**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ДОПУСТИТИ ДО ЗАХИСТУ:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)

**спеціальність** 125 Кібербезпека
(код і назва спеціальності)

**освітній ступень** бакалавр

**освітня програма** Кібербезпека
(назва освітньо-професійної програми)

**на тему:** Комплексний аудит систем контролю витоків даних на об'єктах медичного спрямування

**Виконавець:** студентка IV курсу, групи КБ-42

_____ **Мар'яна ЛЕВИЦЬКА**
(підпис) (ім'я прізвище)

| | **Підпис** | **Прізвище, ініціали** |
|---|---|---|
| **Керівник** | | Сергій ДАКОВ |
| **Нормоконтроль** | | Олександр ТОРОШАНКО |

**Київ 2025**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____Іван ПАРХОМЕНКО
«29» листопада 2024 р.

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньо-професійної програми)

**Студентці** **КБ-42** **Левицькій Мар'яні Вадимівні**
(група) (прізвище ім'я по батькові)

**Тема кваліфікаційної роботи** Комплексний аудит систем контролю витоків даних на об'єктах медичного спрямування

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Відомості про сучасний стан захисту персональних даних у медичних закладах України, чинні нормативно-правові акти у сфері захисту даних (GDPR, Закон України «Про захист персональних даних», HIPAA, NIST CSF 2.0), типові, вразливості інформаційних систем E-Health, Healthy та інших медичних платформ міжнародна практика управління ризиками кібербезпеки, методи організаційного й технічного захисту даних (DLP, SIEM, криптографічний захист, контроль доступу), сучасні підходи до побудови моделей загроз, порушника та ризиків у медичних IT-системах.

## 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Аналіз проблем захисту персональних та медичних даних у медичних закладах, характеристика типових інцидентів та помилок використання інформаційних систем, огляд і порівняння законодавчих вимог (GDPR, HIPAA, NIST CSF 2.0), розробка моделей загроз, моделі порушника та оцінки ризиків, формування HLD-архітектури захисту даних, створення методології оцінки зрілості захисних систем, розробка детальних рекомендацій і дорожньої карти з впровадження заходів підсилення захисту персональних даних, формулювання висновків і практичних порад для медичних установ.

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** Розроблені комплексні методичні рекомендації щодо, удосконалення та підсилення захисту персональних даних у медичних закладах, створені моделі загроз, порушників і ризиків, запропонована архітектура HLD захисту відповідно до вимог HIPAA, GDPR і NIST CSF 2.0, сформована покрокова дорожня карта впровадження захисних заходів згідно рекомендацій, розроблено авторську методологію оцінювання зрілості систем захисту, надано перелік дієвих рекомендацій з виявлення реагування та усунення інцидентів витоку даних. Отримані результати та напрацювання мають безпосереднє практичне застосування, вони використовуються мною у професійній діяльності, що пов’язана із оцінкою зрілості процесів кібербезпеки у медичних установах та розробкою рекомендацій та дорожніх карт впровадження щодо покращення заходів інформаційної безпеки в медичних установах. Враховуючи постійну загрозу витоку персональних медичних даних та зростаючі вимоги до їх захисту, існує виробнича необхідність впровадження ефективних рішень, описаних у даній роботі. Захист даних пацієнтів є ключовим елементом довіри до системи охорони здоров’я та одним із критичних пріоритетів сучасної медичної кібербезпеки.

## 5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

| | | |
|---|---|---|
| Завдання видав | _____ (підпис) | Сергій ДАКОВ (ім’я, прізвище) |
| Завдання прийняла до виконання | _____ (підпис) | Мар’яна ЛЕВИЦЬКА (ім’я, прізвище) |

# КАЛЕНДАРНИЙ ПЛАН

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.11.2024 – 13.12.2024 | *виконано* |
| 2 | Аналіз літературних джерел та нормативно-правових актів | 14.12.2024 – 28.12.2024 | *виконано* |
| 3 | Аналіз сучасного стану захисту персональних даних у медичних закладах | 29.12.2024 – 12.01.2025 | *виконано* |
| 4 | Дослідження типових вразливостей і інцидентів у медичних інформаційних системах | 13.01.2025 – 27.01.2025 | *виконано* |
| 5 | Огляд і аналіз міжнародних стандартів і вимог (HIPAA, GDPR, NIST CSF 2.0 тощо) | 28.01.2025 – 11.02.2025 | *виконано* |
| 6 | Моделювання загроз, моделі порушника та моделі ризиків для медичної IT-інфраструктури | 12.02.2025 – 26.02.2025 | *виконано* |
| 7 | Розробка HLD-архітектури системи захисту | 27.02.2025 – 13.03.2025 | *виконано* |
| 8 | Вироблення комплексних рекомендацій і дорожньої карти впровадження заходів захисту персональних даних | 14.03.2025 – 30.03.2025 | *виконано* |
| 9 | Розробка методології оцінювання зрілості систем захисту і процедур аудиту | 31.03.2025 – 13.04.2025 | *виконано* |
| 10 | Оформлення розрахунково-пояснювальної записки, підготовка додатків, схем | 14.04.2025 – 12.05.2025 | *виконано* |
| 11 | Підготовка до захисту кваліфікаційної роботи, рецензування, презентація результатів | 13.05.2025 – 13.06.2025 | *виконано* |

Завдання видав _____ Сергій ДАКОВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Мар’яна ЛЕВИЦЬКА
(підпис) (ініціали, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

# РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків, має 54 сторінки основного тексту, 9 таблиць, 5 рисунків та 9 додатків. Список використаних джерел містить 20 найменувань і займає 3 сторінки.

*Мета* кваліфікаційної роботи полягає підвищенні ефективності систем захисту персональних даних, шляхом розробки рекомендацій щодо удосконалення систем контролю витоків персональних даних в об'єктах критичної інфраструктури медичного спрямування з урахуванням вимог міжнародних стандартів (HIPAA, GDPR та NIST CSF 2.0) і сучасних методів захисту інформації.

Для досягнення поставленої мети необхідно вирішити наступні *завдання*:

- дослідити проблему витоків персональних даних у медичних ОКІ, зокрема аналіз актуальних інцидентів і кіберзагроз у медичних закладах;
- провести аналіз ризиків та сформувати матрицю ризиків витоку персональних даних відповідно до вимог GDPR;
- дослідити нормативні вимоги щодо захисту персональних даних, визначені стандартами HIPAA, GDPR та NIST CSF 2.0;
- розглянути існуючі методи, засоби і технології захисту інформації в медичних ОКІ;
- розробити модель загроз та модель потенційного порушника безпеки для ІС ОКІ медичного спрямування;
- сформувати High-Level Design (HLD) та надати конкретні рекомендації щодо впровадження нових та покращення існуючих заходів та засобів захисту персональних даних відповідно до HIPAA та NIST CSF 2.0.

*Об'єктом дослідження* кваліфікаційної роботи є процес забезпечення захисту персональних даних в інформаційних системах медичних закладів, які є об'єктами критичної інфраструктури.

*Предметом дослідження* є методи, засоби, стандарти та практичні рекомендації щодо підвищення рівня захисту персональних даних у медичних інформаційних системах.

*Практична цінність* роботи полягає у розробці комплексних методичних рекомендацій, спрямованих на удосконалення та посилення захисту персональних даних у медичних установах. У межах дослідження створено моделі загроз, порушників і ризиків, запропоновано архітектуру HLD-захисту відповідно до вимог міжнародних стандартів HIPAA, GDPR і NIST CSF 2.0, а також сформовано покрокову дорожню карту для впровадження необхідних заходів безпеки. Крім того, розроблено авторську методологію оцінювання зрілості систем захисту персональних даних та наведено дієві рекомендації щодо виявлення, реагування та усунення інцидентів витоку інформації.

*Методами дослідження* кваліфікаційної роботи є:

- аналіз наукових джерел та НПА;
- аналіз документів та звітів про інциденти КБ;
- порівняльний аналіз міжнародних стандартів (HIPAA, GDPR, NIST CSF 2.0);
- узагальнення зарубіжної та вітчизняної практики;
- формалізація моделі загроз і моделі порушника;
- розробка рекомендацій щодо впровадження заходів кіберзахисту.

У роботі проаналізована існуюча література та нормативні акти з питань захисту персональних даних у медичних закладах, виконано детальний аналіз документів, порівняльний аналіз міжнародних стандартів та вітчизняного законодавства, досліджено та узагальнено вітчизняну і зарубіжну практику

щодо захисту персональних даних пацієнтів у медичних об'єктах критичної інфраструктури.

Проведено аналіз ризиків та сформована матриця ризиків витоку персональних даних відповідно до вимог GDPR. Побудовані модель загроз та модель потенційного порушника інформаційної безпеки, які наведені у додатках.

Розроблено рекомендації щодо удосконалення систем контролю витоків персональних даних із застосуванням міжнародних стандартів HIPAA, GDPR та NIST CSF 2.0. Сформовано High-Level Design (HLD) рішення, що містить чіткі вказівки щодо впровадження нових та удосконалення існуючих заходів і засобів захисту персональних даних.

Розроблені рекомендації призначені для керівників і співробітників медичних закладів, спеціалістів у сфері інформаційної безпеки та осіб, відповідальних за обробку і захист персональних даних у медичних об'єктах критичної інфраструктури.

*Ключові слова*: захист персональних даних, критична інфраструктура, медичні інформаційні системи, кібербезпека, HIPAA, GDPR, NIST CSF 2.0, OSINT, ризики витоку даних.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| GDPR | – | General Data Protection Regime |
| HIPPA | – | Health Insurance Portability and Accountability Act |
| NIST CSF 2.0 | – | National Institute of Standards and Technology Cybersecurity Framework version 2.0 |
| ІС | – | Інформаційна система |
| КБ | – | Кібербезпека |
| НПА | – | Нормативно-правовий Акт |
| ОКІ | – | Об’єкт Критичної Інфраструктури |
| ПД | – | Персональні дані |
| МІС | – | Медичні інформаційні системи |
| ПЗ | – | Програмне забезпечення |
| DPO | – | Data Protection Officer |
| DPIA | – | Data Protection Impact Assessment |
| SOC | – | Security operation center |
| DLP | – | Data leak prevention system |
| SIEM | – | Security information and event management |
| ЕМЗ | – | Електронні медичні записи |
| PACS | – | Picture Archiving and Communication System |
| LIS | – | Laboratory Information System |
| CRM | – | Customer Relationship Management |
| EHR | – | Electronic Health Record |
| ЕМК | – | Elektronische Medizinische Karte, Electronic Medical Card |
| VPN | – | Virtual Private Network |

# ЗМІСТ

# ВСТУП

*Актуальність* кваліфікаційної роботи визначається стрімким розвитком цифрових технологій, який призвів до глибокої інтеграції інформаційних систем у сферу охорони здоров'я. На сьогоднішній день медичні заклади є частиною критичної інфраструктури держави, оскільки вони працюють із чутливими персональними даними пацієнтів, витік яких може спричинити не лише економічні та репутаційні втрати, а й загрожувати національній безпеці держави та правам громадян на приватність. Інформаційні активи у сфері охорони здоров'я є особливо вразливими, що пов'язано з їх високою цінністю для зловмисників та недостатнім рівнем технічного і організаційного захисту в медичних установах.

За даними IBM, середня вартість витоку даних у закладах критичної інфраструктури (включно з медичними) перевищує 4,8 млн доларів США, що на 1 млн більше, ніж у некритичних галузях. 83% організацій стикались з витоками даних неодноразово, а 60% змушені були підвищити ціни на послуги чи продукти після інциденту.

Найбільш поширеною причиною витоків залишаються викрадені або скомпрометовані облікові дані — вони стали джерелом 19% випадків. Ці витоки мали найдовший життєвий цикл: 243 дні на виявлення і ще 84 дні на локалізацію.

На Рисунку 1.1 представлено порівняння витрат на ліквідацію наслідків витоку даних у різних секторах економіки. Найбільші фінансові втрати фіксуються саме у медичній сфері (Healthcare) — $10,10 млн у найгіршому сценарії та $9,23 млн у середньому. Це майже вдвічі більше, ніж у більшості інших критичних галузей.

Системи захисту персональних даних у медичних закладах України та інших країн світу регулярно піддаються серйозним викликам, пов'язаним з

активізацією кіберзлочинності, зростанням складності атак та наявністю численних вразливостей у застарілих інформаційних системах.


Рисунок 1.1 – Статистика IBM середня вартість витоку даних у різних галузях (в мільйонах доларів)

Чутлива інформація, така як історії хвороби, результати аналізів, персональні дані пацієнтів, фінансові відомості та інші дані, перебувають під постійною загрозою витоку, що створює необхідність розробки нових та удосконалення існуючих заходів із забезпечення інформаційної безпеки відповідно до сучасних міжнародних стандартів.

Крім фінансових втрат, витоки персональних даних у медичних установах несуть за собою значні репутаційні ризики та юридичні наслідки. Згідно з дослідженнями, медична галузь протягом останніх років утримує лідерство за середньою вартістю інцидентів витоку даних. Така ситуація обумовлена як високою вартістю медичної інформації на чорному ринку, так і низьким рівнем впровадження сучасних систем безпеки, зокрема AI-рішень, Zero Trust-архітектури та повної відповідності вимогам HIPAA, GDPR і NIST CSF 2.0. У зв’язку з цим зростає потреба у комплексному переосмисленні підходів до захисту даних у сфері охорони здоров’я.

# РОЗДІЛ 1
# АНАЛІЗ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНИХ ЗАКЛАДАХ

## 1.1 Значимість захисту персональних медичних даних і характер загроз

Персональні дані пацієнтів та інформація про стан здоров'я відносяться до категорії чутливих даних, що потребують особливої охорони. За визначенням GDPR, будь-яка інформація щодо здоров'я людини належить до спеціальних категорій персональних даних, а значить, стандарти їхнього захисту є підвищеними [7].

В медичних інформаційних системах зберігаються електронні медичні записи (ЕМЗ), які містять такі критично важливі дані, як: ідентифікаційні відомості про пацієнта (ПІБ, дата народження, адреса тощо), дані медичної картки (діагнози, історія хвороби, призначені ліки, результати обстежень та аналізів), страхова інформація, фінансові дані (для розрахунків з страховиками або оплати послуг) і інша інформація. Компрометація цих відомостей може призвести до: порушення конфіденційності (розголошення діагнозів третім особам), шахрайства (наприклад, використання викрадених даних для отримання медичних послуг чи ліків), шантажу пацієнтів, підробки медичних документів, а також створює ризик втручання в процес лікування (якщо зловмисник здатен модифікувати записи, це може спричинити неправильне лікування) [2,5].

Тому цілісність і конфіденційність медичних даних безпосередньо пов'язані з безпекою пацієнтів. Недарма законодавчі акти, такі як HIPAA та GDPR, приділяють особливу увагу захисту саме інформації про здоров'я [1,6,7].

З точки зору кібербезпеки, медичні установи стикаються з широким спектром загроз. Дослідження показують, що домінуючим типом інцидентів, які

призводять до витоків у охороні здоров’я, є зловмисні атаки – зокрема злом інформаційних систем або мереж (“hacking/IT incidents”). На них припадає найбільша частка випадків компрометації, далі за поширеністю йдуть несанкціоновані дії зсередини (витоки через працівників або помилки персоналу). Серед типових загроз та векторів атак, актуальних для медичних інформаційних систем, можна виокремити такі:

- Зовнішні кібератаки через інтернет: зловмисники (хакери) можуть експлуатувати вразливості веб-порталів лікарень, електронних реєстрів, серверів баз даних або мережевого обладнання. Наприклад, використання вразливостей у популярному програмному забезпеченні медичних систем або brute-force атаку для отримання доступу до облікових записів. Один із випадків – атака на мережу Community Health Systems у США, коли хакери (ймовірно, з Китаю) скористались вразливістю програмного забезпечення та встановили складне шкідливе ПЗ, викравши дані 4,5 млн пацієнтів. Отже, експлуатація технічних вразливостей є реальним ризиком для медичних закладів [4,5].
- Програми-вимагачі (ransomware) та шкідливе ПЗ: лікарні останнім часом стали мішенню для угруповань, що поширюють ransomware. Такі атаки шифрують медичні дані, паралізують роботу закладу, а зловмисники вимагають викуп. Часто перед шифруванням дані також таємно копіюються (крадуться) – аби мати важіль тиску через погрозу витоку. Прикладом є атаки на медичні центри в різних країнах у 2021–2022 роках, коли персональні дані пацієнтів виставлялись на продаж у разі відмови платити. Ransomware-атаки можуть призвести не лише до витоку, а й до збою лікувальних процесів (як було з нападом вірусу WannaCry у 2017 році, що вразив десятки лікарень по всьому світу) [4,5,18].
- Внутрішні загрози (інсайдери): медичний персонал має широкий доступ до чутливих даних, тому навмисні зловживання або необережність працівників є серйозною загрозою. Несумлінний співробітник може скопіювати

базу пацієнтів з метою продажу (відомі випадки торгівлі базами даних медичних установ на чорному ринку). Так само працівники можуть несвідомо викликати витік – наприклад, переславши дані пацієнта на особисту електронну пошту без шифрування, забувши ноутбук зі списком пацієнтів у громадському місці, або неправильно налаштувавши доступ до хмарного сховища, зробивши його публічним [2,4].

