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

Бакалаврська кваліфікаційна робота на тему
«Методика комплексного захисту медичних інформаційних систем»

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

Керівник: к. т. н., доц., доцент каф. ЗІ
_____Андрій ДУДАТЬЄВ
«17» червня 2025р.

Рецензент: к. т. н. доцент каф. ПЗ
_____Галина ЧЕРНОВОЛИК
«17» червня 2025р.

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

Вінниця ВНТУ – 2025 року

Міністерство освіти і науки України
Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (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
Ярославу МЕТЮ

1. Тема роботи: «Методика комплексного захисту медичних інформаційних систем»
керівник роботи: Андрій ДУДАТЬЄВ, к. т. н., доцент кафедри ЗІ,
затверджені наказом ректора ВНТУ від 20 березня 2025 року за №97.
2. Строк подання студентом роботи 17 червня 2025 р.
3. Вихідні дані до роботи:
– Галузь застосування: медичні інформаційні системи.
– Тип дослідження: розробка методики комплексного захисту з урахуванням актуальних ризиків і нормативних вимог.
– Методологічна база: Аналіз ризиків за стандартами NIST SP 800-30, ISO/IEC 27005, побудова моделі загроз, модель порушника.
4. Зміст текстової частини: Вступ. 1 Теоретичні основи захисту медичних інформаційних систем. 2 Аналіз загроз та ризиків для медичних інформаційних систем в Україні. 3. Методика комплексного захисту медичних інформаційних систем. Висновки. Список використаних джерел.
5. Зміст ілюстративної частини: Загальна структура персоналу підприємства. Загальна схема ікс підприємства. Основні учасники кібер протистояння. Діаграма розподілу ймовірностей. Діаграма обсягів ризиків. Порівняння характеристик різних атак.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	А. ДУДАТЬЄВ, к.т.н., доц. каф.ЗІ	04.03.25	10.06
2	А. ДУДАТЬЄВ, к.т.н., доц. каф.ЗІ	14.05	10.06
3	А. ДУДАТЬЄВ, к.т.н., доц. каф.ЗІ	20.05	10.06

7. Дата видачі завдання 21.03.2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	24.03.25 - 30.03.25	
2	Аналіз літературних джерел за напрямком бакалаврської кваліфікаційної роботи	31.03.25 - 13.04.25	
3	Розробка рішень, моделей, алгоритмів	14.04.25 - 04.05.25	
4	Практична реалізація, моделювання, експериментування, результати	05.05.25 – 14.05.25	
5	Аналіз виконання ПЗ, висновки	15.05.25 – 18.05.25	
6	Оформлення пояснювальної записки	19.05.25 – 26.05.25	
7	Попередній захист БКР	27.05.25 – 30.05.25	
8	Виправлення зауважень, підготовка ілюстративного матеріалу	31.05.25 – 10.06.25	
9	Представлення БКР до захисту, рецензування	11.06.25 – 17.06.25	

Студент _____ Ярослав МЕТЬ

Керівник роботи _____ Андрій ДУДАТЬЄВ

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота складається з 60 сторінок формату А4 містить 8 рисунків, 22 таблиці, список використаних джерел налічує 20 найменувань. Робота присвячена розробці та експертній оцінці комплексної методики захисту медичних інформаційних систем (МІС) на прикладі КНП «Вінницький міський лікувально-діагностичний центр».

Проведено аналіз архітектури системи, визначено основні вразливості та слабкі місця захисту, побудовано модель порушника з урахуванням сучасних загроз — як традиційних (SQL-ін’єкції, ransomware, DDoS), так і гібридних, що виникають в сучасних умовах. Запропонована методика базується на міжнародних стандартах ISO/IEC 27002:2022, ISO/IEC 27799:2016, NIST SP 800-30 Rev.1 та нормативній базі МОЗ України. Вона поєднує технічні (шифрування, резервне копіювання, SIEM-моніторинг, захист API, багатофакторна автентифікація, WAF) і організаційні заходи (аудит безпеки, навчання персоналу, оновлені політики доступу).

У роботі проведено експертну оцінку ефективності запропонованої методики, визначено приріст рівня захищеності на основі шести ключових критеріїв безпеки, який склав 21,5 %.

Ключові слова: медична інформаційна система, захист даних, конфіденційність, модель порушника, NIST, ISO/IEC 27002, ISO/IEC 27799, аудит безпеки, резервування, багаторівнева захищеність.

ABSTRACT

The bachelor's qualification thesis comprises 60 A4 pages, includes 8 figures and 22 tables, and cites 20 references. The work is devoted to the development and expert evaluation of a comprehensive protection methodology for medical information systems (MIS) using the example of the Vinnytsia City Medical and Diagnostic Center.

An analysis of the system architecture was carried out, its main vulnerabilities and weak points identified, and a threat actor model constructed that takes into account both traditional threats (SQL injections, ransomware, DDoS) and hybrid threats arising in modern conditions. The proposed methodology is based on the international standards ISO/IEC 27002:2022, ISO/IEC 27799:2016, NIST SP 800-30 Rev.1, and the regulatory framework of the Ministry of Health of Ukraine. It combines technical measures (encryption, backup, SIEM monitoring, API protection, multi-factor authentication, WAF) with organizational measures (security audits, staff training, updated access policies).

An expert assessment of the methodology's effectiveness was performed, yielding a 21.5 % increase in the overall protection level based on six key security criteria.

Keywords: medical information system, data protection, confidentiality, threat actor model, NIST, ISO/IEC 27002, ISO/IEC 27799, security audit, backup, defense-in-depth.

ЗМІСТ

ВСТУП

У сучасних умовах цифровізації охорони здоров’я медичні інформаційні системи (МІС) стали критично важливими для обробки та зберігання персональних даних пацієнтів. Зі зростанням обсягів електронного документообігу зростають і ризики несанкціонованого доступу, витоку, зміни або знищення чутливої інформації. Згідно з публічними звітами, у 2023 році кількість кібератак на медичні заклади зросла на понад 35 %.

Актуальність теми зумовлена необхідністю удосконалення підходів до захисту МІС шляхом комплексного впровадження технічних та організаційних заходів, що базуються на міжнародних стандартах і враховують сучасні загрози.

Метою роботи є підвищення рівня захищеності МІС шляхом розробки методики комплексного захисту.

Для досягнення мети були поставлені наступні завдання: 1) провести дослідження архітектури МІС і виявити потенційні загрози; 2) побудувати модель порушника та оцінити ризики; 3) проаналізувати сучасну методологічну базу 4) розробити комплекс заходів захисту, що охоплює технічні та організаційні рішення; 5) провести матричну експертну оцінку пропонованої методики комплексного захисту.

Методологічною основою дослідження стали стандарти ISO/IEC 27002, NIST SP 800-30, Наказ МОЗ №246, НД ТЗІ 3.7-003 2023.

Об’єктом дослідження є процеси, які відбуваються в МІС, предметом - технічні та організаційні рішення, які використовуються в комплексних системах захисту інформації.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Аналіз та структура медичного закладу та його інформаційної системи

Інформаційно-комунікаційна система (ІКС) комунального підприємства «Міський лікувально-діагностичний центр» (вулиця Київська, буд.68, Вінниця, Вінницька область) являє собою сукупність технічних, програмних, організаційних та правових засобів, які забезпечують обробку, зберігання та передачу інформації, необхідної для виконання медичних, діагностичних та адміністративних функцій закладу.

Центр обслуговує близько 100 000 звернень на рік, пропонуючи пацієнтам амбулаторно-діагностичні та консультативні послуги: клініко-діагностичну лабораторію, рентген / УЗД-діагностику, функціональну діагностику (ЕЕГ, ЕКГ) та ендоскопічні дослідження. У підприємстві великий штат співробітників, з різними рівнями доступу до інформації: лікарі, середній медичний персонал, молодший персонал і адміністративно-технічні співробітники.

Керівником Вінницького міського лікувально-діагностичного центру є головний лікар, який несе повну відповідальність за стратегічне планування діяльності закладу, взаємодію з органами місцевої влади та Міністерством охорони здоров’я, затвердження політик і наказів, а також контроль виконання ключових показників роботи. Йому підпорядковується низка заступників: заступник головного лікаря з медичної частини координує роботу діагностичних підрозділів – лабораторії, рентген-діагностики, функціональної діагностики та ендоскопії – і відповідає за організацію та безпеку проведення всіх медичних досліджень; заступник головного лікаря з поліклінічної роботи відповідає за амбулаторний прийом пацієнтів, контроль запису на прийом, організацію роботи сімейних лікарів, терапевтичних та педіатричних кабінетів; заступник головного лікаря з

господарської частини керує допоміжними службами — пральнею, харчоблоком, центральною стерилізаційною та дезінфекторіями, а також забезпечує технічне обслуговування приміщень і обладнання. Головна медсестра організовує діяльність середнього медичного персоналу, формує раду медсестер, забезпечує навчання та контроль дотримання стандартів догляду і санітарно-гігієнічних норм. Головний бухгалтер, у свою чергу, відповідає за фінансово-економічне забезпечення Центру, складення бюджету, ведення бухгалтерського обліку та взаєморозрахунки зі страховими компаніями, а також за своєчасну виплату заробітної плати персоналу, графічне зображення блок схеми закладу представлено на рисунку 1.1.

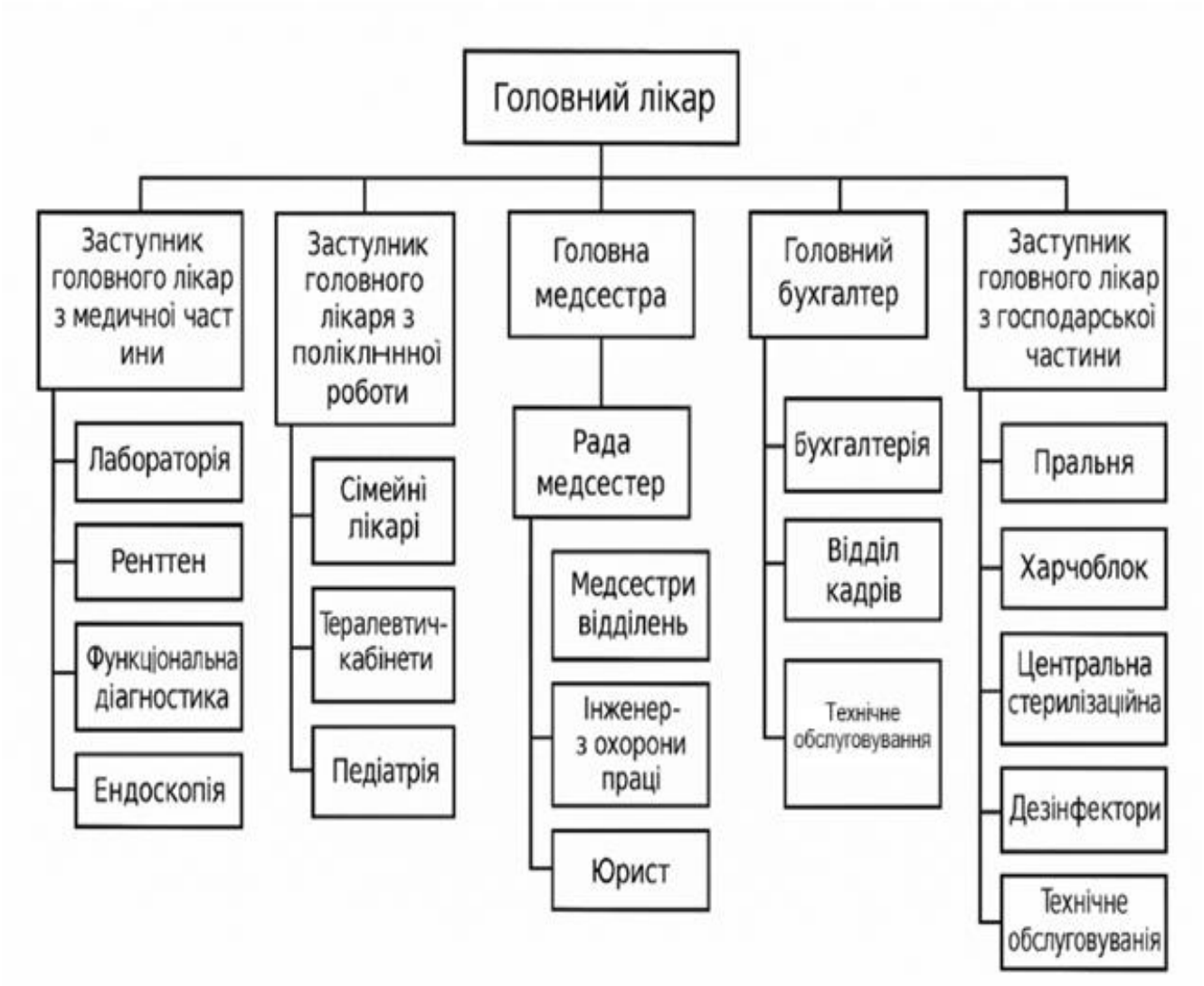


Рисунок 1.1 — Загальна структура персоналу ІКС КП МЛДЦ

Автоматизована частина ІКС охоплює ключові бізнес-процеси: 1) електронна реєстрація та запис (онлайн-портал і кол-центр), 2) ведення електронних медичних карток (EMR), 3) формування та передача результатів лабораторії й діагностичних відділень, 4) управління черговістю й госпіталізацією , 5) фінансовий облік: формування рахунків та взаєморозрахунків зі страховиками. У результаті в ІКС циркулюють такі типи даних: 1) особисті (ПІБ, дата народження, контактні дані), 2) медичні (історії хвороби, діагнози), 3) цифрові зображення та звіти, 4) фінансові (платіжні транзакції, інформація про страховиків).

Весь цей потік інформації передається всередині локальної обчислювальної мережі закладу (LAN), яка об’єднує робочі станції реєстратури, кабінетів лікарів, відділень лабораторії та бухгалтерії, а також сервери баз даних і портали зовнішнього доступу через захищений VPN-канал. Управління й моніторинг інфраструктури здійснюється через відділ інформаційних технологій Центру, який відповідає за підтримку серверного обладнання, резервне копіювання та захист від кіберзагроз, узагальнену структурну схему ІКС Центру, що ілюструє взаємозв’язки між користувачами, прикладним програмним забезпеченням, серверами даних та мережею, зображено на рисунку 1.2. У структурі інформаційно-комунікаційної системи «Міського лікувально-діагностичного центру» центральним елементом захисного периметра є універсальний пристрій Firewall/UTM. Його основне завдання — глибока фільтрація всіх зовнішніх і внутрішніх пакетів, запобігання DDoS-атак та організація шифрованих VPN-з’єднань для віддаленого доступу як співробітників Центру, так і офіційних партнерів (МОЗ, платформи eHealth). Завдяки модулю проксі та IDS/IPS, цей пристрій здатний відсіювати підозрілий трафік на ранніх етапах і блокувати відомі шкідливі підключення до мережі закладу. За межами внутрішньої LAN створено демілітаризовану зону (DMZ), що містить сервери зовнішніх сервісів – веб-портал реєстрації пацієнтів, модуль телемедицини та сервіс електронних рецептів. Поєднуючись із Firewall через окремий інтерфейс, DMZ дозволяє ізолювати користувачів Інтернету від основної мережі закладу: у разі успішного зламу публічного порталу зловмисник опиниться в строго обмеженому сегменті, не отримавши доступу до внутрішніх ресурсів.

