та авторизації, моніторингу безпеки.

2.3 Аналіз основних протоколів захищеної передачі інформації у СВС: OnVif та RTSP

Основні протоколи, які використовуються для передачі даних і захисту інформації в СВС для каналів та інформаційних потоків від камер це: IP, HTTP [25], HTTPS, RTSP (Real Time Streaming Protocol) [26], OnVif [27], TLS/ SSL, OAuth(802.1x/q)[24]. Це базові технології захисту мереж, які зазвичай включають сучссні і перевірені технології і методи захисту на рівні пропрацбованих рішень. По самим протоколам СВС, можно відмітити наступне: TLS(Transport Layer Security) і SSL(Secure Sockets Layer): протоколи криптографічного захисту на рвнві транспортної безпеки пакетів даних, які забезпечують більше-менш захищене передавання даних в мережі IP СВС. TLS/ SSL працюють на транспортному рівні в мережі і забезпечують шифрування трафіку між хостами чи між хостом та сервером, підвищуючи захист пакетів даних. TLS широко використовується для забезпечення захищеної передачі в СВС нарівні камер відеоспостереження.

Протокол SRTP (Secure Real-Time Transport Protocol) [25 - 27] - це захищена версія протоколу RTP (Real-Time Transport Protocol), який забезпечує захист даних при передачу відеоданих в каналаз мережі. Використання протоколів RTP/SRTP [26] дозволяє ефективно передавати дані із пакетним пакуванням і з шифруванням із забезпеченням цілісності та їх автентифікацію в мережах СВС. Протоколи шифрування, такі як TLS (Transport Layer Security) [25] або VPN (Virtual Private Network), можуть бути використані для захисту

даних під час передачі. Налаштувати мережеві пристрої, такі як маршрутизатори, комутатори та файрволи, з урахуванням заходів безпеки.

Протокол IP (Internet Protocol) [25] і його захищена версія IPsec (Internet Protocol Security) - це основний протокол передачі даних в мережах IP, який забезпечує пакетну передачі даних в ІКС із розміром пакетів MCU 1504 байт. Він реалізовує захист даних, а версія IPsec ще й забезпечує безпеку мережі. Робота стеку IPsec в парі TLS/SSL забезпечує захищену передачу пакетів даних на рівні мережевого транспорту. Сам протткол IPsec в СВС використовується для шифрування та аутентифікації пристроїв і джерел трафіку даних між вузлами мережі СВС, включаючи захищений режим камер відеоспостереження та серверів зберігання даних.

Проколи HTTPS (Hypertext Transfer Protocol Secure) і HTTP [25] є базовими для формування запитів між камерами, реалізація різних API іж вузлами мереж СВС і пристроями,та формування різних запитів длязабезпечення функціоналу і взаємодії в рамках системи відеоспостереження. Захищений режим HTTP - протокол HTTPS дозволяє захист даних при передачі через мережу СВС та мережу Інтернет. Використання HTTPS для API і передачі даних через мережу доступу до WEB-сокетів і камер СВС, а також систем управління дозволяє захищати і передавати захист і команди та режиму керування налаштуваннями.

Протокол аутонтифікації 802.1x/q [24] забезпечує захищену перевірку автонтичності механізмів захисту і механізмів аутентифікації на рівні мережевого доступу до цих пристроїв. Це контролювати атаки несанкціонованого доступу до мережевих пристроїв і ресурсів. Використання протоколу 802.1X допомагає уникнути несанкціонованого доступу до каналів інформаційних мереж СВН. Аналіз кібербезпеки та вразливості протоколів RTSP та OnVif показав їх проблеми кібербезпеки та вразливості (табл. 2.1) на якій наведено аналіз проблем протоколів передачі і стиснення відеопотоків.

Таблиця 2.1 – Аналіз проблем та вразливостей протоколів відеоспостереження OnVif та RTSP

Вразливість	**Опис**	**OnVif**	RTSP
Вразливості доступу до пам'яті(Buffer Overflow Vulnerabilities)	Вразливість, при якій зловмисники можуть використати некоректно оброблені введені дані для переповнення буферу пам'яті. **Атаки**: 1.)Експлойт; 2.) Brute-force URL(Перебір логінів/паролів до відкритих rtsp:// адрес.)	1.)+2.)-	1.)-2.)+
HTTP Basic Auth	У багатьох реалізаціях ONVIF , автентифікація базується на простому HTTP Basic, і можно легко перехопити (без HTTPS). **Атаки:** Brute-force логіна (Слабкий пароль або логіка аутентифікації → повний контроль над камерою. Часто немає автентифікації або використовується admin:admin.)	+	+ і -
WSDL інформаційне витікання	HTTPS трафік ONVIF може бути перехоплений і змінений (Man-in-the-Middle). **Атаки:** DoS через SOAP Flooding (Відправка великої кількості SOAP-запитів паралізує пристрій.)	+	-
Відсутність шифрування	Атаки на сам кодек, що використовують вразливості в його реалізації для атак на систему або виконання інших видів атак. **Атаки:** Remote Configuration Hijack. (Зміна параметрів камери, включно з переадресацією RTSP-потоку).Більшість RTSP-з'єднань — відкриті (rtsp://) без TLS (тобто rtsp замість rtsps).	+	+

Продовження таблиці 2.1

Command Injection	Вразливі прошивки дозволяють відправити шкідливі SOAP-запити, що виконують shell-команди. **Атаки:** 1.) Установка бекдора (Через ONVIF API можливо створити адміністративного користувача.) 2.)Витік конфіденційних URL (Через Shodan/Censys відкриті rtsp://login:pass@ip знаходяться публічно.) 3.) Sniffing (Перехоплення відеопотоку (особливо в LAN).) 4.) Replay атака (Повторення попереднього запиту — можливість дивитись потік без авторизації.)	1.)+ 2.) 3.)-4.)-	1.)- 2.) +3.)+4.)+
Підробка токенів	ряді реалізацій можна обійти автентифікацію шляхом підробки XML-токенів. **Атаки:** 1.) SSRF (Через несанітаризовані URI-запити до зовнішніх адрес); 2.) Session Hijacking (Перехоплення RTSP-сесії без захисту) .	1.)+ 2.) -	1.)- 2.) +

По результатам аналізу таблиці 2.1 було встановлено, що основними кіберзагрозами та вразливостями для протоколів OnVif та RTSP в СВС є: вразливості пам’яті буферів, кібератаки, внутрішні загрози безпеки, атаки на API та інше.

Внутрішні загрози ONVIF:

1.)Адміністратори/техніки можуть навмисно змінити RTSP /HTTP доступ;

2.)Якщо СВС мережа не ізольована —і з іншого сегменту легко отримуєиться контроль.

Протокол RTSP (Real Time Streaming Protocol) використовується для потокової передачі аудіо/відео між IP-камерою і клієнтом.

Внутрішні загрози RTSP:

1.)Внутрішні працівники можуть знайти відкриті rtsp:// адреси і вивести відеопотік.

2.)Внутрішні проксі/шлюзи можуть кешувати або клонувати трафік.

Загальні проблеми захисту ONVIF/RTSP (проблема безпеки і наслідки):

- Відсутність шифрування Легко перехопити або підмінити запити/потік;
- Погані паролі: Типово — admin/admin.
- Відкриті порти: RTSP (554), ONVIF (80/8080/8000) — доступні ззовні.
- Стара прошивка Камери СВС із CVE з 2014–2022 років досі в мережах.
- Відсутність сегментації: камери СВС часто у тій ж мережі, що Інтернет.

Рекомендації по захисту:

- Вимкнути режим ONVIF на камерах СВС або обмежити IP доступ.
- Використовувати HTTPS/WSS для ONVIF-сервісів.
- RTSP через VPN або TLS (rtsps://).
- Встановити складні паролі та змінювати їх регулярно.
- Обмежити доступ через брандмауер (ACL).
- Регулярне оновлення прошивки камер.
- Виявлення камер у мережі ;
- Моніторинг підозрілої активності (наприклад, нетипові підключення RTSP).
- Використовувати VLAN / ізоляцію камер (FireWall)від загальної мережі.

Основні вразливості CVE-(приклади) для ONVIF камер СВС:

CVE-2021-32934 – уразливість в ONVIF реалізації (бібліотека WS-Discovery).

CVE-2017-7921 – Hikvision, bypass авторизації через ONVIF.

CVE-2020-6750 – RTSP heap buffer overflow в Dahua/NVR.

Ці обставини потребують оперативного втручання і розробки нових та практичних підходів захисту обладнання СВН на базі цих кодеків.

Інші протоколи СВС - TCP/IP та SNMP, також можеть мати свої власні проблеми безпеки. TCP/IP може бути вразливим до атак на пам'ять та прямих зламів паролів. Протокол SNMP має вразливості на переповнення буфера та перехоплення даних .

Всі ці протоколи відіграють важливу роль у мережевому зв'язку СВС для медичного сектору, але їх вразливості можуть стати перепоною длярозвитку і

широкого впровадження СВС в секторі, якщо не приділено достатньо уваги заходам безпеки та регулярному оновленню. Рекомендується проводити регулярні аналіз і тестування безпеки СВС, використовувати захист від відомих атак та ретельно контролювати доступ до ресурсів СВС.

2.4 Розробка структурної моделі кіберзахисту СВН для сектору охорони здоров'я на базі комплексного підходу

Структурна модель кіберзахисту СВН може бути розроблена тільки враховуючи широкий ландшафт кіберзагроз і комплексність факторів необхідного захисту СВС. Так, враховуючи проведені аналіз рис.1.3-рис.1.4 (розділ 1), а також аналіз факторів кіберзагроз в СВС у медичних закладах, можна запропонувати модель кіберезпеки для системи відеоспостереження для медичних установ (рис.2.1).

Така модель (рис.2.1) може враховувати різін ризики кіберзагроз із врахуванням конктерних факторів ризику і мати різний прояв в різних системах.

Ця модель може адаптовуватись до не чітко визначеної СВС і під конкретні умови чи під конкретну схему в різних закладах охорони здоров'я використання із врахуванням різних типів ризиків кіберзагроз.

В загальному випадку ймовірність ризику визначається сумарно по всім видам ризиків , що описуються ймовірносями:

$$Pi=SUM_{i=1}^{N}[p_i], \qquad (2.1)$$

де pi – однична ймовірність кібірзагроз по факторам ,відповідно до метожду кіберзахисту (табл.2.2, перший стовпець). Як правило для P_i : $0 < P_i < 1$.

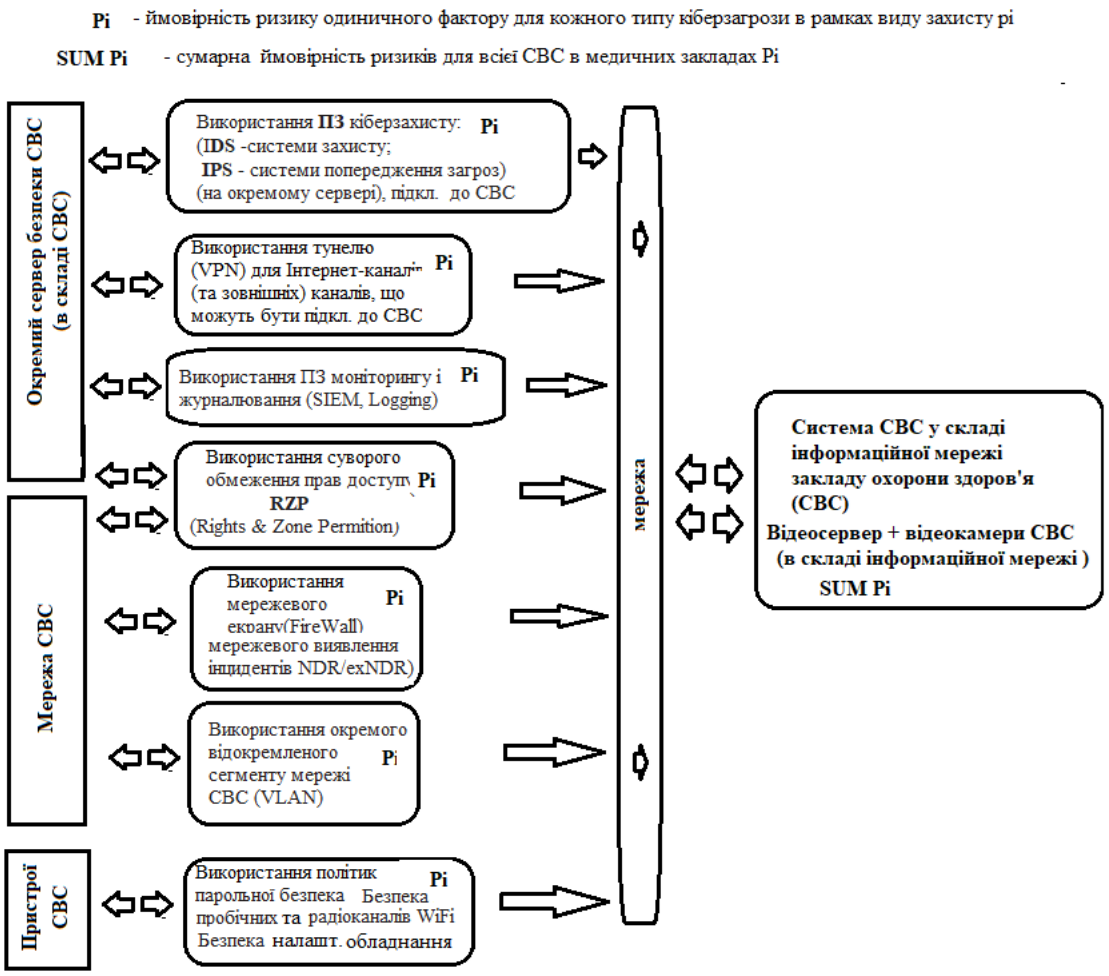


Рисунок 2.1 – Структурна модель кіберзахисту СВС у медичних закладах

Структурна модель (див. рис. 2.1) що враховує ризики кіберзагроз на базі ряду технологій кіберзахисту СВС. Сумарна ймовірність кіберзагроз може дозволити визначити кількість інформації (або умовну ентропію), яка буде формувати рівень інформації, що піддається ризикам і потребує захисту в СВС :

$$I_i = P_i log_2 P_i = \Sigma_{i=1}^{N} [p_i] \; log_2 \; [p_i] \qquad (2.2)$$

де, P_i наближеність до 0 значення Pi означатиме вищий рівень захисту і менший обсяг даних в СВС (2.2), який піддіється ризикам кіберзагроз, і навпаки - наближеність до 1 означатиме меньший рівень захисту і відповідно більший рівень даних, які піддаються ризикам кіберзагроз в СВС.

По досягненні певного порогу $p_i < p_{pori}$. може формуватись умова включення захисту в моделі захисту (рис.2.1). тобто коли $p_i > p_{por\,i}$. - спрацьовує компонент захисту в моделі (рис.2.1). Сама модель (рис.2.1) тісно повязана і відтворює процеси захисту інформації із структурою захищеної СВС для медичних закладів (рис.1.5).

Основна задача підвищення захисту СВС - наблизити рівень ймовірність ризику кіберзагрози p_i до 0, або принаймні до мінімальних значень $p_i = p_{min}$.

2.5 Розробка рекомендацій для захисту систем відеоспостереження в секторі охорони здоров'я

Враховуючи аналіз ризиків кіберзагроз і самих кіберзагроз в СВС для сектору охорони здоров'я (табл. 2.2).

Таблиця 2.2 – Рекомендації кіберзахисту СВС у медичному секторі

Тип атаки	**Основні рекомендації**	**Ефект від нейтралізації наслідків**	**Загроза**
Ненадійні паролі та заводські облікові дані	Провести аудит паролів та облікових даних СВС. Провести зміни паролів (в тому числі регулярні зміни) на всіх пристроях СВС із зах.надійним їх зберіганням.	Запобігання НСД та виведення із ладу великої кількості відеокамер, сервера СВС, уникнення збоїв та витоків даних, запобіг. компром. облік. даних	Більшість IP-камер поставляються з типовими логінами/паролями (наприклад, admin/admin/.
Відкриті порти (RTCP, HTTP, Telnet, SSH)	Провести аудит досьтупних зовні портів СВС та камер і мережі СВС. закрити порти СВС і усунути вразливості у прошивці. Викрристати фаєрвол, VPN, або Zero Trust.	Запобігання НСД та виведення із ладу великої кількості відеокамер, сервера СВС, уникнення збоїв. Запобігання доступу зловмисника до відеоданих та захопленню управління камерами.	Камери можуть мають відкриті порти для адміністрування чи відеопотоку (наприклад, RTCP), які можна просканувати

Продовження таблиці 2.2

Неоновлене ПЗ або вразливі прошивки камер СВС	Оновити ПЗ і вразливі прошивки камер СВС до останніх версій. Використати контроль оновлень та запровадити механізми регулярних оновлень прошивки, із офіційних джерел.	Повний контроль над камерами, можливість шпіонажу; НСД, викрадення даних, RCE, злам за допомогою автоматизованих засобів ПЗ .	Використання експлойтів для отримання доступу до камер. Виробники часто затримують випуски патчів або зовсім їх не надають.
Недостатньо зашифровані канали (відеопотік, API) та використання RAT для СВС	Використати апратний FireWall і апаратно-програмний IDS/IPS із контрлером адміністрування через антивірусні спец. пакети чи окркемий сервер безпеки із антивірусним ПЗ і системами протидії ШПЗ на рівні мережі (NDR/XDR/SIEM).	Запобігання НСД та виведення із ладу великої кількості відеокамер, сервера СВС, уникнення збоїв. Запобігання доступу зловмисника до відеоданих та захопленню управління камерами.	Компроментація RTSP-відеопотік або API-передачі, яка відбувається без TLS/SSL — через проведення MITM-атаку.
Атаки через ONVIF, UPnP і P2P	Використати ПЗ захисту, яке встановлене на комп'ютери користувачів системи.	Запобігання перехоплення або підміні відеоміток та відеопотоків, джерел відеоданих, крадіжка облікових даних.	
Ін'єкції через веб-інтерфейс (XSS, CSRF, Command Injection)	Включити по максимуму функціонал безпеки в самих пристроях СВН: камерах та відеосервері/відеореєстраторі. Включити апраатне шифрування на камерах СВС: HTTPS, SRTP, VPN.	Запобігання повному контролю над комп'ютерами і камерами, викрадення даних Запобігання віддаленому підключення до камер без дозволу.	Встановлення шкідливого ПЗ і шкідливих мікромодулів ПЗ чи оновлень через фішингові дії чи іншіканали

Аналіз розроблених рекомендацій і методів захисту від кібератак на СВС (табл. 2.2) дозволяє створювати захищені системи відеоспостереження для медичного сектору із менш вразливими компонентами і мережею для деякних типів кібератак, включаючи атаки через брутфорс і вгадування облікових даних, атак

через протоколи ONVIF,RSTP, IP, UPnP, та із використанням P2P-SQL-ін'єкції, DDoS-атак, та інших технолоогій атак на ПЗ камер і сервера СВС. Основний захист від таких атак (табл. 2.2) - Використання сучасних веб-бібліотек, перевірка на OWASP та IoT cybersecurity framwork.