- Технічні помилки та неправильна конфігурація систем: навіть без цілеспрямованого втручання зловмисників дані можуть опинитися у відкритому доступі через банальне нехтування безпекою. Помилки конфігурації баз даних чи серверів – як от залишені без пароля або з паролем за замовчуванням інтерфейси адміністрування, відкриті порти, публічно доступні резервні копії – усе це може призвести до випадкового витоку великої кількості даних. Розглянутий вище приклад з українською клінікою в Дніпрі це підтверджує: десятки тисяч записів були відкриті онлайн саме через неправильні налаштування систем. Такі ситуації можуть бути виявлені шляхом OSINT-моніторингу – наприклад, скануванням відкритих сегментів мережі на наявність незахищених баз даних [11,12,13].

Концепція OSINT походить від визначення «інформація з відкритих джерел» (Open Source Information). У найпростішій формі вона стосується інформації, яка не класифікується як «секретна». Розвідувальне співтовариство США визначає цей тип інформації як « загальнодоступні матеріали, які можна легально отримати шляхом запитів, покупок або спостереження, дотримуючись правил захисту авторських прав.

Основою збору розвідувальних даних є дослідження, яке, як видається, є перевіркою потреб розвідувальних даних з використанням існуючих джерел з метою створення продукту, що задовольняє життєво важливі потреби. Цей загальний підхід до збору даних однаково застосовується як до вже засекречених джерел, так і до відкритих джерел.

– Компрометація підрядників або партнерів: медичні установи взаємодіють із зовнішніми сервісами – лабораторіями, страховими компаніями, IT-підрядниками (наприклад, розробниками медичних інформаційних систем). Витік може статися у сторонньої організації, яка обробляє дані пацієнтів. Згідно з сучасними оцінками, до 47% витоків пов'язані з контрагентами або постачальниками послуг. Тому слабка безпека у партнера (наприклад, IT-компанії, що супроводжує лікарняну базу даних) також ставить під загрозу дані лікарні [4].

На Рисунку 1.2 нижче наведено огляд елементів процесу збору відкритої розвідувальної інформації (OSINT) [11,12,13].

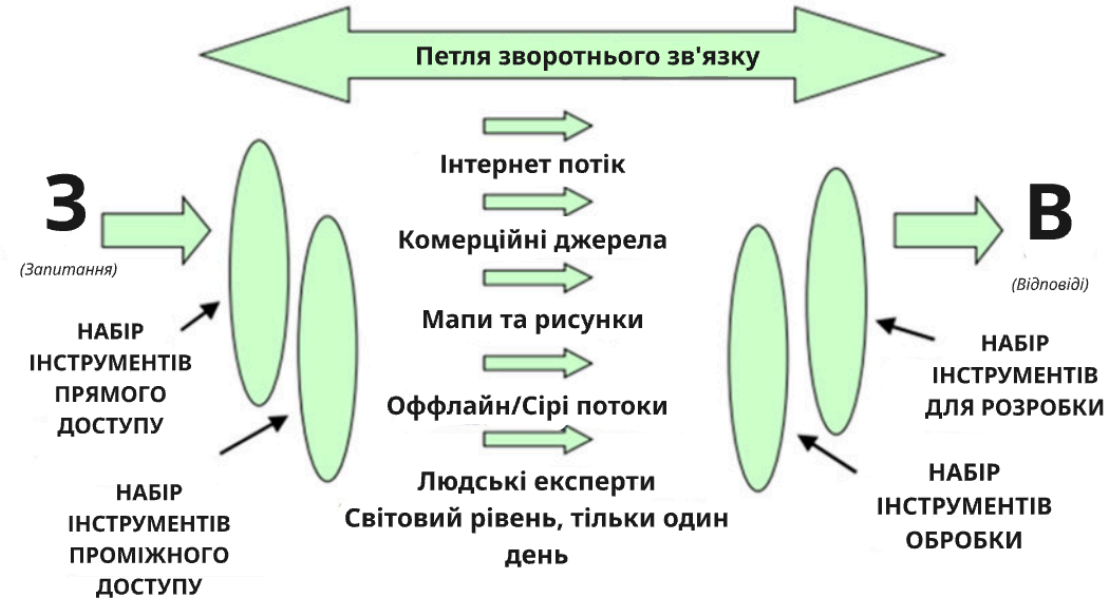


Рисунок 1.2 – Процес збору OSINT-даних [11,12,13]

– Соціальна інженерія та фішинг: медперсонал може стати жертвою цільового фішингу – коли нападник, маскуючись під колегу чи технічну підтримку, виманює облікові дані для доступу до систем. У середовищі лікарні, де завантаженість роботою висока, а багато процесів екстрені, людина може не

завжди уважно перевіряти підозрілі листи. Фішингові атаки часто є першим кроком перед більш серйозним проникненням у мережу закладу.

Таким чином, середовище охорони здоров'я є багатокомпонентним і складним з точки зору кібербезпеки, і загрози витоку можуть надходити як ззовні, так і зсередини. Необхідно розуміти мотивацію зловмисників: для кіберзлочинців основний стимул – фінансова вигода (продаж медичних даних на чорному ринку, вимагання викупу); для хактивістів – можливо, дискредитація певної клініки чи протест; для державних хакерів – шпигунство або дестабілізація (особливо актуально під час військових конфліктів, коли дані про здоров'я населення або конкретних осіб можуть бути розвідувальними цілями).

Цінність медичних даних на чорному ринку дуже висока – повний медичний профіль пацієнта може коштувати сотні доларів, що перевищує ціну інших типів персональних даних (наприклад, даних кредитних карток). Це робить медицину привабливою мішенню для атак. За період з 2005 по 2019 роки глобально було скомпрометовано близько 249 мільйонів записів, що стосуються охорони здоров'я, причому понад половина з них – лише за останні п'ять років того періоду. У 2018 році медична галузь пережила 536 витоків (із ~2216 інцидентів у всіх галузях), що зробило її лідером за кількістю порушень серед усіх секторів економіки. В 2019 році було вже 505 інцидентів у сфері охорони здоров'я по світу, які призвели до експозиції 41,2 млн записів. Ця тенденція до зростання кількості та масштабу витоків, на жаль, зберігається – як зазначалося, 2023 рік перевершив попередні, принісши новий антирекорд за числом зламаних записів.

Високі фінансові втрати від інцидентів додатково підкреслюють серйозність проблеми. Середня вартість одного витоку даних у сфері охорони здоров'я є найвищою серед усіх галузей протягом останніх років. Так, за даними IBM, середня шкода від однієї компрометації медичних даних у США сягає ~$15 млн (для порівняння, середній показник по усіх галузях ~$8 млн). Вартість порушення на один запис у медицині також найвища і зростає швидше, ніж в інших сферах.

Це враховує не тільки прямі фінансові витрати на ліквідацію наслідків, але й штрафи регуляторів, судові позови від пацієнтів, втрату репутації та довіри [4,5,18].

## 1.2 Типові проблеми та вразливості інформаційних систем у медичних закладах

Медичні інформаційні системи (МИС) охоплюють різноманітні програмно-апаратні комплекси: електронні реєстри пацієнтів, системи управління лікарнею (HIS), лабораторні інформаційні системи, портали для пацієнтів, мобільні додатки здоров'я, медичні прилади з підключенням до мережі (Internet of Medical Things, IoMT) тощо. В Україні функціонує центральна електронна система охорони здоров'я (ЕСОЗ або eHealth), до якої підключені численні приватні МИС, такі як Helsi, Medics, Doctor Eleks та інші. Кожна з цих систем може мати свої особливості і потенційні вразливі місця. Розглянемо типові проблеми безпеки, властиві медичним ІТ-системам:

Багато лікарень історично використовують застарілі ОС (напр. Windows 7/XP) [4,18] та медичне обладнання зі вбудованими системами, які давно не оновлювались. Вразливості таких систем відомі публічно, і відсутність оновлень створює проломи в безпеці. Сумнозвісний випадок – епідемія вірусу WannaCry (2017), яка швидко поширилась через незакриту вразливість у Windows; лікарні, що не встановили патч, постраждали найбільше. На 2023 рік проблеми з оновленнями залишаються: в деяких медичних приладах (МРТ, апаратах ШВЛ тощо) використовуються старі ОС, які важко оновити, і вони стають "троянським конем" в мережі лікарні.

Типова ситуація – спільні облікові записи для медперсоналу або відсутність багатофакторної автентифікації. Наприклад, медсестри можуть користуватися одним логіном для входу в систему запису пацієнтів, що ускладнює аудит і підвищує ризик компрометації (пароль відомий багатьом). Нерідко паролі задаються слабкі або не змінюються роками. Відомий випадок у

Португалії: лікарня отримала штраф, коли з’ясувалося, що сотні працівників мали доступ до електронних записів пацієнтів поза межами їхніх повноважень (дефіцит належної диференціації доступів). Отже, принцип найменших привілеїв часто не дотримується [5].

Якщо бази даних зберігаються у відкритому вигляді, зловмисник, отримавши до них доступ, одразу заволодіває усіма даними. Шифрування “на спочинку” (at-rest) є критично важливим для медичних даних, але не завжди реалізованим. Аналогічно, шифрування трафіку: якщо внутрішні сервіси передають дані незашифрованим HTTP, їх можна перехопити при компрометації мережі. Вимоги GDPR [7] прямо не диктують конкретні технології, але наголошують на "відповідних технічних і організаційних заходах", серед яких згадується псевдонімізація та шифрування персональних даних як спосіб захисту (ст.32 GDPR) – проте не всі медичні заклади впровадили ці засоби повною мірою.

Ідеально медична мережа повинна бути сегментована [4], робочі станції відділені від серверів, медичне обладнання – у власному VLAN, з обмеженим доступом до інтернету тощо. Проте на практиці часто вся лікарняна мережа є пласкою: з будь-якого комп’ютера можна дістатися до будь-якого сервера. Це полегшує зловмиснику переміщення всередині (lateral movement) після початкової компрометації.

У багатьох медичних закладах відсутній централізований журнал аудиту доступу до даних або систем виявлення вторгнень [4,5]. Це означає, що витік може довго залишатися непоміченим. Наприклад, якщо інсайдер скопіював дані на флешку, а журнал пристроїв USB не ведеться – інцидент може взагалі не бути виявлений. Відповідно, реагування на інциденти також страждає – немає плану чи команди, відповідальної за кібербезпеку, особливо в невеликих клініках.

Медперсонал, зайнятий лікуванням, часто не проходить достатніх навчань з інформаційної безпеки. Як наслідок – відкриваються фішингові листи, використовуються особисті месенджери для передачі даних пацієнтів,

ігноруються базові правила (не залишати екран без блокування, не вкладати в електронну пошту нешифровані виписки тощо). Культура захисту даних може бути слабкою, якщо керівництво не приділяє цьому уваги [2,4].

З поширенням мобільних технологій лікарі можуть використовувати власні смартфони для доступу до інформації (наприклад, сфотографувати результати аналізів на екран монітора, щоб проконсультуватися віддалено). Якщо при цьому пристрій не захищений або використано ненадійний додаток, дані можуть "витекти" через нього [4].

Вищенаведені проблеми є типовими точками слабкості, які в сукупності підвищують ризик витоку даних. Наприклад, у згаданому кейсі в Дніпрі фактором стали саме помилки конфігурації та недбалість у забезпеченні безпеки. Клініка не реагувала на повідомлення експертів про вразливості і тривалий час тримала дані у відкритому доступі, що свідчить про брак процедур реагування.

Інший приклад: уявімо, що в популярній українській системі Helsi сталася умовна вразливість API, яка дозволила б неавторизовано отримувати дані пацієнтів [3,11,13]. Якщо розробники та адміністратори не проводять регулярних тестів на проникнення і перевірок безпеки, така дірка могла б довго існувати. У поєднанні з тим, що Helsi містить записи мільйонів українців, наслідки потенційно катастрофічні. На щастя, на даний момент значних витоків саме з центральної системи eHealth не зафіксовано, проте це не знімає ризиків – більшість інцидентів трапляються на рівні окремих медичних закладів або їхніх підрядників.

### 1.3 Аналіз реальних інцидентів витоку даних та їх наслідки

Для глибшого розуміння проблеми розглянемо декілька реальних кейсів витоку даних у сфері охорони здоров'я, зазначаючи причини та наслідки:

Витік даних у приватній клініці (Дніпро, Україна, 2020) – описаний вище випадок, коли відкритий сервер клініки дозволив зловмисникам отримати

десятки тисяч записів пацієнтів. Причина: неправильна конфігурація бази даних (відсутній контроль доступу). Наслідки: розголошення медичної таємниці (дані про діагнози, COVID-статус тощо), загроза модифікації даних сторонніми (тобто потенційна шкода пацієнтам), репутаційні втрати для клініки. Правоохоронні органи були повідомлені, клініка зобов'язана усунути вразливості; можлива відповідальність керівництва. Цей кейс показує важливість проактивного моніторингу (витік знайшли кіберфахівці НКЦК) і те, що навіть приватні заклади повинні дотримуватися стандартів безпеки, як це робить державна система eHealth [11,12,13].

Anthem (США, 2015) – один з найбільших відомих витоків у медицині. Компанія Anthem (страхова та медична організація) повідомила про злам, в результаті якого зловмисники отримали доступ до записів ~78,8 млн осіб (пацієнтів та страхувальників). Причина: цільова хакерська атака (імовірно, з використанням викрадених облікових даних або шкідливого ПЗ). Наслідки: витік імен, дат народження, Social Security Number, медичної інформації та ін. Anthem заплатила штрафи та компенсації, сукупні витрати перевищили $100 млн. Цей випадок підштовхнув посилення вимог HIPAA щодо шифрування та моніторингу [4,5].

WannaCry (Велика Британія, 2017) – атака ransomware, що вразила Національну службу охорони здоров'я (NHS) [18]. Хоча головною метою атаки не було викрадення даних, а вимагання, наслідком стало порушення доступності даних: десятки лікарень не мали доступу до медичних записів, скасували операції. Причина успіху атаки: на багатьох комп'ютерах NHS не було встановлено критичне поновлення безпеки.

University of California, Los Angeles (UCLA) Health (США, 2014-2015) – кібератака, виявлена у 2015, яка тривала кілька місяців. Зловмисники отримали доступ до систем UCLA Health і компрометували особисті та медичні дані 4,5 млн пацієнтів. Причина: неоголошено публічно детально, але підозрюється зовнішнє зламувачування мережі. UCLA зазнала суттєвих фінансових і репутаційних втрат, інвестувала в значне посилення безпеки після інциденту

(впровадили двофакторну автентифікацію, аналітику поведінки для виявлення аномалій доступу) [4,5].

Організаціями часто не розголошуються публічно випадки меншого масштабу, але які трапляються повсюдно. Наприклад, викрадення ноутбука лікаря, на якому не було шифрування диска, і містилася база даних пацієнтів клініки. Такі локальні витоки теж підпадають під дію законів: у США компанія повинна повідомити регулятора (HHS OCR) про інцидент протягом 60 днів, а в Європі GDPR зобов'язує повідомити наглядовий орган протягом 72 годин [7] з моменту виявлення порушення. У цьому й різниця в підходах: GDPR більш жорсткий по строках, HIPAA – по звітуванню (зокрема, якщо більше 500 осіб постраждало, необхідно також інформувати ЗМІ та всіх суб'єктів даних) [1,6].

**Висновок до розділу 1**

Аналіз сучасних загроз, типових вразливостей та реальних інцидентів витоку медичних даних переконливо демонструє, що сфера охорони здоров'я є однією з найбільш уразливих до порушень кібербезпеки. Особливість цієї сфери полягає в тому, що вона обробляє вкрай чутливу інформацію про пацієнтів, де порушення конфіденційності, цілісності або доступності даних може мати не лише фінансові чи репутаційні наслідки, але й безпосередньо впливати на здоров'я та життя людей. У багатьох випадках витоки трапляються не лише через дії зовнішніх зловмисників, а й унаслідок внутрішніх помилок, недбалості персоналу, неправильної конфігурації систем або відсутності належного захисту критичних активів.

Показові кейси з українських і міжнародних медичних установ підтверджують, що жодна організація не застрахована від інцидентів незалежно від її масштабу. Витоки можуть виникати як у приватній клініці, так і в транснаціональній корпорації з мільйонами записів. Характер наслідків варіюється: від штрафів, судових позовів та зниження довіри до установи — до потенційної шкоди пацієнтам, якщо змінено або викрадено дані про алергії,

призначення або результати аналізів. Така ситуація вимагає не лише базового рівня захисту, а й системного впровадження високих стандартів інформаційної безпеки, заснованих на міжнародних нормативних вимогах і передових практиках.

Загальна тенденція свідчить про те, що організації, які дотримуються регуляторних вимог, таких як HIPAA і GDPR, впроваджують сучасні технічні та організаційні заходи безпеки, а також активно розвивають культуру захисту даних серед персоналу, демонструють значно вищу стійкість до атак та швидшу здатність до виявлення і нейтралізації загроз. Це особливо актуально в умовах постійного зростання обсягів даних і поширення нових векторів атак, таких як фішинг, шкідливе ПЗ, інсайдерська діяльність і помилки конфігурації.