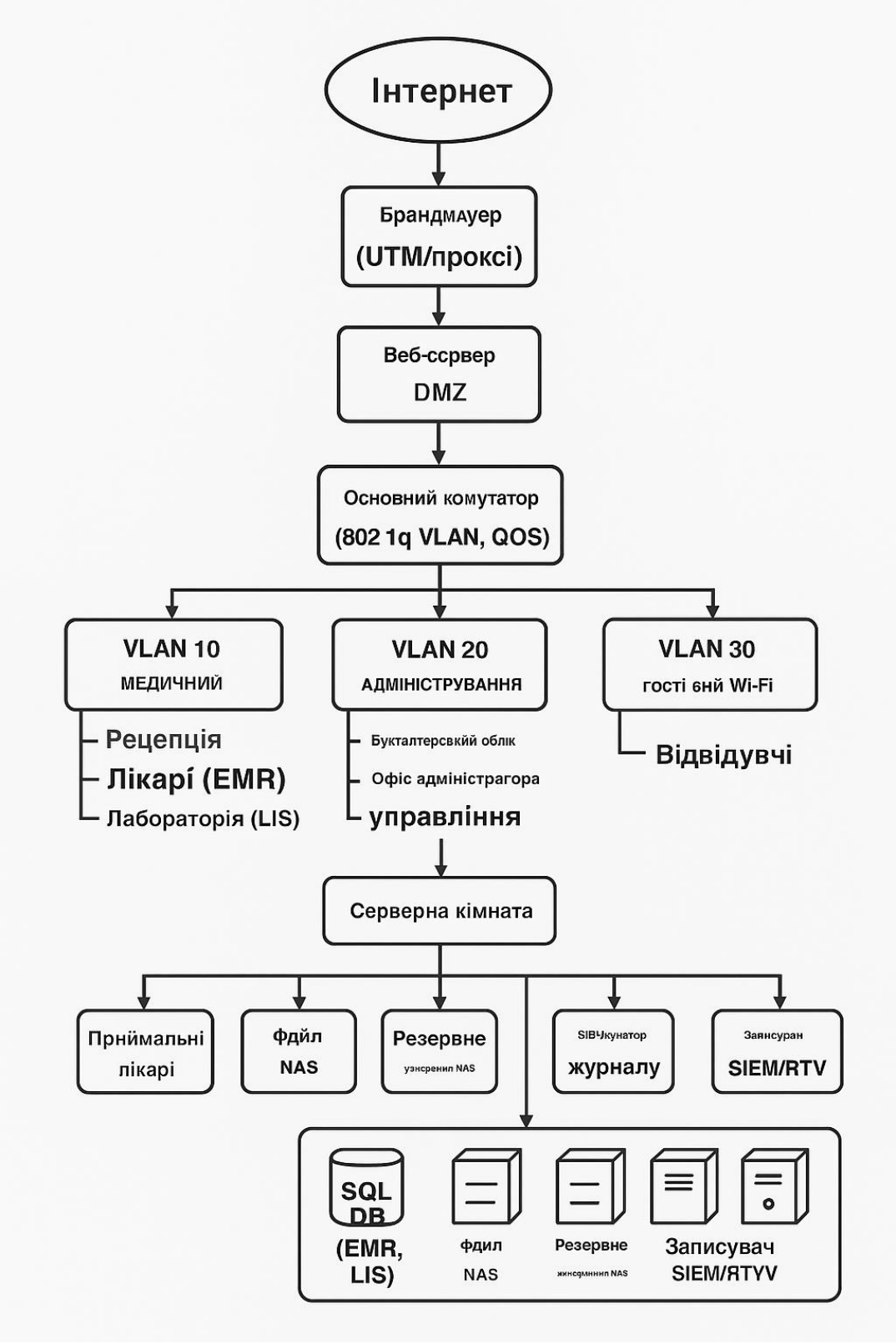


Рисунок 1.2 — Загальна схема ІКС КП МЛДЦ

Від DMZ і VPN-терміналів весь внутрішній трафік потрапляє на ядро мережі – Core Switch, що реалізує 802.1Q-сегментацію на три віртуальні локальні мережі

(VLAN). У VLAN10 («медичний трафік») об’єднані робочі станції лікарів та реєстратури, які взаємодіють із системами EMR та LIS. VLAN20 («адмінтрафік») призначений для бухгалтерії, управлінського персоналу та IT-відділу, а VLAN30 ізольовано від двох перших і надає пацієнтам гостьовий Wi-Fi для виходу в Інтернет без ризику доступу до внутрішніх серверів.

На рівні користувацьких пристроїв у Центрі застосовуються тонкі клієнти та настільні ПК із встановленими засобами захисту інформації (антивірус, EDR-агент, локальний брандмауер). Усі кінцеві точки централізовано реєструються в SIEM-системі, що здійснює кореляцію подій і автоматичне оповіщення про аномалії в поведінці користувачів чи трафіку.

У серверній кімнаті розгорнуто п’ять основних класів обладнання: SQL-СУБД для зберігання електронних медичних карток і результатів діагностичних досліджень із підтримкою транзакцій та реплікації; File NAS для архівації DICOM-зображень УЗД, рентген- та ендоскопічних матеріалів разом із шаблонами документів; Backup NAS (RAID), який виконує щоденне й щотижневе резервне копіювання всіх ключових даних, а також георезервування в хмарний сховище для аварійного відновлення; SIEM/Log Server, котрий централізує логи мережевих пристроїв, серверів і кінцевих точок, проводить їхню кореляцію за індикаторами компрометації й формує звіти для IT-безпеки; NVR/CCTV Recorder, що приймає й зберігає відео потоки з камер спостереження, забезпечуючи архівування із можливістю миттєвого пошуку за датою, часом і зоною.

Завдяки такій багаторівневій архітектурі Центр отримав можливість не лише жорстко контролювати доступ і розподіляти ролі в мережі, але й оперативно виявляти аномалії трафіку, поєднуючи технічні засоби захисту з автоматизованими процесами моніторингу та реагування. Це забезпечує надійний рівень безпеки для даних клієнтів та безперебійну роботу клініко-діагностичних сервісів.

1.2 Класифікація інформаційних потоків і ризиків

У межах Вінницького міського лікувально-діагностичного центру інформація рухається через локальну мережу (LAN), що об’єднує робочі станції, маршрутизатори та комутатори. Мережа розділена на VLAN-сегменти для медичного трафіку (VLAN10), адміністративного трафіку (VLAN20) та гостьового Wi-Fi (VLAN30).

На фізичному рівні робочі станції реєстратури, лабораторії, діагностичних відділень, бухгалтерії й технічного відділу підключені до комутаторів, які через VLAN 802.1Q передають дані на ядра мережі — Core Switch. Далі трафік маршрутизатором потрапляє на універсальний Firewall/UTM, де відбувається фільтрація і шифрування каналів (IP-Sec VPN для віддаленого доступу). Частина серверів (онлайн-портал реєстрації, телемедицина) винесена в DMZ для ізоляції від внутрішньої LAN.

У Центрі обмін даними між підрозділами організовано через внутрішню VLAN-сегментовану мережу, що гарантує розмежування медичного, адміністративного та гостьового трафіків. Основний потік починається в реєстратурі, де після введення персональних даних пацієнта (прізвище, ім’я, по батькові, дата народження, група крові) інформація передається по захищеному HTTPS-каналу із застосуванням протоколу TLS. Далі цей трафік спрямовується у VLAN10 на EMR-сервери, де відбувається первинне збереження й обробка даних для подальшого використання лікарями та лабораторією.

Після отримання направлень від лікарів біоматеріали та цифрові зображення (DICOM-файли) з лабораторії й діагностичних відділень спочатку зберігаються на File NAS у серверній кімнаті. Поширення результатів для лікарів здійснюється через захищений SMB-тунель, що шифрує дані на рівні каналу, — таким чином виключається ризик перехоплення під час передачі у внутрішній VLAN10.

Паралельно фінансовий відділ обмінюється рахунками та підтвердженнями зі страховими компаніями через виділений VPN-канал. Для передачі конфіденційних документів використовується протокол SFTP, що забезпечує як

шифрування даних, так і їхню цілісність під час транзиту до зовнішніх серверів партнерів.

Сервіс телемедицини працює в демілітаризованій зоні (DMZ). Відео та текстові консультації з пацієнтами проходять через WebRTC-сервер, доступ до якого організовано по захищеному HTTPS. Аутентифікація користувачів виконується за механізмом OAuth 2.0 з одноразовими токенами, що забезпечує безпечний вхід навіть з домашніх мереж пацієнтів.

Усі критичні дані регулярно резервуються: щодня автоматизований процес виконує шифрування архівів і копіювання їх на Backup NAS у серверній кімнаті. Одночасно ці резервні копії дублюються в хмарне сховище для забезпечення георезервування і швидкого відновлення в разі аварії.

Моніторинг подій і логів організовано за допомогою SIEM-платформи, розміщеної в VLAN20. Вона централізовано збирає мережеві та системні логи із серверів, робочих станцій і мережевого обладнання, виконує кореляцію за індикаторами компрометації та зберігає архів із можливістю пошуку протягом щонайменше 90 діб. Такий підхід дозволяє в режимі реального часу виявляти аномальні події й оперативно реагувати на потенційні загрози у єдиному інформаційному просторі Центру.

Для детального розуміння роботи підприємства необхідно проаналізувати, інформаційні потоки які циркулюють у підприємстві. Вхідні інформаційні потоки: 1) Медичні історії пацієнтів: від пацієнтів та їхніх лікарів надходять медичні історії, які містять інформацію про стан здоров'я, діагнози, лікування і результати досліджень. 2) Екстрені повідомлення: вхідні екстрені повідомлення з відділень Служби екстреної медичної допомоги (СЕМД) та пацієнтів із критичними станами, що потребують госпіталізації. 3) Лабораторні і діагностичні результати: інформація про результати клінічних аналізів, рентгенограм, УЗД та інших досліджень. 4) Інформація про прийом пацієнтів: реєстрація прийому пацієнтів, інформація про час і місце консультацій та операцій. 5) Запити з медичних відділень: запити лікарів щодо додаткових досліджень, консультацій і лікувальних заходів. 6) Вихідні інформаційні потоки: медичні записи та історії пацієнтів: після обробки і лікування

інформація зберігається у медичних записах і історіях пацієнтів, які можуть використовуватися для подальшого лікування і аналізу. 7) Рецепти та медикаменти: виписування рецептів для пацієнтів і видача лікарських засобів і медикаментів з аптеки або у самому медичному закладі. 8) Звіти і аналізи: підготовка звітів для адміністрації лікарні та медичних організацій, аналіз статистичних даних про захворювання і лікування. 9) Листи до пацієнтів: інформування пацієнтів про їхній стан, рекомендації щодо лікування та подальших дій. 10) Звіти для страхових компаній і фінансових організацій: підготовка і надання звітів для страхових компаній та інших організацій для отримання оплати за медичні послуги. 11) Інформація для навчання і досліджень: надання інформації для медичних досліджень, навчання студентів і підвищення кваліфікації медичного персоналу. 12) Кореспонденція з іншими медичними закладами: обмін інформацією та консультації з іншими лікарнями і клініками. 13) Аналіз інформаційних потоків в лікарні вказує на необхідність захисту інформації в кожному із відділів. 14) Для цього побудуємо таблицю розмежування прав доступу для вхідних інформаційних потоків.

Позначення:

r – дозвіл на читання

w – дозвіл на запис

c – дозвіл на створення

d – дозвіл на видалення

Результати відображено в таблиці 1.1

Таблиця 1.1 — Розмежування прав доступу до вхідних інформаційних потоків

Потік	БД медичної історії пацієнтів	БД із записами екстрених повідомлень	БД із лабораторними дослідженнями	БД з інформацією про прийом пацієнтів	БД запитів з медичних відділень
Відділ з медичними історіями пацієнтів	rwcd	r-c-	r---	rwcd	rwcd
Відділ з екстреними повідомленнями	r-cd	rwcd	r---	rwcd	r--d

Продовження таблиці 1.1

Лабораторні і діагностичні результати	rwcd	rwcd	rwcd	rwcd	r---
Інформація про прийом пацієнтів	rwcd	rwcd	rwc-	rwcd	r-c-
Запити з медичних відділень	r---	r---	r---	r---	rwcd

Для кожного потоку даних визначено загрози, вразливості та рівень ризику (H – високий, C – середній, N – низький). Доповнення до таблиці відображають низку специфічних ризиків, притаманних роботі діагностичного центру. Зокрема, увага до перехоплення SMB-трафіку та потенційних атак типу ransomware на File NAS обумовлена необхідністю захисту великих обсягів DICOM-зображень і лабораторних документів, що передаються та зберігаються у централізованому файловому сховищі. Включення загроз, пов’язаних із несанкціонованим VPN-підключенням і DoS-атаками на сервіси в DMZ, підкреслює потребу посилити захист зовнішніх інтерфейсів центру — як для віддаленого доступу лікарів і партнерів, так і для стабільності роботи телемедичного порталу. Окремий акцент на вразливостях гостьового Wi-Fi та скануванні внутрішньої мережі демонструє, що сегментація трафіку без належного моніторингу не здатна гарантувати безпеку пацієнтів та працівників, тож необхідно впровадити сучасні алгоритми шифрування та внутрішню систему виявлення загроз. Крім того, враховано вплив людського фактора — зокрема ризики, пов’язані з помилковим налаштуванням мережевих ресурсів або недостатнім рівнем обізнаності персоналу щодо фішингових загроз. Оцінка базується на стандартах NIST SP 800-30[1] та ДСТУ ISO/IEC 27005:2010[2] з використанням якісних та напівкількісних критеріїв, результати відображено в таблиці 1.2.

Таблиця 1.2 — Розширена оцінка загроз, вразливостей і заходів захисту

Загроза	Вразливість	Ризик	Інформаційний потік	Запобіжні заходи	Категорія даних
Несанкціонований доступ до медкарток	Відсутність VLAN-сегментації медичного трафіку (VLAN10); слабкі паролі; відсутня MFA	високий (H)	Медичні історії пацієнтів (VLAN10)	Впровадження VLAN10, MFA, шифрування AES-256	К0 Критична
Витік даних через веб-портал реєстрації	Незахищений HTTP; відсутність WAF; вразливість до SQL-ін’єкцій	середній (C)	Онлайн-запис пацієнтів (DMZ)	HTTPS (TLS 1.3), WAF, регулярний аудит коду	К1 Дуже важлива
Перехоплення лабораторних даних	Використання старих версій SMB без шифрування end-to-end	середній (C)	Результати аналізів та DICOM-зображення (VLAN10)	Перехід на VPN або SMB over TLS	К0 Критична
Ransomware-атака на File NAS	Відсутність сегментації RAID-групи; загальний доступ “adm” до NAS	високий (H)	Усі файлові сховища (File NAS)	Політика WORM, сегментація сховищ, регулярні оновлення та моніторинг	Ц0 Критична
Несанкціоноване використання VPN-доступу	Відсутність мультифакторної аутентифікації; слабкі IP-Sec ключі	високий (H)	Віддалений доступ (VPN)	MFA, ротація ключів, обмеження IP-діапазонів	К0 Критична
DoS-атаки на телемедичний сервіс	Відсутність анти-DDoS / rate-limiting у DMZ	середній (C)	Телемедицина (WebRTC у DMZ)	Cloudflare DDoS Protection, локальний IDS/IPS	Д1 (Дуже важлива)
Перехоплення гостьового Wi-Fi трафіку	Відкритий SSID; WPA2 без сучасних алгоритмів (WPA3)	середній (C)	Гостьовий Wi-Fi (VLAN30)	Перехід на WPA3, ізоляція клієнтів, captive-portal	Д2 Важлива
Видалення резервних копій	Відсутність політики WORM; недостатній контроль доступу до Backup NAS	високий (H)	Резервні копії (Backup NAS)	Політика WORM, розділення прав, георезервування в хмарі	Ц0 Критична

Продовження таблиці 1.2

Сканування внутрішньої мережі та портів	Відсутність внутрішнього IDS/IPS у VLAN20; відсутня кореляція з SIEM	середній (C)	Мережевий трафік і логи (VLAN10/20)	Впровадження внутрішнього IDS/IPS, інтеграція з SIEM	К3 Значима
Фішинг-атаки на персонал	Недостатній рівень кіберосвіти; відкриті SMTP-порти	середній (C)	Електронна пошта, VPN	Фільтрація спаму, регулярні тренінги з кібергігієни	К2 Важлива
Втрата даних через збій маршрутизатора/комутатора	Відсутність SLA-моніторингу стану обладнання; нерегулярні оновлення прошивок	середній (C)	Усі ключові потоки (EMR, лабораторія, фінанси)	Моніторинг SLA, автоматичні оновлення прошивок, резервні лінії зв’язку	Ц1 Дуже важлива
Підробка електронних рецептів	Відсутність цифрового підпису (ЕЦП)	високий (H)	Рецептурний потік	Впровадження ЕЦП за ДСТУ 4145, інтеграція з eHealth	К0 Критична
Природні катаклізми (пожежа, повінь)	Відсутність георезервування та аварійного відновлення; єдиний ЦОД	низький (N)	Фінансові звіти та інші БД (VLAN20)	Георезервування в 2+ ЦОД, аварійний план, UPS для критичних систем	Ц3 Значима

Нарешті, загроза видалення резервних копій наголошує на важливості реалізації політики незмінності даних (WORM) і суворого контролю доступу до Backup NAS, а також на необхідності георезервування й багаторівневого зберігання архівів, щоб забезпечити швидке відновлення інформації в разі надзвичайних ситуацій.

1.3 Регламенти інформаційної безпеки в медичній галузі

У медичній галузі регламенти інформаційної безпеки базуються на принципах «триади» CIA: конфіденційність, цілісність і доступність. Конфіденційність передбачає, що до медичних даних мають доступ лише авторизовані особи – лікарі, медсестри чи адміністратори з відповідними правами. Цілісність гарантує, що будь-які зміни в інформації про пацієнтів не можуть бути виконані без відповідних процедур і фіксацій аудиторськими журналами, а доступність забезпечує безперервну роботу сервісів, щоб у критичній ситуації персонал завжди міг отримати необхідні дані.

Нормативною основою впровадження цих принципів є міжнародний стандарт ISO/IEC 27002:2015 [3], зокрема його розділи, що регламентують політики безпеки (розд. 5), управління активами (розд. 8), контроль доступу (розд. 9), операційну безпеку (розд. 12) та реагування на інциденти (розд. 17). В Україні ця норма під лаштована у ДСТУ ISO/IEC 27002:2015 [4], де окремо виділено заходи з шифрування даних, ведення журналів обліку подій та внутрішній аудит. Окрім того, наказ МОЗ № 246 [5] «Про затвердження порядку захисту медичної інформації» встановлює обов’язкові організаційні та технічні вимоги: від призначення відповідальних за безпеку осіб до впровадження засобів контролю доступу, резервного копіювання та шифрування інформації.