Базові і найбільш розповсюджені вразливості включають використкання паролів від виробників, вразливості в прошивці камер, помилки ПЗ, немає шифрування.

2.6 Оцінка параметрів СВС для оптимального кіберзахисту

Розробка структурних та математичних моделей захисту даних у СВС є важливою частиною завдання забезпечення кібербезпеки систем відеоспостереження в секторі охорони здоров'я. Структурна модель кіберзахисту СВС (рис. 2.1) описана в табл.2.2 із врахування ризиків СВС (табл.2.1), і включає різні компоненти кіберзехисту системи відеоспостереження та різні заходи і засоби безпеки. Модель захисту повинна враховувати ряд таких елементів як:

- рівні захищеності камер відеоспостереження: можливість парольного захисту, функції захисту і шифрування відеопотоків в камерах СВС. Захищені механізмами аутентифікації в камерах;

- рівні захищеності мережевого обладнання (комутаторів, марштрутизаторів шлюзів, відеосервера): використання функцій і засобів захисту мережі СВС для передачі даних. Використання мережевих екранів і шлюзів, а також безпекових налаштувань мережевого облоаднання (маршрутизщатори, комутатори) для захисту мережі СВС. Сюди також відноситься і включення VLAN та VPS/proxy у мережі.

- рівні захисту сервера СВС та систем зберігання даних: 1.) Шифрування даних на дисках відеосервера; 2.) Захищені серверні приміщення; 3.) Захист та налаштування клієнтських пристроїв АРМ та моніторів СВС; 4.) Використання організаційних методів захисту: регулярні оновлення та аудити кібербезпеки СВС. Виконання політик доступу та управління ресурсами СВС. Схема із заходів

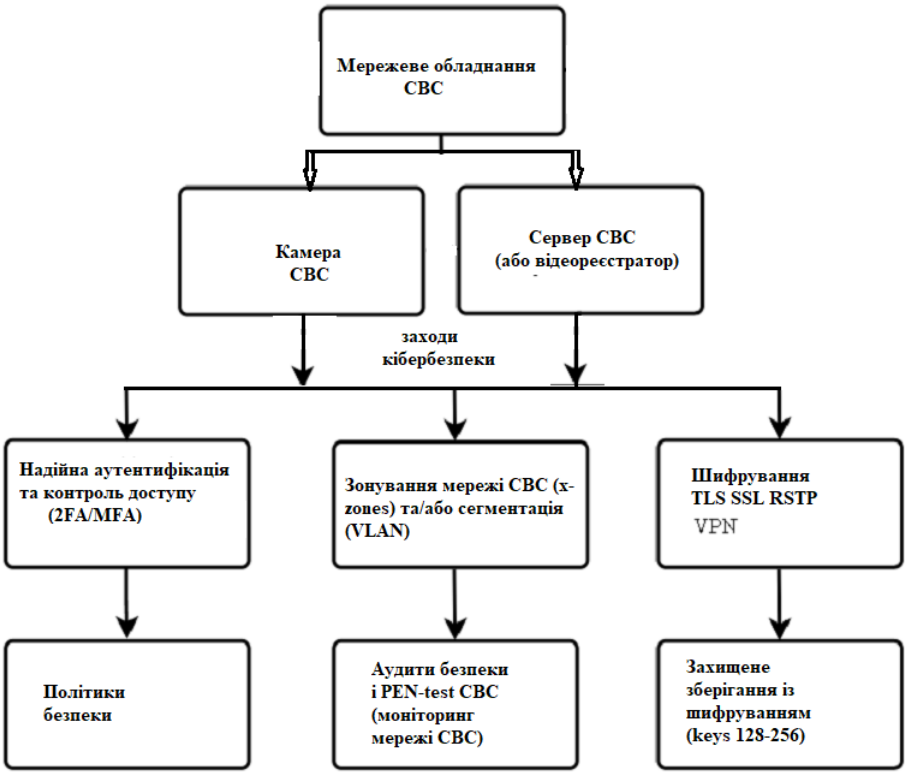


Рисунок 2.1 – Схема із заходів кіберзахисту в СВС медичного сектору

Сама ймовірність виникнення загрози описується подіями W_i в як:

$$P_{sec}(x) = Sum\ [P_i \times W_i\ ]. \quad (2.3)$$

Кожному фактору загроз p_i , яка матиме місце в СВС у певний період часу T_i присвоюється ймовірність її виникнення $P_i. = Sum[p_i\ ]$.

Оцінка впливу на ресурси CBC і збитків від кіберзагроз в СВС може бути визначена по подіям Wi в СВС, які можуть мати місце в силу різних причин. Оцінка ризиків кіберзагроз в СВС медичного сектору дозволяє оцінити потенційний ризик для кожної загрози $Ri,$ обчислюється як добуток ймовірності загрози та потенційних втрат: $Ri= P_i.(Ti)\times Li$.

Для кожної загрози визначаються відповідні захисні заходи захисту із, які зменшують її ймовірність p_i впливу цієї загрози. Захисні заходи можуть включати: надійну автонтифікацію пристроїв в системі СВС; надійше шифрування(AES або DES) даних в СВС за доступними технологіями; надійну авторизація користувачів

в СВС та на пристроях за допомогою захищених паролів; використання захищених віртуальних тунелів (VPN або VPS) у СВС в каналах які взаємодіють із Інтернет; моніторинг, контроль та аудит кібербезпеки в СВС; оновлення прошивок камер СВС та ПЗ відеосервера. Використання оцінок загроз (2.1) – (2.2) і захисних підходів СВС в сфері медичного сектору може суттєво знизити загальні ризики атак на СВС і ризики кіберзагроз. Формула (2.3), що описує кібербезпеку в СВС і може описати кіберзахист дозволяє оцінити процес впливу негативних факторів на СВС, оцінки ризиків та умовний рівень захисту компонентів СВС. Це допоможе прийняти обґрунтовані рішення щодо впровадження необхідних заходів для забезпечення безпеки СВС в лікарнях.

3 СТРУКТУРНА І АЛГОРИТМІЧНА ОРГАНІЗАЦІЯ ЗАХИЩЕНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ СЕКТОРУ ОХОРОНИ ЗДОРОВ'Я

3.1 Структурна схема захищеної системи відеоспостереження на базі розподіленої і сегментованої структури СВС

Структура захищеної СВС для сектору охорони здоров'я включає наступні мережеві компоненти: 1.) камери відеоспостереження; 2.) сервер СВС (або пристрій відеореєстратора СВС); 3.) мережеві пристрої із комунікаціями СВС; 4.)засоби кіберзахисту - мережеві екрани або пристроїв безпеки типу FW/NGFW для СВС; 5.)окремий сервер безпеки, на якому можно розмістити кібербезпекове ПЗ і IDS/IPS/NDR/SIEM системи для контиролю мережі; 6.) логічні та організаційні заходи захисту СВС. Загальну структуру СВС із кібезахистом показано на рисунку 3.1.

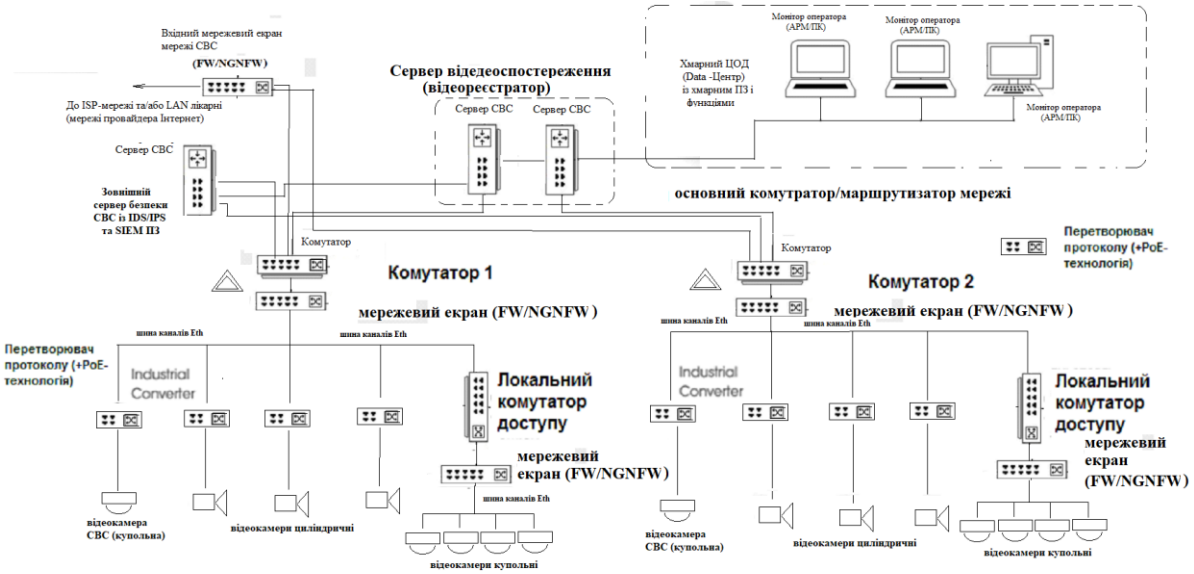


Рисунок 3.1 – Схема кіберзахисту ресурсів в системах СВС

Основними компоненти структури (рис. 3.1) є відеокамери та відео сервер. Це є класичною складовою і традиційною частиною будь якого СВС-системи. В плані безпеки в структурі (рис 3.1) додані ще : засоби кіберзахисту у вигляді

мережевих екранів FW/NGFW для СВС та окремий сервер безпеки СВС.

Рисунок 3.2 – Схема застосуванян заходів кіберзахисту в структурі СВС

До складових кіберзахисту (рис. 3.2) належать: мережеві екрани; системами виявлення вторгнень IDS|IPS на сервері СВС (із розгорнутими політиками доступу); комутатори мережі СВС(із запровадженими правилами сегментації та листами доступу (Accsess lists & ACL)); логічний сервер автонтифікації LDAP/RADIUS із контролером автонтифікації пристроїв, який розміщений на окремому сервері безпеки СВС, який контролює камери СВС та інші пристроїв в мережі.

Структури захищених СВС(рис.3.1-рис.3.2) тісно пов'язані із моделлю кібірбезпеки (рис. 2.1) і визначаються і керуються нею.

Розроблена структура дозволяє реалізовувати захист від кіберзагрроз СВС у різних точках та здійснювати контроль доступу до мережі СВС.

Використання засобів захисту на базі комутатору мережі СВС (із запровадженими правилами зонуванням і сегментацією та листами доступу (Accsess lists, ACL)) та на базі логічного контролеру(серверу) автонтифікації пристроїв СВС, що працює в складі ПЗ відео сервера та ПЗ СВС, а також наявність засобів захисту на базі мережевого екрану СВС дозволяє підвищити

кібербезпеки, порівняно із традиційними технологіями та структурами СВС. запобігання від більшості кібератак на базі мереж СВС дозволяє забезпечити вищу стабільність мережі та її стійкість, що досить актуально для високо критичних СВС, які самі по собі є засобами безпеки і від яких залежить безпека підприємств та організацій, де вони використовуються.

3.2 Оцінка захисту і вразливостей систем СВН та камер відеоспостереження

Оцінка захисту камер і інших компонент системи відеоспостереження (СВС) в лікарнях є важливим процесом для забезпечення їхньої кібербезпеки. Сама оцінка передбачає аналіз потенційних загроз, оцінку існуючих ризиків і врахування вразливих місць. Нижче наведено вразливі місця і кроки для проведення підвищення захисту в обладнанні СВС: камери відеоспостереження, мережеве обладнання (маршрутизатори, комутатори), сервер СВС, монітори СВС.

Для розгляду прикладів кіберзагроз в СВС можно розглянути методи і функції доступу до відеокамер СВС, (на мові Python):

```
def scan_local_network(ip="192.168.1.23 "):
    arp = ARP(pdst=ip)
    ether = Ether(dst_MAC="fe:2f:00:oA:1f:df")
    packet = ether/arp
    result = srp(packet, timeout=3, verbose=0)[0]
    devices = [{'ip': received.psrc, 'mac': received.hwsrc} for sent, received in result]
    return devices
```

можно побачити, що введення і використання прямих адрес IP та MAC створює загрозу прямого і жорсткої закріплення їх в коді, із можливістю спцфінгу та обходу авторизації для цього пристрою (із цими адресами) шляхом підробки. Аналогічно можно побачити подібні вразливості на дані автронтифікації на сервері СВС,при використанні Python-скриптів із обробкою запитів і автоматичним доступом до камер:

```
if IPcamI name == "main name":
    # Параметри вашої камери і адреса
```

```
    host = "192.168.1.23 "
    port = 80  # Для WEB 80 або 8000
    username = "admin"
    password = "admin"

    try:
        rtsp_url = get_rtsp_url_onvif(host, port, username, password)
        print("RTSP URL:", rtsp_url)
        read_rtsp_stream(rtsp_url)
    except Exception as e:
        print("Помилка:", e)
```

або якщо використоувати код на сервері СВС на пряму, типу:

```
rtsp_url = get_rtsp_url_onvif(192.168.1.23, 80, admin, admin)
        print("RTSP URL:", rtsp_url)
        read_rtsp_stream(rtsp_url)
    except Exception as e:
        print("Помилка даних відео:", e)
```

можно побачити, що можно отримати доступ до відеопотоків функцією get_rtsp_url_onvif(host, port, username, password) для цієї камери. Якщо враховувати і використовувати цей незахищений код і процедуру доступу в реальних прожктах, можно спричинити до відомих атак на СВС, а саму систему відеоспостереження зробити вразливою.

Також можно побачити приклади коду із іншими вразливостіми, (наприклад, використання прямих і не захищених ключів API доступу:

```
#  Перевірка доступу по API . типу за accsess API
def data_accsess (192.168.1.23, fe:2f:00:oA:1f:df):
    try:
        api = Restfull.restfull(fe:2f:00:oA:1f:df)
        host = api.host(192.168.1.23)
        pulns = host.get('vulns', [])
        return pulns
    except Exception as e:
        return [str(e)]
```

наприклад, така функція використовує прямий ключ дотсуп API в скрипті Python і дозволяє отримати НСД до камери із IP 192.168.1.23, перехопивши або вичитавши сам ключ API по сторонньому каналу, наприклад функцією :

```
def stream _accsess (get):
```

```
try:
get  = Restfull.get(api)
api= api.get('Restfull', [])
return api
   except Exception as e:
      return [str(e)]
```

В такому випадку можно вичитати доступ вичитавши значення ключа API.

Окремі положення і випадки кібербезпеки і атак НСД можно показати на прикладі використанні доступу до камер із перевищенням прав доступу і скануванням мережі ,наприклад:

```
class CameraScanner:
   def __init__(self, root):
      self.root = root
      root.title("IP-Камери безпека")
            self.ip_listbox = tk.Listbox(root, width=40)
      self.ip_listbox.pack()
      self.scan_btn = tk.Button(root, text="Сканувати мережу", command=self.scan_network)
      self.scan_btn.pack(pady=5)
```

Або використання експлойту із доступом до багатьох камер, які мають відкриті незахищені порти із публічними інтерфейсами по протоколам ONVIF або RTSP. Доступ при цьому буде без автентифікації чи із використанням тривіальних паролів.

Сам код запиту (приклад у вигляді скріпту на bash):

```
# Захоплення RTSP відео потоку без автентифікації
ffplay rtsp://admin:admin@<ip=192.168.1.23>:554/stream1
```

це дозволить отримати доступ до відеопотоку із камери з IP-адресою 192.168.1.23, на якій буде використані дані паролів та імя користувача, по замовчуванню.

Захист від такоє атаки : 1.) Змінити логін/пароль камери з IP 192.168.1.23; 2.)Вимкнути протоколи ONVIF ізпрямим доступом до RTSP, якщо вони не використовуються; 3.) Обмежити доступ по IP фаєрволу.

Інший приклад атаки - використання відаленого виконання кодів на камері : Remote Code Execution (RCE) через WebUI або CGI

Сама вразливість камери повязана із використанням застарілих CGI/API інтерфейсів, де нефільтрований параметр може викликати shell-команди.

такі вразливості (CVE) СВС таблично задані і відомі: 1.) CVE-2017-17106 (для СВС Huawei) — дозволяє виконання команд через CGI-запити; 2.) CVE-2020-9527 (для HiSilicon SoC) — дозволяє виконати RCE .

Для кіберзахисту потрібно: 1.)Оновити прошивки камер СВС на більш нові; 2.) Блокування HTTP-доступу назовні фаєрволом; 3.)проводити моніторинг аномалій у веб-логах і трафіку від цієї камери.

Іншим типом реальної загпрози є CVE з фабричними бекдорами.
Деякі камери СВС(особливо СВС із OEM-версіями китайських виробників) мають бекдор в облікових записах: root, 666666, admin: 123456, або сервісні API, що дозволяють змінити пароль без автентифікації. Приклади: 1.)Вразливість CVE-2017-7921 – для камер Dahua: зловмисник змінює пароль через бекдор API; 2.)Вразливість CVE-2021-36260 –для камер Hikvision RCE, зловмисник отримує доступ без авторизації. Для захисту потрібно: 1.) Змінити паролі і видалити всі невідомі акаунти і сесії; 2.)Виконати сегментацію мережі СВС за допомогою VLAN: 3.) Використати технології кіберзахисту IDS/IPS.

Також може мати місце вразливості із витоками прошивки та зворотній інжинірингом: прошивки (firmware) для камер СВС часто доступні онлайн. зловмисники витягують їх, знаходять уразливі бібліотеки, API або hardcoded ключі і використовують їх для написання експлойтів і використанні у своїх методів доступу до ресурсів цих камер СВС. Основні інструменти, які можуть бути використані для цього:

-binwalk – для аналізу прошивки

-strings, ghidra, radare2 – для аналіз коду прошивки.