Таким чином, у сфері охорони здоров’я не існує "дріб’язкових" витоків — кожен інцидент піддає ризику як приватність конкретних осіб, так і загальну довіру до системи. Проактивний підхід, що включає превентивні заходи, регулярний аудит, впровадження технологій шифрування, контроль доступу, навчання персоналу та реагування на інциденти, має стати основою захисту медичних інформаційних систем. У наступному розділі буде розглянуто нормативні акти та стандарти, які формують правову і практичну основу побудови ефективної системи захисту персональних даних у сфері охорони здоров’я.

# РОЗДІЛ 2
# ДОСЛІДЖЕННЯ ВИМОГ ТА МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ В МЕДИЧНИХ ЗАКЛАДАХ

У сфері захисту інформації в охороні здоров’я діють як міжнародні регуляторні акти, так і галузеві стандарти. Розглянемо три ключові з них, а саме американський закон HIPAA [1,6], рамковий стандарт NIST CSF 2.0 [8] та європейський регламент GDPR [7].

## 2.1 Стандарт HIPAA – вимоги до безпеки медичних даних

HIPAA (Health Insurance Portability and Accountability Act) – федеральний закон США, прийнятий у 1996 році, що встановлює стандарти конфіденційності та безпеки для захисту медичної інформації. З точки зору інформаційної безпеки, найбільш значущим є так зване Правило Безпеки HIPAA (HIPAA Security Rule), яке вимагає від усіх охоплених суб’єктів охорони здоров’я (постачальників медпослуг, страхових планів, центрів обробки даних) забезпечити конфіденційність, цілісність та доступність електронної захищеної медичної інформації (ePHI) шляхом впровадження належних адміністративних, фізичних та технічних заходів безпеки. До кола охоплених осіб (Covered Entities) належать практично всі організації, які обробляють медичні дані в електронному вигляді, а також їх бізнес-партнери (Business Associates), що мають доступ до таких даних [1,6].

Основні вимоги HIPAA Security Rule можна підсумувати так:

Адміністративні заходи безпеки – це політики, процедури та управлінські дії, покликані убезпечити обробку ePHI. Сюди входять: призначення відповідальної особи за безпеку (Chief Security Officer), навчання співробітників правилам захисту даних, проведення оцінки ризиків і впровадження плану управління ризиками. HIPAA прямо вимагає регулярного проведення

ретельного аналізу ризиків для виявлення потенційних загроз і вразливостей ePHI, а також вжиття заходів для їх мінімізації. Також адміністративні вимоги включають контроль доступу користувачів (призначення ролей, обмеження прав), процедури реагування на інциденти, плани безперервності (на випадок аварій), договори з підрядниками про дотримання конфіденційності і т.д.

Фізичні заходи безпеки – стосуються захисту середовища, де зберігаються чи обробляються меддані. Наприклад: обмеження доступу до приміщень з серверами (системи контролю доступу, замки, охорона), відеоспостереження, захист робочих місць (екрани від перегляду, політика чистого столу), безпечна утилізація носіїв інформації (диски, паперові копії) тощо. Мета – не допустити фізичного викрадення або ознайомлення з даними [1,6].

Технічні заходи безпеки – це конкретні технологічні рішення для захисту ePHI. Серед них: контроль доступу (у тому числі унікальні ідентифікатори користувачів, паролі, двофакторна автентифікація), аудит та журналювання (відстеження хто і коли переглядав/змінював дані), захист даних під час передавання (шифрування каналів зв’язку) та захист даних при зберіганні (шифрування баз даних, резервне копіювання), цілісність даних (механізми перевірки цілісності, щоб дані не були несанкціоновано змінені), а також засоби автентифікації об’єктів (щоб система впевнилась, що дані надходять від легітимного джерела) [1,6]. HIPAA не нав’язує конкретні алгоритми чи продукти, але вимагає “reasonable and appropriate” заходів – тобто таких, що обґрунтовані розміром та ризиками конкретної організації.

Крім Security Rule, HIPAA включає Privacy Rule (Правило конфіденційності), що регулює кому і в яких випадках можна розкривати медичні дані. Наприклад, пацієнт повинен дати згоду на передачу своїх даних третій стороні, за винятком випадків лікування, оплати або операцій охорони здоров’я. Privacy Rule також гарантує права пацієнтів: право знати, які їх дані обробляються, отримувати копії, вимагати виправлення помилок. Це теж пов’язано з безпекою: обмеження кола осіб, що бачать дані, знижує ризик витоку.

Ще одне важливе доповнення – Правило про повідомлення про витоки (Breach Notification Rule), яке зобов'язує організацію, що підпадає під HIPAA, сповіщати постраждалих пацієнтів та регулятор (HHS Office for Civil Rights) про випадки витоку незашифрованої медичної інформації. Якщо інцидент стосується понад 500 осіб, інформація також має бути повідомлена засобам масової інформації. Термін сповіщення – не пізніше 60 днів з моменту виявлення порушення [1,6].

Відповідальність за недотримання HIPAA: контроль за виконанням закону здійснює Управління громадянських прав HHS (OCR). За порушення передбачені значні штрафи – від десятків тисяч до мільйонів доларів, залежно від ступеня вини та масштабу (максимальні штрафи можуть сягати $1.5 млн за одну категорію порушень на рік). Наприклад, у 2019 році компанію-оператора медичних записів було оштрафовано на $3 млн за несвоєчасне повідомлення про витік. Крім штрафів, можливі й кримінальні покарання у випадку навмисного недотримання або продажу даних. Також втрата репутації – суттєвий наслідок, що мотивує дотримуватися HIPAA [5].

## 2.2 NIST Cybersecurity Framework 2.0: сучасна рамка кібербезпеки

NIST CSF (Cybersecurity Framework) – це не закон, а набір рекомендацій та найкращих практик з кібербезпеки, розроблений Національним інститутом стандартів і технологій США (NIST). Перша версія з'явилась у 2014 році (як добровільний стандарт для критичної інфраструктури), оновлення 1.1 – в 2018 році. Версія 2.0, на яку ми орієнтуємося, була фіналізована в 2023 році (проєкт обговорювався у 2022, офіційний випуск відбувся в 2024). Ця нова версія має низку змін і доповнень порівняно з 1.1, що відображає еволюцію загроз і практик [5,8].

Основою NIST CSF є поділ кібербезпеки організації на 5 основних Функцій: Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування), Recover (Відновлення). У версії 2.0 додано ще шосту Функцію –

Govern (Управління). Кожна функція ділиться на Категорії та підкатегорії (всього у CSF 2.0 понад 20 категорій і ~100 підкатегорій), яким відповідають конкретні заходи чи результати, яких слід досягти [5,8].

Govern (Управління) – НОВА функція в CSF 2.0, яка акцентує увагу на питаннях управління кібербезпекою на рівні організації. Сюди входять: визначення ролей і відповідальності за безпеку, інтеграція кіберризиків у загальне управління ризиками, залучення керівництва (борду) до прийняття рішень з безпеки, управління політиками, відповідність вимогам. Раніше ці аспекти були розпорошені по інших категоріях, а тепер виділені окремо як важливий стовп. Це зроблено, аби зв’язати бізнес та безпеку, донести до вищого керівництва важливість кібербезпеки. Як зазначає NIST, функція Govern покликана забезпечити обізнаність стейкхолдерів про кіберризики та інтегрувати їх у плани дій.

Identify (Ідентифікація) – включає категорії: розуміння контексту організації, визначення критичних активів (систем, даних), аналіз бізнес-середовища, оцінка кіберризиків, визначення залежностей (наприклад, від постачальників). Мета – щоб організація знала, які інформаційні активи має і які ризики для них існують.

Protect (Захист) – охоплює заходи захисту і превентивного контролю: управління ідентичностями та доступом, захист даних (шифрування, бекапи), забезпечення життєздатності систем (обслуговування, патчі), навчання та підвищення обізнаності персоналу, впровадження технологій захисту на рівні мережі, додатків, кінцевих пристроїв тощо. Тут фокус саме на попередженні інцидентів.

Detect (Виявлення) – описує можливості з моніторингу та виявлення аномалій: безперервний моніторинг безпеки, виявлення вторгнень, аналіз журналів, виявлення потенційних витоків або спроб несанкціонованого доступу. Згідно CSF, організація повинна мати засоби для своєчасного виявлення інцидентів.

Respond (Реагування) – настанови щодо того, як реагувати, коли інцидент таки стався: плани реагування, комунікація (внутрішня і зовнішня, включно з повідомленням регуляторів чи клієнтів), аналіз першопричин, стримування загрози, усунення наслідків. В CSF 2.0 цю функцію трохи розширено/уточнено за результатами досвіду останніх років.

Recover (Відновлення) – передбачає заходи з відновлення нормальної роботи після інциденту: плани відновлення, резервні копії, відновлення репутації, впровадження уроків, отриманих з інциденту.

Одним з важливих оновлень CSF 2.0 є посилення уваги до ризиків ланцюга поставок і безпеки ПЗ. В новій версії з’явилися додаткові категорії для Cybersecurity Supply Chain Risk Management (C-SCRM) – зокрема, в функції Govern тепер явно присутні результати, пов’язані з управлінням ризиками постачальників та безпекою ланцюга поставок. Це реакція на зростання кількості атак через третіх осіб і уразливі бібліотеки (типу випадку SolarWinds або Log4Shell). Прогнозується, що до 2025 року 45% організацій у світі постраждають від атак через ланцюг поставок ПЗ, тому NIST намагається проактивно підготувати до цього компанії [5,8].

CSF є гнучким інструментом: він не диктує конкретних технологій, але дає структуру для побудови/оцінки програми кібербезпеки. Він також постачається з довідником "Core", де перераховані контрольні заходи і посилання на інші стандарти (ISO 27001, COBIT, NIST SP800-53 тощо) для кожної підкатегорії. Таким чином, організація може порівняти свій стан з рекомендованим.

Для оцінки прогресу в CSF існує концепція Рівнів реалізації (Implementation Tiers). У версії 1.1 було 4 рівні: Tier 1 (Partial) – процеси кібербезпеки непослідовні, реактивні; Tier 2 (Risk Informed) – розуміння ризиків є, але практики не стандартизовані повністю; Tier 3 (Repeatable) – політики формалізовані, діють по всій організації; Tier 4 (Adaptive) – передовий рівень, коли безпека інтегрована в культуру, постійно вдосконалюється. У CSF 2.0 ці

рівні теж використовуються для самооцінки зрілості, хоча акцент більше на якісному описі, ніж на рейтингу.

Для медичних закладів NIST CSF 2.0 є корисним як модель побудови системи захисту. Наприклад, в контексті витоків даних:

Identify: визначити, які системи містять критичні персональні дані пацієнтів, хто постачальники (наприклад, хмарний сервіс) і які ризики (оцінка, що буде якщо дані витечуть, як це може статися).

Protect: впровадити засоби (контроль доступу, шифрування, DLP-системи для запобігання копіюванню/відправленню даних, навчання персоналу щодо фішингу).

Detect: моніторити мережевий трафік на наявність аномалій (наприклад, масове вивантаження даних), використовувати системи Data Leak Detection (наприклад, сканування даркнету на появу даних лікарні).

Respond: мати план дій при витоку (кого сповіщати – пацієнтів, МОЗ, поліцію; як ізолювати скомпрометовані системи, тощо).

Recover: забезпечити резервні копії, щоб можна було відновитися після інциденту, провести розбір інциденту і вдосконалити процеси.

CSF 2.0, порівняно з регуляторами як HIPAA/GDPR, не є обов’язковим, але став фактично світовим стандартом “де-факто”. Його перевага – універсальність і актуальність. Версія 2.0 підкреслює, що рамка тепер індустріально-нейтральна (перший випуск був спрямований на критичну інфраструктуру, тепер же чітко зазначено, що CSF 2.0 застосовний до організацій будь-якої галузі). Для медицини NIST CSF також застосовується (HHS рекомендує медичним установам використовувати CSF для підсилення програм відповідності HIPAA) [5,8].

Отже, NIST CSF 2.0 ми розглядаємо як основу для оцінки зрілості та формування дорожньої карти покращень у Розділі 3.

## 2.3 Регламент GDPR: захист персональних даних у ЄС

GDPR (General Data Protection Regulation, Загальний регламент захисту даних) – це законодавчий акт Європейського Союзу, що набув чинності 25 травня 2018 року. Він є одним з найсуворіших у світі законів про приватність і стосується будь-яких організацій, які обробляють персональні дані резидентів ЄС (не залежно від країни реєстрації організації). Хоча GDPR охоплює всі сфери, для медичних даних він має особливе значення, оскільки визначає їх як спеціальну категорію (sensitive data) з додатковим рівнем захисту [7].

Принципи обробки даних: GDPR встановлює 7 фундаментальних принципів – законність, справедливість, прозорість; обмеження цілей; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність. Для медзакладу це означає: збирати тільки ті дані, що потрібні для надання послуг; використовувати їх лише з конкретною метою (лікування, ведення медичних записів); зберігати не довше, ніж потрібно; забезпечувати їх точність і актуальність; захищати від несанкціонованого доступу (це прямо вказано принципом цілісності та конфіденційності) [7].

Правові підстави обробки: Для обробки персональних даних повинна бути підстава – зокрема, згода суб’єкта або необхідність для виконання договору, законний обов’язок, захист життєво важливих інтересів, суспільний інтерес в сфері охорони здоров’я тощо. Для медичних даних (спецкатегорія) звичайною підставою є явна згода пацієнта або необхідність для надання медичних послуг та охорони здоров’я. Тобто лікарня повинна мати документально оформлені згоди чи інші підстави для всіх персональних даних, що збирає.

Права суб’єктів даних: GDPR детально прописує права осіб – право на доступ до своїх даних, право на виправлення, право на видалення (“право бути забутим”), право на перенесення даних, право на обмеження обробки, право заперечувати проти обробки. У контексті медичних даних: пацієнт у ЄС може вимагати видалення своїх записів за певних обставин (якщо це не суперечить

обов’язку зберігати їх, наприклад, медзаклад може мати законний обов’язок зберігати історію хвороби X років). В Україні поки що GDPR не імплементований, але Закон про захист персональних даних дає схожі права [7].

Вимоги безпеки (ст. 32 GDPR): Організації зобов’язані впровадити «належні технічні та організаційні заходи» для забезпечення рівня безпеки, відповідного ризикам. Прямо згадуються: псевдонімізація та шифрування персональних даних; забезпечення постійної конфіденційності, цілісності, доступності та стійкості систем; здатність вчасно відновити доступність даних після інциденту; регулярне тестування ефективності заходів безпеки. Важливо, що GDPR не диктує конкретних технологій – він принципово технологічно нейтральний, але вимагає підходу, орієнтованого на ризик: більш ризиковані операції повинні мати сильніший захист. У випадку медичних даних (які є високоризиковими) очікується підвищений рівень захисту.

Data Protection by Design та by Default (ст.25): вимагається, щоб захист даних був вбудований у процеси і системи з самого початку їх розробки (privacy by design) і за замовчуванням оброблявся мінімум необхідних даних (privacy by default). Для медичної IT-системи це означає: ще на стадії проектування врахувати вимоги безпеки – наприклад, щоб за замовчуванням доступ до запису пацієнта мав лише лікар, що його лікує (мінімізація доступу) [7].

Призначення Data Protection Officer (DPO): Якщо організація систематично обробляє здоров’яні дані у великих обсягах, GDPR вимагає призначити посадову особу із захисту даних (ст.37). Лікарні в ЄС зазвичай повинні мати DPO, який контролює дотримання правил.

Повідомлення про витоки: GDPR зобов’язує контролера даних повідомити наглядовий орган (наприклад, національну службу із захисту даних) про факт порушення протягом 72 годин після виявлення, якщо витік несе ризик для прав і свобод осіб. Якщо ж витік може спричинити високий ризик (наприклад, розкриття медичних діагнозів), слід повідомити і самих постраждалих суб’єктів без зайвої затримки. Цей обов’язок аналогічний HIPAA,

але більш жорсткий за термінами і фактично глобальний (бо стосується навіть компаній поза ЄС, якщо дані європейців).

Санкції за порушення GDPR [7] надзвичайно суворі. Максимальні штрафи – до 20 млн євро або 4% світового річного обороту компанії, залежно що більше. Для менш тяжких порушень – до 10 млн або 2%. Були прецеденти, коли великі компанії отримували штрафи в десятки мільйонів (наприклад, Google, British Airways). У сфері охорони здоров'я теж були випадки: наприклад, португальську лікарню штрафували на 400 тис. євро за надмірно широкий доступ до даних пацієнтів (коли 985 користувачів мали профіль "лікар", хоч лікарів було менше). Це сигнал, що регулятори серйозно ставляться до захисту медичної інформації. GDPR також дозволяє потерпілим вимагати компенсації через суд [2].

GDPR не є суто "безпековим" стандартом – це більше про приватність загалом. Але з точки зору нашого завдання, він задає орієнтир, що має бути результатом захисту: дані пацієнтів недоступні стороннім, пацієнти контролюють свої дані, витоків не стається, а якщо сталося – вплив мінімізовано і всі повідомлені.

Україна, як країна що прагне до вступу в ЄС, поступово адаптує своє законодавство. Наразі діє Закон "Про захист персональних даних", але він м'якший ніж GDPR. Проте в медичних проєктах, особливо міжнародних, вже рекомендується дотримуватися принципів GDPR. Тому методологія з удосконалення систем проти витоків повинна враховувати і ці вимоги, особливо щодо прозорості, шифрування та мінімізації даних [7].