Для оцінки ефективності впроваджених заходів використовуються такі ключові критерії: зниження кількості інцидентів; скорочення часу виявлення і реагування; підтримка рівня доступності сервісів (uptime) на позначці не нижче за 99,5 %; а також щоквартальні внутрішні перевірки на відповідність вимогам стандартів із позитивним висновком. Застосування цих регламентів і критеріїв дозволяє гарантувати комплексний захист медичної інформації та безперервність роботи діагностичного центру в умовах зростаючих кіберзагроз, , порівняльна таблиця нормативних вимог розділів ISO/IEC 27002:2015 реалізуються у ДСТУ та наказі МОЗ представлено у в таблиця 1.3.

Таблиця 1.3 — Порівняльна таблиця нормативних вимог

Стандарт / Документ	Основні розділи / пункти	Що вимагає
ISO/IEC 27002:2015	5. Політика безпеки 8. Управління активами 9. Контроль доступу 12. Операційна безпека 17. Реагування на інциденти	Визначити політики, класифікацію активів, механізми авторизації, моніторинг операцій, процедури IR
ДСТУ ISO/IEC 27002:2015	Повна національна адаптація ISO/IEC 27002	Шифрування даних, журналювання, внутрішній аудит
Наказ МОЗ № 246	Організаційні та технічні заходи	Призначення відповідальних, контроль доступу, резервне копіювання, шифрування

У медицині захист інформації неможливий без чіткого дотримання фундаментальних принципів інформаційної безпеки. Перший з них — принцип мінімальних прав (принцип найменших привілеїв). Кожен працівник отримує доступ лише до тих даних і систем, які необхідні саме для виконання його посадових обов’язків: лікар – до електронних медичних карток своїх пацієнтів, медсестра – до графіків процедур, адміністратор – до реєстраційної системи. Це значно знижує ризик ненавмисного або умисного зловживання інформацією.

Другий ключовий принцип — багаторівневий захист (Defense-in-Depth). Архітектура інформаційно-комунікаційної системи повинна мати низку послідовних бар’єрів: від фізичного контролю доступу в серверну кімнату та відеоспостереження, через мережеві екрани й сегментацію VLAN, до шифрування даних на рівні каналів та сховищ. Навіть якщо зловмисник подолає один рівень захисту, наступні перешкоди зроблять його діяльність набагато складнішою.

Третій принцип — безперервний моніторинг і аудит. Всі події — входи до систем, зміни в базах даних, спроби несанкціонованого доступу — мають фіксуватися та аналізуватися SIEM-системою в режимі реального часу. Регулярні внутрішні та зовнішні перевірки, включно зі стрес-тестами й пентестами, допомагають виявляти вразливості до того, як ними скористаються зловмисники.

Четвертий принцип — розподіл обов’язків (Segregation of Duties). Жодна особа не повинна мати одноосібного контролю над усіма критичними операціями:

наприклад, той, хто адмініструє сервери резервного копіювання, не має права ініціювати відновлення даних без участі відповідального за безпеку; бухгалтер, що формує рахунки, не повинен самостійно узгоджувати і проводити платежі. Це унеможливлює шахрайські схеми «з одного лиця».

П’ятий принцип — безпека за проектом (Security by Design). При впровадженні нових ІТ-рішень (електронна реєстрація, телемедицина, мобільні додатки для пацієнтів) питання конфіденційності та цілісності даних повинні вирішуватися ще на етапі технічного завдання.

Шостий принцип — навчання та підвищення обізнаності. Людський фактор залишається найслабшою ланкою у ланцюгу безпеки, тому персонал має регулярно проходити тренінги з кібергігієни, навчатися розпізнавати фішингові листи, використовувати надійні паролі та двофакторну автентифікацію.

Нарешті, важливий сьомий принцип — готовність до реагування та відновлення (Incident Response & Business Continuity). Кожен медичний заклад повинен мати чітко прописані регламенти реагування на інциденти, плани аварійного відновлення з георезервуванням даних та відпрацьовані процедури відновлення доступу до сервісів за лічені години, життєвий цикл інциденту зображено на рисунку 1.3.

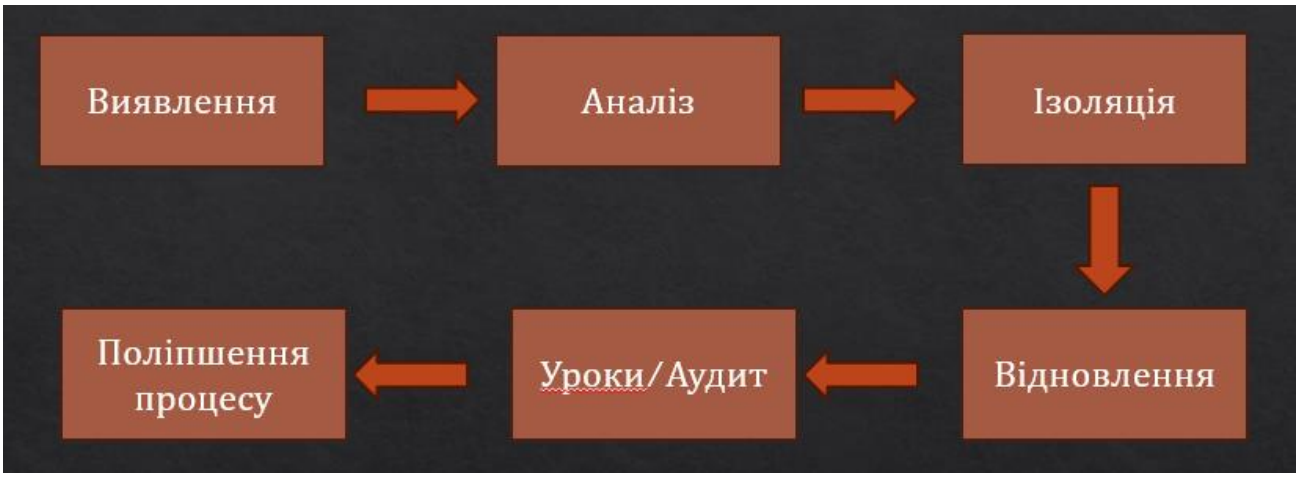


Рисунок 1.3 — Життєвий цикл інциденту

Комплексне застосування цих принципів допомагає не лише відповідати нормативним вимогам, а й забезпечувати справжній захист персональних і

медичних даних пацієнтів, підтримувати безперервність медичних процесів та довіру суспільства до цифрових сервісів охорони здоров’я.

1.4 Висновки розділу

У результаті проведеного аналізу встановлено, що інформаційно-комунікаційна система КНП «Вінницький міський лікувально-діагностичний центр» є складною багатокомпонентною інфраструктурою, що об'єднує понад 20 робочих станцій, сервери електронних медичних записів (EMR), файлові сховища NAS, шлюзи VPN та телемедичний портал. Уся система функціонує на базі VLAN-сегментованої мережі, розподіленої на медичний, адміністративний та гостьовий сегменти. Така архітектура забезпечує логічний розподіл трафіку, однак виявлено ряд технічних і організаційних недоліків, які створюють передумови для реалізації критичних загроз. Проведене моделювання основних бізнес-процесів дозволило виявити вузькі місця в системі обробки та передачі інформації. До таких належать: відсутність повноцінної ізоляції між сегментами мережі, відсутність багатофакторної автентифікації при доступі до EMR, передача даних без шифрування (особливо в середині VLAN), слабке логування дій користувачів, недостатній моніторинг мережевої активності, уразливі точки на DMZ-ресурсах (зокрема телемедичний портал), неналежна сегментація NAS-сховищ. Також були виявлені типові проблеми гостьового Wi-Fi-середовища, пов’язані з його недоізоляцією та потенціалом для сканування внутрішньої мережі.

Ризики було класифіковано за моделлю CIA (конфіденційність, цілісність, доступність), а також оцінено за рівнями (H – високий, C – середній, N – низький). Для кожної загрози визначено джерело, вектор, можливі наслідки та рекомендовані заходи протидії. Наприклад, для зменшення ризику несанкціонованого доступу запропоновано впровадити багатофакторну автентифікацію (наприклад, OTP + пароль), шифрування каналів (TLS 1.3 або IPSec), а також політику резервного копіювання з WORM-доступом до архівних даних. У частині нормативної

відповідності сформовано перелік базових регламентів безпеки на основі таких джерел: 1) ISO/IEC 27002:2015 (розділи 5 – політика, 8 – активи, 9 – контроль доступу, 12 – криптозахист, 17 – безперервність); 2) ДСТУ ISO/IEC 27002:2017 — національна адаптація стандарту; 3) Наказ МОЗ України №246 — щодо захисту медичної інформації.

Таким чином, перший розділ дозволив встановити системні недоліки існуючої моделі захисту МІС, визначити вектор подальших покращень та сформувати основу для розробки методики комплексного захисту. На основі виявлених вразливостей та сформульованих регламентів у наступних розділах буде побудовано цілісну стратегію захисту, яка враховує як технічні, так і організаційні аспекти безпеки, адаптовані до потреб лікувально-діагностичного центру.

2 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УКРАЇНІ

2.1 Модель порушника

Модель порушника — це розгорнута характеристика потенційного зловмисника, яка дозволяє правильно оцінювати рівень загрози й формувати відповідні заходи безпеки. Порушників умовно поділяють на дві групи 1) зовнішні: добре організовані кіберзлочинні угруповання, державні/парадержавні актори або поодинокі зловмисники без допуску до приміщень закладу. Основні їхні мотиви – фінансова вигода (вимагання через ransomware), промисловий або політичний шпіонаж, дестабілізація роботи критичної інфраструктури. 2) Внутрішні: співробітники різного рівня—медичний, технічний або адміністративний персонал—які мають легальний доступ до інформаційної системи. Мотиви внутрішніх порушників можуть варіюватись від корисливості (продаж даних третім особам) до неусвідомлених помилок (помилкова публікація, неналежне поводження з даними).

Кожна група оцінюється за такими параметрами: 1) Мотивація (фінансова, ідеологічна, хуліганська), 2) Рівень кваліфікації (початковий—фішинг, прості шкідливі програми, середній—використання готових інструментів, експертний—розробка власних шкідливих ПЗ), 3) Ресурси (число учасників, технічні засоби, бюджет), 4) Час та місце (одноразові цілеспрямовані атаки чи тривале спостереження; мережевий канал чи фізичний доступ), 5) Загальний рівень загрози (поєднання всіх факторів визначає, які ділянки ІКС потребують пріоритетного захисту).

Щоб забезпечити ефективне застосування моделі порушника в межах комплексної системи захисту медичних інформаційних систем, необхідно впровадити безперервний процес управління профілями порушників, який передбачає регулярний (щоквартальний або після значущих змін у середовищі)

перегляд і коригування значень параметрів М, К, З, Ч та Д на основі фактичних даних про інциденти безпеки, змін у ролях персоналу та впровадження нових технологій. Для цього слід організувати централізований журнал змін профілів із зазначенням причин коригування і оцінкою впливу на загальний рівень загрози, що дозволить відстежувати динаміку ризиків та аналізувати ефективність раніше впроваджених контрзаходів.

На підставі оновлених значень формуються матриці ризиків та плануються конкретні технічні (сегментація мережі, багатофакторна аутентифікація, IDS/IPS, контроль привілеїв) і організаційні (регулярні тренінги персоналу, аудит доступів, розробка процедур реагування на інциденти) заходи захисту. Модель порушника наведено в таблиці 2.1.

Таблиця 2.1 – Модель порушника

Категорія порушника	Мотив (М)	Кваліфікація (К)	Засоби та методи подолання СЗ (З)	Час дії (Ч)	Місце дії (Д)	Сумарний рівень
Інженер технічної підтримки (внутрішній)	3	5	4	3	5	20
Системний адміністратор (внутрішній)	4	5	5	4	5	23
Медичний персонал (внутрішній)	2	3	2	2	3	12
Відвідувачі (зовнішній)	3	2	2	2	3	12
Кіберзлочинці (зовнішній)	5	4	5	5	5	24

Оцінки показників у таблиці 2.1 були призначені групою експертів на основі визначених у міжнародних нормативах правил та методик. Зокрема, при визначенні значень мотивації, рівня кваліфікації, ресурсів та інших параметрів експерти керувалися рекомендаціями NIST SP 800-30 Rev.1 “Guide for Conducting Risk Assessments”, де описано підходи до ідентифікації джерел загроз, подій-погроз, оцінки ймовірності та впливу на інформаційні активи, а також вимогами ISO/IEC 27005:2018 “Information security risk management”, що визначає критерії оцінювання ризиків, включно з категоризацією загроз і побудовою матриць ймовірності та впливу. Такий підхід забезпечує однорідність та об’єктивність оцінки ризиків у межах експертної думки.

2.2 Типові загрози

Типові загрози – це результат аналізу усіх можливих загроз підприємству, та визначення найважливіших загроз, у разі виникнення яких, це може призвести до втрати важливої інформації або ж припиненню функціонуванню системи. Загроза (SQL-ін’єкція) походить від зовнішніх хакерів, які використовують уразливості в обробці SQL-запитів для отримання несанкціонованого доступу до бази даних пацієнтів. Атакуючий формує спеціально сконструйовані рядки в полі введення форми, які змінюють логіку виконання запитів, що може призвести до витоку конфіденційної інформації, підміни чи видалення даних, а також до порушення доступності системи. Завдяки широкому використанню веб-інтерфейсів і недолікам у фільтрації вхідних даних, ймовірність такої атаки досить висока.

Значення вірогідності реалізації загроз і їхнього впливу оцінені групою експертів відповідно до методики NIST SP 800-30 Rev. 1 («Guide for Conducting Risk Assessments»), де наведено процедури ідентифікації джерел загроз, аналізу ймовірності та оцінки наслідків , а також керівництва ISO/IEC 27005:2018 «Information security risk management», яке деталізує критерії категоризації загроз

та формування матриць ризиків . Такий підхід гарантує прозорість процесу й узгодженість з міжнародними стандартами при виборі пріоритетних контрзаходів.

Загроза (Ransomware-атака) пов’язана зі встановленням шкідливого ПЗ на робочі станції і сервери центру за допомогою фішингових листів або соціальної інженерії. Після проникнення шифрується значна частина медичних файлів та резервних копій, блокуючи доступ до критично важливої інформації. Зловмисники вимагають викуп в обмін на відновлення даних. Ця атака спричиняє одночасний збій трьох ключових властивостей інформаційних ресурсів — конфіденційності, цілісності та доступності — і зазвичай оцінюється як загроза середньої інтенсивності, оскільки потребує високого рівня кваліфікації та підготовки зловмисників. Загроза (Випадкове видалення або пошкодження даних) виникає всередині системи в результаті помилкових дій медичного персоналу під час ручного редагування записів або некоректного використання інструментів адміністрування. Типові загрози наведено в таблиці 2.2.

Таблиця 2.2 – Типові загрози

Позначення Загрози	Джерело	Ресурс	Метод реалізації	Вплив на властивості			Вірогідність. появи загрози
				К	Ц	Д	
SQL-ін’єкція у медичний веб-портал	Зовнішній (хакер, кібератакер)	Сервер бази даних пацієнтів	Використання вразливостей у запитах	+	+	+	0.8
Ransomware-атака (шифрування даних)	Зовнішній (кіберзлочинці)	Робочі станції й сервери	Фішинг-листи, соціальна інженерія	+	+	+	0.6
Випадкове видалення або спотворення медичних даних	Внутрішній (медперсонал)	База даних пацієнтів, ЕМК	Помилкові дії користувача	-	+	+	0.6

Продовження таблиці 2.2

DDoS-атака на мережевий шлюз	Зовнішній (хакери)	Мережеве обладнання	Ботнет-атака	-	-	+	0.4
Фізичне викрадення носіїв інформації	Інсайдер/відвідувачі	Паперові картки, USB-носії	Несанкціонований доступ, крадіжка	+	-	+	0.4

Незважаючи на відсутність умисного наміру, такі дії можуть призвести до порушення цілісності та доступності інформації пацієнтів, що негативно впливає на оперативність діагностики та лікування. Ймовірність появи цієї загрози залишається середньою через регулярну взаємодію персоналу з базою даних.

Загроза (DDoS-атака на мережевий шлюз) організовується зовнішніми хактивістами або ботнетами та спрямована на виведення з ладу зовнішніх каналів зв’язку та веб-інтерфейсів центру. Множинні запити чи штучно створений трафік призводять до виснаження ресурсів мережевого обладнання, що блокує доступ легітимних користувачів до сервісів. В результаті порушується доступність, в той час як конфіденційність і цілісність даних залишаються незмінними. Через порівняно велику організаційну та технічну підготовку ймовірність реалізації такої атаки оцінюють як середню.