наприклад, експлойт (скрипт на bash)

```
binwalk firmware.bin -e
```

дозволить проаналізувати прошивку на предмет відкритих даних в ній або змінити її, і витяглит ці дані. Для захисту потрібно використати цифровий підпис прошивки, або регулярне оновлення прошивки. Також не зайвим буде

шифрування важливих даних.

Також проблему на практиці створюють відкриті потоки доступних камер СВС через мережу Інтернет (Наприклад, із використанням інструментів Shodan, ZoomEye). Уразливість. що використовує доступ до потоків через rtsp://, http://, https:// знаходиться в Shodan або ZoomEye. Приклад пошукового запиту в Shodan (vbnet):

```
port:554 has_screenshot:true
title:"Network Camera"
```

Для захисту треба використати перевірку зовнішньої доступності через Shodan або використати VPN-доступ замість відкритих портів для цих камер СВС. Не зайвою буде постійна і регулярна зміна паролів на камери СВС.

Іншим типом атак є використання ін'єкцій. Наприклад, шкідливі ін'єкції (SQL/Command/Path) у DVR/NVR систем СВС у камерах можуть створити значні проблеми їх функціональності, використавши вразливості на веб-панелі із відеореєстратора, який не фільтрує введення запитів. Це вразливості (CVE) для камер : CVE-2018-9995 – DVR login bypass ; CVE-2020-6756 – SQL ін’єкція в TVT DVR . наприклад, експлойт (bash):

```
curl -X POST "http://ip/login" -d "username=admin'--&password=abc"
```

це дозволить виконати шкідливу ін'єкцію безпосердньо у веб-панель відеореєстратора, створивши значні проблеми. Для захисту потрібно використати: 1.) веб-брандмауер; 2.)блокування POST-запитів із зовні до СВС; 3.) виконати оновлення прошивок камер і відеореєстратора до нових версій із пропатченими вразливостями CVE-2018-9995 і CVE-2020-6756.

Загальні рекомендації для камер СВС для їх кіберзахисту :

- зміна паролів по замовчуванню одразу після встановлення СВС;
- використовувати зв'язку HTTPS / TLS по можливості;
- виконати сегментацію мережікамери в окремому VLAN;
- використати IDS/IPS(наприклад, Suricata, Snort, Cisco DirectIDS ;
- виконати Логи/Моніторинг всіх спроб входу і трафіку RTSP, ONVIF;
- вимкнути непотрібних сервісів FTP, Telnet, SSH .

Оцінка захисту і вразливостей СВС систем відеоспостереження та камер

відеоспостереження дозволяє виявити слабкі місця в СВС в медичному секторі і вчасно вжити відповідних заходів для захисту. Самі базові оцінки наведені у табл. 3.1 та табл.3.2.

Таблиця 3.1 – Оцінка захисту і вразливостей СВС в медичному секторі

Активи СВС	**Загроза**	**Вразливість**	**Захисний захід**	**Оцінка ризику (R_i)**
Відеокамери СВС	НСД	Слабка аутентифікація	Багатофакторна аутентифікація	Висока
Мережеве облад.	Перехоплення даних	Відсутність шифрування	Використання VPN VLAN	Середня
СерверСВС/відеореєстратор	Відмова в обслуговуванні (DoS), експлойти	Відсутність захисту від Кібер і ШПЗ	Налаштування файрволів та IDS/IPS	Висока
Інформацій і відеопотоки СВС	Перехоплення та зміна СВС даних	Відсутність шифрування	Шифрування даних (DES|AES)	Висока
Користувачі і доступ до СВС	Шкідливі дії і ШПЗ	Недостатній контроль доступу	Ролі та політики доступу	Середня
Ризики пощшкодженняідоступ у до обладнання СВС	Фізичне пошкодженняСВС	Слабкий фізичний захист	Захищені серверні приміщення	Низька

Таблиця 3.2 – Оцінка ризиків кіберзагроз СВС всекторі охорони здоров'я

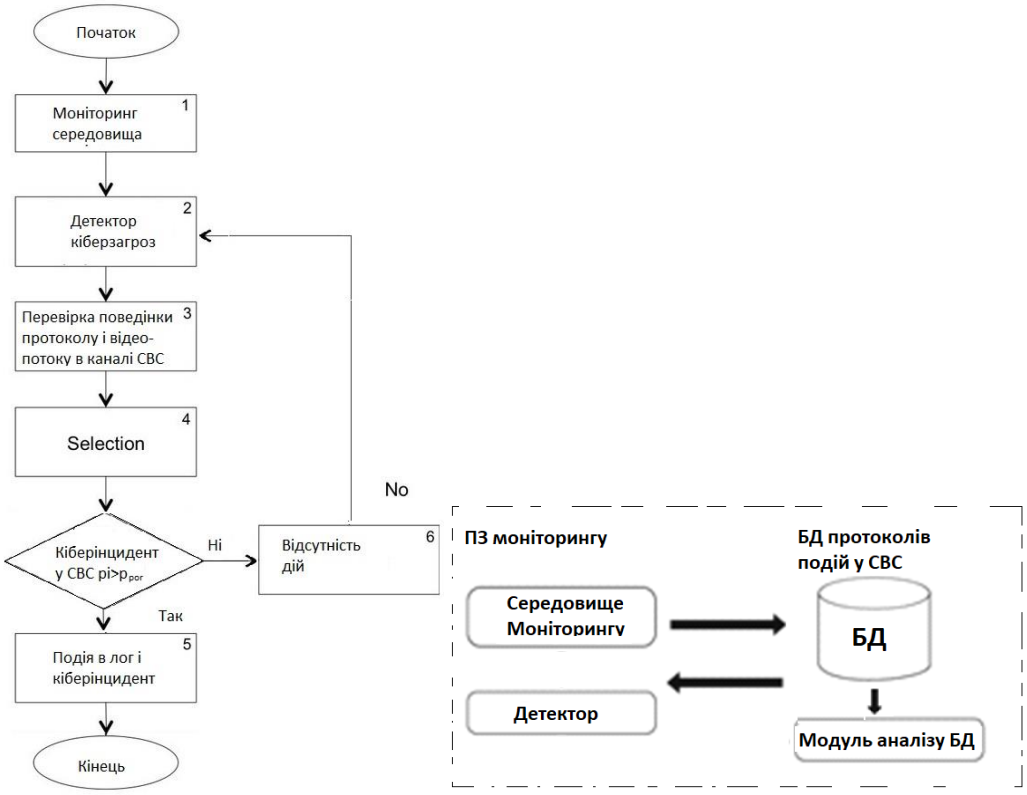
Загроза	**Ймовірність**	**Збитки**	**Ризик (Ri) = Ймовірність × Збитки**
Несанкціонований доступ	Висока	Високі	Високий
Перехоплення трафіку	Середня	Високі	Середній
Відмова в обслуговуванні (DoS)	Середня	Середні	Середній
Зловмисна діяльність співробітників	Низька	Високі	Середній
Природні катастрофи	Низька	Високі	Середній

Використання комплексного підходу кберзахисту до СВС в медичному секторі оцінка ризиків забезпечить порівняно високий рівень кібербезпеки.

3.3 Розробка алгоритмів кіберзахисту СВС для медичного сетору

Базовий алгоритм роботи системи безпеки ІС включає: аналіз, контроль

поведінки СВС: реагування на інциденти. Базовий алгоритм захисту системи відеоспостередення згідно моделі рис.2.2 (розділ 2) показаний на рис.3.3.



a) b)

Рисунок 3.3 – Базовий алгоритм кіберзазхисту СВС від атак: а) основний робочий цикл кіберінциденту в СВС; б) визначення за ознакою

Алгоритм (рис. 3.3) для класичних засобів захисту СВС передбачає використання функцій аналізу подій відеопотоків камер СВС, ПЗ на сервері СВС та ряду додаткових показників. На основі аналізу кіберзагроз для СВС і аналізу ризиків запропоновано більш широкий алгоритм СВС, точніше алгоритм захисту від кібератак СВС, що передбачає виявлення і реагування на кіберінцидент, згідно моделі кіберзахисту СВС (рис.2.2, розділ 2). Цей алгоритм (показаний на рис.3.4) передбачає глибинний аналіз трафіку відеопотоків і застосування правил файерволу (FW/NGFW) в залежності від наявності кіберінциденту в СВС в часі по частоті появі їх ризиків $p_i(x)$ (формула (2.4), розділ 2). Сам алгоритм представлений на рис. 3.4.

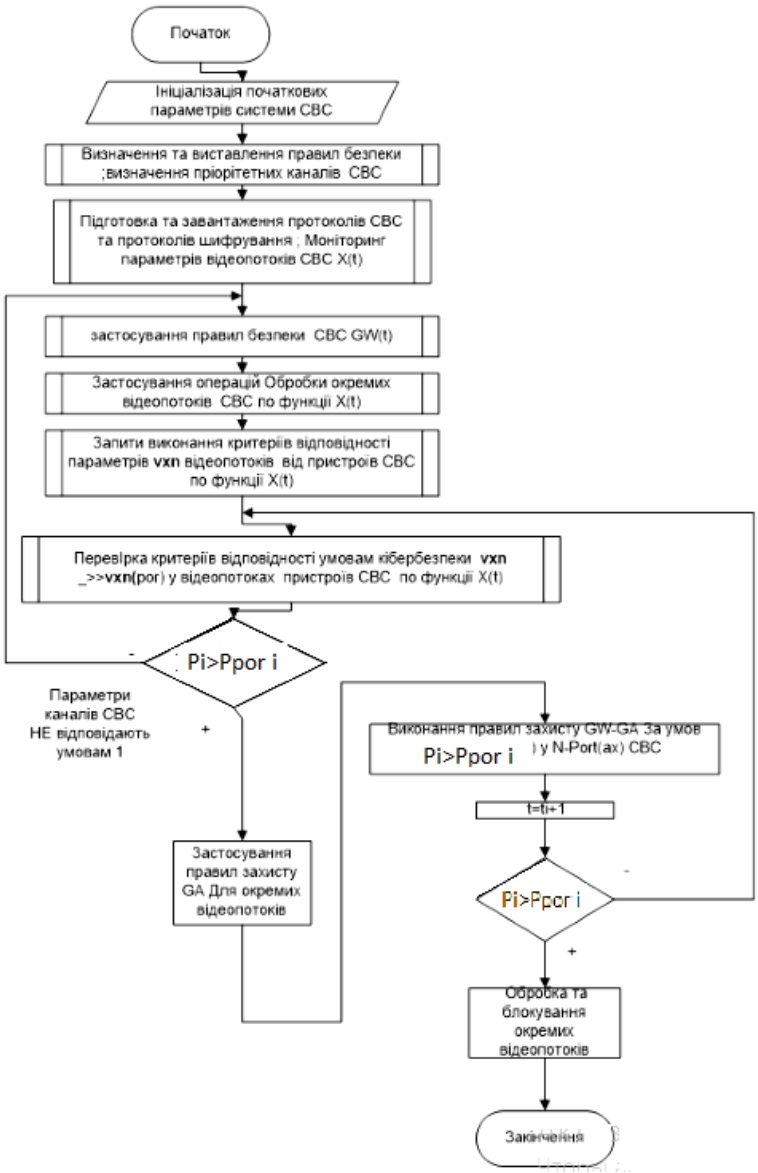
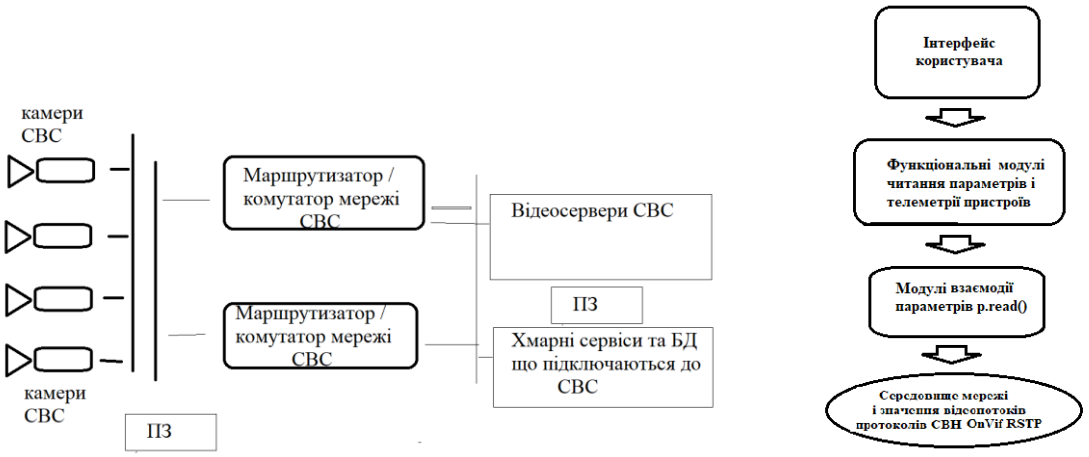


Рисунок 3.4 – Вдосконалений алгоритм кіберзахисту СВС

Алгоритм (Рис. 3.4) передбачає використання засобів захисту СВС згідно моделі (рис.2.2, розділ 2) і реагування на кіберцінцидент по групі умов *pi (як* правило по 4-м умовам), які забезпечують більш чіткий контроль за станом кібербезпеки СВС.

3.4 Структурна організація кіберзахисту в СВС на різних рівнях

Структрна організація на різних рівнях систем СВСв секторі охорони здоров'я із розподіленим збереженням показана на рис. 3.4.



а) б)

Рисунок 3.4 –Структурна організація кіберзахисту СВС : а) структура СВС із ПЗ моніторингу камер; б) структура ПЗ модуля для моніторингу камер СВС

ПЗ модуля для моніторингу камер СВС і структура СВС на базі алгоритму кіберзахисту передбачають використання як однієї, так і декількох ознак(умов) *1xn* створення кіберінциденту, по параметру із порогом ймовірності *pi*, які більш точно перевіряють наявність кіберзагрози і можуть забезпечити високий рівень кіберзахисту (згідномоделі рис.3.2) для СВС у медичному секторі із більш чіткий контроль можуть використовуватись в структурі рис.3.4, саме на пристроях мережевого рівня, де запроваджується засіб контролю і підвищення кіберзахисту СВС на цій основі. Універсальна версія алгоритму (рис.3.3-рис.3.4) показаний на рис.3.5. Дана блок-схема (рис.3.5) передбачає використання груп и параметрів *4xn*, і *p*i, для визначення кіберзагрози та її блокіівання по каналу СВС згідно моделі (рис.2.2, розділ 2) на рівні мережевої архітектури різними засобами. Даний алгоритм (рис.3.5) перевіряє фактор кіберзагрози в СВС та здійснює її оперативну агрегацію і нейтралізацію. Універсальна розподілена структура ПЗ модуля моніторингу СВС показана на рис.3.6.

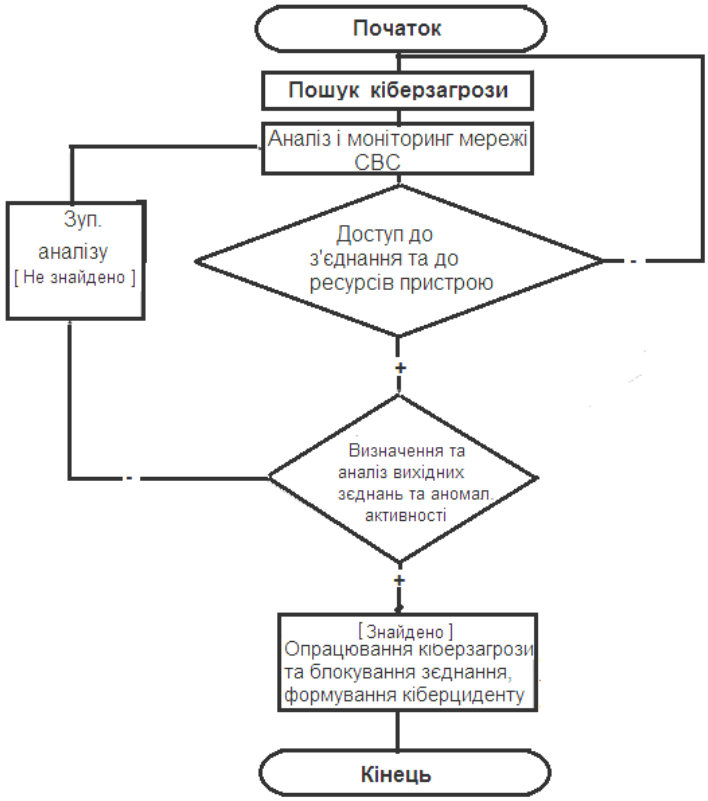


Рисунок 3.5 – Спрощений універсальний алгоритм формування кіберінциденту в СВС медичного сектору

Для забезпечення високого рівня кіберзахисту СВС в медичном секторі алгоритм (рис.3.5) може використати декілька засобів безпеки в СВС.

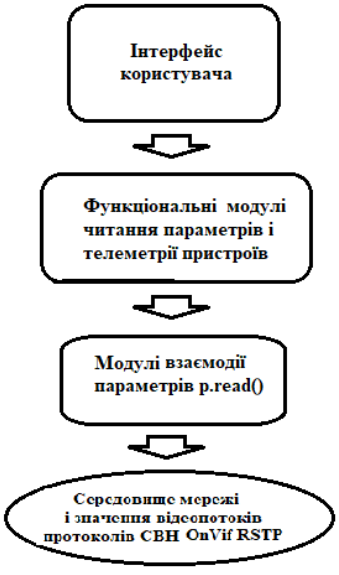


Рисунок 3.6 – Розроблена універсальна структура ПЗ моніторингу камер СВС

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАСОБІВ КІБЕРЗАХИСТУ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ СЕКТОРУ ОХОРОНИ ЗДОРОВ'Я

4.1 Реалізація програмних модулів моніторингу камер СВС для забезпечення їх кіберзахисту

Реалізація передбачає використання бібліотек моніторингу та окремих функцій на мові Python для роботи із відеокамерами СВС.