### 2.4 Методи захисту медичних даних: моделі загроз, порушників та матриця ризиків

Для медичних IT-систем, що обробляють чутливі дані пацієнтів, критично важливо визначити потенційні загрози витоку даних, типи порушників та оцінити ризики. Нижче наведено три таблиці: модель загроз, модель порушника

та матриця ризиків, складені з урахуванням специфіки медичних закладів та стандартів безпеки.

У таблиці 2.1 (див. Додаток Е) подано основні загрози витоку даних у медичних інформаційних системах, включно з назвою загрози, її описом, джерелом походження, вектором атаки та компонентом, на який націлена атака.

Дані пацієнтів є надзвичайно цінними для кіберзлочинців (вартість медичних записів на чорному ринку перевищує навіть банківські дані). Тому медичні заклади стикаються з різноманітними загрозами: від зовнішніх атак до внутрішніх інсайдерів. Більшість витоків інформації спричиняють або атаки хакерів (наприклад, через фішинг чи уразливості), або дії співробітників – навмисні чи випадкові. Ці загрози враховуються при розробці систем DLP (Data Loss Prevention) для медичного сектору.

У таблиці 2.2 (див. Додаток Є) наведено основні типи порушників інформаційної безпеки медичних систем – від зовнішніх хакерів до внутрішніх співробітників. Для кожного типу зазначено мотивацію, технічні можливості, рівень привілеїв та типові дії.

Зовнішні кіберзлочинці становлять найбільшу групу загроз для медичних закладів, здебільшого керуючись фінансовою мотивацією (за даними ENISA, 83% інцидентів у сфері охорони здоров’я мали на меті саме фінансову вигоду). Водночас інсайдери – як зловмисні, так і випадкові – також є суттєвим фактором ризику, спричиняючи значну частку витоків даних. Тому комплексна система безпеки повинна враховувати усі типи порушників: і зовнішніх, і внутрішніх, і партнерів.

У таблиці 2.3 (див. Додаток Ж) наведено матрицю ризиків для загроз витоку даних. Матриця ризиків оцінює ймовірність та вплив реалізації кожної загрози, визначаючи рівень ризику (низький, середній, високий) та відповідні заходи реагування. Враховано специфіку медичних даних: витік персональної медичної інформації має високий вплив через можливі штрафи, репутаційні втрати та загрозу пацієнтам. Ймовірність оцінено на основі частоти подібних інцидентів у галузі.

Оцінка рівнів ризику проводилась на основі поєднання ймовірності та впливу. Для медичних установ характерні часті фішингові атаки та ransomware-інциденти, що підтверджується статистикою (понад 90% атак на медичну сферу починаються з фішингу; вибухове зростання ransomware у 2020-2023 роках) [4,5]. Витоки даних ведуть до серйозних наслідків – від фінансових втрат до загрози життю пацієнтів. Запропоновані заходи захисту відповідають сучасним стандартам безпеки (зокрема, рекомендаціям NIST, ISO 27799 для охорони здоров'я та вимогам законодавства щодо захисту персональних даних). Впровадження цих заходів у комплексі дозволить удосконалити систему контролю витоків даних у медичних інформаційних системах [11,12,13].

**Висновок до розділу 2**

Аналіз нормативних вимог і підходів до захисту персональних медичних даних, визначених у трьох провідних стандартах — HIPAA (США), NIST Cybersecurity Framework 2.0 (США) та GDPR (ЄС), засвідчив, що незважаючи на відмінності в юридичному статусі, сфері застосування та методологічному підході, всі ці документи формують цілісну й взаємодоповнюючу основу для побудови ефективної системи захисту даних у сфері охорони здоров'я.

HIPAA є галузевим нормативним актом, що має силу федерального закону та орієнтований насамперед на медичні установи США. Він містить чітко визначені вимоги до захисту електронної медичної інформації (ePHI), включаючи адміністративні, технічні та фізичні заходи безпеки. Закон фокусує увагу на відповідальності за збереження конфіденційності, цілісності та доступності медичних даних і передбачає жорсткі санкції за недотримання, зокрема за неналежне повідомлення про витоки. Унікальною рисою HIPAA є чітке розмежування обов'язків між охопленими суб'єктами (Covered Entities) та їх бізнес-партнерами, що дозволяє регулювати взаємодію в розгалужених медичних екосистемах.

NIST CSF 2.0, на відміну від HIPAA, є гнучкою рекомендаційною рамкою, призначеною для підвищення кіберстійкості організацій будь-якого типу. Його ключовою перевагою є системна структура з шести функцій (Govern, Identify, Protect, Detect, Respond, Recover), яка охоплює повний цикл управління інформаційною безпекою. CSF забезпечує можливість адаптації заходів відповідно до рівня зрілості організації, оцінки ризиків, галузевої специфіки та масштабу операцій. В охороні здоров'я цей стандарт є цінним інструментом для формування стратегії безпеки, інтеграції з іншими вимогами (наприклад, HIPAA або ISO 27001) і розвитку системи безперервного вдосконалення захисту даних.

GDPR, у свою чергу, виступає як всеосяжна законодавча рамка приватності, що зобов'язує всі організації, які працюють із даними резидентів ЄС, дотримуватися принципів законності, мінімізації, прозорості, точності та безпеки обробки персональної інформації. Регламент особливо суворо регулює обробку чутливих даних, таких як медичні, і висуває обов'язкові вимоги щодо вбудованого захисту даних (privacy by design), обов'язкових оцінок впливу (DPIA), призначення уповноважених осіб із захисту даних (DPO) та обов'язкового повідомлення про витоки протягом 72 годин. GDPR також встановлює жорсткі санкції у разі порушень, що стимулює організації до формування систем превентивної безпеки.

Узагальнюючи, можна стверджувати, що HIPAA, NIST CSF 2.0 та GDPR разом охоплюють усі ключові компоненти системи захисту персональних медичних даних: правову регламентацію, організаційне управління, технічну реалізацію, оцінку ризиків, контроль за дотриманням політик, а також реагування та відновлення у випадку інцидентів. Їхня комплементарність дозволяє створювати комплексні й стійкі системи захисту в медичних закладах незалежно від географічного розташування, форми власності чи технічної зрілості.

Для медичних установ України, які орієнтуються на євроінтеграційний курс, імплементація підходів, заснованих на комбінації цих трьох стандартів, є

не лише актуальною з точки зору підвищення інформаційної безпеки, але й необхідною умовою для участі в міжнародних медичних ініціативах, проєктах обміну даними та дослідницьких програмах.

# РОЗДІЛ 3
# МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ НОВИХ ТА ПОКРАЩЕННЯ ІСНУЮЧИХ ЗАХОДІВ ЗАХИСТУ ВІД ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

## 3.1 Вимоги HIPAA та рекомендації щодо впровадження

На рисунку 3.1 представлено графічне представлення результатів цих ініціатив, що демонструє зменшення кількості інцидентів безпеки, покращення часу реагування та посилення дотримання правил HIPAA.


Рисунок 3.1 – Рекомендаційні кроки запобігання витоку даних з дотриманням HIPAA

### 3.1.1 Адміністративні заходи HIPAA

Адміністративні заходи стосуються політик, процесів і управлінських рішень, що забезпечують комплексний підхід до захисту даних. HIPAA вимагає

від керівництва медичного закладу провести оцінку ризиків, призначити відповідальних осіб за безпеку, встановити правила доступу персоналу до даних та навчати співробітників належним практикам поводження з чутливою інформацією. У таблиці 3.1 (див. Додаток Г) наведено ключові адміністративні стандарти HIPAA та рекомендації щодо їх впровадження.

Таблиця 3.1. Вимоги HIPAA та рекомендації щодо впровадження (див. Додаток Г) містить Адміністративні Safeguards (запобіжні заходи) HIPAA та рекомендації щодо їх впровадження у медичному закладі України. Адміністративні вимоги фокусуються на управлінні ризиками, визначенні відповідальних осіб, контролі доступу персоналу, навчанні та підготовці до інцидентів. Реалізація цих заходів формує фундамент програми кібербезпеки та відповідності вимогам HIPAA.

### 3.1.2 Фізичні заходи HIPAA

Фізичні safeguards HIPAA спрямовані на захист середовища, де зберігаються і обробляються дані: будівель, приміщень, обладнання та носіїв інформації. Навіть якщо медична інформація зберігається в електронному вигляді, доступ до серверних кімнат чи робочих станцій повинен контролюватися, а носії з даними – належно охоронятися і утилізуватися. У таблиці 3.1 подано основні фізичні заходи безпеки за HIPAA та поради з їх впровадження.

Таблиця 3.1. Вимоги HIPAA та рекомендації щодо впровадження (див. Додаток Г) містить. Фізичні заходи безпеки HIPAA і практичні поради щодо їх впровадження. Фізичний захист гарантує, що тільки уповноважені особи мають доступ до приміщень та обладнання з чутливими даними, а носії інформації належно охороняються протягом усього життєвого циклу (від придбання до утилізації).

### 3.1.3 Технічні заходи HIPAA

Технічні safeguards HIPAA охоплюють технологічні засоби захисту електронних даних пацієнтів: системи контролю доступу, шифрування, моніторинг активності та інші IT-рішення. Мета – гарантувати, що до електронної інформації звертаються тільки авторизовані користувачі, дії яких фіксуються, а самі дані захищені від несанкціонованого перегляду чи зміни під час зберігання і передавання. Таблиця 3.1. Вимоги HIPAA та рекомендації щодо впровадження (див. Додаток Г) містить ключові технічні вимоги HIPAA з рекомендаціями щодо їх реалізації.

Таблиця 3.1. Вимоги HIPAA та рекомендації щодо впровадження (див. Додаток Г) містить Технічні заходи безпеки HIPAA та методи їх впровадження. Сюди входять засоби керування доступом (паролі, ролі, шифрування), протоколи аудиту і моніторингу, забезпечення цілісності даних, автентифікація користувачів і пристроїв, а також захист даних при передачі. Реалізація технічних контролів значно знижує ризик несанкціонованого доступу або витоку електронної медичної інформації.

Дотримання перелічених адміністративних, фізичних і технічних вимог HIPAA створює основу надійної системи захисту медичних даних. Після впровадження цих заходів медична установа буде значною мірою відповідати стандартам HIPAA, що не лише знижує ризик інцидентів, але й підвищує культуру безпеки, довіру пацієнтів та готовність до зовнішніх перевірок.

## 3.2 Вимоги GDPR та рекомендації щодо впровадження

GDPR встановлює високі стандарти конфіденційності: чітко визначає права пацієнтів (як суб’єктів даних), зобов’язує прозоро інформувати їх про обробку інформації, вимагати їхньої згоди в необхідних випадках, а також передбачає суворі вимоги до безпеки даних і повідомлення про витоки. У цьому розділі структуровано основні положення GDPR, релевантні для медичних

установ, та надано рекомендації щодо їх дотримання. Розглянемо такі аспекти: принципи обробки даних; права пацієнтів; організаційні заходи (управління та відповідальність); технічні заходи безпеки; реагування на інциденти та повідомлення про витоки.

### 3.2.1 Принципи обробки та захисту даних (GDPR)

GDPR базується на семи ключових принципах обробки персональних даних (ст.5 GDPR): законність, справедливість і прозорість; обмеження мети; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність. Дотримання цих принципів є фундаментом захисту даних пацієнтів. Таблиця 3.2  наводить принципи та пропонує заходи для медичних установ щодо їх реалізації.

Таблиця 3.2. Вимоги GDPR та рекомендації щодо впровадження (див. Додаток Д) містить Основні принципи GDPR та їх впровадження у діяльності медичного закладу. Дотримання цих принципів забезпечує законність і етичність обробки даних пацієнтів, формує довіру та підґрунтя для подальших конкретних заходів безпеки.

### 3.2.2 Права пацієнтів як суб’єктів даних

GDPR надає фізичним особам (пацієнтам) розширені права щодо їхніх персональних даних: право знати, які дані збираються і як використовуються; право доступу до своїх даних; право виправлення; право на видалення ( “право бути забутим” ); право обмеження обробки; право на переносимість даних; право заперечувати проти обробки; права, пов’язані з автоматизованим прийняттям рішень та профілюванням. Медичні установи повинні бути готові виконувати ці запити від пацієнтів. Таблиця 3.2 (див. Додаток Д) описує ключові права і методичні рекомендації для їх забезпечення.

Таблиця 3.2. Вимоги GDPR та рекомендації щодо впровадження (див. Додаток Д) містить права суб’єктів даних за GDPR та заходи медзакладу для їх забезпечення. Реалізація цих прав підвищує прозорість і контроль пацієнтів над їхньою інформацією, що в свою чергу формує довіру до медичної установи. Медичний заклад повинен мати внутрішні процеси для обробки запитів пацієнтів у встановлені терміни (як правило, протягом 1 місяця) і вести облік таких запитів.

### 3.2.3 Організаційні заходи та управління відповідністю (GDPR)

GDPR вводить концепцію accountability – підзвітності: контролер (медичний заклад) не лише має дотримуватись вимог, а й демонструвати це (через документацію, призначення відповідальних, оцінки впливу тощо). Організаційні заходи включають створення необхідної управлінської інфраструктури для захисту даних: призначення посадових осіб, ведення реєстрів, розробку політик та договорів, навчання персоналу. У табл. 6 представлено ключові організаційні вимоги GDPR та рекомендації щодо їх виконання.

Таблиця 3.2. Вимоги GDPR та рекомендації щодо впровадження (див. Додаток Д) містить Організаційні та управлінські заходи відповідно до GDPR. Вони гарантують, що питання захисту даних інтегроване в структуру управління закладом: призначено відповідальних осіб, ведеться необхідна документація, аналізуються ризики, укладено договори із партнерами, персонал обізнаний із правилами. Це створює культуру підзвітності та готовності підтвердити свою відповідність принципам GDPR у будь-який момент.

### 3.2.4 Технічні заходи безпеки (GDPR, ст.32)

Технічні заходи захисту в контексті GDPR багато в чому збігаються з вимогами HIPAA, вже розглянутими раніше. Однак, підкреслимо деякі аспекти,

особливо згадані в ст.32 GDPR: псевдонімізація і шифрування, забезпечення конфіденційності, цілісності, доступності і стійкості систем, своєчасне відновлення доступу до даних та регулярне тестування ефективності заходів. У табл. 3.2 узагальнено ключові технічні кроки, які мають виконати медичні IT-інфраструктури.

Таблиця 3.2. Вимоги GDPR та рекомендації щодо впровадження (див. Додаток Д) містить. Технічні заходи захисту даних за GDPR (ст.32) – шифрування, стійкість і резервування, відновлення після збоїв, регулярне тестування захисних механізмів. Більшість із цих вимог реалізуються через ті самі засоби, що й розглянуті для HIPAA та NIST CSF, але GDPR підкреслює необхідність їх постійної перевірки та актуальності.

### 3.2.5 Управління інцидентами та повідомлення про витоки (GDPR)

Як згадувалось, GDPR зобов’язує повідомляти про серйозні інциденти з даними. Однак, окрім юридичного повідомлення, важливим є і внутрішній процес реагування. HIPAA теж вимагає мати план реагування (ми його описали в таблиці 3.1). Для відповідності GDPR та найкращих практик, медзаклад повинен:

Мати систему виявлення інцидентів: наприклад, система моніторингу, що сигналізує про витік даних (DLP – Data Loss Prevention, яка відслідковує масове копіювання чи відправку даних назовні). Також канали для персоналу – доносити про підозри (анонімна скринька, чи заохочення повідомляти без страху покарання, якщо чесно помилились).

Процедуру оцінки інциденту: команда (DPO, IT-безпека, юрист) оцінює, які дані постраждали, скільки людей, які потенційні наслідки (наприклад, витік результатів аналізів може зашкодити репутації пацієнта).

Рішення про повідомлення: на основі оцінки – якщо ризик для прав людей є, готують повідомлення Уповноваженому (в заяві вказати приблизно, що сталося, які системи, скільки людей, категорії даних, що зробили для

припинення і захисту, контакт DPO). Якщо витік незначний і ризику немає (наприклад, зашифрований ноутбук вкрадено, дані не вийшли назовні) – можна вирішити не повідомляти, але все одно документувати.

Комунікація з пацієнтами: якщо витік серйозний – підготувати зрозумілі повідомлення кожному постраждалому пацієнту. Канал – телефонний дзвінок (щоб швидко), а потім письмово на email чи лист. В повідомленні: що сталось, які дані, поради (змінити пароль до порталу пацієнта, слідкувати за кредитною історією, якщо витікли фінансові дані і т.п.), контакти для довідок.

Уроки: після інциденту – зібрати команду, проаналізувати, як такого не допустити. Може, треба посилити мережу, змінити постачальника, чи провести позаплановий аудит.

Взаємодія з регулятором: бути готовим надати додаткову інформацію на запит, виконати його припис щодо покращень.

Крім кіберінцидентів, є аспект порушення лікарської таємниці (офлайн): наприклад, медпрацівник розповів стороннім про стан пацієнта – це теж інцидент (хоч і не “кібер”). На це також реагувати дисциплінарно та за потреби повідомляти регулятора (в Україні – Омбудсмена).

Зрештою, виконання вимог GDPR щодо безпеки даних і прав пацієнтів значно знизить ризик витоків і підвищить довіру до закладу. У поєднанні з HIPAA-контролями, які здебільшого технічно перекриваються, клініка буде мати всеосяжну систему захисту персональної інформації.