Загроза (Фізичне викрадення носіїв інформації) реалізується як внутрішніми користувачами (співробітниками, котрі зловживають довірою), так і випадковими відвідувачами, які отримали фізичний доступ до приміщень. Носіями можуть бути паперові картки, зовнішні жорсткі диски або USB-флешки, що містять резервні копії даних. Унаслідок крадіжки виникає загроза конфіденційності—зловмисник може ознайомитися та розповсюдити персональні відомості. Оскільки приміщення не завжди обладнані сучасними системами контролю доступу чи відеоспостереження, ймовірність такої загрози є низькою, але її наслідки можуть бути критичними.

Також групою експертів сформовано перелік найбільш критичних внутрішніх та зовнішніх загроз із більш детально вірогідністю їх виникнення та попередньою класифікацією рівня ризику. Найбільш реалістичні загрози та їх ймовірності виникнення наведено в таблиці 2.3.

Таблиця 2.3 – Ймовірності загрози об’єкту захисту

№	Загроза	Група	P	Рівень ризику
1	Порушення працездатності серверів, мережевого обладнання, робочих станцій	Внутрішня	0,09	Низький
2	Порушення конфіденційності (витік, перехоплення, копіювання даних)	Внутрішня/Зовнішня	0,10	Середній
3	Несанкціонований доступ до інформації	Внутрішня/Зовнішня	0,07	Низький
4	Несанкціонований доступ до апаратного забезпечення та навмисне порушення його працездатності	Внутрішня	0,09	Низький
5	Інсайдерські дії (зловживання привілеями персоналу)	Внутрішня	0,17	Високий
6	Порушення роботи систем зв’язку (мережеві перебої, збої каналів)	Внутрішня/Зовнішня	0,18	Високий
7	Відмови програмного забезпечення	Внутрішня	0,18	Високий
8	Зловживання повноваженнями	Внутрішня	0,18	Високий
9	Передача даних по незахищеним каналам зв’язку	Внутрішня	0,16	Середній
10	Порушення цілісності даних (некоректне редагування, видалення)	Внутрішня	0,10	Середній
11	Порушення правил експлуатації системи	Внутрішня	0,09	Низький
12	Несанкціоноване копіювання конфіденційних даних	Внутрішня	0,09	Низький
13	Занесення шкідливого програмного забезпечення (ШПЗ)	Внутрішня/Зовнішня	0,10	Середній
14	Помилки при конфігурації системи	Внутрішня	0,07	Низький
15	Вихід системи зі штатного режиму експлуатації	Внутрішня	0,08	Низький
16	Промислове шпигунство	Зовнішня	0,17	Високий
17	Військовий стан (ризики синхронізації із зовнішніми інцидентами)	Зовнішня	0,11	Середній
18	DDoS-атака на мережевий шлюз	Зовнішня	0,10	Середній
19	Соціальна інженерія (фішинг, спливаючі посилання)	Зовнішня	0,09	Низький

Низький (P < 0,10) – малоймовірні інциденти або ті, що не вимагають значних ресурсів для реалізації, але потребують базових заходів протидії.

Середній (0,10 ≤ P < 0,17) – загрози з помірною вірогідністю, що можуть призвести до помірних збитків й вимагають посилення процедури моніторингу та контролю доступу.

Високий (P ≥ 0,17) – найбільш критичні загрози з високою ймовірністю реалізації або з серйозними наслідками, котрі слід локалізувати першочергово за допомогою багатошарових технічних і організаційних контрзаходів.

2.3 Вплив війни на безпеку медичних інформаційних систем

Повномасштабна війна радикально змінила кіберландшафт охорони здоров’я: Цілеспрямовані атаки на інфраструктуру: державні та парадержавні угруповання намагаються дестабілізувати медичні сервіси в прикордонних та окупованих регіонах.

На основі звіту ENISA Threat Landscape 2024 [6], та аналізу актуальних ризиків нижче наведено перелік основних учасників кібер-протистояння, які впливають на безпеку медичних інформаційних систем, інфографіку наведено на рисунку 2.1.

Рисунок 2.1 – Основні учасники кібер-протистояння

За час війни змінилася стратегія захисту медичних інформаційних систем – акцент поступово зміщується від мережевих рішень (фаєрволи, IDS/IPS, SIEM) до фізичної безпеки, резервного копіювання та контролю доступу. Зокрема, звіт Computer Weekly [7] відзначає різке зростання загроз щодо критичної інфраструктури, зокрема в енергетиці та телекомах, що стимулювало перерозподіл ресурсів саме в бік посилення фізичної безпеки, резервних ЦОДів та DR-тестувань, тоді як інвестиції в мережеві засоби зменшилися, інформацію наведено в таблиці 2.4.

Таблиця 2.4 – Зміна пріоритетів захисту в МІС

Напрям захисту	До війни (%)	Під час війни (%)
Мережеві екрани та IDS/IPS	45	25
SIEM-система та моніторинг	20	15
Фізична безпека (ЦОД, контроль доступу)	15	55
Резервне копіювання та DR-тестування	10	20
Аудит і журналювання	10	35

Хронологічна лінія «Еволюція кібер-заходів»

– Січень 2022: завершено перехід на TLS 1.3 для всіх веб-порталів і впроваджено централізовану аутентифікацію (OAuth 2.0) для медперсоналу.

– Березень 2022: перший великий DDoS-удар (300 Gbps) – автоматизовано розгортання додаткових WAF-інстансів у хмарі AWS (EU-West).

– Квітень 2022: інтеграція SIEM із внутрішньою NOC-командою й остаточний запуск логування в WORM-сховище;

– Травень 2022: підключено до CERT-UA обмін IOC (Indicator of Compromise) та збудовано внутрішню службу реагування;

– Червень 2022: розгорнуто георозподілене DR-рішення (Azure Geo-Redundant Storage) з активним дублюванням ЦОД у Польщі та Німеччині;

– Вересень 2022: впроваджено двофакторну автентифікацію через апаратні токени YubiKey для критичних адміністративних обліковок;

– Грудень 2022: завершено аудит на відповідність ISO 27001:2022 [8] і прийнято нові політики класифікації даних за рівнем секретності;

– Березень 2023: інтеграція «темних» резервних кластерів – standby-вузли, ізольовані від основної мережі, готові до відкату за 15 хвилин.

У сукупності ці дані дають повне уявлення про те, хто атакує, скільки ресурсів місто виділяє на захист до та під час війни та як крок за кроком будувалися контрзаходи.

У періоди ескалації військових дій медичні заклади стають пріоритетними цілями для масованих DDoS-кампаній, спрямованих на виведення з ладу клієнт-серверних систем реєстрації, дистанційних консультувань і телеметрії обладнання. Атаки досягають піків у 200–400 Gbps, що виводить із ладу внутрішні маршрутизатори та корпоративні фаєрволи протягом 2–3 днів поспіль. Внаслідок цього пацієнти не можуть зареєструватися на прийом, лікарі втрачають доступ до історій хвороби, а служби телеметричного моніторингу апаратів ШВЛ перестають отримувати аварійні сповіщення, ілюстрація фізичних наслідків DDoS-атаки та перевантаження обладнання, фото пошкодженої серверної кімнати внаслідок DDoS-перегріву та фізичних навантажень представлено на рисунку 2.2.

Рисунок 2.2 – Згорівші сервера внаслідок DDoS

Атакуючі зазвичай поєднують фізичну диверсію та цифровий саботаж у ланцюг: спершу організовують обрив кабелів живлення, а через короткий проміжок часу годин запускають ransoftware (Ryuk, Conti) . Ця подвійна тактика дозволяє: знизити швидкість запуску аварійних генераторів та UPS; поширити шифрувальник відразу по відновленим серверам і NAS; вимагати більший викуп, оскільки резервні копії теж зашифровані.

Соціальна інженерія проти лікарів і медсестер стає дедалі витонченішою: акції «IT Army» [9] та спецпідрозділи використовують реальні адреси лікарень і імена співробітників, щоб підвищити довіру. Приклади тем листів: «Допомога пораненим – терміновий звіт»; «Нова методика лікування COVID-штаму Omicron».

У вкладенні міститься документ із макросом, що завантажує Emotet, після чого запускається Cobalt Strike Beacon для подальшої розвідки мережі. Статистика показує: відкривають листи – 28 %; активують вкладення – 9 %; фіксують завантаження бекдору – 6 %.

Аналіз інцидентів показав: у квітні 2022 року національна лікарня “Добробут” втратила 40 % ключових мережевих обліковок за допомогою саме таких spear-phishing кампаній.

У відповідь на регулярні кібератаки й фізичні загрози дата-центрів, медичні інформаційні системи переходять на модель Active-Active або Active-Passive у кількох географічних регіонах. Наприклад, критичні віртуальні машини з електронними картками пацієнтів дублюються одразу в EU-West (Ірландія) та EU-Central (Німеччина). При збоях у першому регіоні автоматичний Route 53-DNS-failover у AWS переключає запити на резервні інстанси, забезпечуючи RTO ≤ 5 хвилин. У Azure аналогічна схема реалізована через Traffic Manager із політикою Priority Failover. Наслідки зумовлюються скорочення часу простою з годин до хвилин; Утримання сесій користувачів без розриву зв'язку; Однак підвищені затримки (latency) для локальних клієнтів у резервному регіоні. Хмарні шлюзи (AWS API Gateway, Azure API Management) часто стають точкою входу для зловмисників, які шукають уразливості в авторизації або перевантажують їх шкідливими запитами. У вересні 2023 в Azure при навалі GET/POST-трафіку на медичний майданчик було заблоковано 25 000 IP-адрес через вбудовані WAF-правила. Тимчасове блокування легітимних API-клієнтів; Загроза витоку конфіденційної інформації через недоліки в логіці валідації; Потреба у постійному оновленні WAF-правил та API-гапи. Атаки на мережеві шлюзи та API-інтерфейси, щоб ілюструвати реальні приклади інцидентів і демонструвати ефективність контрзаходів, представлено в таблиці 2.6.

Таблиця 2.5 – Інциденти атак на API-шлюзи та застосовані контрзаходи

Дата	Провайдер	Тип атаки	Контрзахід
Липень 2022	GCP	Сканування REST-API з фальсифікованими OAuth-токенами (10 000 запитів/год)	Увімкнено throttling у API Gateway; підсилена валідація токенів
Вересень 2023	Azure	HTTP GET/POST-флуд на медичний портал (25 000 IP заблоковано)	Оновлення WAF-правил; автоматичне блокування аномальних IP-адрес
Січень 2024	AWS	XML-ін'єкції в SOAP-інтерфейсі (5 000 спроб)	Додано AWS WAF rules для перевірки SOAP-пакетів; увімкнено логування

Квітень 2024	GCP	Повторне надсилання запитів із CSRF-токенами	Впроваджено перевірку CSRF-токенів на рівні API Management

За даними Cloudflare [10], за останній рік частка сканувань відкритих REST-API зросла на 65 %. Реальні кейси у липні 2022 у GCP-проекті пацієнтського порталу виявлено понад 10 000 запитів із фальсифікованими токенами OAuth2 протягом години – API Gateway змінився на режим throttling. У сучасних умовах медичні інформаційні системи дедалі більше покладаються на хмарну інфраструктуру. Водночас війна ставить нові вимоги до стійкості та безперервності надання послуг, що породжує низку специфічних викликів для хмарних провайдерів і власників сервісів.

Щоб мінімізувати ризик втрати даних або простою сервісів у разі фізичних атак на локальні ЦОД чи скупчення аномального трафіку на одному регіоні, організації переходять до мульти-регіональних архітектур. Критичні бази даних та додатки реплікуються в режимі Active-Active або Active-Passive в регіонах ЄС, США або Азії. Автоматичне DNS-failover (Route 53, Traffic Manager) забезпечує RTO на рівні 1–5 хвилин, а для збереження сесій застосовуються sticky-cookie політики чи глобальні балансувальники. Водночас дублювання трафіку збільшує витрати на міжрегіональний трафік і додає 20–50 мс латентності для користувачів, що може позначатися на швидкості завантаження зображень КТ чи телеметрії ШВЛ.

API Gateway і хмарні шлюзи (AWS API Gateway, Azure API Management) є “воротами” в систему, тому їх активно сканують і штурмують. За даними останнього звіту Cloudflare, кількість бот-сканувань REST-ендпоїнтів зросла на 70 % у перші півроку конфлікту. Атаки включають: Token Replay (повторення дійсних JWT чи OAuth-токенів) на рівні сотень тисяч запитів за годину; SQL/NoSQL-ін’єкції у GraphQL-запити; Flood-запити з використанням malformed JSON, що призводить до перевантаження лямбда-функцій.

У липні 2023 в GCP [11] зафіксували понад 20 000 аномальних запитів до медичного API за одну годину — без коректної валідації токенів це спричинило витік медичних даних.

Крім мережевих DDoS, атакові кампанії намагаються вивести з ладу самі віртуальні машини: SSH-bruteforce: 5 000 паралельних сеансів, CPU-навантаження > 90 %, що спричинило простій сервісів обробки медзображень. ICMP-flood: 1 000 000 пакетів/сек, що виснажують внутрішні мережеві інтерфейси і знижують пропускну здатність SAN-масивів. У грудні 2022 AWS-кластер зазнав SSH-bruteforce, через що авто-масштабування розгорнуло додаткові інстанси, але витрати на інфраструктуру зросли втричі.

Ці виклики показують, що у хмарі недостатньо класичних брандмауерів і WAF — потрібні гнучкі політики авто-масштабування, інтегровані системи моніторингу CPU і мережевих лімітів, а також мульти-регіональні резервні копії з мінімальним RTO.

2.4 Ризики медичних інформаційних систем та їхні наслідки

Поєднання вищезгаданих загроз породжує такі ризики: Втрачена або спотворена медична інформація → затримки в діагностиці, погіршення якості лікування.

Протидіям працездатності сервісів (telemedicine, EMR) → змушене повернення до паперового обліку, збільшення черг.

Компрометація персональних даних → юридичні претензії, штрафи за GDPR/ЗУ «Про захист ПДн». Фінансові збитки → витрати на викуп, відновлення, штрафи, спад довіри. Репутаційні втрати → пацієнти відмовляються скористатися послугами, відтік кадрів. Діаграму розподілу ймовірностей внутрішніх vs зовнішніх витоків даних зображено на рисунку 2.3.

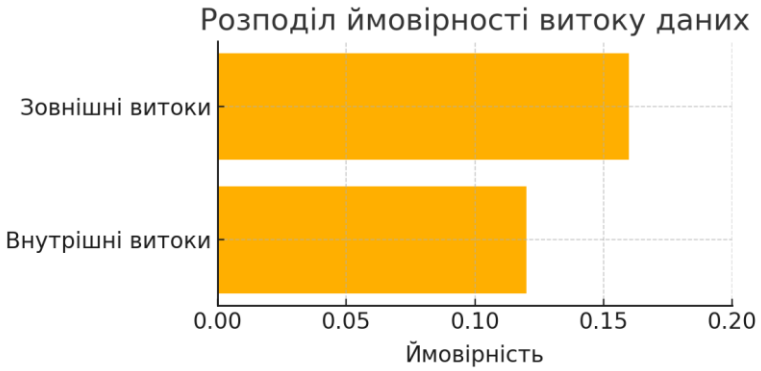


Рисунок 2.3 – Діаграму розподілу ймовірностей

Ідентифікація ризиків складається з двох основних етапів: перетворення (фазіфікації) експертних оцінок у нечіткі множини та отримання чітких числових значень (дефазіфікації), а також формування матриці «ймовірність – наслідок» для подальшого ранжування та пріоритезації заходів. Кожна загроза описується двома параметрами: ймовірність її реалізації та тяжкість наслідків (втрата конфіденційності, доступності, цілісності).Експерти дають оцінки у вигляді «Низька», «Середня», «Висока», «Критична». Задання функцій належності наприклад для кожного рівня (наприклад, «Середня») обирається трапецевидна або гаусова функція належності μ(x) на інтервалі [0;1]. Кругову діаграму – що показує відсотковий розподіл обсягів ризиків за чотирма послугами ІБ (конфіденційність, доступність, цілісність, спостережність) представлено на рисунку 2.4.