Окремий блок коду налаштування роботи СВС (на мові програмування Python): Зокрема налаштування технології e-Active PVS про повідомлення кіберінцидентів в СВС буде показаний нижче:

Для того, щоб моніторити камер використовується функція яка сканує IP-камери в мережі:

```
def scan_local_network(ip_range="192.168.1.0/24"):
    print(f"[+] Сканування локальної мережі {ip_range}")
    arp = ARP(pdst=ip_range)
    ether = Ether(dst="ff:ff:ff:ff:ff:ff")
    packet = ether/arp
    result = srp(packet, timeout=3, verbose=0)[0]
    devices = []
    for sent, received in result:
        devices.append({'ip': received.psrc, 'mac': received.hwsrc})
    return devices
```

Для цього потрібно імпортувати декілька зі стандартних бібліотек у Python:

```
import nmap
import requests
import time
```

Сам блок коду сканера визначений як:

```
# встановлюємо ралежності через pip bash:
pip install scapy requests python-nmap
Код утиліти (python юазова версія 1.0):
python :

import nmap
import requests
```

```
from scapy.all import ARP, Ether, srp
# Відомі порти камер
CAMERA_PORTS = [80, 443, 554, 554, 8000, 8080, 3702]
# CVE keywords
KNOWN_VULN_KEYWORDS = {
   "hikvision": ["CVE-2021-36260", "CVE-2017-7921"],
   "dahua": ["CVE-2021-33044", "CVE-2018-9995"],
}
def scan_local_network(ip_range="192.168.1.0/24"):
   print(f"[+] Сканування локальної мережі {ip_range}")
   arp = ARP(pdst=ip_range)
   ether = Ether(dst="ff:ff:ff:ff:ff:ff")
   packet = ether/arp
   result = srp(packet, timeout=3, verbose=0)[0]
   devices = []
   for sent, received in result:
      devices.append({'ip': received.psrc, 'mac': received.hwsrc})
   return devices
      else:
         print("  > Камера не реагує або порти закриті")
if __name__ == "__main__":
   main()
```

Можно дещо вдосконалити код ПЗ модуля, додавши у нього : виявлення ONVIF/RTSP сервісів глибше; перевірка за базою Shodan (через API); графічний інтерфейс (на Tkinter або PyQt); логування та вивід у CSV.

Повний код цього програмного модуля наведений в додатку В.

Дана підпрограма дозволяє отримувати дані із камер СВС, моніторити їх кібербезпеку, як це показано на рис. 4.1.

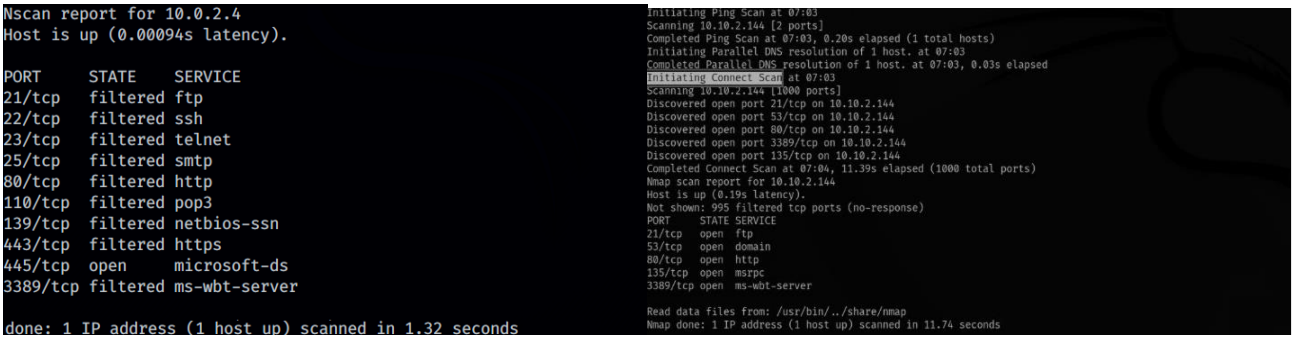


Рисунок 4.1 - Результати роботи програми моніторингу камер СВС та їх безпеки

Модуль (у вигляді бібліотеки) nmap наразі не встановлений у середовищі. Щоб ПЗ працювало локально, потрібно встановити залежності вручну:

Команди встановлення додаткових модулів (bash):

```
pip install python-nmap scapy requests shodan
```

Підтримка ONVIF (wsdl) (bash):

```
pip install onvif-zeep
```

Це дозволить: отримати список сервісів камери; перевірити підтримку ONVIF; запитати профілі відео.Для того щоб зробити нагадування про сервіс безпеки Shodan, точніше для його роботи (функція check_shodan(ip)) потрібно Зареєструватися на ресурсі URL: shodan.io, отримати API-ключ. Вставити цей API-ключзамість YOUR_SHODAN_API_KEY_HERE у коді програми (додаток В.).Також, потрібно звернути увагу що потрібно вказувати правильний шлях до WSDL-файлів. Найпростіший варіант — викликати ONVIF Camera без параметра wsdl_dir, і бібліотека сама знайде файли, наприклад,

```
cam = ONVIFCamera(ip, port, username, password)
```

Оновлена частина analyze_camera() з ONVIF (python):

```
def analyze_camera(ip, open_ports):
    suspicious = []
    if len(open_ports) > 5:
        suspicious.append("Занадто багато відкритих портів")
    for port in open_ports:
        banner = grab_banner(ip, port)
        vuln_info = detect_vulns(banner)
        if "hikvision" in banner.lower() or "dahua" in banner.lower():
            suspicious.append(f"Виявлено камеру: {banner}")
        if vuln_info:
            suspicious.append(vuln_info)
    suspicious.append(check_shodan(ip))
    if 3702 in open_ports or 80 in open_ports:
        try:
            from onvif import ONVIFCamera
            cam = ONVIFCamera(ip, 80, "admin", "admin")
            devicemgmt = cam.create_devicemgmt_service()
            info = devicemgmt.GetDeviceInformation()
            suspicious.append(f"[ONVIF] Модель: {info.Model}, Виробник: {info.Manufacturer}")
        except Exception as e:
            suspicious.append(f"[ONVIF] Не вдалося підключитись: {e}")
    return suspicious
```

Цей код дозволяє : сканувати IP-камеру у локальній мережі; виконати аналіз відкритих портів камер СВС; пошук CVE за банерами; підтримку ONVIF (wsdl); інтеграція із сервісом тестування безпеки Shodan; підтримку інтерфейсу; збереження даних в CSV. Для безпеки: потрібно згенерувати файл camera_scanner.spec або упакувати GUI з авторизацією та вибором збереження

*.CSV.

Базові функції доступу до IP-камер через ONVIF (стандарт для управління IP-камерами) та RTSP, з поясненнями для кожного блоку.

Приклад блоку підключення та читання відеопотоку з IP-камери через ONVIF (для виявлення/отримання URL потоку) та RTSP (для перегляду відео). Все написано на Python із використанням популярних бібліотек: zeep — для роботи з ONVIF; Onvif-Zeep або onvif-py — ONVIF клієнт ; cv2 (OpenCV) — для читання RTSP-потоку. Функції ONVIF + RTSP доступ до IP-камери:

```
from onvif import ONVIFCamera
import cv2
# --- ONVIF частина ---
def get_rtsp_url_onvif(host, port, username, password):
    # Підключення до ONVIF сервісу
    cam = ONVIFCamera(host, port, username, password)
    # Отримання сервісу медіа
    media_service = cam.create_media_service()
    # Отримання профілів (налаштувань відео)
    profiles = media_service.GetProfiles()
    profile = profiles[0]  # Вибір першого профілю

    # Отримання URL RTSP
    stream_setup = {
        'StreamSetup': {
            'Stream': 'RTP-Unicast',
            'Transport': {'Protocol': 'RTSP'}
        },
        'ProfileToken': profile.token
    }

    uri = media_service.GetStreamUri(**stream_setup)
    return uri.Uri
```

Даний блок коду (ПЗ модуль) дозволяє отримувати дані із камер СВС, моніторити їх кібербезпеку, як це показано на рис.4.2.

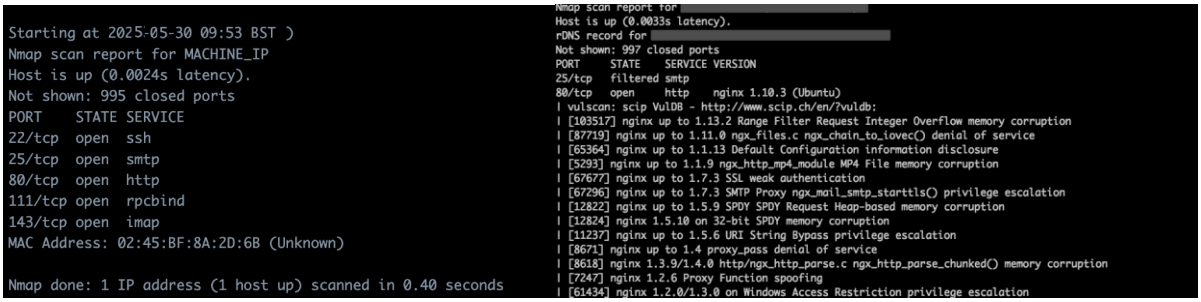


Рисунок 4.2 – Результати роботи ПЗ модуля сканування камер і хостів СВС

По результатам аналізу рис.4.2 можно побачити ряд вілкритих портів у мережі, до якої входять хости на прикладі камер СВС, що свідчить про функціональність програмного модуля і можливість використання її для аудиту і контролю безпеки існуючих мереж СВС.

4.2 Розробка сервісних кодів моніторингу інцидентів кібербезпеки в СВС

У більшості систем СВС, які працюють із IP-камерами по протоколу RSTP, відеопотік ділиться на 1-йосновний і 2-й додатковий : основний потік URL і Субпотік URL . Для цього необхідно вказати строку запиту протоколу RTSP-потоку, у форматі:

rtsp://[Login]:[Password]@[IP-adres]:[Port]/[Request]

• Логін(Login) і Пароль(Password) користувача, які зберігаються на самому пристрої - камері СВС.
• IP-адреса (IP-adres)- ip-адреса пристрою (камери СВС), до якій відбувається підключення.
• Порт(Port)- номер RTSP-порта мережевого IP-пристрою (відеокамери СВС). Сам Порт відрізняється від номеру порту WEB-інтерфейсу, зазвичай для RSTP 554).
• Запит(Request) - власне строка запиту RTSP-потоку.

Основний потік (1-й) – це відеодані високої якості від камери СВН, призначені для детального перегляду подій відеосигналу, з камери СВН. Даний потік буде записуватись у архів.

Додатковий потік(2-1) - це відеодані власне низької якості, потрібні для відображення декількох відеоканалів на одному екрані можно організувати функцією

```
ask()
def DF(n):
   message("Введіть будьласка параметри стану СВС, %s!" % n)
def fail():
   alert("СВС не відповідає !")
DF("Запуск СВС. Введіть початкові дані)
```

```
DF("Запуск СВС. Введіть початкові дані, 60символів , "пароль")
```

Програма після завершення виклакає одну із доступних функцій. 1-ша функція повинна бути із одним параметром, уякий записується дані параметрів. 2-гафункція викликає при натисканні кнопка Esc.

Можно вказати затримку у [с], після якого вікно ПЗ само закриється із відміною процесів, а також початкову строку станів

```
question()

def yes(): message(1)
def no(): message(2)
def dont_know(): message(3)
def other(): message(4)
question("Чи надійно підключено з‘єднання ?",
   "Так", yes,
   "Ні", no,
   "Не відомо", dont_know,
(60)
```

Інший код скрипта (на мові програмування Python) дозволяє виявляти події на камерах по умові, наприклад коли виникає рух в полі зорукамер, то він створює подію .приклад функції (Python):

```
def show_channel_with_motion(event):
 object("Інтерфейс  [Ім‘я сервера СВС]").\
 show_channel(event.origin,2)
activate_on_events("Motion Start", "", show_channel_with_motion)
```

Окремий блок коду програми опрацювання і взаємодії із СВС (на мові програмування Python) показиний в додатку В. Код може бути реалізований окремим модулем у ПЗ вищого рівня і дозволяє опрацьовувати кібербезпеку і події в СВС (зокрема від сервера СВС по стороннім API). Сам цей код (на мові програмування Python) показаний у додатку В: перша (ver.1.0) і друга (ver.1.1) частини .

4.3 Реалізація програмних модулів визначення кіберінцидентів у СВС

Нижче наведено код, який формує простий кіберінцидент у вигляді події вимірювання станів завантаженості процеора сервера СВС . Рівень процесора сервера СВС.

```
from collections import deque
a = deque()
i = 0
l = 15 #довжина черги
t = 30000 #періодичність вимірів у [мс]
k = 85 #критичне завантаження центрального процесора
def iter_func():
 global a, i, l, t, k
 if len(a) >= l:
  a.popleft()
 i = settings("CPUhealth&status")["CPU_performanceusage"]
 a.append(i)
s = 0
 c = 0
        for j in xrange(0, len(a)):
s += a[j]
 c = s / l
 if c >= k :
 settings("health")["user_defined_health_indicator"] = 0
 else :
 settings("health")["user_defined_health_indicator"] = -1
 timeout(t, iter_func)
def start_script():
 iter_func()
start_script()
```

1. В цій частині

```
if len(a) >= l:
  a.popleft()
 a.append(i)
i = settings("health")["cpu_usage"]
```

кожну область перевіряє на предмет довжини черги і записує наступне значення навантаженості процесора сервера СВН:

2. В наступній частині коду сумується значення всіх елементів двухсторонніх черг визначено як:

```
s = 0
c = 0
for j in xrange(0, len(a)):
s += a[j]
```

3. Далі обчислюється середнє значення завантаженості СВС процесора із порівнянням його з критичними пороговим значеннями k(умова $p_i > p_{pori}$), наприклад 80%. Якщо середнє значення більше чи дорівнює критичному, стан сервера СВН вручну змінюється. Якщо середнє значення менше критичного,

стан сервера СВС переключається на нормальний:

```
 c = s / l
if c >= k :
 settings("health")["user_defined_health_indicator"] = 0
else :
 settings("health")["user_defined_health_indicator"] = -1
timeout(t, iter_func)
```

Даний код також може визначати простий потенційний кіберінцидент, який впливає на рівень стану кібербезпеки: і виявляє приховану програмну загрозу DoS – по каналам СВС; атаки і шкідливі запити (ін’єкції) по стороннім каналам і API. Тобто ті кіберзагрози, які завантажують сам процесор СВС.

4.4 Розрахунки і оцінки рівня захищеності СВС для сектору охорони здоров'я у випадку впливу кіберзагрози

Для розрахунків і оцінок основних показникі були використані формули і математичні залежності, наведені у розділі 2 БКР, зокрема по (2.1) - (2.3).

Так, для оцінки ймовірностей бралась тестова базова СВС із 10 камер відеоспостереження і 1 відеосервером і 1 комутатором, яка має всі ризики і фактори, вказані у табл..2.2.-табл.2.4(розділ 2.). Результати оцінок ймовірностей атак у СВС га базі формули (2.1) наведені у табл.4.1.

Таблиця 4.1 – Результати оцінок кіберзахисту у моделі СВС із 10камер

Тип атаки	**Основні рівня ризику pi, Sum[pi]=1**	**Умовний рівень захищеноті СВС (1-10)s***	**Можливість нейтралізаї загрози**
Ненадійні паролі та облікові дані	0.6-0.65	2-3	так
Відкриті порти (RTCP, HTTP, Telnet, SSH)	0.12-0.15	1-2	так, частково
Неоновлене ПЗ або вразливі прошивки камер	0.08-0.1	1-3.	так, частково
Недостат.Зашифр. канали (відеопотік, API) та використання RAT	0.12-0.16	0.5-1	ні
Атаки через ONVIF, UPnP і P2P	0.08-0.11	1-3	ні
Ін'єкції через веб-інтерфейс	0.05-0.1	1-4	так, частково

Аналіз ризиків і рівня захисту від кібератак на СВС (табл. 4.1) дозволяє оцінити необхдні заходи і створювати перелік заходів для захисту системи відеоспостереження для медичного сектору із менш вразливими компонентами і мережею для деякних типів кібератак.

Припустимо, що в системі СВС наявні такі фактори і сценарії:

Т1 (несанкціонований доступ до камери): P(I1)=0.15, L1=100

Т2 (перехоплення трафіку): P(I2)=0.21, $L$2=200 (Psum=0.36)

Захисний захід L1 (шифрування даних в протоколів СВС- RSTP): P(I1)=0.9

Обчислення умовного рівня ризику кіберзагрози на основі ймовірності:

Ризик без захисних заходів:

R1=P(I1)×$L$1=0.15×100=15ум.одиниць.

R2=P(I2)×$L$2=0.21×200=44 ум. –.

Загальний ризик без захисних заходів:

Rtotal_без_захисту=$R$1+$R$2=15+44=59 ум. одиниць.

Загальний ризик з урахуванням захисних заходів:

Rtotal із захистом=($R$1×(1−P(I1)))+($R$2×(1−P(I1))) =32 ум. одиниць.

$P(I_{sum})$ із захистом=[(15×(1−0.9)) ×Li+(44×(1−0.9))]x0.1=(1.5+4.4)=0.23.

Це свідчить про зменшення ризику та підвищення захищеності при застосуванні цільових заходів захисту.

ВИСНОВКИ

Бакалаврська кваліфікаціна робота присвячена розробці захищеної системи відеоспостередення для сектору і закладів охорони здоров'я із виявленням і реагуванням на атаки на камери і інші пристрої відеоспостереження. У процесі виконання роботи було проведено аналіз наявних ризиків кібербезпеки для СВС, аналіз технологій і методів захисту систем відеоспостереження. Проаналізовані основні кіберзагрози та кібербезпеки у різних пристроях СВС, які використовуються у закладах охорони здоров'я. Проаналізовано основні кібератаки із врахуванням специфіки і вразливостей СВС у лікарнях. Проаналізовані проблеми кібербезпеки протоколів OnFiv та RTSP у СВС. Це дозволило визначити основні вимоги та рекомендації кібербезпеки. На основі проведеного аналізу було розроблено модель кіберзахисту СВС, захищену структурну схему СВС та алгоритм роботи захисту для закладів охорони здоров'я. Це дозволяє будувати більш інформаційно захищену систему відеоспостередення, що може використовуватись у біомедичному секторі. Така СВС базується на комплексному підході кіберзахисту. Розроблено програмний модель для моніторингу стану камер відеоспостереження, що доволяє їх моніторити і використовується в складі захищеної СВС для закладів охорони здоров’я. ПЗ модуль дозволяє вихначати прості, елементарні інциденти в мережах СВС шляхом сканування мережевої інфраструктури і активності пристроїв. Дані програмний модуль дозволяють виявляти базові проблеми захищеності СВС, що є практично потрібними рішеннями для їх безпеки СВС.