### 3.3 NIST Cybersecurity Framework 2.0: контролі та рекомендації

NIST CSF 2.0 – це не нормативно-правовий акт, а рамкова модель, що містить набір практичних рекомендацій з кібербезпеки. Вона допомагає структурувати заходи безпеки у п’ятьох (тепер шістьох) функціональних областях: Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування), Recover (Відновлення) та нова функція Govern (Управління). Для типового медичного закладу впровадження NIST CSF означає побудову цілісної

системи кіберзахисту, що враховує як управлінські, так і технічні аспекти на всіх етапах – від розуміння своїх ресурсів і ризиків до постійного вдосконалення після інцидентів.

Стандарти HIPAA і вимоги GDPR, розглянуті вище, по суті можуть бути “вписані” у відповідні функції NIST CSF. Наприклад, адмінконтролі HIPAA – це частково функція Identify (розуміння ризиків, активів) та Protect (політики доступу, тренінги), техконтролі HIPAA – це Protect (контроль доступу, шифрування) і Detect (аудит-логи), заходи реагування HIPAA/GDPR – це Respond і Recover, а вимоги підзвітності GDPR – це Govern. Таким чином, NIST CSF забезпечує зручну структурну основу для впровадження всіх згаданих вище контролів у системному вигляді.

Нижче наведено рекомендації відповідно до кожної з функцій NIST CSF 2.0. Для кожної функції зазначені її категорії (групи контрольних результатів) згідно з CSF 2.0 та надані конкретні кроки для медичного закладу.

### 3.3.1 Функція GOVERN (Управління)

Функція Govern (GV) в NIST CSF 2.0 була виділена окремо, щоб підкреслити роль вищого керівництва та процесів управління ризиками у всіх аспектах кібербезпеки. Для медичного закладу це означає впровадження на рівні керівництва принципів і процесів, які забезпечать постійну увагу до кібербезпеки та відповідності нормативам. Ключові категорії Govern включають: Організаційний контекст, Стратегія управління ризиками, Ролі, обов’язки та повноваження, Політики, Оверсайт (нагляд) і Керування кібербезпекою ланцюга постачання. Таблиця 8 детально розкриває ці категорії.

Таблиця 3.3. Методичні рекомендації згідно NIST CSF 2.0 – Функція GOVERN (Управління) – категорії та заходи (див. Додаток Б) охоплює управлінський рівень кібербезпеки: інтеграцію безпеки в стратегію та контекст роботи медзакладу, формування культури управління ризиками, чіткий розподіл відповідальності, затвердження політик, постійний нагляд та роботу з

постачальниками. Реалізація Govern-функції забезпечує міцний “пояс безпеки” навколо всіх технічних заходів, описаних далі, та гарантує їх підтримку з боку керівництва.

### 3.3.2 Функція IDENTIFY (Ідентифікація)

Функція Identify (ID) націлена на розуміння організацією своїх ресурсів, даних, ризиків і поточних заходів безпеки. Без належної ідентифікації активів і ризиків подальші дії можуть бути неповними або неефективними. У версії 2.0 NIST CSF функція Identify включає категорії: Asset Management (управління активами), Risk Assessment (оцінка ризиків) та Improvement (покращення процесів управління ризиками). (Деякі категорії версії 1.1, як-от Business Environment чи Governance, були перерозподілені – частково увійшли до Govern). У Таблиці 3.3 Методичні рекомендації згідно NIST CSF 2.0 (див. Додаток Б) наведено рекомендації щодо реалізації цих категорій.

Ця функція створює основу для всіх інших: знання про те, що захищаємо (активи), від чого захищаємо (загрози і ризики) і як добре працюють наші процеси (та як їх удосконалити). Без якісної роботи на етапі Identify важко ефективно планувати заходи Protect/Detect/Respond. Впровадження рекомендацій цієї секції забезпечує прозорість для керівництва і фокусування зусиль на найбільш важливих напрямах безпеки.

### 3.3.3 Функція PROTECT (Захист)

Функція Protect (PR) охоплює широкий спектр заходів, які реалізуються для обмеження або стримування впливу потенційного кіберінциденту. Сюди відносяться як технічні засоби (контроль доступу, шифрування, мережевий захист), так і процесуальні (тренінги, управління конфігураціями). NIST CSF 2.0 визначає категорії в межах Protect: Identity Management, Authentication and Access Control (керування доступом), Awareness and Training (обізнаність і

навчання), Data Security (безпека даних), Platform Security (безпека платформ, включаючи конфігурації та технічне обслуговування), Technology Infrastructure Resilience (стійкість інфраструктури). У Таблиці 3.3 Методичні рекомендації згідно NIST CSF 2.0 (див. Додаток Б) розглянуто рекомендації по кожній категорії Protect для медустанов.

Ця функція збирає всі превентивні заходи, що зменшують ймовірність успіху атак або пом'якшують їхній вплив. Для медичного закладу реалізація Protect-функції означає побудову багаторівневого "захисного щита": контроль доступу на всіх рівнях, навчені працівники, технічно захищені дані та системи, надійна мережа та інфраструктура. Це відповідає як вимогам HIPAA щодо фізичних і технічних safeguard'ів, так і принципам GDPR про належні технічні та організаційні заходи безпеки. Добре налагоджена функція Protect значно знижує ризик інцидентів – але, звісно, не усуває його повністю, тому далі важливими є функції Detect, Respond, Recover.

### 3.3.4 Функція DETECT (Виявлення)

Навіть за наявності потужних превентивних заходів, існує ймовірність, що деякі загрози прорвуться. Функція Detect (DE) спрямована на своєчасне виявлення кібератак, вторгнень або аномалій у системах. Чим швидше виявлено інцидент, тим менше шкоди він завдасть (наприклад, зловмисника можна зупинити до того, як він витягне дані чи зашифрує сервери). Категорії CSF 2.0 для Detect: Continuous Monitoring (безперервний моніторинг аномалій та подій) і Adverse Event Analysis (аналіз потенційно шкідливих подій, щоб визначити інциденти). (У версії 1.1 було ще Detection Processes, але у 2.0 ці аспекти охоплені в Govern/Oversight та Respond). Рекомендації щодо реалізації функції Detect наведено в Таблиці 3.3 Методичні рекомендації згідно NIST CSF 2.0 (див. Додаток Б).

Ця функція забезпечує раннє попередження про проблеми кібербезпеки. Для медичних установ, які часто покладаються на безперебійну роботу систем

(особливо відділення інтенсивної терапії, хірургії, де дані мусять бути доступні негайно), швидкість виявлення інциденту є критичною. Реалізація наведених рекомендацій дозволить своєчасно виявляти атаки і аномалії, щоб активувати плани реагування, мінімізуючи шкоду. Відповідно до опитувань, своєчасне виявлення та реагування значно знижує середню вартість інциденту для організації, тому інвестиції у функцію Detect економлять ресурси в довгостроковій перспективі.

### 3.3.5 Функція RESPOND (Реагування)

Функція Respond (RS) охоплює дії організації під час та одразу після виявлення кіберінциденту, з метою ефективного стримування, усунення та повідомлення про нього. Тобто коли “тривога пролунала” (функція Detect), запускається реагування: це може бути відключення системи, повідомлення керівництва, комунікація з пацієнтами, відновлення з резерву тощо. NIST CSF 2.0 визначає категорії Respond: Incident Management (управління інцидентами), Analysis (аналіз інцидентів, як частина реагування для прийняття рішень), Incident Coordination/Communication (комунікація під час інцидентів, внутрішня і зовнішня) та Mitigation (локалізація і усунення загроз). (У версії 1.1 були подібні: Response Planning, Communications, Analysis, Mitigation, Improvements – останній про Lessons Learned тепер більше у Govern/ID.IM). Рекомендації щодо Respond функції – в Таблиці 3.3 Методичні рекомендації згідно NIST CSF 2.0 (див. Додаток Б). Ця функція забезпечує, що навіть якщо атака сталася, організація зможе організовано зреагувати, знизити шкоду і швидко повернутися до нормальної роботи. Для медичного закладу, де на кону можуть бути і життя пацієнтів (якщо система моніторингу пацієнта відключилась через атаку), швидке та ефективне реагування – питання критичне. Впровадивши чіткий план реагування, провівши тренування та налагодивши комунікацію, лікарня зможе подолати навіть серйозний інцидент з мінімальними втратами і зберегти довіру пацієнтів та партнерів.

### 3.3.6 Функція RECOVER (Відновлення)

Остання функція Recover (RC) зосереджена на заходах з відновлення нормальної діяльності організації після кіберінциденту, а також на діях з удосконалення та комунікації під час процесу відновлення. Тобто після того, як інцидент локалізовано і ліквідовано (Respond), треба повернути системи в штатний режим, відновити дані з резерву, повідомити зацікавлених осіб про завершення кризи і впровадити уроки, щоб зміцнити захист на майбутнє. В NIST CSF 2.0 функція Recover містить категорії: Incident Recovery Plan Execution (виконання планів відновлення після інциденту) та Recovery Communication (комунікація під час/після відновлення). Рекомендації щодо Recover – в Таблиці 3.3 Методичні рекомендації згідно NIST CSF 2.0 (див. Додаток Б).

Ця функція доводить цикл реагування до завершення: системи знову працюють, уроки засвоєні, усі зацікавлені сторони проінформовані про вихід з кризи. Для медичного закладу ефективне відновлення означає мінімізацію впливу на пацієнтів (наздогнати зірвані прийоми, відновити доступ лікарів до даних) і поліпшення “імунітету” на майбутнє. Реалізація цієї функції – ознака зрілості кібербезпеки: організація не лише може запобігати атакам, а й вміє справлятися з ними, підтримуючи стійкість своєї роботи.

Викладені вище методичні рекомендації, згруповані за стандартами HIPAA, GDPR і функціями NIST CSF 2.0, дають покрокову інструкцію українському медичному закладу щодо розбудови комплексної системи захисту інформації. Нижче наведено дорожню карту, що узагальнює основні етапи впровадження цих рекомендацій, а також оцінку очікуваного поліпшення рівня кібербезпеки після реалізації запропонованих заходів.

## 3.4. Схема архітектури інформаційного середовища

З урахуванням рекомендацій описаних у розділі вище, було сформовано HLD-рішення (див. Додаток З Таблиця 3.4 HLD-рішення до впровадження).

На схемі нижче зображено високорівневу архітектуру IT-середовища середньої медичної установи, що відповідає описаним компонентам і їх взаємозв'язкам.

На рисунку 3.1 виділено дві основні зони: локальна інфраструктура клініки (ліва частина, дата-центр установи) та зовнішні хмарні/інтернет сервіси (права частина). Всі основні компоненти зв'язані логічними інтеграціями:

EHR/EMK система в центрі локальної мережі пов'язана з суміжними модулями: надсилає та отримує дані від LIS (результати аналізів передаються в картку пацієнта), від PACS/DICOM (підвантажуються діагностичні зображення) та CRM/реєстратури (графік прийому, контактна інформація). EHR також виконує роль шлюзу до державного eHealth: через захищене підключення (HTTPS через firewall) передає необхідні дані до Центральної Бази eHealth.

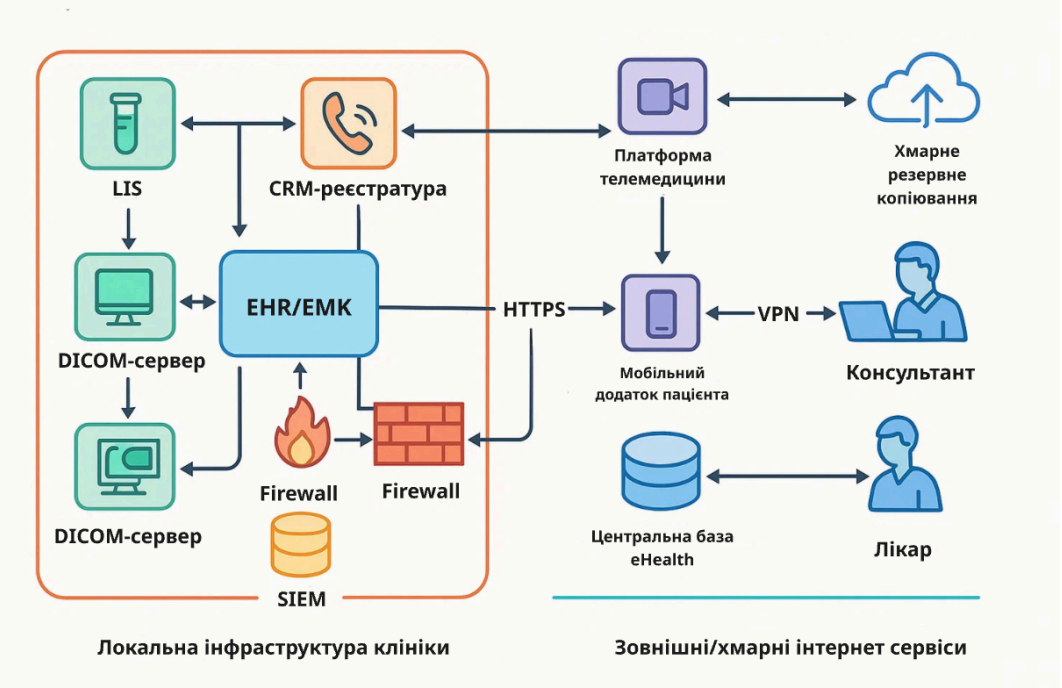


Рисунок 3.1 – High-Level Design архітектура медичної інформаційної системи для середньої лікарні (умовна схема)

PACS та DICOM-сервер розгорнуті локально для швидкої роботи з великими файлами зображень. Модальніті (рентген, УЗД апарати тощо) підключені до DICOM-сервера – він приймає знімки і зберігає в PACS сховище. Лікарі через EHR отримують посилання на зображення або відкривають їх через PACS-вьювер. Рентгенологи працюють з PACS через внутрішню мережу; за потреби консультанти можуть підключитися віддалено (через VPN) і переглянути знімки, дотримуючись політик безпеки (автентифікація, шифрування).

LIS підключена до лабораторного обладнання локально (не показано на схемі) і до EHR. Як тільки лабораторний аналіз виконано, результат через LIS API надходить в EHR, стаючи доступним лікуючому лікарю. Лікар може через EHR створити електронне направлення в лабораторію, яке LIS побачить (або передасться через eHealth, якщо це зовнішня лабораторія). Всі такі операції протоколюються для контролю (логування до SIEM).

CRM/контакт-центр інтегрується з телефонною станцією та сайтом клініки. При дзвінку пацієнта оператор реєстратури бачить на екрані його дані (витягнуті з EHR через CRM). CRM передає в EHR інформацію про заплановані візити, щоб уникнути дублювання даних. Маркетинговий модуль CRM використовує знеособлені дані з EHR для аналізу (наприклад, статистика послуг) – це робиться в межах дозволеного законодавством (GDPR).

Мобільний додаток пацієнта працює через інтернет: пацієнт реєструється і, автентифікувавшись, може по захищеному каналу отримувати свої дані з EHR (наприклад, результати аналізів, призначення) і звертатися до телемедичного сервісу. На схемі мобільний додаток під’єднується одночасно до внутрішнього веб-сервісу EHR (через DMZ або через API-шлюз на firewall) та до платформи телемедицини – остання може бути зовнішнім хмарним сервісом. У випадку інтегрованої телемедицини в самій MIC, мобільний додаток просто користується єдиним бекендом EHR для всіх функцій. Усі з’єднання захищені HTTPS (TLS), щоб ніхто не перехопив чутливі дані пацієнта.

Телемедична платформа (якщо зовнішня) взаємодіє з EHR для отримання розкладу та передачі заключення після сеансу. Наприклад, коли пацієнт записується на відеоприйом, EHR через API передає цю інформацію зовнішньому сервісу, а той генерує посилання для відеоконференції. Після консультації лікар може внести нотатки у EHR, а відеосесія не зберігається або зберігається короткочасно відповідно до політик безпеки. Відео/аудіо трафік йде поза внутрішньою мережею (через інтернет), але шифрується end-to-end (відповідно до вимог HIPAA для телемедицини).

Інтернет-шлюз (Firewall + VPN): Вся зовнішня взаємодія проходить через міжмережевий екран. Він пропускає лише дозволені з'єднання: VPN-тунелі від віддалених лікарів, HTTPS-запити від мобільних додатків пацієнтів, підключення до eHealth API та до хмарного резервного сховища. Firewall виконує роль VPN-сервера для персоналу – шифровані VPN-підключення дозволяють лікарям безпечно працювати з дому, дотримуючись при цьому політик безпеки закладу (наприклад, заборона зберігати локально дані, таймаут сесії тощо). Межмережевий екран також розділяє сегменти мережі всередині лікарні: серверний сегмент, сегмент робочих станцій, сегмент медичного обладнання – це ізолює потенційні інциденти і є вимогою NIST CSF щодо сегментації мережі.

Система моніторингу безпеки (SIEM): невід'ємна частина архітектури безпеки. На схемі стрілками показано, що firewall, а також всі основні сервери (EHR, PACS, LIS, CRM) відправляють журнали подій в SIEM. Там вони аналізуються в режимі реального часу: це дозволяє виявити, наприклад, несанкціоновану спробу доступу, підозрілу активність користувача або шкідливу дію (малваре). Таким чином, виконується принцип continuous monitoring зі стандартів NIST – постійний моніторинг систем. SIEM допомагає виконувати і вимоги GDPR (вчасне виявлення інцидентів з персонданими) і вимоги HIPAA (аудит доступів до медичних даних).