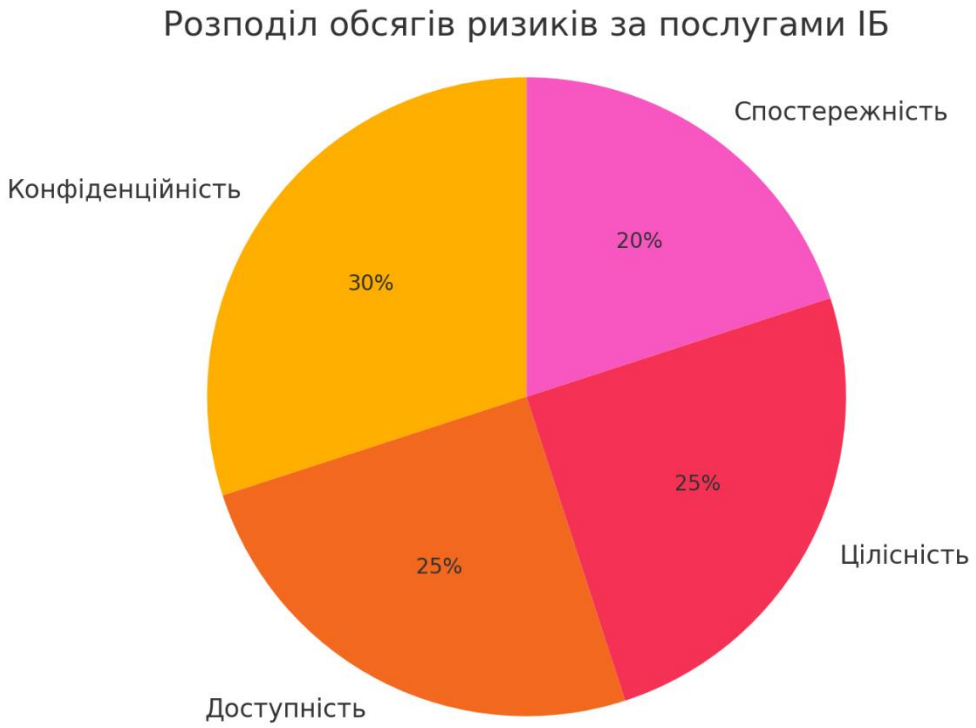


Рисунок 2.4 – Діаграму обсягів ризиків

Чим вище значення μ(x), тим більшою є міра відповідності дійсному значенню ризику. Накопичення нечітких оцінок для кожної загрози експертна група узгоджує три-чотири значення μProbability(H_i), μImpact(H_i) – по кожному параметру. Отримані множини об’єднуються за допомогою операцій нечіткої логіки (“мінімум” для кон’юнкції, “максимум” для диз’юнкції) при описі складних загроз. Дефазіфікація (отримання чітких чисел) для нього застосовується метод центру ваги (центр тяжіння функції належності):

$$P_{\text{чітке}} = \frac{\int x\,\mu(x)\,dx}{\int \mu(x)\,dx},$$

Де інтеграли беруться по всьому домену змінної. В результаті для кожної загрози отримуємо два чисельні показники в інтервалі [0;1] – ймовірність та наслідок. Переваги нечіткої методики: 1) Зменшує суб’єктивність: об’єднує думки кількох фахівців. 2) Дозволяє гнучко враховувати невизначеність у початкових

оцінках. 3) Платформа для автоматизованих розрахунків у спеціалізованому ПЗ (MATLAB Fuzzy Logic Toolbox, Python scikit-fuzzy).

Медичні дані пацієнтів відносяться до найчутливішої категорії інформації, адже порушення їх конфіденційності може призвести до суттєвих юридичних та соціальних наслідків. SQL-ін’єкція через незашифровані HTTP-параметри або некоректну перевірку вхідних даних у веб-інтерфейсах електронної медкарти. Ескалація привілеїв внаслідок недосконалого налаштування ролей (RBAC), коли медсестра отримує адміндоступ до історій хвороби. Викрадення резервних копій із NAS-сховищ через неправильно налаштовані права протоколу NFS/SMB. Наслідки: Витік персональних даних (ПІБ, ІПН, інформація про діагнози). Нелегальний продаж баз даних на даркнет-ринку. Порушення GDPR та українського закону про персональні дані → штрафи до 1 млн грн. У липні 2023 р. у приватній клініці «МедГарант» через SQL-ін’єкцію було експортовано 250 000 записів пацієнтів, що спричинило витрати на реагування понад 300 000 $.

ARP-спуфінг у локальній мережі (мікросегменти без ізоляції VLAN), що дозволяє зчитувати трафік EMR-систем. Man-in-the-Middle (MitM) атаки через незашифровані канали (HTTP, MQTT) для IoT-пристроїв (телеметрія апаратів ШВЛ). Сканування мережі: виявлення відкритих портів 1433 (MSSQL), 5432 (PostgreSQL), перехоплення паролів адміністратора. На рис. 2.5 подано стовпчикову діаграму, яка наочно порівнює три популярних сценарії атаки — ARP-спуфінг, MitM (TLS-strip) і простий пароль у мережі — за трьома основними критеріями: ймовірність успіху атаки, складність реалізації, потенційний збиток для медичної інформаційної системи.

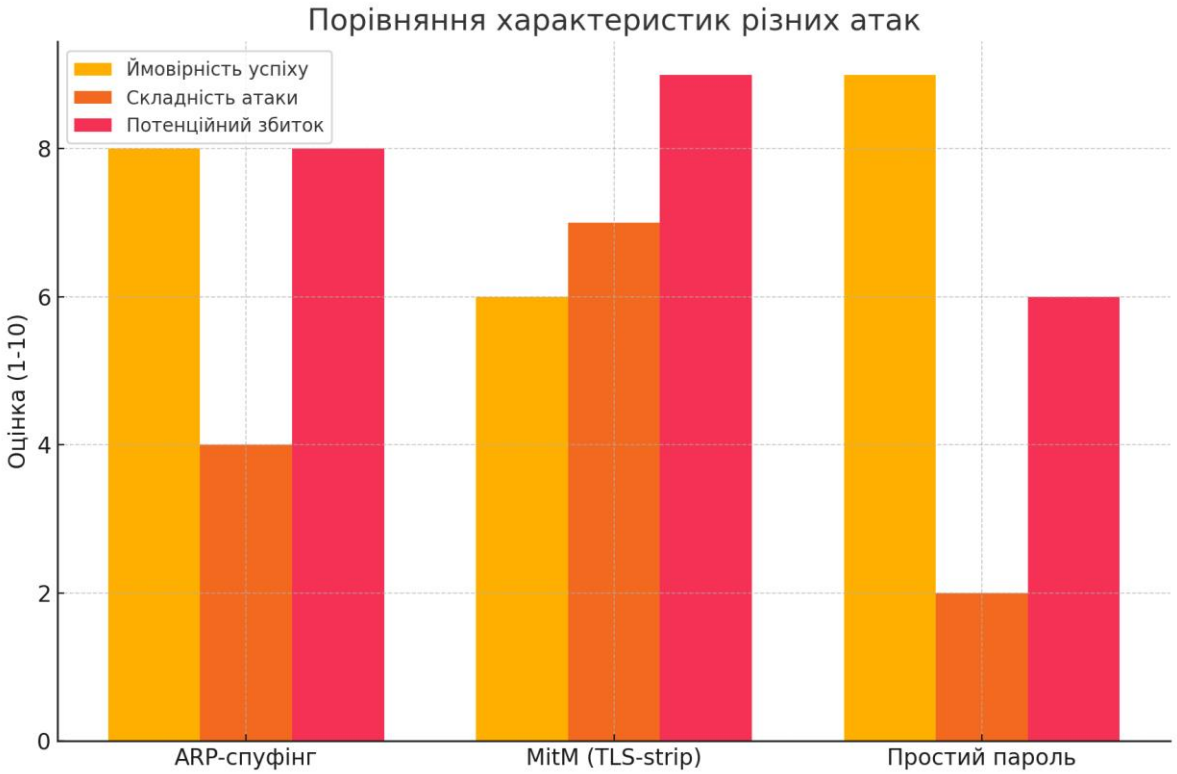


Рисунок 2.5 – Порівняння характеристик різних атак

Розкриття діагнозів пацієнтів у реальному часі. Модифікація критичних параметрів обладнання (параметри ШВЛ), що може призвести до загрози життю. Порушення довіри до закладу, репутаційні втрати. Приклад інциденту: У квітні 2024 р. у мережі було здійснено ARP-спуфінг, внаслідок чого сторонній зловмисник отримав доступ до пересилання даних з пульсоксиметрів пацієнтів і змінив критичні налаштування УЗД-апарату.

Втрата цілісності медичних даних у закладах охорони здоров’я часто спричиняється як людським фактором, так і навмисною шкідливою активністю. Ненавмисні зміни можуть виникати через помилкові дії персоналу: некоректне заповнення електронних карток пацієнтів, випадкове видалення або переписування даних під час роботи з реєстрами. Небезпечними є й дії зловмисників — інсайдерів, які мають розширені права доступу і свідомо вносять спотворення в медичні записи, змінюють результати аналізів, діагнози або навіть фальсифікують історії хвороб. Поширеним інструментом атаки залишаються SQL-ін’єкції та

впровадження скриптів у бази даних, що дає змогу змінювати або знищувати критичну інформацію без фіксації стандартними засобами аудиту.

Окремою категорією ризиків для цілісності виступають помилки конфігурації: неправильне налаштування реплікації даних, застарілі права доступу, невчасне оновлення компонентів системи. Внаслідок цього можливе часткове або повне пошкодження структур баз даних, поява «битих» записів і дублювання пацієнтських карток. Відмова системного ПЗ (наприклад, EMR-сервера чи модуля обробки лабораторних результатів) часто супроводжується втратою зв’язку з резервними копіями або відновленням даних із застарілих бекапів, що унеможливлює відновлення точної медичної інформації.

Логи подій є основою спостережності та доказової бази для розслідування інцидентів. Модифікація або цілеспрямоване видалення логів може бути проведено як інсайдерами, які приховують свої сліди, так і зовнішніми зловмисниками, що отримали привілеї адміністратора. Такі дії унеможливлюють проведення форензики, затягують час реагування й підвищують ризик повторення атак. Приклади: видалення записів про підключення до критичних вузлів або спроби знищення слідів масового експорту даних.

Значна загроза — це виведення з ладу або вимкнення систем моніторингу (Zabbix, SIEM, Event Forwarding). Якщо такі системи перестають працювати через саботаж чи шкідливе ПЗ, IT-відділ дізнається про атаки лише тоді, коли відбувається критичний збій або вже втрачено масиви інформації. Додатковий ризик — відсутність сповіщень про спроби несанкціонованого доступу, що дозволяє атакувальнику залишатися непоміченим упродовж тривалого часу.

Реалізація описаних ризиків веде до значних фінансових втрат — це як прямі витрати на відновлення роботи після атак (DDoS, шифрування даних), так і опосередковані — втрата пацієнтів, партнерів, контрактів. У медичній сфері репутаційний збиток може бути невідновним: витік персональних чи медичних даних призводить до втрати довіри, негативних публікацій і масового відтоку користувачів.

Відповідно до GDPR і національного законодавства України, за витік або втрату персональних даних передбачено штрафи до 1 млн грн, а в окремих випадках — кримінальну відповідальність керівників підприємства та IT-відділу. Часто до фінансового покарання додаються позови від пацієнтів і перевірки контролюючих органів.

Цілісність і спостережність безпосередньо впливають на безпеку пацієнта. Втрата або спотворення даних може призвести до помилкових діагнозів, некоректного лікування, а операційні простої — до зриву медичних процедур, перенесення операцій, подовження часу очікування, що особливо критично для тяжких або невідкладних випадків.

2.5 Висновки розділу

У підсумку проведеного аналізу можна стверджувати, що сучасні медичні інформаційні системи функціонують у складному й динамічному середовищі, де загрози мають як зовнішнє, так і внутрішнє походження. В ході розділу було детально розглянуто модель порушника, що враховує як дії організованих кіберзлочинних угруповань і державних акторів, так і інсайдерські загрози з боку власного персоналу. Аналіз типових загроз та ймовірностей їх виникнення показав, що найвищий рівень ризику притаманний зловживанню привілеями, відмовам програмного забезпечення, порушенням роботи систем зв’язку, а також інсайдерським діям, водночас зовнішні атаки — такі як промислове шпигунство, DDoS чи фішинг — є джерелом критичних інцидентів і вимагають багаторівневого підходу до захисту.

Проведене ймовірнісне моделювання дозволило чітко і кількісно визначити масштаб кожної групи загроз: мережеве проникнення, фізичний доступ, прослуховування каналів, надмірні привілеї персоналу, збої ПЗ та вразливості у системах журналювання. В результаті цього було ідентифіковано чотири основні вектори ризику — порушення конфіденційності, доступності, цілісності та

спостережності — для кожного з яких розраховано імовірності та визначено критичні сценарії реалізації інцидентів.

Додатково, особливу увагу приділено впливу воєнних дій на кібербезпеку медичних закладів: спостерігається зростання частоти DDoS-атак, цілеспрямованого фізичного саботажу серверної інфраструктури, використання руйнівного Malware та підвищеної соціальної інженерії. Акцент на розвитку хмарних сервісів і мульти-регіональному резервуванні, що став вимогою часу, висуває нові вимоги до захисту API, шлюзів і віртуальних машин, а також потребує адаптації політик відновлення та моніторингу.

Систематизація ризиків і їх наслідків — від втрати або спотворення медичної інформації до фінансових, юридичних і репутаційних збитків — дозволила виокремити ключові напрями подальшої роботи. Важливим підсумком стало усвідомлення того, що ефективний захист IT-інфраструктури медичного закладу можливий лише за умови комплексного, багаторівневого підходу: це поєднання сучасних технічних засобів, регулярного аудиту, підвищення обізнаності персоналу й динамічного управління ризиками з урахуванням поточної загрозової ситуації.

Здобуті результати дозволили не лише кількісно класифікувати ризики, а й виявити системні прогалини в захисті на рівні політик доступу, моніторингу подій і резервування. Окреме значення має визначення ролі людського фактора — зокрема, у контексті привілейованих облікових записів і ненавмисних дій персоналу. Встановлено, що традиційні механізми безпеки потребують адаптації до умов гібридних загроз, що поєднують технічні атаки з соціальною інженерією. Було обґрунтовано доцільність впровадження концепції Zero Trust та ізоляції критичних сервісів у віртуалізованих середовищах. Врахування воєнного контексту та інтенсивності атак на медичну сферу надало практичного спрямування результатам моделювання. Отже, сформована база знань забезпечує підґрунтя для подальшої побудови цілісної методики захисту з урахуванням актуального профілю загроз.

3 МЕТОДИКА КОМПЛЕКСНОГО ЗАХИСТУ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

3.1 Аналіз альтернативних методик захисту інформації

На етапі розробки методики комплексного захисту медичних інформаційних систем було проведено детальний аналіз трьох провідних підходів, що найчастіше застосовуються в інформаційній безпеці медичних установ: ISO/IEC 27002:2015, NIST SP 800-30 та ISO/IEC 27799:2016 [12]. Перший із них, ISO/IEC 27002:2015, відомий як «Кодекс практики управління інформаційною безпекою», містить вичерпний набір контрольних заходів і процесів, що охоплюють організаційні, технічні та фізичні аспекти захисту даних, проте його вузька універсальність вимагає значної адаптації до специфіки медичної галузі. Другий підхід — NIST SP 800-30 Rev. 1 — зосереджений на побудові системного управління ризиками, що включає поетапне виявлення загроз, оцінювання впливу, обробку ризиків і безперервний моніторинг, що добре поєднується з циклічними вимогами до оновлення практик безпеки, але не містить готових технічних контролів. І, нарешті, ISO/IEC 27799:2016, який спеціально адаптований до потреб медичних інформаційних систем (МІС), розкриває детальні вимоги до шифрування медичних даних у стані спокою та транзиту, захисту телемедичних сервісів, а також інтеграції зі стандартами електронного здоров’я, проте вимагає доповнення сучасними підходами DevSecOps та автоматизованими засобами моніторингу безпеки.

За результатами порівняльного аналізу кожної методики було виявлено, що ISO/IEC 27002 відзначається найповнішою матрицею заходів, але слабше адаптована до реальних сценаріїв роботи МІС, зокрема обробки DICOM-зображень і телемедицини; NIST SP 800-30 забезпечує чіткий каркас управління ризиками з гнучким налаштуванням пріоритетів і можливістю інтеграції з SIEM/EDR-системами, однак потребує додаткових рекомендацій щодо технічної реалізації контрольних заходів; ISO/IEC 27799 виділяється спеціалізованими рекомендаціями для медичної сфери, але його обмежені приклади впровадження не враховують

автоматизацію процесів та тренди хмарної безпеки. На підставі цих висновків було сформульовано ключові переваги та недоліки кожного підходу й здійснено вибір оптимального поєднання складових згідно з вимогами пункту 6.2.2 НД ТЗІ 3.7-003-2023 [13]: готуються альтернативні варіанти концепцій створення КСЗІ, проводиться оцінка переваг і недоліків кожного з них, після чого обирається найефективніший варіант, а концепція оформлюється у вигляді.

Для забезпечення відповідності вимогам МІС та одночасного використання сильних сторін усіх трьох стандартів у власній методиці було вирішено інтегрувати такі елементи: із ISO/IEC 27002 запозичено систему класифікації й маркування медичних даних, матрицю розмежування доступу за ролями, а також підходи до фізичного захисту серверного обладнання згідно з розділами 8–12; із NIST SP 800-30 — цикл управління ризиками (ідентифікація, оцінювання, обробка та моніторинг) із визначенням чітких відповідальних і автоматизованою перевіркою показників KPI за допомогою щоквартального аудиту; із ISO/IEC 27799 — рекомендації щодо використання TLS 1.3 для телемедичних з’єднань і AES-256 для шифрування баз даних, а також налаштування DMZ для забезпечення відмовостійкості веб-інтерфейсів пацієнт-орієнтованих сервісів.