Проведений аналіз інформаційних та кіберзагроз в системах СВС допомагає ідентифікувати потенційні ризики та розробити структури і заходи захисту систем відеоспостереження для закладів охорони здоров’я для захисту відеоданих, безпечного налаштування і експлатації СВС поряд із іншими інформаційними системами в медичних закладах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Метик А. В., Сєвєрінов О. В. Аналіз загроз безпеки в системах безконтактної передачі даних [Електронний ресурс:] / Conferences thesis. – 2021. – Тип доступу URL: https://openarchive.nure.ua/handle/document/15762 (дата звернення: 05.03.2025).

2. Маліновський В.І. Сучасні кіберзагрози і захист даних в системах і пристроях інтернету речей [Електронний ресурс:] /**Між**народна Інтернет-конференція. – 2022. – с.63-73. – Тип доступу URL: http://konferenciaonline.org.ua/ua/article/id-595/ дата звернення: 05.03.2025).

3. Топчій Н.В. Аналіз захищеності IP-камер відеоспостереження [Електронний ресурс] : / Н.В Топчій, О.С. Білевська // Інформатика, обчислювальна техніка та автоматизація (Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки). – № 3. – 2021. – с.157-161. – Режим доступу URL: https://www.tech.vernadskyjournals.in.ua/journals/2021/3_2021/27.pdf (дата звернення 09.05.2025р.).

4. Кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури / Ю. І. Катков, С. О. Сєрих, А. В. Шашлов, Д. С. Вергун // Наукові записки Державного університету інформаційно-комунікаційних технологій. – № 3. – 2019. – с.63-73.

5. Аналіз систем відеоспостереження. [Електронний ресурс]./ Портал ukrbukva.net.– Режим доступу: URL: http://ukrbukva.net/page,2,73985-Analiz-sistm-videonablyudeniya.html (дата звернення 09.05.2025р.).

6. Відеоспостереження і охоронні системи. [Електронний ресурс]. / Портал secur.ua.– Режим доступу: URL: http:// https://secur.ua. (дата звернення 09.05.2025р.)

7. Технології для відеоспостереження [Електронний ресурс] / Портал viatec. – Режим доступу: URL: https://viatec.ua (дата звернення 09.05.2025р.).

8. Відеоспостереження, спеціалізована відеотехніка [Електронний ресурс] / Портал Bezpeka-shop. – Режим доступу до ресурсу: https://www.bezpeka-shop.com.

9. Алтуєв М. Перспективи розвитку цифрового CCTV. Думки фахівців //

Алгоритм Безпеки. – 2004. – № 5. - 57с.

10. Гринюк С., Поліщук М. Використання технології шифрування інформації для безпечної передачі в мережі. *Computer-Integrated Technologies: education, science, production*. – 2020. – № 39. – С. 122–126. URL: https://doi.org/10.36910/6775-2524-0560-2020-39-21 (дата звернення: 06.03.2025).

11. Дейбук В.О. Проблеми побудови систем відеоспостереження у медичних закладах» [Електрониий ресурс] / Тези доповідей науково-технічну конференцію «Молодь у науці 2025», ВНТУ, 2025. – 2с , Режим доступу URL: https://kbwww.b.conferences.vntu.edu.ua/index.php/mn/mn2025/paper/view/25680/21179

12. Системи відеоспостереження -[Електроний ресурс]. – Режим доступа: https://bezpeka.club/ ; URL:http://www.elvis.com.ua/ua/cctv-ua.html

13. Відеокамери види та різниця – [Електронний ресурс]. – Режим доступу: URL:http://www.bezpekacity.com.ua

14. Види систем відеоспостереження - [Електронний ресурс]. – Режим доступу: URL:https://ohrana.ua/uk/stati-i-obzory/vidi-sistem-videonablyudeniya.html

15. Все про відеокамери – [Електронний ресурс].– Режим доступу до ресурсу: https://pipl.ua

16.PoE-комутатори в системах відеоспостереження [Електронний ресурс]. – Режим доступу: URL: https://worldvision.com.ua/dlya-chego-nuzhny-poe-kommutatory-vsistemakh-videonabludeniya/

17. Загальний підхід до проектування систем відеоспостереження [Електронний ресурс]. – Режим доступу: URL: http://solis.in.ua/zahalnyj-pidhid-do-proektuvannya-systemvideosposterezhennya.html

18. Інтегровані системи безпеки відеоспостереження [Електронний ресурс]. – Режим доступу: URL: https://відеокамери.com.ua/integrovani_sustemu_bezpeku/

19. Проект відеоспостереження //[Електронний ресурс]. –

Режим доступу: URL:
https://www.vostok.dp.ua/ukr/infa1/sistemy_vidyeonablyudeniya/psv/
20. Проектування системи відео спостереження // Режим доступу:
https://відеокамери.com.ua/proektyvannya_videosposterejennya/
21.Erez Yalon. Exposing Wireless IP Camera Security Flaws. [Електронний ресурс] . – Тип доступу URL: www.checkmarx.com. (дата звернення: 01.05.2025).
22. Орлов С. IP-камери з інтеллектом. . –Журнал мережевих рішень LAN. . – 2013. . –№ 11. . –С. 44–63.
23. Paul Barry. Head First Python: A Brain-Friendly Guide – 2016. – 622 с.
24.Анісімов А.В. Цифрова автентифікація: досягнення та перспективи // Вісник НАН України, 2023. – Вип. №8. – С. 65-68.
25. Типи мережевих протоколів і їх призначення (HTTP, IP, SSH, FTP, POP3, MAC) - [Електронний ресурс]. – Режим доступу URL: https://deltahost.ua/ua/tipi-merezhevix-protokoliv-i-ih-priznachennya-http-ip-ssh-ftp-pop3-mac.html?srsltid=AfmBOoozjtGwq-ubst0Z9_BbrdafEM_anovQgij_T75bzoBMFd4RLzuf (дата звернення: 01.05.2025).
25. Протоколи RTP і RTSP - [Електронний ресурс]. – Режим доступу: URL: https://wiki.cusu.edu.ua/index.php/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8_RTP_%D1%96_RTSP
27. Що таке протокол OnVif- [Електронний ресурс]. – Режим доступу: URL: https://greenvision.ua/ua/blog/chto-takoe-protokol-ONVIF?srsltid=AfmBOopPlcY28m3os65kLPJSorVYY4gZY36r2KhBe99ttguizMlAlUPy
28. Системи відеоспостереження для безпеки будинку і офісу - [Електронний ресурс]. – Режим доступу: URL:
https://worldvision.com.ua/videonabludenie/
29. Монтаж камер відеоспостереження- [Електронний ресурс]. – Режим доступу: URL:https://shop-digital.com.ua/ua/blog/montazh-kamer-videosposterezhenniapokrokova-instruktsiia
30. Юкарчук Д., Логінова І. Штучний інтелект у системах автентифікації. Київ: Наукова думка. – 2019. –320 с.

Додатки

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Захищена система відеоспостереження для закладів охорони здоров'я

Автор роботи: Дейбук В'ячеслав Олександрович

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ, група 1БС-21 б

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **4,7 %**

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб приховання плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не допускається.

Експертна комісія:

Завідувач кафедри ЗІ д. т. н., проф. _____ Володимир ЛУЖЕЦЬКИЙ

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем» к. т. н., доц. _____ Леонід КУПЕРШТЕЙН

Особа, відповідальна за перевірку _____ Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Малиновський В.Т.

Здобувач _____ Дейбук В.О.

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Захищена система відеоспостереження для закладів охорони здоров'я

Автор роботи: Дейбук В'ячеслав Олександрович

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ, група 1БС-21 б

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **4,7** %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

√ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Завідувач кафедри ЗІ д. т. н., проф. _____ Володимир ЛУЖЕЦЬКИЙ

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем» к. т. н., доц. _____ Леонід КУПЕРШТЕЙН

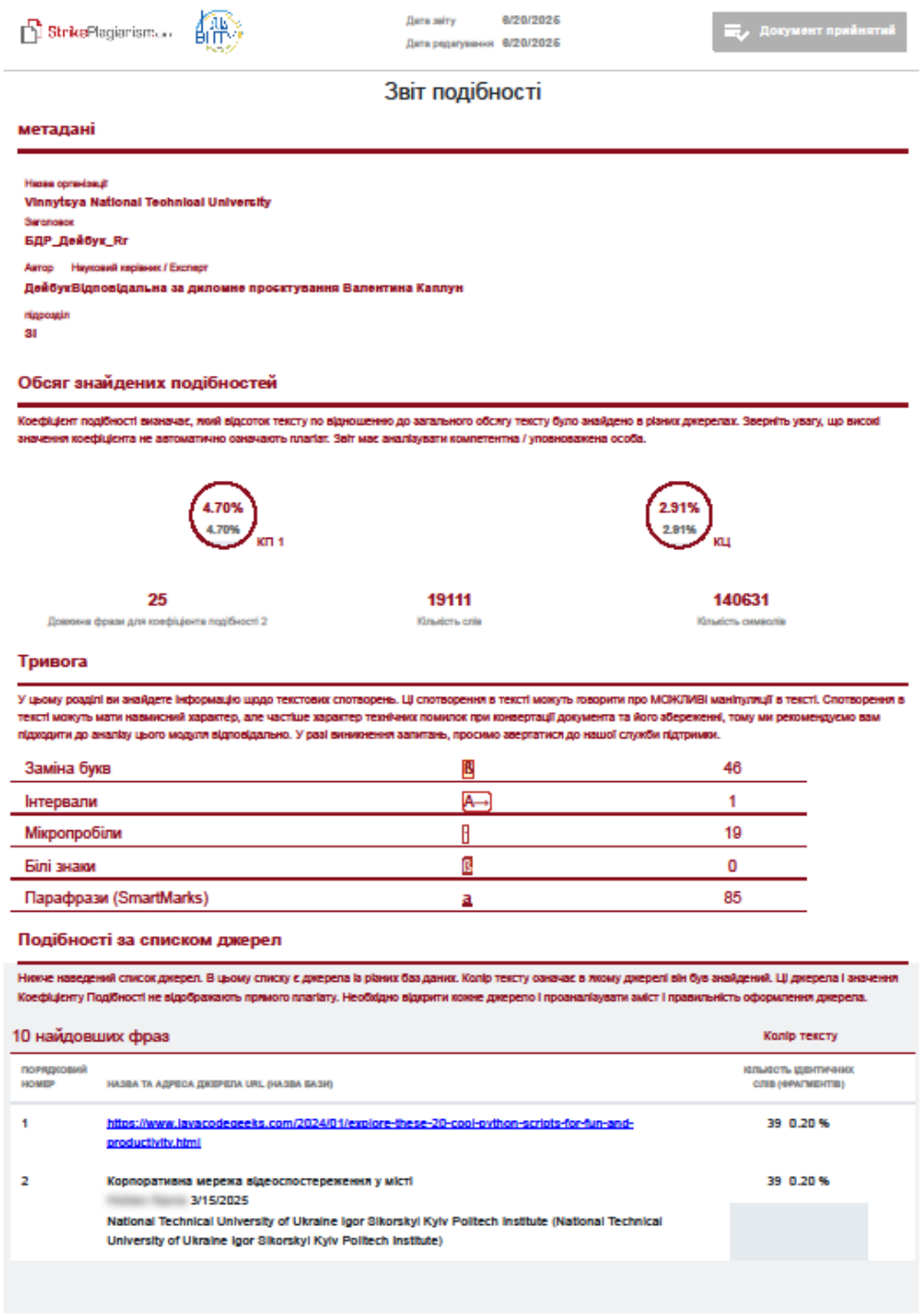
Особа, відповідальна за перевірку _____ Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник _____ _____

Здобувач _____ _____

Результати перевірки бакалаврської кваліфікаційної роботи на наявність текстових запозичень системою StrikePlagiarism



StrikePlagiarism.com

Дата звіту 6/20/2025
Дата редагування 6/20/2025

Документ прийнятий

Звіт подібності

метадані

Назва організації
Vinnytsya National Teohnloal University
Заголовок
БДР_Дейбук_Rr
Автор Науковий керівник / Експерт
ДейбукВідповідальна за дипломне проєктування Валентина Каплун
підрозділ
ЗІ

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

4.70% 4.70% КП 1

2.91% 2.91% КЦ

25	19111	140631
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		46
Інтервали		1
Мікропробіли		19
Білі знаки		0
Парафрази (SmartMarks)		85

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз | Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://www.javacodegeeks.com/2024/01/explore-these-20-cool-python-scripts-for-fun-and-productivity.html	39 0.20 %
2	Корпоративна мережа відеоспостереження у місті [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	39 0.20 %

Додаток Б

Код конфігурації мережевих екранів СВС

Нижче представлений сам код системної конфігурації мережевого екрану(FW/NGFW) представлений для моделей Cisco ASA 5505-5506, який забезпечує фільтрацію трафіку і відео потоків по відео портам протоколу RSTP для камер СВС для їх захисту в мережі СВС.

Передбачено що в СВС використано 2 взаємоповязаних мережевих екрани FW/NGFW, як це показано на структурі рис.3.1.

Початкові налаштування мережевого екрану SW0(Cisco command line):

SW1(config)#**interface fa0/12**
SW1(config-if)#**shutdown**
SW1(config)#**interface f0/16**
SW1(config-if)#**shutdown**
SW1(config)#**interface fa0/12**
SW1(config-if)#**no shutdown**
SW1#
setting bridge id (which=3) prio 4097 prio cfg 4096 sysid 1 (on) id 1001.0011.bb0b.3600
RSTP(1): initializing port Fa0/12
RSTP(1): Fa0/14 is now designated
RSTP(1): transmitting a proposal on Fa0/12
The fa0/14 interface on SW1 will be blocked and it'll send a proposal to SW2.
Режим відлагодження (debug mode):
SW1#**debug spanning-tree events**
Режим відлагодження для Spanning Tree (Налаштування режим відлагодження (протоколу Spanning Tree)
SW2#**debug spanning-tree events**
Spanning Tree event debugging is on
SW2#**debug spanning-tree events**
SW0(config)#**spanning-tree mode rapid-pvst**
SW2(config)#**spanning-tree mode rapid-pvst**
SW2(config)#**spanning-tree mode rapid-pvst**
SW2#
RSTP(1): initializing port Fa0/12
RSTP(1): Fa0/14 is now designated
RSTP(1): transmitting a proposal on Fa0/12
RSTP(1): updt roles, received superior bpdu on Fa0/12
RSTP(1): Fa0/12 is now root port

Налаштування другого мережевого екрану для СВС SW2 в режимі повного адміністратора(root) здійснюється через основний магістральний лінк типу «міст»,

оскільки він отримав верхній BPDU на своєму інтерфейсі FA0/12. Він змінює свій інтерфейс FA0/12 на магістральний порт. Інтерфейс FA0/15 на SW2 тепер перейде в режимSync Mod:SW2# RSTP(1): syncing port Fa0/15. Цей інтерфейс, який під'єднані до SW2 відповість на SW1 надіславши запит на з'єднання :

SW2# RSTP(1): synced Fa0/12
RSTP(1): transmitting an agreement on Fa0/14 as a response to a proposal
Ми можемо побачити це на vtht;tdjve засобі (роутері вбо комутаторі) SW1 as well:
SW1# RSTP(1): received an agreement on Fa0/12
%LINK-3-UPDOWN: Interface FastEthernet 0/12, змінив стан на „Up"
%LINEPROTO-5-UPDOWN: лінійний протокол на інтерфейсі Interface FastEthernet0/12, змінив стан на „Up"
SW1 отримує підтвердження від SW2 і інтерфейс fa0/12 буде прокинуто до SW2 , і також буде надіслані пакети на інші сегменти мережі (робить доступними проходження пакетів на інші сегменти мережі):
SW2# RSTP(1): transmitting a proposal on Fa0/15
Коли SW2 отримає його, він надішле запит на з'єднання:
SW3# RSTP(1): dslcbkf' запит на з'єднання yf synthatqcs Fa0/15, який надсилає контрольні запити
SW2отримує запит-підтвердження від SW1:
SW2# RSTP(1): отримує запит-підтвердження від на інтерфейсі Fa0/15
%LINK-3-UPDOWN: Інтерйфейс (Interface) FastEthernet0/14, змінив стан на „Up"
Стан портів (Port States):
SW1(config)#**interface fa0/16**
SW1(config-if)#**no shutdown**
Моєна переглянути стани:
SW1#**show spanning-tree**
Налаштування сегментації мережі шляхом VLAN:
VLAN0001

Реультати роботи налаштувань:

Протокол STP дозволяє протокол RSTP (Spanning tree enabled protocol rstp), вкл. підтримки RTCP на TCP.

```
  Root ID    Priority    4097
             Address     0011.bb0b.3600
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0011.bb0b.3600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/14           Desg FWD 19        128.16   P2p
Fa0/17           Desg FWD 19        128.19   P2p
```

Ми можемо перевірити, що фаєрволл SW1 – знаходиться в режимі

«магістрального мосту». Команда „show“ також показує і виявляє, що ми проводимо швидке обстеження деревовидної топології. Зауважимо, що використовуються тип посилання - P2P(точка-точка). Це тому, що мої інтерфейси FastEthernet за замовчуванням в повному дуплексі. Давайте запустимо ту саму команду на інших двох мережевих екранах:

```
SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     0011.bb0b.3600
             Cost        19
             Port        15 (FastEthernet0/12)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 10 sec
  Bridge ID  Priority    8193   (priority 8192 sys-id-ext 1)
             Address     0019.569d.5700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface          Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/12             Root FWD 19        128.16   P2p
Fa0/15             Desg FWD 19        128.18   P2p
SW3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     0011.bb0b.3600
             Cost        19
             Port        12 (FastEthernet0/12)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000f.34ca.1000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/14           Root FWD 19        128.14   P2p
Fa0/16           Altn BLK 19        128.16   P2p
```

Налаштування BPDU

Протокол BPDUs надсилає кожні дві секунди hello-запити (hello baecon):

```
SW2#debug spanning-tree bpdu
```

Можемо використовувати команду BPDU налагодження, щоб переглянути або отримані або отримані BPDU.

```
SW2#
STP: VLAN0001 rx BPDU: config protocol = rstp, packet from FastEthernet0/13  , linktype
```

IEEE_SPANNING , enctype 2, encsize 17
STP: enc 01 80 C2 00 00 00 00 11 BB 0B 36 10 00 27 42 42 03
STP: Data
000002023C10010011BB0B360000000000010010011BB0B3600801000001400020 00F00
STP: VLAN0001 Fa0/12:0000 02 02 3C 10010011BB0B3600 00000000 10010011BB0B3600 8010 0000 1400 0200 0F00
RSTP(1): Fa0/12 repeated msg
RSTP(1): Fa0/12 rcvd info remaining 6
RSTP(1): sending BPDU out Fa0/15
RSTP(1): sending BPDU out Fa0/16
STP: VLAN0001 rx BPDU: config protocol = rstp, packet f

Можемо побачити вміст BPDU вище. Якщо хочемо знати вміст BPDU, то засіб SW2 отримує BPDU і надсилає їх на свої інтерфейси. Якщо хочемо подивитися на вміст BPDU, можно використовувати Wireshark.