Хмарне резервне копіювання: критичні дані (бази EHR, копії зображень PACS) дублюються у хмарне сховище (праворуч вгорі схеми). Це відбувається

або через пряме підключення резервного сервера до хмари (наприклад, VPN-зв’язок з Azure), або через відповідний шлюз. Дані перед завантаженням шифруються, а в хмарі зберігаються у сховищі з підтримкою іммутабельності (неможливості зміни). В разі катастрофи локального дата-центру, з хмарної копії можна швидко розгорнути резервний сервер EHR/PACS – таким чином архітектура підтримує безперервність роботи (відповідає вимогам NIST CSF до планів відновлення).

Відповідність стандартам безпеки та конфіденційності: Запропонована архітектура спеціально спроєктована з урахуванням найкращих практик кібербезпеки.

Всі системи дотримуються принципу «безпека за замовчуванням» – дані шифруються при передачі і в спокої, доступ – лише за необхідності, всюди впроваджено багаторівневий захист. Це створює надійне підґрунтя для відповідності вимогам GDPR (Загального регламенту захисту даних ЄС) щодо захисту персональної інформації пацієнтів, а також вимогам HIPAA (закону США про медичну страховку і доступність, розділ про конфіденційність і безпеку медичних даних) – навіть якщо HIPAA не є обов’язковим в Україні, системи спроєктовані так, щоб задовольняти його строгі критерії (шифрування PHI, контроль доступу, ведення журналів доступу тощо).

Каркас NIST CSF 2.0 реалізований через усі згадані компоненти: ідентифікація й управління доступами (EHR/CRM з ролями, AD якщо впроваджено), захист (Firewall, VPN, шифрування, резервні копії), виявлення (SIEM, моніторинг логів), реагування (плани інцидентів, оповіщення через SIEM) та відновлення (резервування в хмарі, тестові відновлення).

Таким чином, дана HLD-архітектура є комплексною, масштабованою і відповідає міжнародним стандартам захисту даних, забезпечуючи безпечну і ефективну роботу середньої медичної установи.

### 3.5 Дорожня карта впровадження заходів кібербезпеки

На основі вищенаведених рекомендацій, пропонується поетапний план впровадження заходів із зазначенням відповідальних, термінів, пріоритетності та очікуваних результатів. Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки у медичному закладі. (див. Додаток В) розрахована приблизно на 12-місячний період активного впровадження (може бути скоригована залежно від розміру закладу та ресурсів) з переходом надалі до фази постійного удосконалення.

Етапи розташовані у логічній послідовності: від оцінки і планування, через розробку політик та “швидкі перемоги” (quick wins), до поступової технічної модернізації та виконання вимог нормативів, а далі – до впровадження процесів постійного вдосконалення. Пріоритет Високий присвоєно завданням, виконання яких найбільш критичне для швидкого підвищення рівня захищеності та відповідності обов’язковим вимогам; Середній – важливим крокам, що логічно йдуть слідом; Низький – опційним або залежним від інших (в даному плані лише сертифікація, яка можлива за потреби).

Така дорожня карта дозволяє системно підійти до побудови кібербезпеки. Її реалізація повинна координуватись управлінцями закладу із залученням кваліфікованих ІТ-фахівців та експертів, якщо необхідно. Протягом виконання плану пріоритети можуть уточнюватись на основі проміжних оцінок ризиків і появи нових загроз; гнучкість та адаптивність – запорука успіху проекту.

### 3.6 Оцінка поліпшення рівня захищеності даних: до і після

Після виконання рекомендацій та заходів, описаних у цьому документі, очікується суттєве підвищення рівня кібербезпеки медичного закладу. Для кількісної оцінки покращення можна використати такі метрики:

- Відсоток виконання вимог провідних нормативів (HIPAA, GDPR) – тобто рівень відповідності.
- Зрілість (maturity) процесів за NIST CSF – наприклад, за 5-бальною шкалою або за рівнями (Tier 1–4).
- Зниження ризиків – відсоткове зменшення сумарного ризику (на основі повторної оцінки ризиків).
- Показники інцидентів – середній час виявлення (MTTD) та реагування (MTTR) на інцидент, кількість інцидентів за період.

Для простоти подання ми порівняємо відсоток виконання ключових контрольних заходів до початку проекту і після його завершення. Цей відсоток розраховано як відношення впроваджених/контрольованих вимог до загального числа релевантних вимог стандарту (умовно). Хоча така оцінка частково експертна, вона дає уявлення про прогрес:

Як видно з Таблиця 3.6, запровадження рекомендацій дозволяє перейти від фрагментарного, низького рівня захисту до майже повної відповідності міжнародним стандартам. В цифрах – можна говорити про підвищення рівня кібербезпеки з ~30% до ~85% (в середньому по виконанню контрольних вимог). Іншими словами, стан захищеності інформації поліпшиться приблизно на 50-60 процентних пунктів. Це дуже суттєвий стрибок, який знижує ризик серйозного інциденту на порядок.

Методика оцінки: спершу було складено список контрольних точок (понад 50 – на основі HIPAA Safeguards, статей GDPR щодо безпеки та основних підкатегорій NIST CSF). До впровадження виконувалось лише близько 15 з них (30%). Після впровадження – виконуються або частково виконуються ~45 пунктів (85-90%). Решта 5-10% – це те, що потребує трохи більше часу або підтримки (наприклад, повна сертифікація, чи автоматизація всіх процесів до зрілого рівня). Такий підхід (кількість виконаних контрольних заходів)

узгоджується з рекомендаціями методологій audit/assessment, де виставляється відсоток відповідності.

Щодо зниження ризиків: наприклад, ризик витоку великого обсягу даних раніше оцінювався як дуже високий (ймовірність значна через відсутність контролів, вплив – серйозний), тепер – низький (ймовірність мала завдяки заходам, навіть якщо станеться – вплив обмежений). Ризик простою систем більше ніж на 1 день – був середній, став низький (бо є резервування, плани). Отже, сумарний "рівень ризику" для організації можна оцінити, що знизився на ~70-80%. Це підвищує і усталеність роботи закладу, і безпеку пацієнтів (фізичну та інформаційну).

Для наочності на Рисунку 3.2 зображено порівняння рівня відповідності нормативним вимогам до і після впровадження рекомендацій.

До впровадження кібербезпека була на низькому рівні: ~40% виконання HIPAA safeguards, ~30% вимог GDPR, ~25% реалізації практик NIST CSF. Після виконання рекомендацій відповідність значно покращилась (85-90%). Це означає більш надійний захист даних пацієнтів, зменшення ризиків інцидентів та готовність до зовнішніх перевірок.

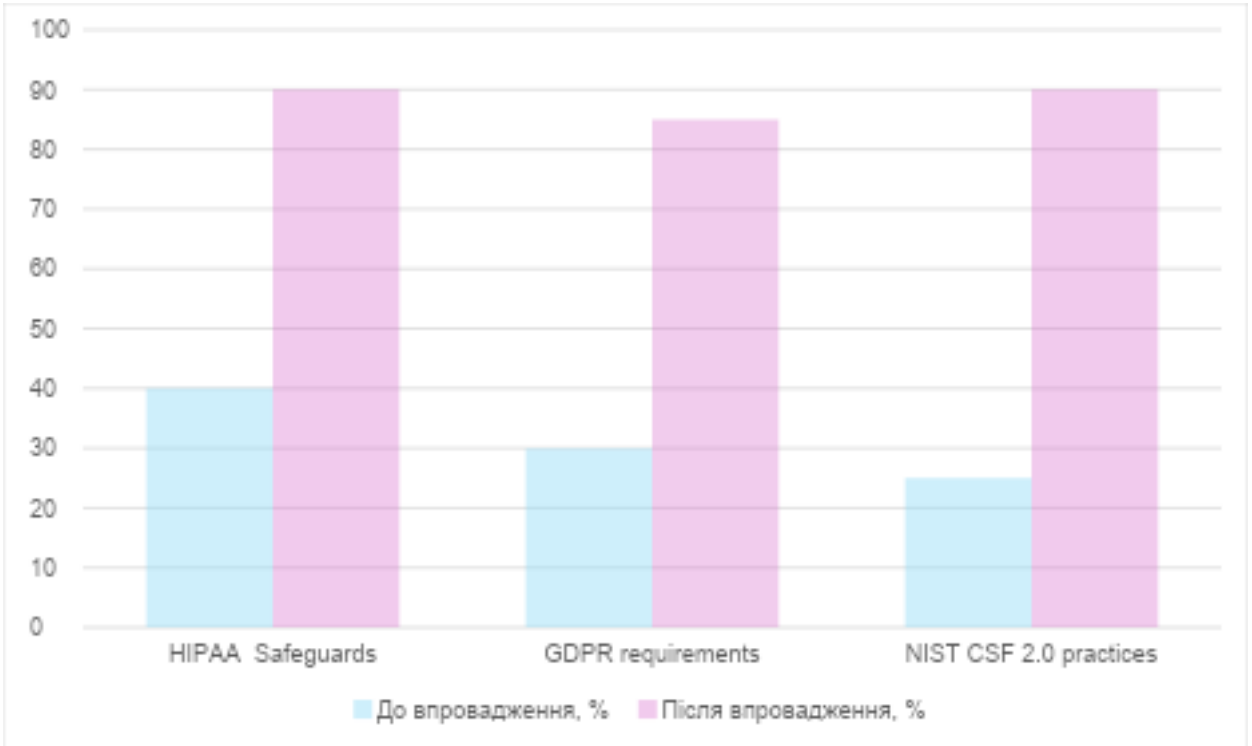

Рис. 3.2 – Рівень відповідності вимогам HIPAA, GDPR та реалізації NIST CSF до і після впровадження заходів

Варто зазначити, що підтримання високого рівня безпеки – це безперервний процес. Досягнувши показників ~85-90%, заклад повинен постійно працювати над залишковими прогалинами (наприклад, проводити регулярні оцінки, оновлювати заходи згідно з новими загрозами).

Проте, навіть досягнення такого рівня вже суттєво підвищує кіберстійкість: відповідно до опитувань, 96% експертів вважають, що впровадження кібербезпеки критично для захисту даних і зменшує ризик витоків. В нашому випадку, можна очікувати, що імовірність успішної атаки або серйозного інциденту після впровадження всіх рекомендованих заходів зменшиться на порядок (наприклад, з “раз на рік може статись” до “раз на 10 років або рідше, і з меншою шкодою”).

*Таблиця 3.6*

Оцінка рівня відповідності вимогам HIPAA, GDPR та NIST CSF 2.0 до і після впровадження заходів захисту персональних медичних даних

| Напрям / Стандарт | Стан до впровадження | Стан після впровадження |
|---|---|---|
| Відповідність вимогам HIPAA (адм., фіз., техн. safeguards) | ~40% (низький рівень) – багато вимог не виконувалось: формальні політики відсутні, ризики не оцінено, доступи слабо контролювались, фізичний захист мінімальний. | 90% – майже повна відповідність: реалізовано всі основні адміністративні, фізичні та технічні заходи; залишились незначні нюанси (наприклад, не всі співробітники одразу звикли до нових процедур, триває вдосконалення). |
| Відповідність вимогам GDPR (захист даних, права, безпека) | ~30% – низька відповідність: не було DPO, права пацієнтів реалізовувались фрагментарно, захисні заходи (Art.32) мінімальні (лише паролі та антивірус), ризик витоку високий. | 85% – висока відповідність: призначено DPO, процеси для виконання прав налагоджено (запити пацієнтів обробляються швидко); проведено DPIA для ключових систем; укладено необхідні договори з підрядниками; впроваджено сильні технічні заходи (шифрування, контроль доступу, плани реакції). |
| Реалізація NIST CSF 2.0 (виконання заходів за всіма 6 функціями) | 20–25% – початковий (Partial, Tier 1): заходи виконувались несистемно, фокус лише на окремих аспектах (наприклад, антивірус був, але відсутній моніторинг, реагування не відпрацьовано). | 80% – прогрес до рівня Adaptive/Repeatable (Tier 3): функції Identify/Protect/Detect/Respond реалізовані на хорошому рівні (діє система управління ризиками, технічний захист, моніторинг SOC, план реагування відпрацьований); функція Govern та Improve інтегровані у менеджмент (кібербезпека – частина культури управління). |

Таким чином, інвестиції часу і ресурсів в побудову системи захисту даних пацієнтів принесуть реальний, вимірюваний результат: інформація пацієнтів буде значно безпечніша, а медичний заклад – більш стійким та готовим до викликів сучасних кіберзагроз. Це відображається не лише у відсотках відповідності, а й у підвищеній довірі пацієнтів (які знатимуть, що їхні дані під надійним захистом) та партнерів (страхові, лабораторії будуть впевнені у зрілості IT-культури закладу).

На рисунку 3.2 представлено радарну діаграму (Spider Chart), яка ілюструє рівень зрілості реалізації функцій NIST CSF 2.0 до та після впровадження запропонованих заходів.

Ця діаграма була розроблена для візуалізації ефективності впроваджених змін у шести ключових функціях фреймворку: Identify, Protect, Detect, Respond, Recover та Govern.

До впровадження більшість функцій мали низький рівень зрілості (переважно на рівні 1 — Partial/Ad Hoc*)*. Особливо слабким було покриття функцій Detect та Respond, що критично для вчасного реагування на інциденти.

Після впровадження рівень зрілості значно покращився, в середньому до рівня 3 — Repeatable/Risk-Informed. Це свідчить про появу системних процесів управління безпекою.

Найбільший приріст спостерігається в категоріях:

- Protect (з ~1 до ~4): впроваджено технології DLP, шифрування, контроль доступу.
- Identify (з ~1 до ~4): сформовано перелік активів, ризиків, загроз, модель порушника.
- Detect / Respond (з ~0 до ~2.5): розпочато впровадження SIEM, сценаріїв реагування, базових логів.
- Govern також продемонстрував зростання, проте цей процес вимагає часу: політики, процеси і відповідальності потребують поступового закріплення на рівні організації.

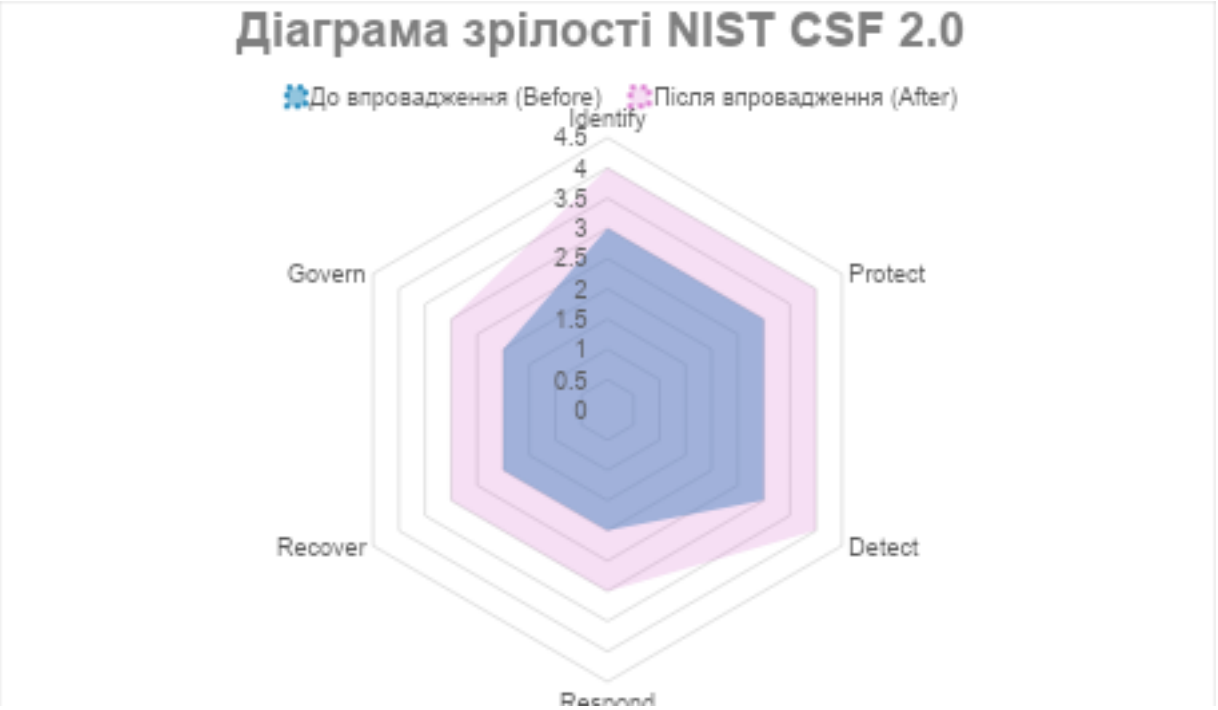


Рис. 3.3 – Діаграма зрілості NIST CSF 2.0 до та після впровадження заходів безпеки

В цілому, результати впровадження проекту з кібербезпеки можна підсумувати так: заклад перейшов від реактивного, майже не захищеного стану до проактивного, керованого стану безпеки. Це відповідає світовим практикам охорони здоров'я – у США та ЄС більшість лікарень вже дотримуються схожих контрольних заходів (HIPAA вимагає цього, GDPR змушує європейські установи робити те саме). Українські медичні установи, що впровадять такі рекомендації, не лише захистять себе від кіберзагроз і конфіденційність пацієнтів – вони також підвищать свою репутацію і довіру, полегшать вихід на міжнародне співробітництво (оскільки партнери бачать відповідність GDPR, HIPAA) та загалом модернізують управління інформацією.