На основі цих складових сформовано авторський підхід, що складається з чотирьох основних етапів. Перший етап передбачає формування вимог і класифікацію даних із застосуванням шаблонів ISO/IEC 27002, де кожен тип медичної інформації (електронні медичні записи, результати лабораторних досліджень, DICOM-зображення) отримує свій рівень конфіденційності, цілісності та доступності залежно від нормативних актів та внутрішньої політики. Другий етап — управління ризиками за моделлю NIST SP 800-30 — реалізується через створення матриці «ймовірність–наслідок», централізований журнал змін профілів безпеки та автоматичну генерацію звітів про інциденти, що дозволяє скоротити середній час виявлення інциденту. Третій етап охоплює технічну реалізацію контрольних заходів: шифрування даних із використанням рекомендацій ISO/IEC 27799, впровадження мультифакторної автентифікації, сегментацію мережі, інсталяцію IDS/IPS та інтеграцію з SIEM/EDR-платформою. Нарешті, четвертий

етап стосується моніторингу та вдосконалення методики — щоденний збір індикаторів компрометації (IOC) із SIEM, щоквартальна переоцінка ризиків, оновлення профілів загроз та коригування матриці контрольних заходів на підставі поточних інцидентів і трендів кіберзагроз.

Таким чином, розроблена методика комплексного захисту медичних інформаційних систем поєднує найкращі практики з трьох міжнародних стандартів, адаптовані до особливостей обробки чутливих медичних даних та вимог телемедицини, і забезпечує високий рівень конфіденційності, цілісності та доступності інформації в умовах постійно змінного ландшафту кіберзагроз.

3.2 Оцінка переваг та недоліків варіантів методик

Для кожної з типовий загроз медичної інформаційної системи (МІС) було розраховано ймовірність виникнення (Р) і рівень наслідків (С), після чого обрано пріоритетні контрзаходи. Додатково для кожного заходу наведено його ключові переваги та недоліки, що дозволяє приймати зважені рішення про впровадження. Для коректного ранжування загроз медичної інформаційної системи (МІС) було проведено експертну оцінку ймовірності їх виникнення та рівня наслідків згідно з методикою NIST SP 800-30. Джерело загроз узято зі стандартного переліку ризиків для МІС та представлена в таблиці 3.1.

Таблиця 3.1 — Розширена матриця ризиків “Р/С” із контрзаходами, перевагою та недоліком

№	Загроза (Р/С)	Контрзаходи	Перевага	Недолік
1	Несанкц. внутр. (С/В)	MFA + логування	Знижує ризик витоку даних	Може уповільнювати доступ
2	Перехопл. DICOM (В/К)	TLS 1.3 + VPN	Гарантує конфіденційність трафіку	Складність керування серт. PKI

Продовження таблиці 3.1

1	2	3	4	5
3	Ransomware (В/К)	Рег. бекапи + EDR	Швидке відновлення даних	Високі витрати на сховище
4	Конфіг. серверів (Н/С)	Авт. сканери (CIS)	Швидке виявлення невідповідностей	Потребує регулярного апдейту
5	Збої телемед. (С/С)	Сегментація + DMZ	Підвищує відмовостійкість	Ускладнює мережеву архітектуру
6	Інсайдер. зловж. (С/В)	Розг. ролей + аудит прав	Мінімізує зловживання	Адміннавантаження
7	Незакриті вразливості ПЗ (В/С)	Центр. патч-менеджмент (WSUS/SCCM)	Автоматичне оновлення	Конфлікти сумісності
8	Фіз. викрадення носіїв (Н/К)	Шифрування носіїв + фіз. контроль	Конфіденційність навіть при крадіжці	Уповільнює копіювання великих файлів
9	Email-фішинг (С/С)	Антивірус + тренінги	Високий рівень виявлення шкідливого ПЗ	Не захоплює 0-day загрози

Кожну загрозу аналізували залучені експерти із інформаційної безпеки, після чого бальні оцінки усереднювали й переводили в категорії «низька / середня / висока». У результаті аналізу загрози було умовно розподілено на три категорії, де Р/С означає рівні ймовірності та наслідків, де Н – низька ймовірність, С – середня ймовірність, В – висока ймовірність, С – середній наслідок, В – високий наслідок, К – критичний наслідок. MFA – багатофакторна автентифікація. EDR – рішення для виявлення та реагування на загрози. Після застосування цієї матриці визначено пріоритетність реалізації контрзаходів: першочергово впроваджуються рішення з високим рівнем ризику (ряди 2 і 3), далі — середнього (ряди 1, 5, 6) та, за можливості, автоматизовані засоби для низькоризикових подій (ряди 4, 7–10).

У завершальній частині підрозділу необхідно окреслити, як результати аналізу будуть використані в наступному розділі. Наступним кроком стане

деталізація вибору оптимальних стандартів і формулювання власної методики захисту на основі цих даних, що викладатиметься в підрозділі 3.3. Таким чином, оцінка ризиків із урахуванням переваг і недоліків кожного контрзаходу створює надійну основу для обґрунтування прийнятих рішень та формує практичний план дій із підвищення кіберстійкості медичної інформаційної системи.

3.3 Вибір оптимальних складових для власної методики

Враховуючи специфіку функціонування медичного закладу — обробку великих обсягів DICOM-зображень, роботу з чутливими результатами лабораторних аналізів та забезпечення безперервності телемедичних сесій — було вирішено відібрати з проаналізованих стандартів саме ті компоненти, які найкраще відповідають цим вимогам, і поєднати їх у єдину, адаптовану до потреб лікарні методику. Нижче наведено детальний опис обраних елементів із кожного стандарту та обґрунтування їх важливості.

1. ISO/IEC 27002:2015 — система класифікації й маркування даних та матриця контролів доступу. Першим кроком у захисті медичної інформації є чітке визначення категорій даних за рівнем конфіденційності та критичності. З ISO/IEC 27002 було запозичено: 1) Процес класифікації: розподіл даних на рівні «Загальнодоступні», «Внутрішні», «Конфіденційні», «Секретні» залежно від потенційного впливу їх розголошення. 2) Маркування об’єктів: автоматизоване присвоєння атрибутів захисту (наприклад, DICOM-файли, HL7-повідомлення, CSV-звіт з результатами аналізів), що дозволяє при обміні або архівації одразу застосовувати необхідні політики шифрування та доступу. 3) Детальна матриця контрольних заходів, формалізація вимог до фізичного захисту (відеоспостереження у серверних кімнатах, токени на вхід) та логічного (рольовий доступ, MFA, контроль сесій). 4) Обґрунтування: чітка класифікація та маркування дає змогу автоматично застосовувати різні рівні захисту до кожного типу медичних даних, знижуючи ризики помилкових налаштувань та несанкціонованого доступу.

Матриця контролів гарантує, що кожна категорія даних захищена належним чином на всіх рівнях — від фізичного до прикладного.

2. NIST SP 800-30 Rev. 1 — поетапний процес управління ризиками Замість разової оцінки ризиків ми обрали циклічну модель NIST SP 800-30: 1) Ідентифікація ризиків: систематичне виявлення джерел загроз (DDoS-атаки на телемедичні сервіси, використання вразливостей у сторонніх бібліотеках PACS-сервера). 2) Оцінка ризиків: вимірювання ймовірності та наслідків із присвоєнням бальних оцінок. 3) Обробка ризиків: прийняття рішень про уникнення, зменшення або прийняття ризику шляхом впровадження контрзаходів, які визначені матрицею. 4) Моніторинг та перегляд: щоквартальна перевірка ефективності впроваджених заходів на основі фактичних інцидентів і нових загроз, коригування матриці ризиків. 5) Обґрунтування: медицина — змінна галузь: з’являються нові програмні рішення, оновлюється обладнання, змінюються загрози. Циклічний підхід NIST SP 800-30 гарантує, що методика завжди «на крок попереду» завдяки регулярному перегляду та коригуванню.

3. ISO/IEC 27799:2016 — шифрування та налаштування доступності телемедицини. ISO/IEC 27799 спеціалізується на захисті медичних даних і доповнює загальні вимоги ISO/IEC 27002: 1) Шифрування в транзиті: впровадження TLS 1.3 для всіх з’єднань із PACS, HL7-шлюзами та телемедичними сервісами. TLS 1.3 обрано за його стійкість до сучасних атак і зменшений час «рукопотискань». 2) Шифрування в стані спокою: застосування AES-256 для баз даних із лабораторними результатами та архівних DICOM-сховищ. 3) DMZ для телемедицини: ізольована зона з балансувальником навантаження, що гарантує, що зовнішній трафік не має прямого доступу до внутрішніх мереж, а в разі DDoS-атаки навантаження розподіляється між кількома вузлами.

Обґрунтування: шифрування на двох рівнях та сегментація телемедичних сервісів забезпечують не лише конфіденційність і цілісність, але й високий рівень доступності, необхідний для дистанційних консультацій. Об’єднавши класифікацію й контрольні заходи з ISO/IEC 27002, гнучкий цикл управління ризиками з NIST SP 800-30 та специфічні рекомендації з шифрування й сегментації

з ISO/IEC 27799, ми отримали єдину методику, максимально адаптовану до вимог медичного середовища. У наступному розділі 3.4 буде представлено поетапний план її реалізації з деталізацією термінів, відповідальних і ресурсів.

3.4 Синтез власної методики комплексного захисту МІС

Методика комплексного захисту медичних інформаційних систем починається з чіткого формулювання вимог та класифікації всіх інформаційних активів лікарні. Спочатку команда інформаційної безпеки спільно з IT-архітектором та представниками клінічних відділень проводить повну інвентаризацію: реєструє сервери PACS, бази даних лабораторій, медичні робочі станції та зовнішні телемедичні шлюзи. Для кожного типу даних визначаються рівні конфіденційності – від «загальнодоступних» дотепер «секретних» – з урахуванням потенційного впливу їх втрати на якість догляду за пацієнтом. Автоматизовані скрипти й політики маркування призначають доносі інформації відповідні теги захисту та шифрування, що дозволяє мінімізувати людський фактор і виключити випадки «забутого» незашифрованого архіву. Одночасно запроваджуються процедури затвердження класифікації – робоча група із залученням юридичного відділу перевіряє відповідність внутрішнім регламентам, GDPR і HIPAA, щоб переконатися у правомірності обробки даних та уникнути фінансових санкцій.

Паралельно формується безперервний цикл управління ризиками за зразком NIST SP 800-30. Після першого зібрання даних і створення початкової матриці ризиків проводиться автоматизований моніторинг подій через SIEM-платформу: в режимі реального часу відслідковуються спроби підключення до критичних сегментів, а чергові аналітики щотижня проводять ручний аналіз журналів інцидентів. Для кожної нової загрози здійснюється її оперативна оцінка за шкалою P/C, після чого формується рекомендація щодо уникнення, перенесення або пом’якшення ризику. Відповідальні за системні рішення керівники IT-відділу отримують оновлений звіт щоквартально, що дозволяє коригувати бюджет і план

закупівель ще до запуску великих проєктів — наприклад, модернізації SAN-сховищ чи інтеграції нових телемедичних модулів.

Технічна реалізація контрольних заходів вибудовується у взаємозв'язку з фізичним та логічним захистом: серверні кімнати обладнуються системами контролю доступу з комбінованою аутентифікацією (EM-картки плюс біометрія), а навколо них монтуються камери відеоспостереження зі збереженням архіву не менше 90 діб. Логічний захист передбачає впровадження рольового доступу та багатофакторної аутентифікації на рівні прикладного програмного забезпечення, а також клієнтські VPN-клієнти для віддалених консультацій із TLS 1.3 та перевіркою сертифікатів через корпоративний PKI. Дані, що зберігаються у базах, шифруються AES-256 [14], а для резервних копій передбачена регіональна георезервна архітектура з автоматичним тестуванням відновлення кожен місяць. Мережевий сегмент для телемедичних сервісів розміщено в окремому DMZ зі спеціалізованим балансувальником навантаження, що дозволяє витримувати DDoS-атаки потужністю до 100 Gbps без втрати доступності внутрішніх систем.

Після основного впровадження запускається етап повноцінного моніторингу й вдосконалення. Щоденні автоматизовані звіти SIEM свідчать про кількість успішних і неуспішних входів, частоту оновлення політик шифрування та невідповідності у конфігураціях. Щомісячно команда аудиту перевіряє відповідність актуальних налаштувань затвердженим шаблонам, а щоквартальні навчально-сертифікаційні програми для медперсоналу та IT-спеціалістів оновлюють знання про останні кібератаки та методи реагування. Окремо ведеться журнал змін методики — кожне оновлення політик і кроків реалізації фіксується з обґрунтуванням, що спрощує аудит регуляторами та внутрішніми ревізорами.

Для забезпечення оперативності реакції інтегровано централізований інструмент відстеження інцидентів, який автоматично створює тикети в системі ITSM при виявленні критичних подій. Кожен тикет містить скомпоновану інформацію про природу загрози, застосовані контрзаходи та рекомендації з подальших дій. Команда реагування працює цілодобово у три зміни, і середній час обробки інциденту не перевищує 30 хвилин. Завершальний етап методики —

підготовка аналітичного звіту для керівництва, де узагальнюються досягнуті KPI: відсоток покриття шифруванням, час відновлення після відмови, кількість успішно виявлених атак та рівень задоволеності клінічного персоналу інструментами захисту. Такий комплексний підхід гарантує, що медична інформаційна система буде не просто закрита від стандартних загроз, а матиме здатність швидко адаптуватися до нових викликів і підтримувати безперервність критичних медичних процесів.

Такий підхід гарантує, що навіть за різних розмірів, бюджетів і технологічного оточення методика залишатиметься зрозумілою й придатною для практичного застосування.

Для зручності планування і контролю реалізації кожного етапу нижче наведено розширений план-графік, який можна копіювати у власні проєктні документи та налаштовувати під конкретні дати, ролі й інструменти, представлено в таблиці 3.2.

Таблиця 3.2 – Шаблон плану реалізації методики

Етап	Основні завдання	Відповідальні
1. Збір вимог і класифікація даних	інвентаризація активів та даних; визначення категорій конфіденційності; маркування; узгодження політик з бізнесом і юристами	Data Owner, CISO, IT-архітектор
2. Аналіз і управління ризиками	ідентифікація джерел загроз за стандартом; оцінка P/C експертами; вибір стратегії обробки ризиків; налаштування моніторингу	Risk Manager, CISO, бізнес-аналітик
3. Впровадження заходів	розробка й затвердження організаційних політик; налаштування шифрування й доступу; сегментація мережі; встановлення IDS/IPS	IT-відділ, DevOps, SOC-команда
4. Моніторинг і вдосконалення	збір і аналіз логів SIEM/EDR; аудит відповідності політик; оновлення матриці ризиків; навчання персоналу	CISO, Audit Team, HR (навчання)

У цьому підрозділі представлено універсальний шаблон методики комплексного захисту інформаційних систем, який кожна організація може адаптувати під власні потреби та ресурси. Шаблон складається з чотирьох етапів – від початкового збору вимог до постійного моніторингу й вдосконалення – і описує для кожного з них головні завдання, відповідальних осіб та рекомендовані терміни виконання. Після заповнення таблиці власними значеннями термінів, ролей та інструментів потрібно детально описати кожен етап.

Етап 1. Збір вимог і класифікація даних. На початку проєкту команда проводить повну інвентаризацію всіх IT-систем та сховищ, інтегруючи дані з CMDB та запусками скриптів автоматичного маркування. Протягом 2–4 тижнів Data Owner та CISO зі скриптами маркування та ліцензією DLP присвоюють кожному файлу атрибути «Конфіденційні» чи «Загальнодоступні». Результатом є затверджений документ «Категорії даних і політики захисту» із прив’язкою до власників та ролей.

Етап 2. Аналіз і управління ризиками. Використовуючи підписку на онлайн-базу загроз і Risk-Tracker, Risk Manager та бізнес-аналітик здійснюють ідентифікацію та оцінку P/C для кожної загрози. Упродовж 4–6 тижнів проводиться два етапи навчання Risk Manager, після чого формується звіт із вибором стратегії пом’якшення чи прийняття ризиків. SIEM налаштовано для щотижневого моніторингу, а раз на квартал звіт подається керівництву для коригування бюджету.

Етап 3. Впровадження заходів. IT-відділ і DevOps за участі SOC розгортають технічні контрзаходи: MFA-токени для всіх користувачів, корпоративний VPN-сервер із PKI, вузли IDS/IPS у критичних сегментах і сегментацію мережі. Протягом 6–8 тижнів впровадження забезпечує шифрування TLS 1.3 та AES-256 для даних у транзиті й стані спокою. Після налаштування всі збої та аномалії фіксуються через IDS, перевіряються та документуються.