Додаток В

Код програми моніторингу камер СВС
(на мові програмування Phyton)

```
import nmap
import requests
from scapy.all import ARP, Ether, srp
import socket
import csv
import tkinter as tk
from tkinter import messagebox, filedialog, ttk
import threading
import shodan

# --- Константи ---
CAMERA_PORTS = [80, 443, 554, 8000, 8080, 3702]
KNOWN_VULN_KEYWORDS = {
    "hikvision": ["CVE-2021-36260", "CVE-2017-7921"],
    "dahua": ["CVE-2021-33044", "CVE-2018-9995"],
}

SHODAN_API_KEY = "YOUR_SHODAN_API_KEY_HERE"  # Замінити на свій ключ

# --- Мережеві функції ---
def scan_local_network(ip_range="192.168.1.0/24"):
    arp = ARP(pdst=ip_range)
    ether = Ether(dst="ff:ff:ff:ff:ff:ff")
    packet = ether/arp
    result = srp(packet, timeout=3, verbose=0)[0]
    devices = [{'ip': received.psrc, 'mac': received.hwsrc} for sent, received in result]
    return devices

def scan_ports(ip):
    nm = nmap.PortScanner()
    nm.scan(ip, arguments='-Pn -T4 --open -p ' + ",".join(map(str, CAMERA_PORTS)))
    open_ports = []
    if ip in nm.all_hosts():
        for proto in nm[ip].all_protocols():
            for port in nm[ip][proto]:
                open_ports.append(port)
    return open_ports

def grab_banner(ip, port):
    try:
        url = f"Помилка."
        response = requests.get(url, timeout=3)
        return response.headers.get('Server', 'Unknown')
    except:
```

```
        return "Unknown"

def detect_vulns(banner):
    lower_banner = banner.lower()
    for brand, cves in KNOWN_VULN_KEYWORDS.items():
        if brand in lower_banner:
            return f"[!!!] Потенційна уразливість: {brand.upper()} → {', '.join(cves)}"
    return ""

def check_shodan(ip):
    try:
        api = shodan.Shodan(SHODAN_API_KEY)
        host = api.host(ip)
        return f"[Shodan] {host['org']} | {host.get('os', 'Unknown OS')}"
    except Exception as e:
        return f"[Shodan] Немає даних: {e}"

def analyze_camera(ip, open_ports):
    suspicious = []
    if len(open_ports) > 5:
        suspicious.append("Занадто багато відкритих портів")
    for port in open_ports:
        banner = grab_banner(ip, port)
        vuln_info = detect_vulns(banner)
        if "hikvision" in banner.lower() or "dahua" in banner.lower():
            suspicious.append(f"Виявлено камеру: {banner}")
        if vuln_info:
            suspicious.append(vuln_info)
    suspicious.append(check_shodan(ip))
    return suspicious

def log_to_csv(results, filename="camera_scan_results.csv"):
    with open(filename, mode='w', newline='', encoding='utf-8') as file:
        writer = csv.writer(file)
        writer.writerow(["IP", "MAC", "Ports", "Аналіз"])
        for r in results:
            writer.writerow([r["ip"], r["mac"], r["ports"], "; ".join(r["issues"])])

# --- GUI ---
def start_scan():
    ip_range = ip_range_entry.get()
    results = []
    devices = scan_local_network(ip_range)
    for device in devices:
        ip = device['ip']
        ports = scan_ports(ip)
        issues = analyze_camera(ip, ports) if ports else ["Немає відкритих портів"]
        results.append({"ip": ip, "mac": device['mac'], "ports": ports, "issues": issues})
        output.insert(tk.END, f"\n{ip} ({device['mac']}) - {ports}\n")
```

```
        for issue in issues:
            output.insert(tk.END, f"  ⚠ {issue}\n")
        output.insert(tk.END, "-" * 40 + "\n")
    log_to_csv(results)
    messagebox.showinfo("Готово", "Сканування завершено. Звіт збережено у CSV.")

def threaded_scan():
    threading.Thread(target=start_scan).start()

# --- Ініціалізація вікна ---
root = tk.Tk()
root.title("IP-Камера Сканер")
root.geometry("700x500")

frame = ttk.Frame(root, padding=10)
frame.pack(fill=tk.BOTH, expand=True)

ttk.Label(frame, text="IP-діапазон:").pack()
ip_range_entry = ttk.Entry(frame, width=40)
ip_range_entry.insert(0, "192.168.1.0/24")
ip_range_entry.pack()

ttk.Button(frame, text="Сканувати мережу", command=threaded_scan).pack(pady=10)

output = tk.Text(frame, height=20, wrap=tk.WORD)
output.pack(fill=tk.BOTH, expand=True)

root.mainloop()
```

Вдосконаений код програми моніторингу камер СВС (код вдосконаленого ПЗ додатку)

#Встановлення необхідних бібліотек:(bash):

```
pip install onvif-zeep opencv-python
pip install onvif-zeep opencv-python
```

#Функції ONVIF + RTSP доступ до IP-камери:

```
from onvif import ONVIFCamera
import cv2
# --- ONVIF частина ---
def get_rtsp_url_onvif(host, port, username, password):
    # Підключення до ONVIF сервісу
    cam = ONVIFCamera(host, port, username, password)

    # Отримання сервісу медіа
    media_service = cam.create_media_service()

    # Отримання профілів (налаштувань відео)
    profiles = media_service.GetProfiles()
```

```
    profile = profiles[0]  # Вибір першого профілю

    # Отримання URL RTSP
    stream_setup = {
        'StreamSetup': {
            'Stream': 'RTP-Unicast',
            'Transport': {'Protocol': 'RTSP'}
        },
        'ProfileToken': profile.token
    }

    uri = media_service.GetStreamUri(**stream_setup)
    return uri.Uri

# --- RTSP потік (читання через OpenCV) ---
def read_rtsp_stream(rtsp_url):
    cap = cv2.VideoCapture(rtsp_url)

    if not cap.isOpened():
        print("Не вдалося підключитися до потоку")
        return

    while True:
        ret, frame = cap.read()
        if not ret:
            print("Кадр не зчитано")
            break

        cv2.imshow("IP-Камера", frame)

        if cv2.waitKey(1) & 0xFF == ord('q'):
            break

    cap.release()
    cv2.destroyAllWindows()

# --- Основна логіка ---
if __name__ == "__main__":
    # Вкажіть параметри вашої камери
    host = "192.168.1.23"
    port = 80  # зазвичай 80 або 8000
    username = "admin"
    password = "admin123"

    try:
        rtsp_url = get_rtsp_url_onvif(host, port, username, password)
        print("RTSP URL:", rtsp_url)
        read_rtsp_stream(rtsp_url)
    except Exception as e:
```

```
        print("Помилка:", e)

# --- Пояснення ---
# --- Компонент        - призначення
# --- ONVIFCamera   - створює підключення до камери через ONVIF
# --- GetProfiles()       - отримує доступні відеопрофілі камери
# --- GetStreamUri()  - повертає URL RTSP для заданого профілю
# --- cv2.VideoCapture()       -  підключається до потоку відео по RTSP
# --- cv2.imshow()     - показує зображення у вікні в реальному часі


# Інтерфейс GUI з автопошуком камер у мережі або інтеграцію з CVE-базою
#Функціонал: Сканування локальної мережі на ONVIF/RTSP камери
#Підключення по ONVIF → отримання RTSP
# Перегляд відео в реальному часі (OpenCV)
# Перевірка IP/прошивки/порта по базі CVE (Shodan API)
# Простий графічний інтерфейс (Tkinter)
#Бібліотеки, які потрібні (bash) :
pip install onvif-zeep opencv-python tk requests shodan netifaces
#Основний код (скорочена архітектура):

import cv2
import threading
import netifaces
import socket
import tkinter as tk
from tkinter import ttk
from onvif import ONVIFCamera
import shodan
import requests
# --- Автопошук камер у мережі ---
def scan_local_network(port=80):
    ips = []
    for iface in netifaces.interfaces():
        try:
            ip = netifaces.ifaddresses(iface)[netifaces.AF_INET][0]['addr']
            net = '.'.join(ip.split('.')[:-1]) + '.'
            for i in range(1, 255):
                try:
                    target = net + str(i)
                    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                    sock.settimeout(0.3)
                    result = sock.connect_ex((target, port))
                    if result == 0:
                        ips.append(target)
                    sock.close()
                except:
                    continue
```

```
        except:
            continue
    return list(set(ips))

# --- ONVIF: Отримання RTSP URL ---
def get_rtsp_url_onvif(host, port, username, password):
    cam = ONVIFCamera(host, port, username, password)
    media_service = cam.create_media_service()
    profiles = media_service.GetProfiles()
    profile = profiles[0]
    uri = media_service.GetStreamUri({
        'StreamSetup': {'Stream': 'RTP-Unicast', 'Transport': {'Protocol': 'RTSP'}},
        'ProfileToken': profile.token
    })
    return uri.Uri

# --- Читання RTSP потоку CBC---
def show_rtsp(rtsp_url):
    cap = cv2.VideoCapture(rtsp_url)
    while cap.isOpened():
        ret, frame = cap.read()
        if not ret:
            break
        cv2.imshow("Потік з IP-камери", frame)
        if cv2.waitKey(1) & 0xFF == ord('q'):
            break
    cap.release()
    cv2.destroyAllWindows()

# --- Перевірка за Shodan API ---
def check_cve_shodan(ip, api_key):
    try:
        api = shodan.Shodan(api_key)
        host = api.host(ip)
        vulns = host.get('vulns', [])
        return vulns
    except Exception as e:
        return [str(e)]

# --- GUI ---
class CameraScannerApp:
    def __init__(self, root):
        self.root = root
        root.title("IP-Камери безпека")

        self.ip_listbox = tk.Listbox(root, width=40)
        self.ip_listbox.pack()

        self.scan_btn = tk.Button(root, text="🔍 Сканувати мережу", command=self.scan_network)
```

```
        self.scan_btn.pack(pady=5)

        self.connect_btn = tk.Button(root, text=" Показати відео", command=self.connect_camera)
        self.connect_btn.pack(pady=5)

        self.cve_btn = tk.Button(root, text=" Перевірити за CVE (Shodan)",
command=self.check_cve)
        self.cve_btn.pack(pady=5)

        self.status = tk.Label(root, text="", fg="blue")
        self.status.pack()

        self.api_key = "ВСТАВТЕ СВІЙ API КЛЮЧ SHODAN"

    def scan_network(self):
        self.status.config(text="Сканування...")
        self.ip_listbox.delete(0, tk.END)
        ips = scan_local_network()
        for ip in ips:
            self.ip_listbox.insert(tk.END, ip)
        self.status.config(text="Сканування завершено")

    def connect_camera(self):
        try:
            selected_ip = self.ip_listbox.get(tk.ACTIVE)
            rtsp_url = get_rtsp_url_onvif(selected_ip, 80, "admin", "admin")  # змінити логін/пароль
            threading.Thread(target=show_rtsp, args=(rtsp_url,)).start()
        except Exception as e:
            self.status.config(text=f"Помилка: {e}")

    def check_cve(self):
        try:
            selected_ip = self.ip_listbox.get(tk.ACTIVE)
            vulns = check_cve_shodan(selected_ip, self.api_key)
            if vulns:
                self.status.config(text=f" Уразливості: {', '.join(vulns)}")
            else:
                self.status.config(text=" Уразливостей не знайдено")
        except Exception as e:
            self.status.config(text=f" {e}")

# --- Запуск ---
if __name__ == "__main__":
    root = tk.Tk()
    app = CameraScannerApp(root)
    root.mainloop()

#Для роботи потрібно зареєструй ключ API  на https://account.shodan.io/
```

```
# Можна додати логер, збереження журналу перевірок  :
# Приклади використання незахищених інтерфейсів в коді ONVIF, RTSP, HTTP через
 #уразливість ONVIF або RTSP без автентифікації або з дефолтними паролями через
#Експлойт (bash):
# Захоплення RTSP відео потоку без автентифікації
 ffplay rtsp://admin:admin@<ip>:554/stream1
```

Код додаткової утиліти для моніторингу RTSP -портів камер СВС (мова програмування Python)

```
import nmap, sys
# отримуємо  цільовой хост з аргументів командної строки
target = sys.argv[1]
# ініціалізуємо сканер портів Nmap
nm = nmap.PortScanner()
print("[]* Сканирование...")
# скануємо мережу СВС CCTV
nm.scan(target)
# отримуємо статистику скануванняя
scan_stats = nm.scanstats()
print(f"[{scan_stats['timestr']}] Пройшло часу: {scan_stats['elapsed']} с " \
   f"Активні  хости камер СВС: {scan_stats['uphosts']} Неактивні хости камер СВС:
{scan_stats['downhosts']} " \
   f"Всього хостів: {scan_stats['totalhosts']} ")
equivalent_commandline = nm.command_line()
print(f"[*] Інша команда: {equivalent_commandline}")
# отримуємо всі хости і камер в мережі СВС
hosts = nm.all_hosts()
for host in hosts:
 # отримуємо імя хосту
   hostname = nm[host].hostname()
 # отримуємо адресу
   addresses = nm[host].get("addresses")
   ipv4 = addresses.get("ipv4")
 # отримуємо MAC-адресу цього хоста/камери
   mac_address = addresses.get("mac")
 # Визначаємо постачальника обладнання,  якщо  доступний
   vendor = nm[host].get("vendor")
# Для кожного відсканованого хосту виймаємо його імя , IP-адрес і MAC-адресу, а також дані
про постачальника обладнання.
#  отримуємо відкриті  порти TCP, UDP та  RTSP
# отримуємо відкриті  TCP-порти
  open_tcp_ports = nm[host].all_tcp()
# отримуємо відкриті   UDP-порти
  open_udp_ports = nm[host].all_udp()
# отримуємо відкриті   RTSP-порти
# open_rtsp_port   s = nm[host].all_rtsp()
```

```
 # виводимо деталі
 print("=" * 30, host, "=" * 30)
 print(f"Ім'я хосту: {hostname} IPv4: {ipv4} MAC: {mac_address}")
 print(f"Виробник: {vendor}")
 if open_tcp_ports or open_udp_ports:
    print("-" * 30, "Відкриті порти", "-" * 30)
    for tcp_port in open_tcp_ports:
        # отримуємо всі доступні деталі порту
        port_details = nm[host].tcp(tcp_port)
        port_state = port_details.get("state")
        port_up_reason = port_details.get("reason")
        port_service_name = port_details.get("name")
        port_product_name = port_details.get("product")
        port_product_version = port_details.get("version")
        port_extrainfo = port_details.get("extrainfo")
        port_cpe = port_details.get("cpe")
        print(f"TCP-порт: {tcp_port} Стан : {port_state} Причина: {port_up_reason}")
        print(f"Служба: {port_service_name} Продукт: {port_product_name} Версія:
{port_product_version}")
        print(f"Додаткова інформація : {port_extrainfo} CPE: {port_cpe}")
        print("-" * 50)

        if open_udp_ports:
            print(open_udp_ports)

       # port_details = nm[host].udp(udp_port)
       # port_state = port_details.get("state")
       # port_up_reason = port_details.get("reason")
       # port_service_name = port_details.get("name")
       # port_product_name = port_details.get("product")
       # port_product_version = port_details.get("version")
       # port_extrainfo = port_details.get("extrainfo")
       # port_cpe = port_details.get("cpe")

       # print(f"UDP-порт: {tcp_port} Стан : {port_state} Причина: {port_up_reason}")
       # print(f"Служба: {port_service_name} Продукт: {port_product_name} Версия:
{port_product_version}")
       # print(f"Додаткова інформація          : {port_extrainfo} CPE: {port_cpe}")
       # print("-" * 50)

       if open_rtsp_ports:
           print(open_rtsp_ports)
       # port_details = nm[host].rtsp(rtsp_port)
       # port_state = port_details.get("state")
       # port_up_reason = port_details.get("reason")
       # port_service_name = port_details.get("name")
       # port_product_name = port_details.get("product")
       # port_product_version = port_details.get("version")
       # port_extrainfo = port_details.get("extrainfo")
```

```
        # port_cpe = port_details.get("cpe")

        # print(f"TCP-порт: {tcp_port} Стан: {port_state} Причина: {port_up_reason}")
        # print(f"Служба: {port_service_name} Продукт: {port_product_name} Версия:
{port_product_version}")
        # print(f"Додаткова інформація          : {port_extrainfo} CPE: {port_cpe}")
        # print("-" * 50)


  if open_udp_ports:
     print(open_udp_ports)

   # ----------------------------------------------\\\\\\----------------------------------------------
```

#Ми отримали відкриті TCP-порті за допомогою метода all_tcp(). Потім робимо перебір всіх відкритих портів і виводимо різноманітну інформацію від них (наприклад, службу, її версію, і т.п. .

#Добре ми можемо отримати відкриті TCP-порти за допомогою методу all_tcp(). Потім перебираємо всі відкриті порти і виводимо різну інформацію, таку як служба, її версія, і багато іншого. Ви можете зробити те саме для портів UDP.