**Висновок до розділу 3**

Резюмуючи, в даному дослідженні представлено комплексний підхід до захисту персональних даних пацієнтів у медичних закладах України, що ґрунтується на найкращих міжнародних практиках та стандартах — зокрема

HIPAA, GDPR і NIST CSF 2.0. Запропоновані рекомендації охоплюють усі ключові напрями забезпечення інформаційної безпеки, включаючи адміністративні, фізичні та технічні заходи, а також вимоги законодавства, механізми реагування на інциденти й підходи до безперервного вдосконалення.

З адміністративного боку передбачено впровадження системи управління безпекою, призначення відповідальних осіб, розробку політик, навчання персоналу та управління ризиками. У сфері фізичного захисту акцент зроблено на контроль доступу до приміщень, захист обладнання й безпечну утилізацію або обіг носіїв інформації. У технічному аспекті реалізовано заходи щодо контролю доступу в IT-системах, шифрування даних, сегментації мереж, впровадження антивірусного захисту, резервного копіювання й моніторингу. Також увагу приділено виконанню вимог законодавства: від гарантування прав суб’єктів даних і ведення належної документації — до готовності повідомляти про інциденти відповідно до термінів HIPAA і GDPR.

Особливої ваги набуває побудова процесів виявлення та реагування на інциденти — шляхом безперервного моніторингу, розробки та тестування планів реагування, а також здатності швидко відновлюватися з мінімальними втратами. Інтеграція кібербезпеки в загальну систему управління установою дозволяє організувати постійний цикл вдосконалення, що включає регулярний аудит, перегляд ризиків і оновлення захисних заходів.

У межах цього підходу було сформовано поетапну дорожню карту реалізації, що дозволяє досягти суттєвого покращення рівня захищеності протягом року. Очікуване зростання рівня відповідності ключовим вимогам — з приблизно 30% до 85% — свідчить про наближення українських закладів охорони здоров’я до світових стандартів у сфері кібербезпеки.

Досягнення цих результатів значною мірою залежить від підтримки з боку вищого керівництва, залучення кваліфікованих спеціалістів, поетапного й контрольованого впровадження змін, а також трансформації культури безпеки серед персоналу через навчання та постійні внутрішні комунікації. Практика показує, що відповідність вимогам і впровадження найкращих практик не лише

знижує ризики штрафів чи витоків, але й створює додаткову цінність: зменшуються збої в роботі, покращується якість обслуговування пацієнтів і зростає довіра до медичних установ.

Таким чином, інвестиції в кібербезпеку є стратегічно необхідними для сучасного медичного закладу. Реалізація запропонованих методичних рекомендацій дозволить українським лікарням і клінікам не лише забезпечити відповідність міжнародним нормативам, а й зміцнити власну стійкість перед зростаючими кіберзагрозами, підвищити надійність національної системи охорони здоров’я та посилити довіру громадян до сфери медицини в цілому.

# ВИСНОВКИ

В роботі проведено дослідження проблеми витоку персональних даних в об'єктах критичної інфраструктури медичного спрямування, визначено мету та завдання дослідження. Сьогодні проблема витоку персональних даних у медичних закладах є надзвичайно актуальною, оскільки обсяг цифрових медичних даних постійно зростає, а загрози стають дедалі складнішими та витонченішими. Недостатня захищеність інформаційних систем у медичних установах, людський фактор, технічні та організаційні вразливості є ключовими причинами виникнення таких загроз.

В роботі було детально проаналізовано сучасні інциденти кібербезпеки, які мали місце у медичних установах як в Україні, так і за кордоном. На основі проведеного аналізу було визначено, що основними причинами витоку персональних даних є відсутність комплексних підходів до забезпечення кібербезпеки, використання застарілого обладнання та програмного забезпечення, а також недостатня підготовленість персоналу до реагування на сучасні кіберзагрози.

В межах роботи проведено аналіз ризиків та побудовано матрицю ризиків витоку персональних даних згідно вимог GDPR. Додатково було створено модель загроз та модель потенційного порушника інформаційної безпеки медичних інформаційних систем, які дозволяють системно оцінювати загрози та вчасно реагувати на них.

Досліджено основні нормативні вимоги до захисту персональних даних у медичних закладах, зокрема, проаналізовано міжнародні стандарти HIPAA та NIST CSF 2.0. HIPAA визначає чіткі адміністративні, технічні та фізичні вимоги до захисту медичних даних, включаючи обмеження доступу, шифрування, аудит та регулярні перевірки. В роботі наведено рекомендації щодо формування внутрішніх політик безпеки медичних установ, які відповідають цим стандартам.

На основі аналізу та узагальнення вітчизняного і зарубіжного досвіду, було розроблено рекомендації щодо впровадження нових та покращення існуючих методів захисту персональних даних відповідно до HIPAA та NIST CSF 2.0. Сформовано High-Level Design (HLD) рішення, яке передбачає комплексний підхід до захисту інформаційної інфраструктури медичних закладів, що включає сучасні технічні та організаційні заходи для проактивного виявлення та реагування на загрози.

Отже, захист персональних даних у медичних об'єктах критичної інфраструктури є ключовим аспектом сучасної інформаційної безпеки, оскільки медичні установи є особливо вразливими до кіберзагроз. Впровадження розроблених рекомендацій дозволить підвищити рівень безпеки, забезпечити відповідність міжнародним стандартам, таким як HIPAA, GDPR та NIST CSF 2.0, автоматизувати процеси моніторингу та реагування на кіберінциденти, а також спростити впровадження найкращих практик інформаційної безпеки у медичних закладах.

Таким чином, правильна реалізація рекомендацій з удосконалення систем контролю витоків персональних даних має сприяти ефективному захисту медичних інформаційних ресурсів і зміцненню довіри пацієнтів до медичних закладів загалом.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міністерство охорони здоров’я та соціальних служб США. (2013). «Короткий зміст Правила конфіденційності HIPAA».

2. Прайс, В. та Коен, І. (2021). «Етика кібербезпеки в охороні здоров’я: забезпечення безпеки пацієнтів та цілісності даних». Журнал медичної етики , 47(9), 652-659.

3. Скотт, К. та Ноель, М. (2018). «Впровадження OSINT у системи кібербезпеки: критичний огляд». Cybersecurity Journal , 5(2), 101-113.

4. Агентство з кібербезпеки та безпеки інфраструктури (CISA). (2022). «Практики кібербезпеки для сектору охорони здоров’я».

5. Сміт, Дж. та Вайт, Л. (2020). «Забезпечення безпеки критичної інфраструктури в охороні здоров’я: найкращі практики та нові тенденції». Healthcare Technology Today , 11(4), 215-229.

6. Health Insurance Portability and Accountability Act (HIPAA), 1996 [Електронний ресурс]. – Режим доступу: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

7. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

8. NIST Cybersecurity Framework (NIST CSF) Version 2.0 [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework

9. ISO/IEC 27001:2022 – Information Security Management [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/82875.html

10. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17

11. Levitska M.V., Havenko K.S., Dakova L.V. 2025. Usage of Open-Source Intelligence for Security of Critical Infrastructure. Security of Information Systems and Techologies. 2, 8 (Mar. 2025), 49–55. DOI: https://doi.org/10.17721/ISTS.2024.8.49-55.

12. Levitska M., Kulaga Y., Stepanenko O. OSINT in Socio-Political Conflicts. Наукові горизонти XXI століття: мультидисциплінарні дослідження [Електронний ресурс] : матеріали Міжнародної наукової конференції,16-17 травня 2024 р., м. Ужгород / уклад. О.П. Адамчо ; УжНУ, УкрІНТЕІ. – Ужгород ; Київ, 2024. – 1696 с. DOI: https://doi.org/110.35668/978-966-479-144-8

13. Levitska M., Dakov S. (2024). Investigating the Security of Critical Medical Infrastructure: Integrating OSINT with HIPAA Compliance to Mitigate Data Leakage Risks. *Proceedings of Taras Shevchenko National University of Kyiv*, Kyiv, 2025.

14. Arif Mohamed. A history of cloud computing [Електронний ресурс]. – Режим доступу: http://www.computerweekly.com/feature/A-history-of-cloud-computing

15. Peter M. Mell, Timothy Grance. The NIST Definition of Cloud Computing [Електронний ресурс]. – Режим доступу: https://www.nist.gov/node/568586

16. SoCC 10: Proceedings of the 1st ACM symposium on Cloud computing, Hellerstein, Joseph M. – N. Y.: ACM, 2010. – ISBN 978-1-4503-0036-0.

17. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. – L.: Springer, 2010. – p. 379.

18. Безпека життєдіяльності. Безпека технологічних процесів і виробництв (Охорона праці): Навч. посібник для вузів / П.П. Кукін, Е.А. Підгорний та ін. – М.: Висш. шк., 1999. – с. 318.

19. European Union Agency for Cybersecurity (ENISA). (2023). “Cybersecurity Guidelines for Hospitals and Healthcare Providers” [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/cybersecurity-guidelines-for-hospitals

20. Ponemon Institute. (2023). “Cost of a Data Breach Report – Healthcare Sector Insights” [Електронний ресурс]. – Режим доступу: https://www.ibm.com/reports/data-breach

# ДОДАТКИ

## Додаток А

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

### Статті у наукових фахових виданнях України

1. Levitska M.V., Havenko K.S., Dakova L.V. 2025. Usage of Open-Source Intelligence for Security of Critical Infrastructure. Security of Information Systems and Techologies. 2, 8 (Mar. 2025), 49–55. DOI:https://doi.org/10.17721/ISTS.2024.8.49-55.

### Тези наукових доповідей:

1. Levitska M., Kulaga Y., Stepanenko O. OSINT in Socio-Political Conflicts. Наукові горизонти XXI століття: мультидисциплінарні дослідження [Електронний ресурс] : матеріали Міжнародної наукової конференції,16-17 травня 2024 р., м. Ужгород / уклад. О.П. Адамчо ; УжНУ, УкрІНТЕІ. – Ужгород ; Київ, 2024. – 1696 с. DOI: https://doi.org/110.35668/978-966-479-144-8
2. Levitska M., Dakov S. (2024). Investigating the Security of Critical Medical Infrastructure: Integrating OSINT with HIPAA Compliance to Mitigate Data Leakage Risks. Proceedings of Taras Shevchenko National University of Kyiv, Kyiv, 2025.

**Додаток Б**

**Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0**

| Категорія GOVERN (CSF 2.0) | Рекомендації щодо впровадження |
|---|---|
| Організаційний контекст (Organizational Context) – розуміння місії організації, очікувань зацікавлених сторін, залежностей, а також правових, регуляторних і договірних вимог у сфері кібербезпеки. | Керівництву медзакладу слід інтегрувати кібербезпеку в загальну стратегію установи. Зокрема:<br>Провести сесію стратегічного планування, де визначити – які бізнес-процеси найбільш критичні (наприклад, надання невідкладної допомоги, збереження репутації, виконання контрактів зі страховиками) і як кіберінциденти можуть на них вплинути.<br>Врахувати очікування зацікавлених сторін: пацієнти очікують конфіденційності та доступності сервісів, держава очікує дотримання законів (МОЗ, регулятор із захисту даних), партнери – надійності в обміні інформацією.<br>Вимоги законів і стандартів: як ми вже розглянули, є HIPAA, GDPR, українські закони, можливо, стандарти НСЗУ чи страхових компаній щодо безпеки даних. Керівництво має явно взяти ці вимоги за основу для політик (наприклад, наказом впровадити вимоги GDPR для всіх пацієнтів, не лише іноземців).<br>Залежності: проаналізувати, від кого ми залежимо у IT-плані – постачальники ЕМК (електронної медкарти), інтернет-провайдер, виробники медичного обладнання (яке |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Організаційний контекст (Organizational Context) – розуміння місії організації, очікувань зацікавлених сторін, залежностей, а також правових, регуляторних і договірних вимог у сфері кібербезпеки. | теж може бути підключене до мережі). Необхідно впевнитися, що вони забезпечують належний рівень безпеки: включити вимоги в контракти, перевіряти сертифікати, оновлення ПЗ обладнання. Документувати всі ці зовнішні залежності у профілі ризиків установи.<br>Вбудувати кібербезпеку у плани розвитку: якщо лікарня планує відкривати нові відділення або впроваджувати телемедицину, вже на етапі планування бюджету враховувати витрати на захист даних (закласти кошти на додаткові ліцензії захисного ПЗ, навчання персоналу, консультації). Таким чином, безпека стає не окремим технічним питанням, а частиною контексту управління закладом. |
| Стратегія управління ризиками (Risk Management Strategy) – визначення пріоритетів, допусків до ризику (risk appetite), обмежень та припущень, які лягають в основу операційних рішень з безпеки. | Керівництво має сформулювати політику управління ризиками інформаційної безпеки.<br>Визначити апетит до ризику – наприклад, “Ми не можемо допустити жодного витоку даних >1000 пацієнтів” або “Допускаємо простої ІТ-систем не більше 4 годин на рік” тощо. Ці порогові значення допоможуть приймати рішення: якщо ризик перевищує поріг – потрібні нові заходи чи інвестиції.<br>Встановити пріоритети – наприклад, захисту підлягають у першу чергу системи з медичними діагнозами і персональними даними, а вже в другу – менш чутлива |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Стратегія управління ризиками (Risk Management Strategy) – визначення пріоритетів, допусків до ризику (risk appetite), обмежень та припущень, які лягають в основу операційних рішень з безпеки. | інформація (наприклад, маркетингова база контактів). Такий пріоритет допомагає розподілити ресурси: найсильніший захист – навколо медичних даних (сегментація мережі, строгий контроль доступу), менш критичні системи – базовий захист.<br>Констрейнти (обмеження) – реалії, які враховуються: бюджетні обмеження, дефіцит IT-фахівців, спадок старих систем, які не підтримують шифрування. Керівництво має бути обізнане про ці обмеження і враховувати їх при плануванні. Наприклад, якщо старий рентген-апарат працює на Windows XP і його не можна оновити – прийняти рішення ізолювати його в окремій мережі, бо повністю захистити стандартними методами не вийде.<br>Припущення – наприклад, припускаємо, що хмарний провайдер надійно захищає нашу базу (тоді маємо сертифікат від нього), або припускаємо, що персонал може помилятися (тоді обов'язково треба багаторівневий захист на такий випадок).<br>Документувати стратегію у Політиці управління ризиками і довести до керівників підрозділів. Регулярно переглядати: якщо, скажімо, апетит до ризику знижується (після інциденту вирішили, що навіть 100 записів – це багато), то посилити заходи. Дотримання чіткої стратегії дозволить всім – від системного адміністратора до директора – розуміти рамки, в яких приймаються рішення щодо безпеки. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Ролі, обов’язки та повноваження (Roles, Responsibilities, and Authorities) – визначення і доведення до відома, хто за що відповідає в сфері кібербезпеки, щоб забезпечити підзвітність та регулярну оцінку виконання. | Як було частково зроблено в HIPAA (призначення відповідального), тут треба піти далі і створити організаційну структуру кібербезпеки.<br>Дорожня карта підпорядкування: визначити, кому підзвітний IT-відділ і функція безпеки (рекомендовано безпосередньо директору або заступнику директора, щоб була підтримка згори).<br>Ролі: CISO/ISO (Chief Information Security Officer або відповідальний за ІБ) – стратегія і координація; DPO – відповідність GDPR і робота з даними; IT-адміністратори – технічне виконання заходів (мережі, сервери); Керівники відділень – відповідальні за дотримання політик підлеглими; Персонал – відповідальний за належне поводження з даними.<br>Опис обов’язків: оновити посадові інструкції ключових осіб – наприклад, завідуючий відділення має контролювати, щоб медсестри не ділилися паролями, а IT-директор – щоквартально звітувати про стан безпеки.<br>Повноваження: надати IT-безпеці мандат зупиняти певні процеси при ризику (скажімо, право відключити від мережі комп’ютер при підозрі на вірус, навіть якщо це комп’ютер заввідділення – з наступним повідомленням керівництва). DPO має |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Ролі, обов'язки та повноваження (Roles, Responsibilities, and Authorities) – визначення і доведення до відома, хто за що відповідає в сфері кібербезпеки, щоб забезпечити підзвітність та регулярну оцінку виконання. | мати повноваження блокувати певні ініціативи, якщо вони суперечать GDPR, до усунення недоліків.<br>Оцінка ефективності: включити пункт в щорічний оцінювання роботи керівників щодо виконання вимог безпеки. Наприклад, KPI заввідділення – 100% співробітників пройшли навчання, 0 випадків порушення лікарської таємниці; KPI IT-директора – виконано >90% заходів з плану безпеки, середній час реагування < X годин.<br>Комунікація: організувати регулярні зустрічі (напр. щомісячно) між DPO, IT-безпекою та представниками підрозділів – обговорювати нові загрози, інциденти, статус проектів. Таким чином формується система підзвітності: кожен знає свою роль і розуміє, кого спитати за певний аспект захисту. Це знижує ймовірність, що якась зона залишиться "нічийною" (наприклад, безконтрольне використання персональних флешок медперсоналом – якщо таке станеться, відповідальний за відділення теж нестиме відповідальність за недотримання політики). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Політика (Cybersecurity Policy) – встановлення, комунікація та впровадження політик кібербезпеки, які регулярно переглядаються та актуалізуються під нові вимоги, загрози, технології. | В попередніх розділах ми вже згадували про розробку політик (і HIPAA, і GDPR цього вимагають). У межах функції Govern важливо, щоб політики були живими документами:<br>Офіційне затвердження – всі ключові політики (інформаційна безпека, конфіденційність пацієнтів, реакція на інциденти, використання пристроїв, резервне копіювання) повинні бути затверджені наказом керівника закладу. Це показує пріоритетність.<br>Доведення до персоналу – ми вже зазначали способи (тренінги, розписки). Переконатися, що нові співробітники отримують весь пакет політик під час адаптації. Регулярний перегляд – призначити відповідальних за перегляд кожної політики (наприклад, IT-безпека переглядає політику паролів щороку і, бачачи, що з'явилась нова загроза, може запропонувати оновлення – як-от вимагати MFA повсюдно). Політики слід оновлювати принаймні раз на 1-2 роки, навіть якщо правок нема – ставити нову дату перегляду і фіксувати "перевірено, актуально".<br>Врахування змін: якщо вводиться нова технологія (скажімо, лікарі почали користуватися планшетами) – негайно переглянути політику використання пристроїв і |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Політика (Cybersecurity Policy) – встановлення, комунікація та впровадження політик кібербезпеки, які регулярно переглядаються та актуалізуються під нові вимоги, загрози, технології. | додати пункт про безпеку планшетів. Якщо виникла нова регуляторна вимога – внести у відповідні політики.<br>Контроль виконання – політика без нагляду нічого не варта. Призначити власників політик (наприклад, голова IT-комітету відповідає за реалізацію технічних політик, начальник відділу кадрів – за політику приватності співробітників). В ході внутрішніх аудитів перевіряти фактичне виконання: чи відповідає реальність написаному. Якщо політика не працює (наприклад, заборона USB-носіїв масово порушується через потребу друку) – або запровадити технічний контроль (блокування USB), або змінити політику на більш реалістичну, але забезпечити інші методи захисту. Тобто політики мають еволюціонувати разом з закладом і технологіями. Наявність актуальних, чітких і дотримуваних політик – ознака зрілого управління кібербезпекою. керівництво і дозволяє прийняти рішення про додаткові ресурси або коригування планів.<br>Моніторинг відповідності: DPO та IT-безпека мають проводити перевірки, чи всі ризики охоплені заходами. Наприклад, виявлено новий ризик – фішингові атаки на лікарів через e-mail. Oversight означає: перевірити, чи є у нас засоби проти цього (спам-фільтри, навчання). Якщо ні – ініціювати заходи. |