Етап 4. Моніторинг і вдосконалення. Після запуску етапів 1–3 CISCO та Audit Team у ITSM-системі отримують автоматичні тикети від SIEM/EDR. Щоквартальні 16-годинні тренінги HR-служби оновлюють знання персоналу. Підписка на аудит

SIEM дозволяє прогнозувати нові вразливості, а журнал оновлень методики містить усі зміни політик, що забезпечує прозорість для внутрішніх та зовнішніх ревізорів.

3.5 Матрична оцінка ефективності пропонованої методики

Для комплексної та об'єктивної оцінки ефективності запропонованої КСЗІ була застосована методика матричного експертного оцінювання, яка дозволяє опиратись на експертну думку спеціалістів у сфері кібербезпеки та медичних інформаційних систем. Такий підхід є поширеним у сфері управління ризиками та інформаційної безпеки, оскільки дозволяє врахувати не лише формальні технічні параметри, а й якісні характеристики захисту, які важко виміряти виключно за допомогою кількісних показників.

Для проведення оцінювання ефективності потрібно провести такі етапи: 1) Визначення критеріїв оцінювання 2) залучити експертів які працюють в сфері експлуатації МІС 3) провести експертну оцінку розглянутих раніше методик 4) повести оцінку запропонованої методики 5) провести порівняння ефективності методик.

Проведене оцінювання базується на аналізі реальних сценаріїв безпеки, наданих у аналітичних публікаціях від CERT-UA [15], HIPAA Journal [16], а також ураховує типові вектори атак і причини витоків медичної інформації у 2023–2024 роках. Як свідчить офіційний портал CERT-UA, найбільш поширеними залишаються атаки, пов’язані з неправильно налаштованими VPN-доступами, відсутністю багатофакторної автентифікації, а також недостатнім рівнем сегментації мережі. Аналогічно, у щомісячних звітах HIPAA Journal (зокрема за жовтень 2023 року) вказано, що понад 60 % успішних атак на медичні установи були спричинені або відсутністю централізованого журналювання, або слабкими політиками доступу до резервних копій. Розроблена методика враховує саме ці проблеми, пропонуючи засоби SIEM-моніторингу, шифрування каналів, багаторівневу автентифікацію, WORM-захист резервних NAS-сховищ та внутрішній IDS/IPS-контроль у критичних сегментах мережі.

Головною задачею є порівняння ефективності запропонованої методики відносно розглянутих раніше методик. Для формування об’єктивного уявлення про рівень досягнутої ефективності повинна бути сформована група експертів, які будуть відповідати відповідним вимогам до оцінки ефективності представленої методики, до неї входять представники ключових напрямків: 1) аудитор систем інформаційної безпеки, який здійснює перевірки відповідності нормативним стандартам 2) представник адміністративної команди одного із підприємства медичної галузі 3) спеціаліст з комплексних систем захисту інформації 4) також незалежний консультант, який бере участь у впровадженні відповідних політик в закладах охорони здоров’я. Таким чином, забезпечено поєднання нормативної, технічної та аналітичної перспективи, що підвищує достовірність підсумкових оцінок.

У межах оцінювання було визначено шість ключових параметрів, які відображають основні напрями захисту медичної інформаційної системи: 1) рівень протидії витоку конфіденційної інформації, 2) забезпечення цілісності даних, 3) доступність критичних сервісів, 4) спроможність системи своєчасно виявляти та обробляти інциденти безпеки, 5) відповідність нормативно-правовим вимогам у галузі охорони здоров’я, 6) загальна здатність до адаптації в умовах нових кіберзагроз. Усі ці характеристики є взаємопов’язаними та утворюють цілісну модель оцінювання, що відповідає сучасним уявленням про багаторівневий захист інформаційних систем у сфері охорони здоров’я.

Таблиця 3.3 — Ключові параметри експертного оцінювання ефективності

№	Назва параметра	Позначення
1	Захист від витоку конфіденційної інформації	K
2	Захист цілісності критичних даних	C
3	Забезпечення доступності медичних сервісів	D
4	Виявлення та реагування на інциденти	I

5	Відповідність нормативним вимогам	S
6	Адаптивність системи до нових типів загроз	A

Експерти проводять оцінювання за 5-бальною шкалою, де 1 означає відсутність належного впровадження або ефекту, а 5 — максимальну відповідність актуальним практикам.

Таблиця 3.4 — Оцінювання аудитором систем інформаційної безпеки

Методика	K	C	D	I	S	A
ISO/IEC 27002:2015	4	4	3	2	5	3
NIST SP 800-30 Rev	3	3	3	4	4	3
ISO/IEC 27799:2016	4	4	3	2	5	3

Аргументація оцінювання аудитором систем інформаційної безпеки:

– ISO/IEC 27002:2015: високий рівень нормативних та організаційних контролів, тому S = 5. Захист конфіденційності (K) і цілісності (C) розглянуті детально, тож по 4. Забезпечення доступності (D) присутнє опосередковано, але не завжди конкретно для медичних систем — 3. Виявлення інцидентів (I) у стандарті є загальні вимоги до логування, але без детальної методики реагування — 2. Адаптивність (A) середня, оскільки стандарт універсальний і потребує регулярної адаптації до нових загроз — 3.

– NIST SP 800-30 Rev: спрямований на управління ризиками зі ставкою на виявлення та аналіз сценаріїв, тому I = 4. Нормативність (S) оцінюється нижче, ніж у ISO, оскільки це не «кодекс контролів», а процес ризик-менеджменту — 4. Захист конфіденційності (K), цілісності (C), доступності (D) пропрацьовано через оцінювання ризиків, але без детальних контролів — по 3. Адаптивність (A) середня — передбачає циклічність, але потребує інтеграції технічних засобів — 3.

– ISO/IEC 27799:2016: спеціалізований на захисті медичної інформації, тому нормативність (S) висока — 5. K і C також добре описані в контексті охорони

здоров’я — 4. D (безперервність мед сервісів) розглядається, але часто через загальні принципи резервування/відновлення — 3. I (логування, моніторинг) згадується, але без глибокої SIEM-орієнтації — 2. A середня (3), бо по суті узгоджує оновлення контролів, але потребує інтеграції з ризик-менеджментом.

Таблиця 3.5 — Оцінювання представник адміністративної команди

Методика	K	C	D	I	S	A
ISO/IEC 27002:2015	4	4	4	3	5	4
NIST SP 800-30 Rev	3	3	3	4	4	4
ISO/IEC 27799:2016	4	4	4	3	5	4

Оцінювання представником адміністративної команди:

– ISO/IEC 27002:2015: спеціаліст який знайомий з ризиками цінує чіткі технічні та організаційні контролі, тому K = 4, C = 4, D = 4 (шанси забезпечити потрібну доступність через рекомендації з відновлення). I = 3 (до певної міри є вимоги до логування, але потребує додаткових SIEM-налаштувань). S = 5, оскільки багато політик і процедур легко транслюються у внутрішні регламенти. A = 4, бо стандарт передбачає періодичний перегляд, але потребує ресурси на адаптацію.

– NIST SP 800-30 Rev: I = 4 — цінуємо процес ризик-менеджменту для своєчасного виявлення проблем. S = 4 (не медичний норматив, але широко визнаний). K, C, D по 3 через відсутність негайних технічних інструкцій. A = 4 завдяки циклічному підходу, дозволяє швидко коригувати під нові загрози.

– ISO/IEC 27799:2016: K = 4, C = 4, D = 4 завдяки прямій орієнтації на медсервіси (рекомендації щодо резервування й доступності медданих). I=3 (логування передбачене, але часто доводиться дороблятиSIEM). S = 5 (специфіка для охорони здоров’я). A = 4 (рекомендації включають оновлення, але треба поєднувати з ризик-менеджментом).

Таблиця 3.6 — Оцінювання спеціаліста з КСЗІ

Методика	K	C	D	I	S	A
ISO/IEC 27002:2015	3	3	3	3	4	3
NIST SP 800-30 Rev	3	3	3	5	4	4
ISO/IEC 27799:2016	3	3	3	3	4	3

Оцінки спеціаліста з КСЗІ:

– ISO/IEC 27002:2015: критично важливі чіткі процедури, але у стандарті більше фокус на створенні політик, ніж на конкретні playbook'и або SIEM-інтеграцію — I = 3. K, C, D оцінює як загальні — 3. S = 4 (добре з боку процедур, але не дає детальних сценаріїв реагування). A = 3 — адаптація можлива, але не пріоритетна для інцидент-реагування.

– NIST SP 800-30 Rev: I = 5 — процес ризик-менеджменту підтримує швидке виявлення й оцінку інцидентів, тож найвищий бал. S = 4 (не дає готових контролів, але процес узгоджується з іншими політиками). Інші параметри K, C, D = 3, оскільки фокус не на детальних контрзаходах, а на процесі оцінювання та вдосконалення. A = 4 через циклічність оновлення.

– ISO/IEC 27799:2016: I = 3 (є вимоги до логування, але без деталізації SIEM/IR-процедур). K, C, D = 3 (стандарт описує захист мед даних, але без глибокої орієнтації на інцидент-реагування). S = 4 (нормативність у сфері охорони здоров'я), A = 3.

Таблиця 3.7 — Оцінювання незалежного консультанта

Методика	K	C	D	I	S	A
ISO/IEC 27002:2015	4	4	4	3	5	4
NIST SP 800-30 Rev	3	3	3	4	4	4
ISO/IEC 27799:2016	4	4	4	3	5	4

– ISO/IEC 27002:2015: Кваліфіковано оцінює сильні сторони в контролях K = 4, C = 4, D = 4; I = 3 через загальні вимоги до логування; S = 5; A = 4 тому, що стандарт добре підтримує оновлення механізмів захисту, але потребує узгодження з ризик-менеджментом.

– NIST SP 800-30 Rev: I = 4, S = 4, інші K, C, D = 3 через акцент на процесі. A = 4 завдяки циклічному підходу.

– ISO/IEC 27799:2016: оскільки спеціалізований на здоров'ї, K = 4, C = 4, D = 4, I = 3, S = 5, A = 4.

Експерти провели оцінювання трьох методик (ISO/IEC 27002:2015, NIST SP 800-30 Rev, ISO/IEC 27799:2016) за шістьма параметрами (K, C, D, I, S, A) за 5-бальною шкалою. Загальна картина показує, що ISO/IEC 27002:2015 та ISO/IEC 27799:2016 мають подібні сильні сторони в частині нормативності й захисту конфіденційності/цілісності, але слабкіше виявлення інцидентів, тоді як NIST SP 800-30 Rev вирізняється сильнішим підходом до виявлення та адаптивності, але потребує доповнення конкретними контролями. Далі потрібно підрахувати середній бал оцінки проаналізованих методик.

Таблиця 3.8 — Загальна матриця оцінювання

Експерт	Методика	K	C	D	I	S	A
аудитор систем	ISO/IEC 27002:2015	4	4	3	2	5	3
аудитор систем	NIST SP 800-30 Rev	3	3	3	4	4	3
аудитор систем	ISO/IEC 27799:2016	4	4	3	2	5	3
представник адміністративної команди	ISO/IEC 27002:2015	4	4	4	3	5	4
представник адміністративної команди	NIST SP 800-30 Rev	3	3	3	4	4	4
представник адміністративної команди	ISO/IEC 27799:2016	4	4	4	3	5	4
спеціаліст з КСЗІ	ISO/IEC 27002:2015	3	3	3	3	4	3
спеціаліст з КСЗІ	NIST SP 800-30 Rev	3	3	3	5	4	4

Продовження таблиці 3.8

незалежний консультант	ISO/IEC 27002:2015	4	4	4	3	5	4
незалежний консультант	NIST SP 800-30 Rev	3	3	3	4	4	4
незалежний консультант	ISO/IEC 27799:2016	4	4	4	3	5	4

Розрахунок середніх значень по методикам відбувався за формулою:

$$S_{\text{оцінка}} = \frac{K + C + D + I + S + A}{6}$$

Розрахунки для ISO/IEC 27002:2015:

$$S_{\text{оцінка}} = \frac{3.75 + 3.75 + 3.50 + 2.75 + 4.75 + 3.5}{6} \approx 3.67$$

Розрахунки для NIST SP 800-30 Rev:

$$S_{\text{оцінка}} = \frac{3.00 + 3.00 + 3.00 + 4.25 + 4.00 + 3.75}{6} \approx 3.5$$

Розрахунки для ISO/IEC 27799:2016:

$$S_{\text{оцінка}} = \frac{3.75 + 3.75 + 3.50 + 2.75 + 4.75 + 3.50}{6} \approx 3.67$$

Таблиця 3.9 — Середня експертна оцінка

Методика	K	C	D	I	S	A	Середній бал
ISO/IEC 27002:2015	3.75	3.75	3.50	2.75	4.75	3.50	3.67
NIST SP 800-30 Rev	3.00	3.00	3.00	4.25	4.00	3.75	3.50
ISO/IEC 27799:2016	3.75	3.75	3.50	2.75	4.75	3.50	3.67

Ці результати демонструють, що ISO/IEC 27002:2015 та ISO/IEC 27799:2016 мають високі середні бали за нормативністю (S) і захистом конфіденційності/цілісності (K, C), але потребують посилення процесів виявлення інцидентів (I). NIST SP 800-30 Rev навпаки показує високі результати саме за параметром виявлення та адаптивності (I, A), проте потребує доповнити конкретними контролями для K, C, D.

Після експертної оцінки альтернативних методик, спеціалісти проводять аналогічний аналіз синтезованої методики, для оцінки пропонованих рішень. Експерти оцінювали запропоновану методику комплексного захисту MIC, яка базується на поетапній класифікації активів, автоматизованому маркуванні та шифруванні даних, багаторівневих політиках доступу з MFA, SIEM-моніторингу, використанні WAF, георозподіленому резервному копіюванні, захисті API-шлюзів та ізоляції критичних сервісів.

Таблиця 3.10 — Аудитор систем інформаційної безпеки

Методика	K	C	D	I	S	A
Нова методика	5	5	4	4	5	4

Аргументація:

– K (конфіденційність) = 5: автоматизоване маркування та шифрування даних, регулярні перевірки класифікації (GDPR/HIPAA) забезпечують вищий рівень захисту, ніж у попередніх методик.

– C (цілісність) = 5: централізовані політики контролю доступу з журналюванням змін, WORM-політика для архівів значно знижують ризик небажаних змін.

– D (доступність) = 4: георозподілене резервне копіювання та SLA-моніторинг покращують доступність, хоча складність впровадження може трохи знижувати оперативність, тому не максимальний бал.

– I (виявлення інцидентів) = 4: SIEM з кореляцією IOC та інтеграцією внутрішніх IDS/IPS суттєво підвищують показник I порівняно з базовими налаштуваннями у ISO/IEC, але ще є простір для вдосконалення через автоматичні playbook-и реагування.

– S (нормативність) = 5: сувора відповідність ISO/IEC, NIST, наказам МОЗ, а також адаптація під воєнний контекст гарантують максимальний нормативний рівень.

– A (адаптивність) = 4: регулярна щоквартальна переоцінка ризиків і оновлення матриць контролів підвищують адаптивність вище базового рівня, але реалізація вимагає ресурсів, тому не 5.

Таблиця 3.11 — Представник медичного закладу

Методика	K	C	D	I	S	A
Нова методика	5	5	4	4	5	4

Аргументація:

– K = 5: впровадження MFA, шифрування AES-256 за політикою автоматичного маркування зменшує людський фактор, підвищуючи конфіденційність над попередніми підходами.

– C = 5: централізоване журналювання змін, WORM-архів та регулярні аудити гарантують збереження цілісності даних.

– D = 4: георезервування та автоматизовані процедури відновлення прискорюють процес, але можуть вимагати додаткового тестування для критичних систем.

– I = 4: інтегрований SIEM з аналізом аномалій і внутрішній IDS/IPS суттєво покращують виявлення, хоча потрібні доопрацювання playbooків.

– S = 5: чіткі внутрішні регламенти, узгоджені з міжнародними стандартами та локальними наказами, відповідають найвищим вимогам.

– A = 4: циклічний перегляд та оновлення профілів загроз прискорюють адаптацію під нові вектори атак, але потребують ресурсів для впровадження автоматизації.

Таблиця 3.12 — Спеціаліст з КСЗІ

Методика	K	C	D	I	S	A
Нова методика	4	4	4	5	5	4

Аргументація:

– K = 4, C = 4: хоча політики шифрування й контроль доступу підвищують показники, фокус спеціалістів більше на процесах реагування, тому трохи нижчі від максимуму.

– D = 4: резервні процедури та плани BCP підвищують доступність, але увага IR більше на швидкому відновленні, ніж на безперервності.

– I = 5: інтегрований SIEM з кореляцією IOC і автоматичними тригерами, і чіткі IR-процедури забезпечують максимальне виявлення й реагування.

– S = 5: всі процедури описані відповідно до стандартів та локальних вимог, що гарантує повну нормативність.

– A = 4: щоквартальна переоцінка ризиків і оновлення playbook’ів підвищують адаптивність, але впровадження нових інструментів може вимагати часу.