#Добре, ми можемо отримати відкриті TCP-порти за допомогою методу all_tcp(). Потім перебираємо всі відкриті порти і виводимо різну інформацію, таку як служба, її версія, і багато іншого. Ви можете зробити те саме для портів UDP. Результат сканування моєї домашньої локальної мережі:

```
        # ------------------------{Результати роботи ПЗ модуля}-----------------------------------------
-
     [*] Scanning...
     [Wed June 06 17:04:28 2025] Elapsed: 198.11s Up hosts: 4
     Down hosts: 252 Total hosts: 256
     [*] Equivalent command: nmap -oX - -sV 192.168.0.1/24

     ============================== 192.168.0.1 ==============================
     Hostname: IPv4: 192.168.0.1 MAC: 68:FF:7E:B1:83:BE
     Vendor: {'68:FF:7B:B7:83:BE': Hikvision Technologies'}

     ------------------------------ Ports Open ----------------------------

     TCP Port: 21 Status: open Reason: syn-ack
     Service: ftp Product: vsftpd Version: 1.0.8 or later
     Extra info: CPE: cpe:/a:vsftpd:vsftpd

     TCP Port: 22 Status: open Reason: syn-ack
     Service: ssh Product: Dropbear sshd Version: 2025.55
     Extra info: protocol 2.0 CPE: cpe:/o:linux:linux_kernel

     TCP Port: 23 Status: open Reason: syn-ack
     Service: telnet Product: Version:
     Extra info: CPE:
```

TCP Port: 53 Status: open Reason: syn-ack
Service: domain Product: dnsmasq Version: 2.65
Extra info: CPE: cpe:/a:thekelleys:dnsmasq:2.65

TCP Port: 80 Status: open Reason: syn-ack
Service: http Product: Version:
Extra info: CPE:

TCP Port: 139 Status: open Reason: syn-ack
Service: netbios-ssn Product: Samba smbd Version: 3.X - 4.X
Extra info: workgroup: WORKGROUP CPE: cpe:/a:samba:samba

TCP Port: 445 Status: open Reason: syn-ack
Service: netbios-ssn Product: Samba smbd Version: 3.X - 4.X
Extra info: workgroup: WORKGROUP CPE: cpe:/a:samba:samba

TCP Port: 555 Status: open Reason: syn-ack
Service: upnp Product: Portable SDK for UPnP devices Version: 1.6.19
Extra info: Linux 3.4.11^19; UPnP 1.0 CPE: cpe:/o:linux:linux_kernel:3.4.ii-rti9

TCP Port: 554 Status: open Reason: syn-ack
Service: upnp Product: MiniDLNA Version: 1.1.4
Extra info: Linux 2.6.32-71.el6.i686; DLNADOC 1.50; UPnP 1.0 CPE:
cpe:/o:linux:linux_kernel:2.6.32 ...

TCP Port: 554 Status: open Reason: syn-ack
Service: btx Product: Version:
Extra info: CPE:

============================== 192.168.0.103 ==============================
Hostname: oldpc.me IPv4: 192.168.1.103 MAC: CA:F7:oA:7E:847D
Vendor: {}

============================== 192.168.0.106 ==============================
Hostname: IPv4: 192.168.1.106 MAC: 04:A2:22:95:7A:C0
Vendor: {'04:A2:22:95:7A:C0': 'Arcadyan'}

============================== 192.168.0.109 ==============================
Hostname: IPv4: 192.168.1.109 MAC: None
Vendor: {}

------------------------------ Ports Open ----------------------------

TCP Port: 135 Status: open Reason: syn-ack
Service: msrpc Product: Microsoft Windows PC Version:
Extra info: CPE: cpe:/o:microsoft:windows

TCP Port: 139 Status: open Reason: syn-ack

Service: netbios-ssn Product: Microsoft Windows netbios-ssn Version:
Extra info: CPE: cpe:/o:microsoft:windows

TCP Port: 5432 Status: open Reason: syn-ack
Service: postgresql Product: PostgreSQL DB Version: 9.6.0 or later
Extra info: CPE: cpe:/a:postgresql:postgresql

#Наприклад, центральний комутатор СВС має безліч портів і даних для виключення, на ньому відкрито порт FTP з використанням vsftpd версії 2.0.8 або більш пізнішої. Також використовується Dropbear sshd версії 2012.55 або Portable SDK для UPnP devices версії 1.3.2 на порту 1900 і 555, а також багато інших портів. Для підключених пристроїв СВС виявлено 3 хости(наприклад 3 камери СВС), ми змогли отримати IP та MAC-адреси на більшості з них, і навіть виявив, що 192.168.0.109 слухає PostgreSQL сервер на порту 5432.

Додаток Г
Ілюстративна частина

ІЛЮСТРАТИВНА ЧАСТИНА

ЗАХИЩЕНА СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я

Виконав: студент 4 курсу групи 1БС-21б
спеціальності 125 Кібербезпека

_____ В'ячеслав ДЕЙБУК

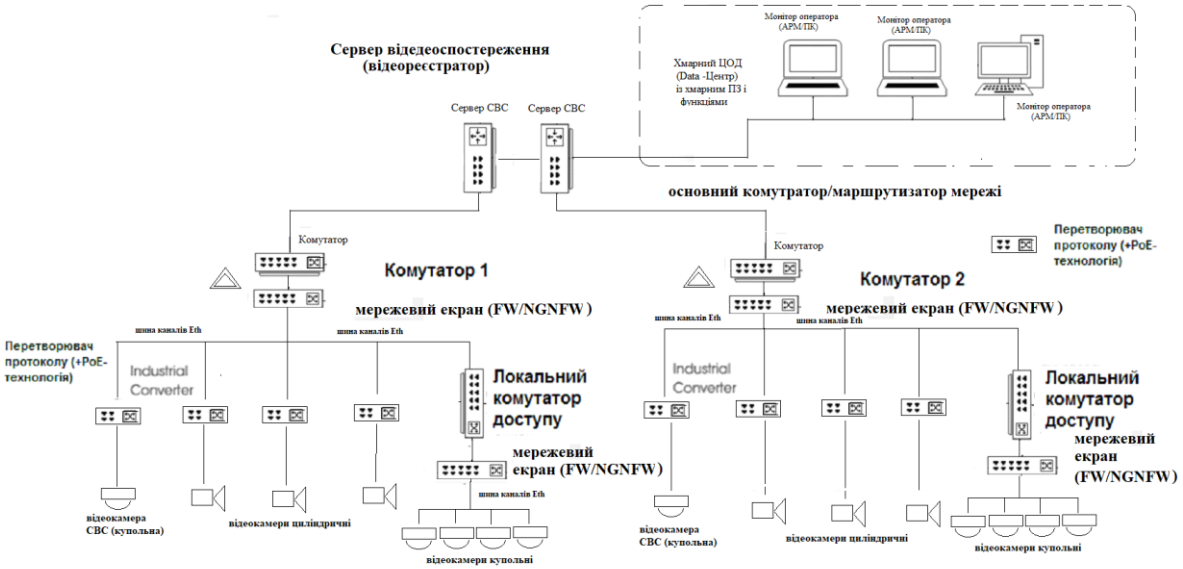
_____ 17 червня 2025 р.

Керівник: к. т. н., доцент каф. ЗІ

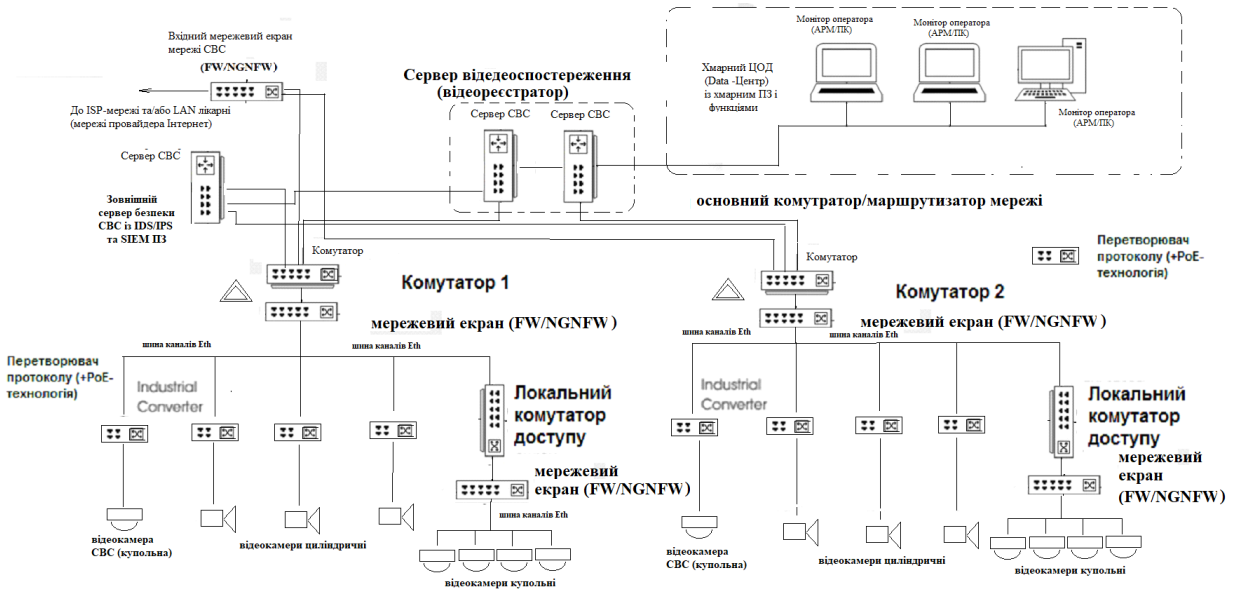
_____ Вадим МАЛІНОВСЬКИЙ

_____ 17 червня 2025 р.

ЗАГАЛЬНА СХЕМА СТРУКТУРИ ЗАХИЩЕНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я



СТРУКТУРА СВС ІЗ МЕРЕЖЕВИМИ ЕКРАНАМИ ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК І ШКІДЛИВИХ МЕРЕЖЕВИХ ВТРУЧАНЬ



СТРУКТУРНА СХЕМА СВС ІЗ СИСТЕМОЮ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ

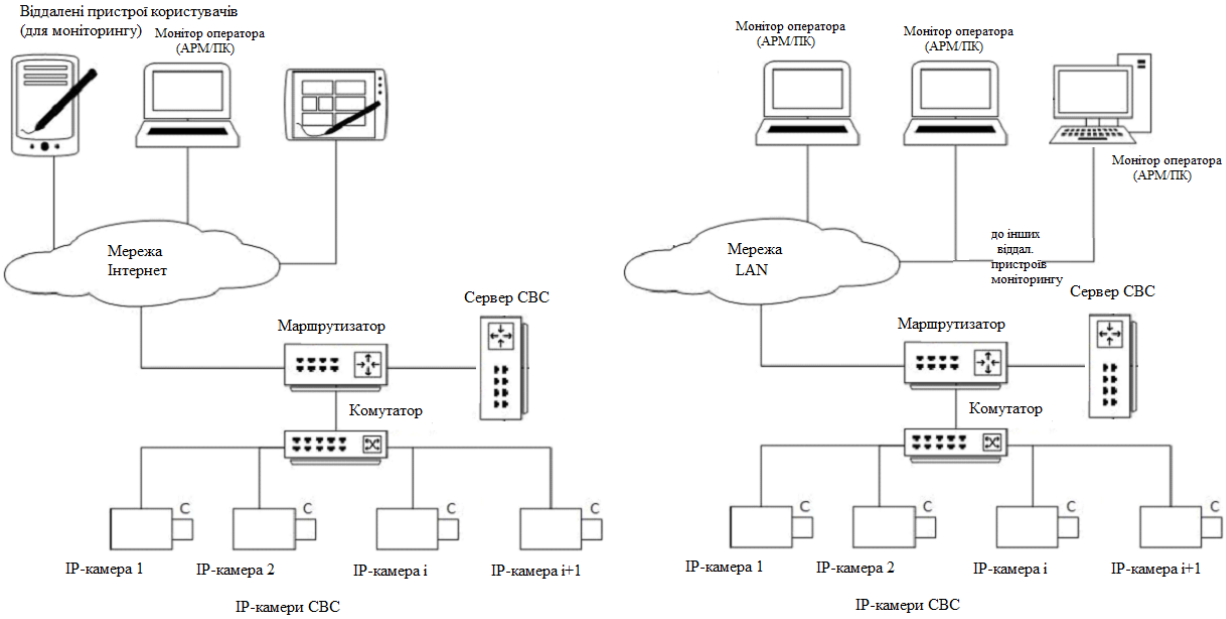
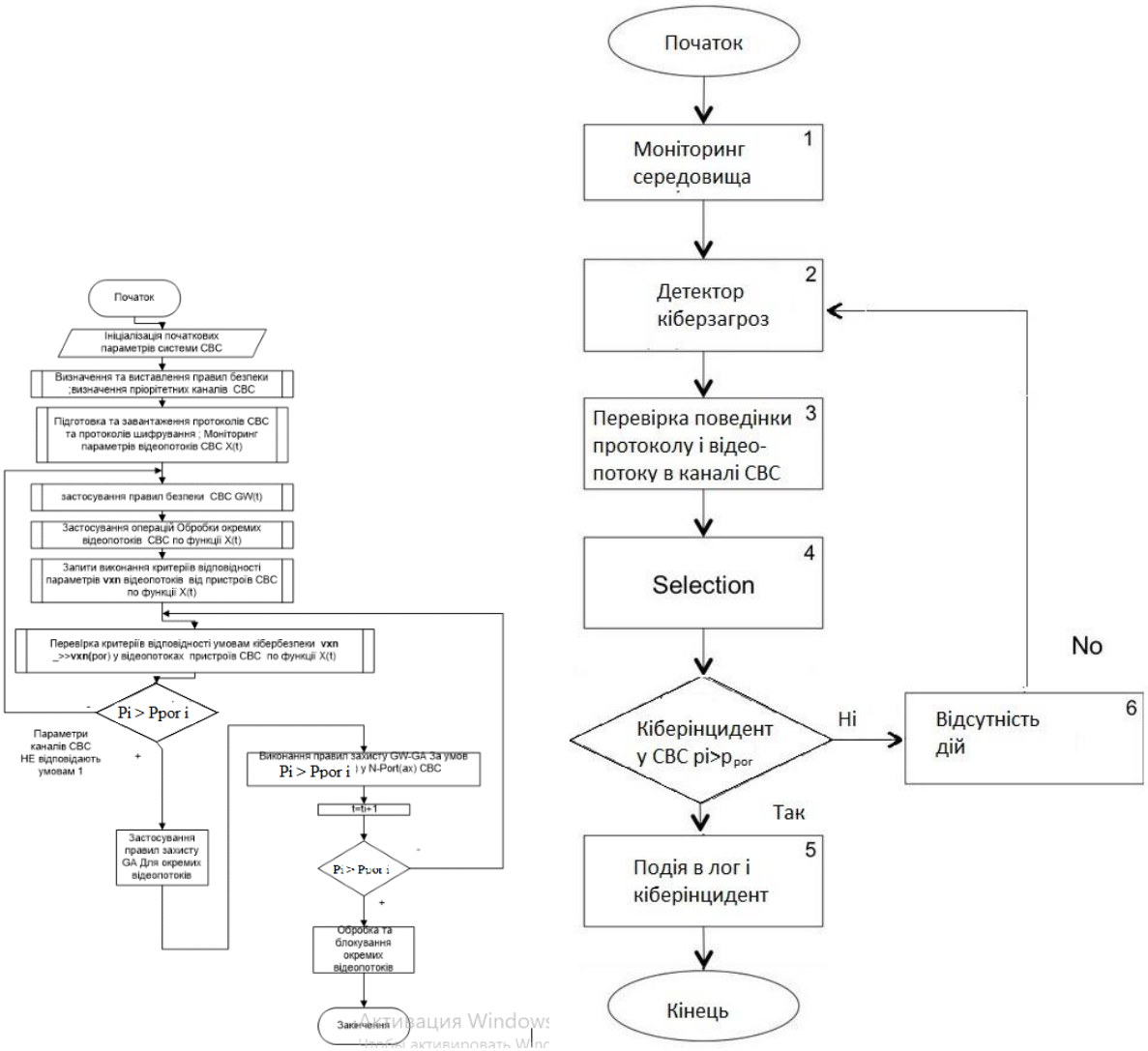
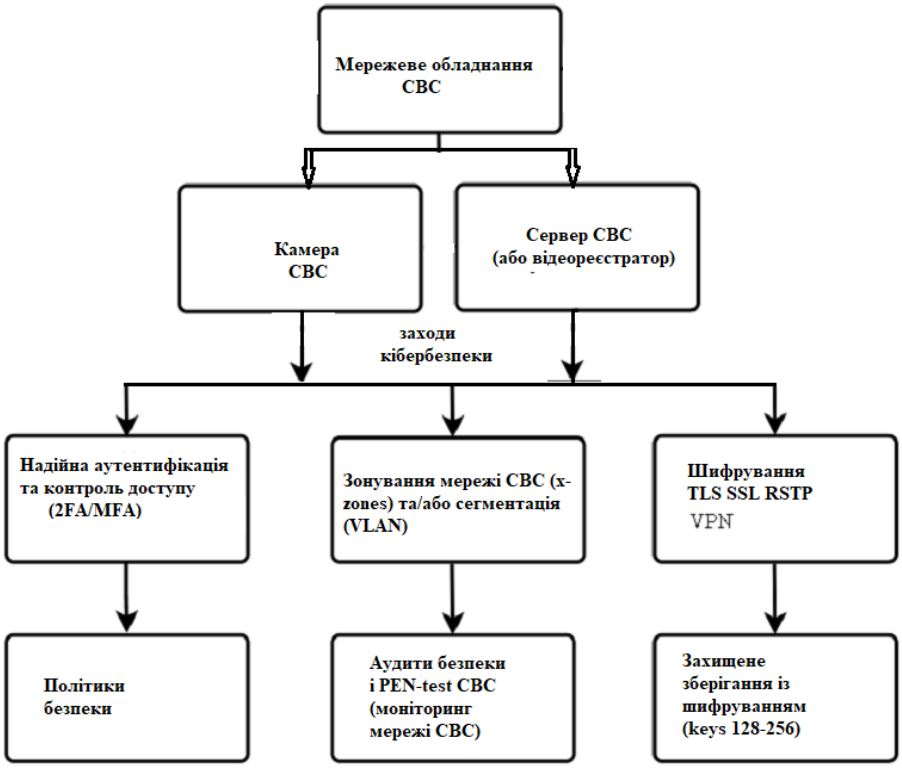


СХЕМА ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ЗАХИСТУ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

БЛОК-СХЕМИ АЛГОРИТМІВ РОБОТИ ЗАСОБУ ВИЗНАЧЕННЯ КІБЕРАТАК ТА КІБЕРЗАХИСТУ У СВС



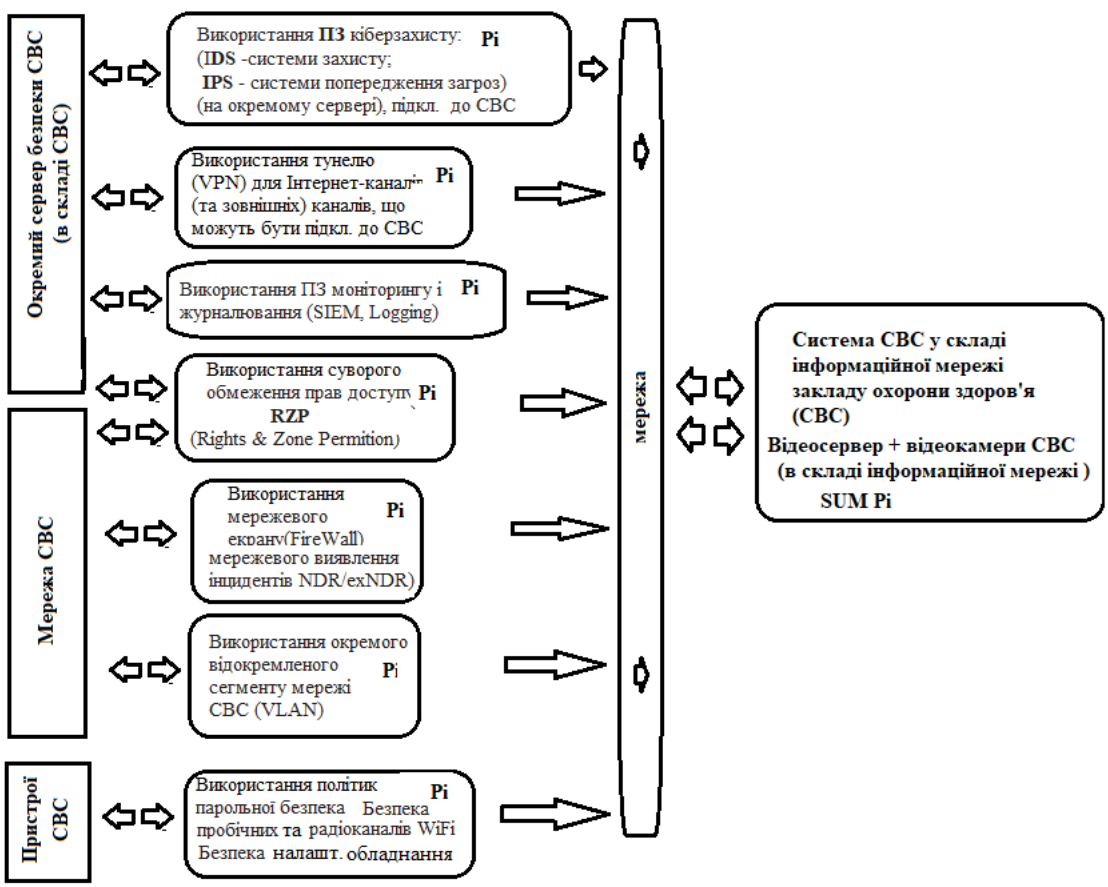
ЗАСОБИ КІБЕРЗАХИСТУ І ВИЗНАЧЕННЯ КІБЕРАТАК У СТРУКТУРІ СВС



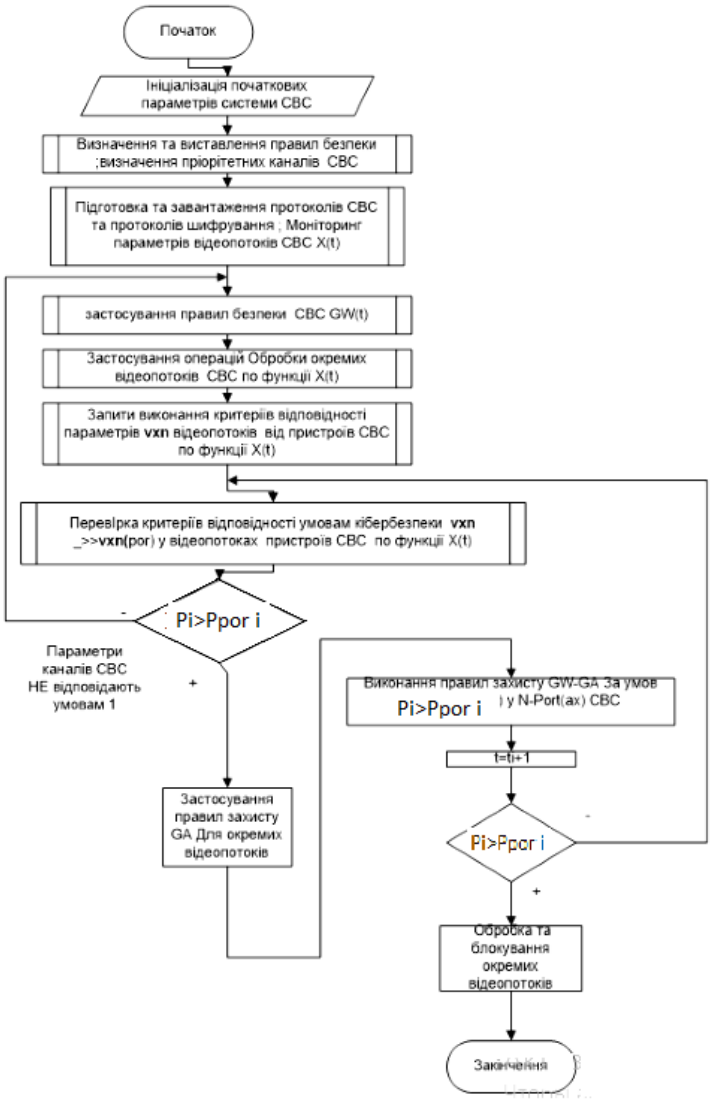
РОЗРОБЛЕНА СТРУКТУРНА МОДЕЛЬ КІБЕРЗАХИСТУ СВС ДЛЯ СЕКТОРУ ОХОРОНИ ЗДОРОВ’Я

Pi - ймовірність ризику одиничного фактору для кожного типу кіберзагрози в рамках виду захисту pi

SUM Pi - сумарна ймовірність ризиків для всієї СВС в медичних закладах Pi



РОЗРОБЛЕНИЙ АЛГОРИТМ КІБЕРЗАХИСТУ СВС ДЛЯ СЕКТОРУ ОХОРОНИ ЗДОРОВ'Я



РЕЗУЛЬТАТИ РОБОТИ ПЗ МОДУЛЯ МОНІТОРИНГУ КАМЕР СВС В СКЛАДІ ЗАХИЩЕНОЇ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

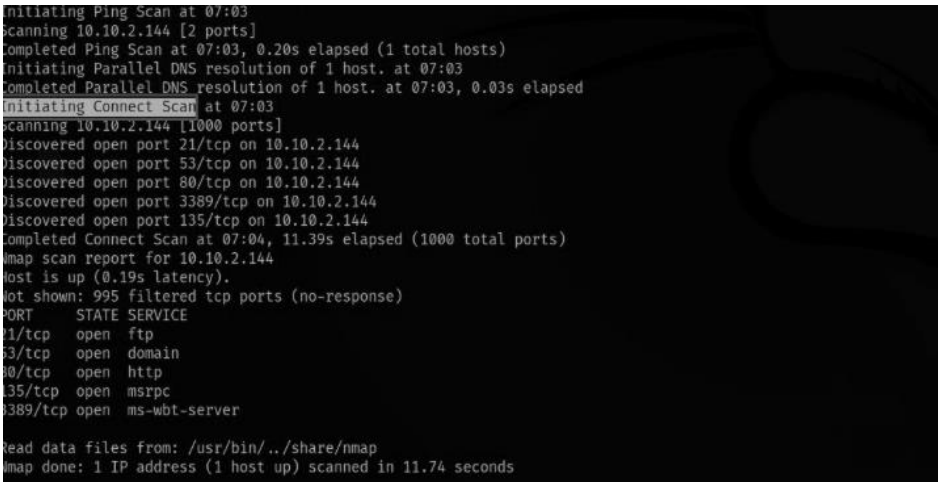
```
Nmap scan report for 10.0.2.4
Host is up (0.00094s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

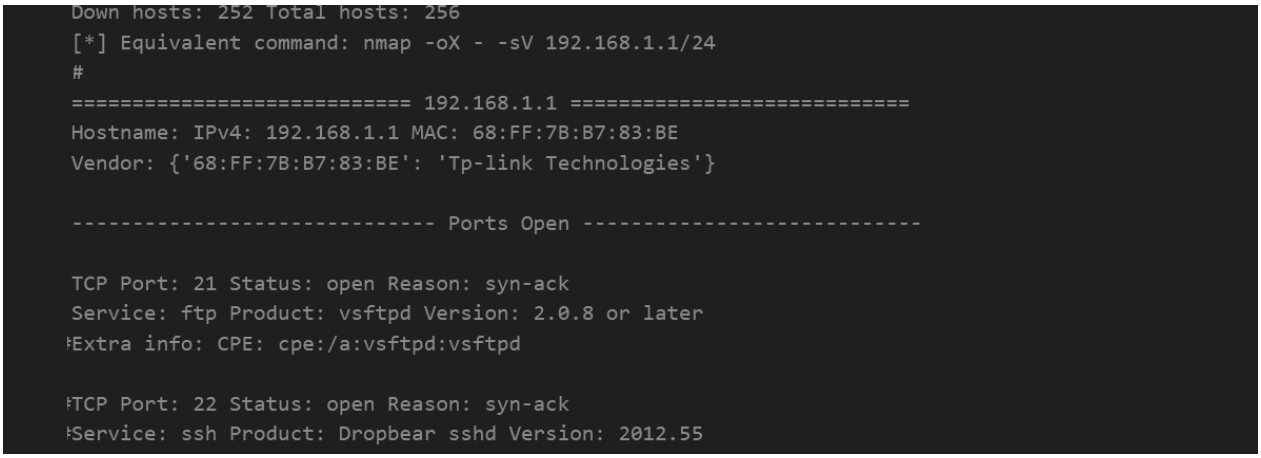
```
Nmap scan report for 10.0.2.4
Host is up (0.00094s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp filtered ms-wbt-server
```

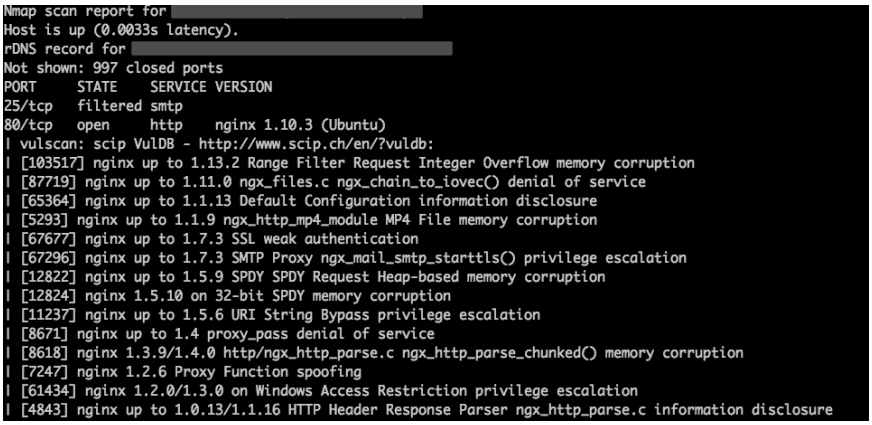
```
Nmap scan report for 10.0.2.1
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT    STATE SERVICE
631/tcp open  ipp

Nmap scan report for 10.0.2.4
Host is up (0.00037s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for google.com (142.250.183.206)
Host is up (0.0089s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:826::200e
rDNS record for 142.250.183.206: bom07s33-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
```

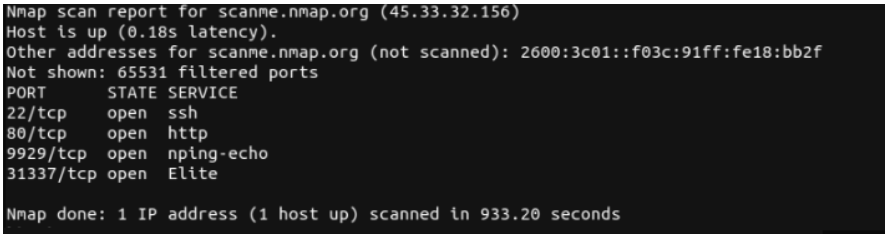
```
Host is up (0.0024s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

ПРОМІЖНІ РЕЗУЛЬТАТИ РОЗРОБКИ І РОБОТИ ПЗ ДЛЯ СКАНУВАННЯ СВС В СКЛАДІ ЗАХИЩЕНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

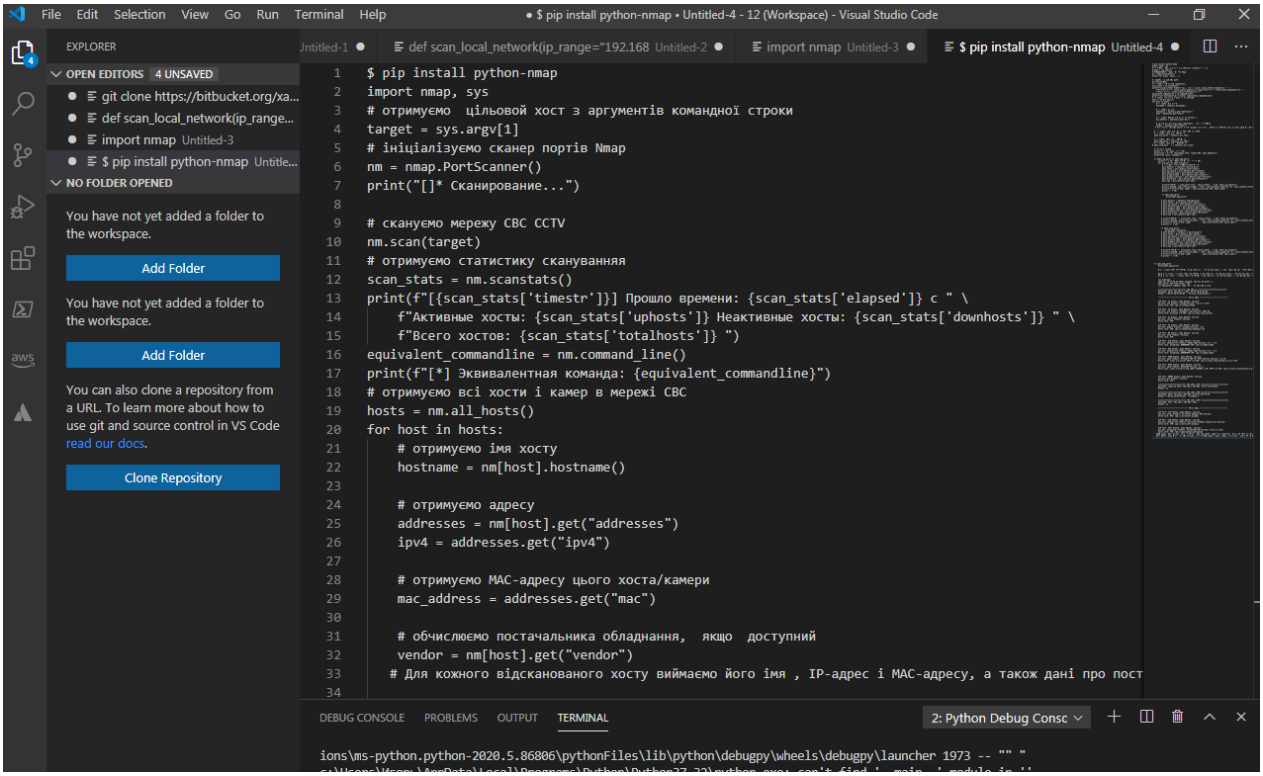


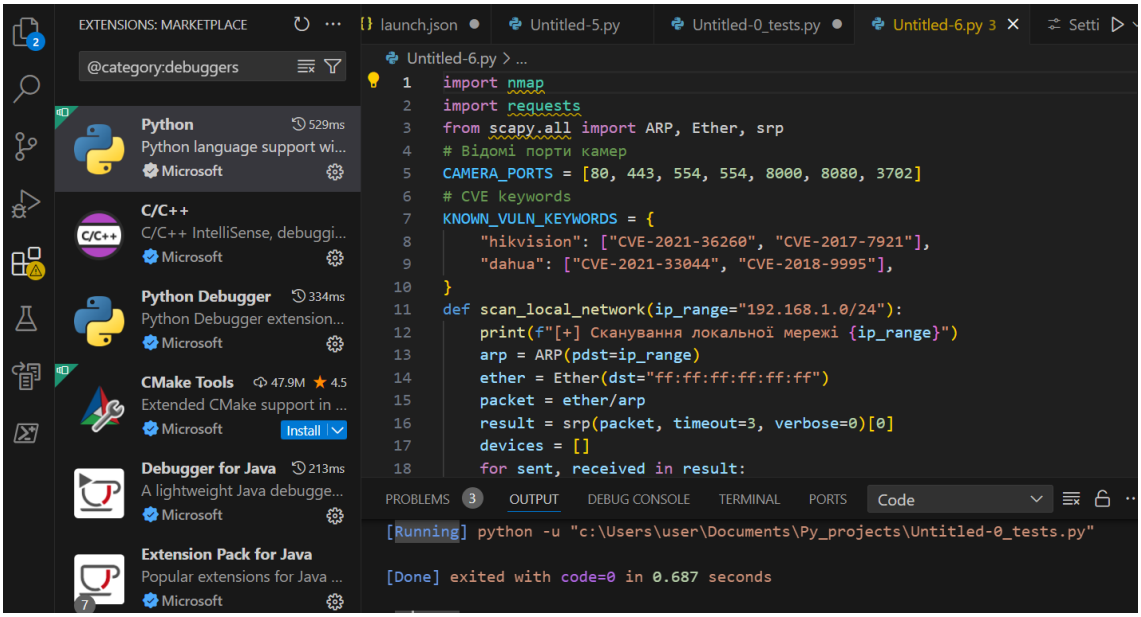






ПРОМІЖНІ РЕЗУЛЬТАТИ РОЗРОБКИ І РОБОТИ ПЗ МОДУЛЯ





ПРОМІЖНІ РЕЗУЛЬТАТИ РОЗРОБКИ І РОБОТИ ПЗ МОДУЛЯ