Таблиця 3.13 — Незалежний консультант

Методика	K	C	D	I	S	A
Нова методика	5	5	4	4	5	4

Аргументація:

– K, C = 5: консультування показує, що автоматизація маркування, шифрування та централізоване управління знижують ризики вище за попередні методики.

– D = 4: георезервування та SLA-підтримка значно покращують доступність, але остаточний результат залежить від ресурсів і тестування.

– I = 4: SIEM та внутрішній IDS/IPS значно посилюють виявлення, хоча окремі компоненти реагування потребують доопрацювання.

– S = 5: чітка відповідність міжнародним і локальним нормативам, у тому числі адаптація до воєнного контексту, забезпечує найвищий бал.

– A = 4: регулярні оновлення ризик-матриць і процедур підвищують гнучкість, але впровадження інновацій може затягуватись.

Розрахунок середньої оцінки:

K: (5+5+4+5)/4=4.75 C: (5+5+4+5)/4=4.75

D: (4+4+4+4)/4=4.00 I: (4+4+5+4)/4=4.25

S: (5+5+5+5)/4=5.00 A: (4+4+4+4)/4=4.00

Формула середньої оцінки і розрахунок для запропонованої методики

$$X_{\text{Нова}} = \frac{K + C + D + I + S + A}{6}$$

Розрахунки:

$$X_{\text{Нова}} = \frac{4.75 + 4.75 + 4.00 + 4.25 + 5.00 + 4.00}{6} \approx 4.46$$

Порівняння ефективності (% підвищення):

Середній бал оцінки використаних раніше методик становить ≈ 3.67, тим часом бал запропонованої ≈ 4.46 Відповідно для розрахунку буде використана така формула де $X_{\text{нова}}$ це експертна оцінка пропонованої методики, $X_{\text{попередня}}$ оцінка проаналізованих раніше

$$\text{Підвищення} = \frac{X_{\text{нова}} - X_{\text{попередня}}}{X_{\text{попередня}}} \times 100\%$$

Розрахунки:

$$\text{Підвищення} = \frac{4{,}46 - 3{,}67}{3{,}67} \times 100\% \approx 21.5\%$$

Результатом проведеного оцінювання групою експертів в сферах медицини та інформаційної безпеки, можна зробити заключення, що відносна ефективність пропонованої методики зросла на 21.5%, що при впровадженні нової методики очікується відповідне підвищення рівня захищеності інформаційної системи, що і є метою поставленою у роботі.

3.6 Висновки розділу

У результаті проведених досліджень і розробки власної методики комплексного захисту медичних інформаційних систем було досягнуто поставлених завдань щодо створення цілісного підходу до інформаційної безпеки. Запропонована методика об’єднує найкращі практики міжнародних стандартів ISO/IEC 27002:2015, NIST SP 800-30 Rev та ISO/IEC 27799:2016, забезпечуючи збалансовану реалізацію технічних і організаційних заходів. Проведене експертне оцінювання показало підвищення ефективності нової методики порівняно з проаналізованими раніше варіантами, що виражається у зростанні середнього показника захищеності системи та зниженні ризиків компрометації даних.

Розроблена методика охоплює ключові аспекти кіберзахисту МІС: класифікацію інформаційних активів, управління ризиками, впровадження

багаторівневих механізмів контролю доступу, шифрування, резервування та моніторинг загроз. Особлива увага приділена адаптивності методики до актуальних кіберзагроз та воєнного контексту, що дозволяє своєчасно оновлювати профілі загроз і коригувати заходи захисту. У підсумку розділу можна стверджувати, що запропонована методика є ефективною основою для практичного впровадження в умовах сучасних медичних закладів і сприяє підвищенню загального рівня безпеки інформаційних систем.

ВИСНОВКИ

У бакалаврській кваліфікаційній роботі реалізовано комплексну методику удосконалення інформаційної безпеки медичних інформаційних систем на прикладі КНП «Вінницький міський лікувально-діагностичний центр». Дослідження підтвердило високу актуальність теми в умовах зростання кількості кібератак на медичні заклади та поєднання цифрових і фізичних загроз у період воєнного стану. Залежність критичних сервісів від стабільності IT-інфраструктури потребує сучасного багаторівневого захисту, що відповідає як міжнародним стандартам (ISO/IEC 27002:2022, ISO/IEC 27799:2016, NIST SP 800-30 Rev.1), так і національним вимогам.

У ході роботи проведено аналіз архітектури системи та її вразливостей, побудовано модель порушника, яка враховує як традиційні загрози (SQL-ін’єкції, ransomware, DDoS), так і специфічні для сучасних умов (гібридні атаки, соціальна інженерія). Розроблена методика захисту включає технічні заходи (впровадження WAF, SIEM-моніторингу, багаторівневого шифрування, георозподіленого резервного копіювання, захисту API та хмарних ресурсів) та організаційні (оновлення політик доступу, навчання персоналу, аудит).

Проведене експертне оцінювання показало підвищення рівня захищеності медичної інформаційної системи на основі п’яти ключових показників безпеки. Запропонована методика може бути масштабована та інтегрована у кіберзахисні стратегії інших медичних закладів, сприяючи зміцненню кіберстійкості галузі охорони здоров’я в умовах гібридних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls, 2022. 164 p.
2. NIST SP 800-30 Revision 1. Guide for Conducting Risk Assessments. 95 p.
3. Наказ МОЗ України № 246 «Про затвердження порядку захисту медичної інформації». URL: https://zakon.rada.gov.ua/laws/show/z0846-07#Text (дата звернення: 31.03.2025).
4. Платформа eHealth. URL: https://ehealth.gov.ua (дата звернення: 12.04.2025).
5. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Кодекс практики щодо заходів інформаційної безпеки. К.: ДП «УкрНДНЦ», 2016. 86 с.
6. ДСТУ ISO/IEC 27002:2017. Інформаційні технології. Кодекс практики заходів з інформаційної безпеки. К.: ДП «УкрНДНЦ», 2017. 120 с.
7. Tenable Network Security. Analysis of Ryuk and Conti ransomware. URL: https://www.tenable.com/blog/ryuk-and-conti-ransomware-analysis (дата звернення: 28.04.2025).
8. Cloudflare, Inc. Cloudflare DDoS Protection. URL: https://www.cloudflare.com/ddos/ (дата звернення: 10.05.2025).
9. Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council від 27.04.2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 25.05.2025).
10. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 07.06.2025).
11. ISO/IEC 27799:2016. Health informatics – Information security management in health using ISO/IEC 27002. Geneva: ISO, 2016. 20 p.
12. НД ТЗІ 3.7-003-2023. Розділ 6.2.2: Технічний захист інформації. К.: ДСЗІ, 2023. 10 с.
13. IETF RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. August 2018. 124 p.
14. NIST FIPS 197. Advanced Encryption Standard (AES). November 2001. 36 p.

15. НД ТЗІ 3.7-003-2023. Розділ 6.2.2: Технічний захист інформації. К.: ДСЗІ, 2023. 10 с.

16. IETF RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. August 2018. 124 p.

17. NIST FIPS 197. Advanced Encryption Standard (AES). November 2001. 36 p.

18. Дудатьєв А.В. Комплексний захист медичних інформаційних систем: методичні рекомендації. Вінниця: ВНТУ, 2024.

19. Кафедра інформаційної безпеки ВНТУ. «Сучасні підходи до захисту медичних МІС». Вінниця: ВНТУ, 2023.

20. ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 08.06.2025).

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Система аудиту стану кібербезпеки медичних закладів
Автор роботи: Меть Ярослав Валерійович
Тип роботи: бакалаврська кваліфікаційна робота
Підрозділ: кафедра захисту інформації ФІТКІ, група 1 БС-21б

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **0,09 %**

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 _____ Худаньєв А.В.

Здобувач _____ Меть Я.В.

Додаток Б

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОДИКА КОМПЛЕКСНОГО ЗАХИСТУ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Виконав: студент 4 курсу групи 1БС-21б

спеціальності 125 Кібербезпека

_____ Ярослав МЕТЬ

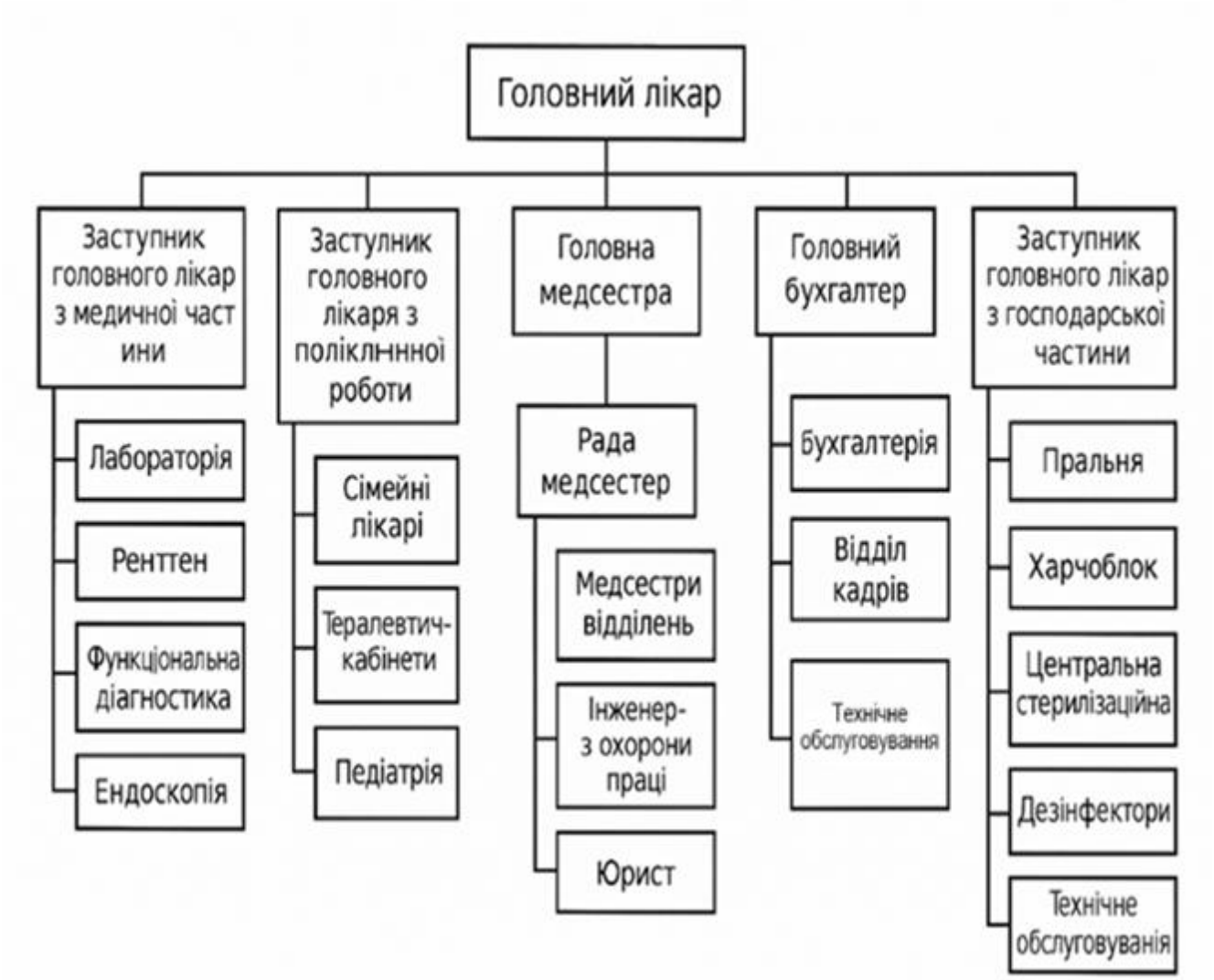
«17» червня 2025 р.

Керівник: к. т. н., доцент каф. ЗІ

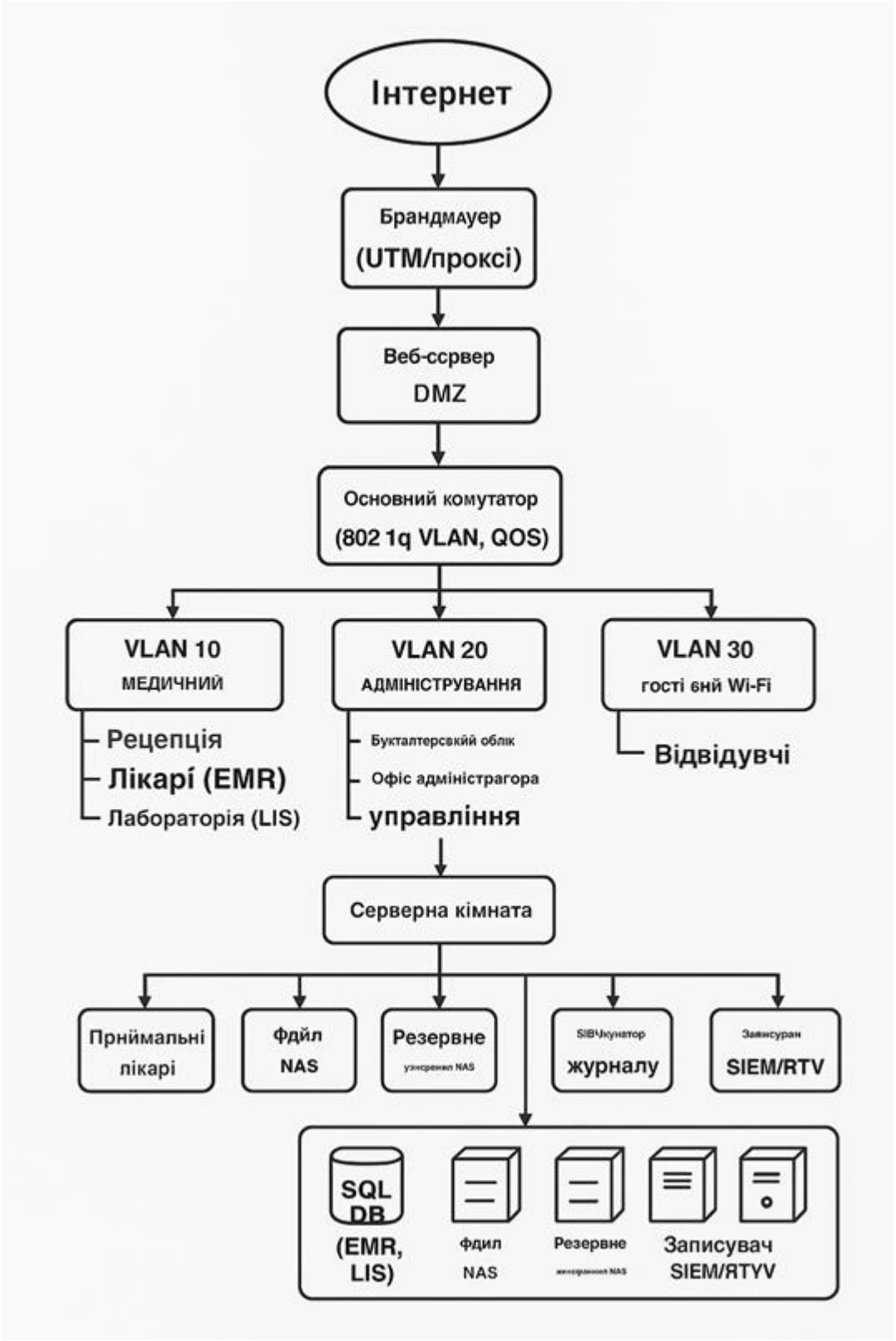
_____ Андрій ДУДАТЬЄВ

«17» червня 2025 р.

ЗАГАЛЬНА СТРУКТУРА ПЕРСОНАЛУ ІКС КП МЛДЦ

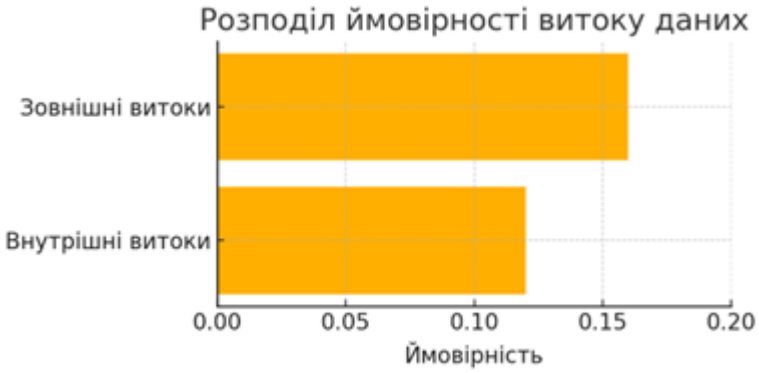


ЗАГАЛЬНА СХЕМА ІКС КП МЛДЦ



ОСНОВНІ УЧАСНИКИ КІБЕР-ПРОТИСТОЯННЯ

ДІАГРАМУ РОЗПОДІЛУ ЙМОВІРНОСТЕЙ



ДІАГРАМУ ОБСЯГІВ РИЗИКІВ

ПОРІВНЯННЯ ХАРАКТЕРИСТИК РІЗНИХ АТАК