| | |
|---|---|
| | Внутрішній аудит і ревізії: незалежний аудит (внутрішня ревізійна комісія або зовнішні експерти) раз на рік перевіряють відповідність політик і практик. Результати аудиту розглядаються керівництвом – це елемент oversight.<br>Коригування стратегії: наприклад, якщо за рік з'явилися нові загрози (скайнери, IoT-атаки на медобладнання), керівництво на основі звітів може вирішити переглянути пріоритети – інвестувати більше в сегментацію мережі, ніж планувалося. Oversight – це як кермо корабля: постійно трохи підкручувати напрямок на основі зворотного зв'язку.<br>Документування: результати oversight – протоколи засідань комітету з безпеки, накази про коригування планів, бюджети – мають зберігатися, щоб показати під час перевірки: ось, ми регулярно переглядаємо стан захищеності. У сфері охорони здоров'я це особливо важливо, бо загрози еволюціонують (сьогодні шифрувальники націлені на лікарні дедалі частіше). Активний oversight гарантує, що кібербезпека залишається динамічним процесом, а не разовим проектом. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Керування кібербезпекою ланцюга постачання (Cybersecurity Supply Chain Risk Management) – інтеграція ризиків ланцюга постачання в програми управління кіберризиками, моніторинг підрядників і постачальників, планування на випадок завершення співпраці. | У медичному закладі багато залежить від зовнішніх постачальників: від виробників медичного обладнання (КТ, МРТ з комп'ютерами) до IT-провайдерів. Управління ризиками ланцюга постачання включає:<br>Інвентаризація постачальників: як згадано раніше, скласти список всіх, хто має відношення до даних або систем (EMR система – постачальник А, лабораторна система – постачальник Б, облачний датацентр – В, постачальник мережевого обладнання – Г і т.д.).<br>Вимоги до них: як мінімум, прописати в договорах вимоги безпеки (це зроблено в межах GDPR DPA – табл.6). Додатково – вимагати від ключових IT-постачальників сертифікацій (ISO 27001, або підтвердження відповідності HIPAA якщо це американський провайдер, тощо).<br>Моніторинг їхньої безпеки: запросити звіти про пен-тести чи аудити, які пройшов постачальник, особливо якщо це хмарна платформа. Стежити за новинами: якщо у постачальника сталася кібератака (наприклад, компрометація ПО), негайно перевірити, чи не зачепило вас, і чи потрібні дії (оновити ПО, змінити паролі API і т.д.). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Керування кібербезпекою ланцюга постачання (Cybersecurity Supply Chain Risk Management) – інтеграція ризиків ланцюга постачання в програми управління кіберризиками, моніторинг підрядників і постачальників, планування на випадок завершення співпраці. | Планування на випадок завершення відносин: дуже практичний аспект – якщо ми вирішимо перейти на іншу систему або постачальник раптом припинить діяльність, як ми заберемо або знищимо наші дані. Треба передбачити це в угоді: право отримати всі дані у читабельному форматі при розірванні договору, обов'язок постачальника видалити копії. Перевірити процедуру: можливо, навіть протестувати міграцію невеликого фрагменту даних.<br>Безпека постачання обладнання: для критичних систем намагатися купувати обладнання у надійних виробників (відсутність бекдорів, підтримка оновлень). Запитувати у постачальників медтехніки їхню політику кібербезпеки: чи оновлюють ПЗ, як захищають від вірусів. Якщо постачальник слабкий у цьому – при встановленні обладнання треба самим ізолювати його та захистити (наприклад, МРТ-машина на Windows XP – поставити її за окремим файрволом і дозволити тільки необхідні з'єднання).<br>Спільне реагування: включити ключових постачальників у ваші плани реагування – тобто мати їхні контакти 24/7. Якщо впала хмарна EMR – знати, кого викликати негайно з боку постачальника. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| Категорія IDENTIFY | Рекомендації щодо впровадження |
|---|---|
| Управління активами (Asset Management) – виявлення та ведення обліку активів (дані, обладнання, програмне забезпечення, системи, сервіси, люди), важливих для виконання завдань організації, з урахуванням їх критичності та цінності. | Як частково вже згадувалось у HIPAA-контексті, потрібно створити повний реєстр інформаційних активів. Сюди входить: Обладнання: сервери, комп'ютери, ноутбуки, маршрутизатори, комутатори, мережеві сховища, медичне обладнання з мережевими модулями (томографи, монітори пацієнтів). Для кожного – вказати відповідального власника (адміністратор або підрозділ), місцезнаходження, серійний номер, конфігурацію, які дані можуть зберігатися. Програмне забезпечення та інформаційні системи: електронна медична система, лабораторна, система управління клінікою, фінансово-бухгалтерська, поштовий сервер, ОС на кожному типі пристроїв, а також версії програм. Сервіси: хмарні сервіси (наприклад, сервіс зберігання резервних копій, SaaS-система для телемедицини), веб-сайти, доменні імена. Дані: визначити категорії даних – медичні дані пацієнтів (EPHI), персональні дані співробітників, фінансові записи, журнали аудиту, дослідницькі дані тощо. Можливо, створити карту потоків даних: звідки і куди дані рухаються (наприклад: пацієнт заповнює онлайн-форму -> дані потрапляють на веб-сервер -> до БД клініки; або лікар відправляє аналізи -> вони йдуть до зовнішньої лабораторії). Така карта допоможе бачити межі систем і потенційні точки виходу/входу даних. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Управління активами (Asset Management) – виявлення та ведення обліку активів (дані, обладнання, програмне забезпечення, системи, сервіси, люди), важливих для виконання завдань організації, з урахуванням їх критичності та цінності. | Це стосується більше управління доступами, але й до активів теж (люди – теж актив, як носії знань). Після збору інформації провести класифікацію активів за критичністю: наприклад, критичні активи – сервер бази даних пацієнтів, основна мережа; важливі – локальні робочі станції, менш критичні – публічний сайт. Також за конфіденційністю даних: меддані – високочутливі, службові електронні листи – середні, публічна інформація – низькі. Цей реєстр і класифікація дозволяють пріоритизувати захист (Protect) та моніторинг (Detect) саме навколо найцінніших активів. Регулярно (раз на пів року) реєстр оновлювати: додали новий сервер – внести; списали комп'ютер – відмітити. Особливо звертати увагу на "тіньові" активи: пристрої або сервіси, про які IT може не знати (наприклад, відділення самостійно підключило Wi-Fi роутер). Проводити сканування мережі для виявлення таких несанкціонованих пристроїв і або взяти їх під управління, або відключити. Загалом, ефективне управління активами – це фундамент: не можна захистити те, про що не знаєш. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Оцінка ризиків (Risk Assessment) – організація розуміє кіберризики для себе, активів і людей; ідентифікує вразливості, загрози, оцінює ймовірність та потенційний вплив атак. | Цей процес значною мірою описаний в розділі про HIPAA (аналіз ризиків) і вдосконалений у GDPR (DPIA). В рамках NIST CSF: Розробити методологію оцінки ризиків – вирішити, будете використовувати якісну шкалу (високий/середній/низький ризик) чи кількісну (бали, грошова оцінка). Для початку підійде якісна: оцінювати ймовірність події (низька, середня, висока) та вплив (низький – мінімальні наслідки, високий – значний простій, витік чутливої інформації, загроза життю пацієнтів). Виявлення загроз і вразливостей: використовувати різні джерела – результати інвентаризації активів (наприклад, знайдено Windows 7 машина – це вразливість, бо більше не підтримується; або в мережі відкритий порт до інтернету), результати зовнішніх аудитів, інформацію з галузевих новин (був інцидент з ransomware у сусідній лікарні). Залучати персонал – опитати, які проблеми бачили (може, у відділенні є комп'ютер, що постійно глючить – ризик втрати даних). Скласти перелік ризикових сценаріїв: наприклад, "вірус-шифрувальник може потрапити через електронну пошту і зашифрувати базу даних – ймовірність середня, вплив високий (зупинка роботи, можлива втрата даних) – загальний ризик високий"; "недобросовісний співробітник скопіює дані VIP-пацієнта і продасть – ймовірність низька (всі свої, перевірені), вплив високий (скандал, суд) – ризик середній"; "відмова |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Оцінка ризиків (Risk Assessment) – організація розуміє кіберризики для себе, активів і людей; ідентифікує вразливості, загрози, оцінює ймовірність та потенційний вплив атак | обладнання (сервер вийшов з ладу) – ймовірність середня, вплив середній (є резервні копії, але простої будуть) – ризик середній". Враховувати різні типи загроз: кібер (атаки хакерів, шкідливе ПЗ), фізичні (пожежа, крадіжка), людський фактор (помилки, зловмисні дії). Пріоритизація: розставити ризики в порядку спадання критичності. Зосередитися на верхніх (наприклад, топ-10 ризиків) для негайного реагування в плані обробки. Планування обробки ризиків: для кожного значущого ризику прийняти рішення – знизити (впровадити контролі, які зменшать ймовірність чи вплив), уникнути (припинити діяльність, що породжує ризик, якщо можливо), передати (страхування кіберризиків – у деяких країнах поширено, або аутсорсинг з відповідальністю), або прийняти (якщо ризик малий і заходи дорожчі, ніж потенційна шкода). Задокументувати, що вирішили – наприклад: ризик шифрувальника – знизити шляхом навчання користувачів, встановлення анти-шифрувальника та сегментації мережі; ризик інсайдера – частково передати (ввести положення про штрафи у трудовий договір, що трохи стримуватиме) і моніторити (DLP-система, журнали доступів); ризик відмови обладнання – знизити (налаштувати кластер серверів) і застрахувати обладнання; ризик стихійного лиха – приймаємо залишковий, бо ймовірність дуже низька, але маємо резервні копії в іншому місці. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Оцінка ризиків (Risk Assessment) – організація розуміє кіберризики для себе, активів і людей; ідентифікує вразливості, загрози, оцінює ймовірність та потенційний вплив атак | пріоритетами і виділили ресурси. Виконання і моніторинг: реалізувати заходи, після чого провести повторну оцінку – ризики мають знизитися (кількісно або хоча б якісно колір змінитися з червоного на жовтий). Включити ризиковий аналіз у постійний процес: оновлювати щороку або при значних змінах (впровадження нової технології, нова загроза). NIST CSF 2.0 також підкреслює важливість обробки вразливостей (ID.RA-01) – тобто мати процес сканування та управління вразливостями: регулярне сканування мережі на відомі вразливості, встановлення патчів, відстеження розсилок від Microsoft, VMware тощо щодо критичних оновлень. Це має бути частиною плану роботи IT. Ціллю категорії “Identify – Risk Assessment” є сформувати у керівництва чітке уявлення: які найгірші сценарії можуть статись з кібербезпекою і що ми робимо, щоб їм запобігти чи пом’якшити. |
| Покращення процесів (Improvement) – постійний пошук шляхів вдосконалення процесів управління кіберризиками, на основі оцінок, тестів, досвіду інцидентів та операційної діяльності. | Ця категорія (ID.IM) у CSF 2.0 відображає ідеологію безперервного вдосконалення. В медзакладі слід запровадити циклічні механізми: 1) Витяг уроків з інцидентів: після кожного серйозного випадку (чи то реального, чи то навчального) проводити зустріч, де обговорити – що спрацювало, що ні, як покращити. Сформувати документ “After Action Report” і план дій. Наприклад, якщо сталася вірусна атака і зупинила |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Покращення процесів (Improvement) – постійний пошук шляхів вдосконалення процесів управління кіберризиками, на основі оцінок, тестів, досвіду інцидентів та операційної діяльності. | реєстратуру на день – розібратися, чому не вдалося ізолювати швидше, чи було повторюваним по розкладу (maturity +1). Оновлено антивірус, і внести зміни (покращити сегментацію, пришвидшити оповіщення). Оцінки та аудити: результати аудитів (внутрішніх чи зовнішніх) не мають складатися “на полицю” – потрібен процес виконання рекомендацій. Створити в системі відстеження завдань (наприклад, Excel або спеціальний софт) список знайдених недоліків і регулярно перевіряти прогрес їх усунення. Призначати відповідальних і дедлайни. Тести і навчання: проводити заплановані випробування (penetration test, фішингові тестування) – і на основі їх результатів покращувати інфраструктуру і навчання. NIST CSF каже: покращення можуть виявлятися з виконання операційних процесів (тобто щоденної роботи). Наприклад, IT-фахівці помітили, що дуже довго обробляти журнали подій вручну – отже, потрібен новий інструмент SIEM або налаштування автоматичних звітів (покращення процесу моніторингу). Внесення змін до документів: якщо запровадили новий крок – оновити політики/процедури, навчити людей. Кероване впровадження новацій: відстежувати нові технології кібербезпеки (наприклад, системи запобігання витокам, Zero Trust архітектура). інновації, планувати пілотні впровадження. |
| Категорія PROTECT | Заходи для впровадження (медичний заклад) |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Управління ідентифікацією та доступом (PR.AA: Identity Management, Authentication and Access | Основні кроки вже були описані в HIPAA (табл. 3: Контроль доступу, Автентифікація) – тут зведемо їх системно: Єдина система управління ідентифікацією: використовувати централізовану директорію (Active |

| | |
|---|---|
| Control) – доступ до фізичних та інформаційних активів обмежено авторизованими користувачами, процесами і пристроями відповідно до принципу найменших привілеїв. | Directory, LDAP) для всіх співробітників. Це дасть змогу оперативно керувати доступами, застосовувати політики паролів глобально, надавати/скасовувати доступ одним місцем. Унікальні користувачі: жодних спільних облікових записів. Навіть для тимчасового персоналу – окремий логін. Роботизовані процеси чи служби – теж окремі ідентифікатори (щоб їхні дії логувалися під своїм ім'ям). Мінімальні привілеї: надавати найменший рівень доступу, потрібний для роботи. Якщо лікарю не треба бачити фінансові дані пацієнта – його роль цього не дозволяє. Періодично переглядати привілеї: можливо, комусь зайве залишили адмін-доступ. Практикувати Just-In-Time Access: наприклад, обліковий запис адміністратора бази включається лише коли треба обслуговування. Решту часу він відключений, щоб зменшити "точки атаки". Багатофакторна автентифікація (MFA): впровадити щонайменше для віддаленого доступу, адміністративних обліковок та доступу до найбільш чутливих даних (наприклад, при вході в ЕМК поза межами лікарні – обов'язково MFA). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Управління ідентифікацією та доступом (PR.AA: Identity Management, Authentication and Access Control) – доступ до фізичних та інформаційних активів обмежено авторизованими користувачами, процесами і пристроями відповідно до принципу найменших привілеїв. | MFA значно знижує ризик компрометації облікових записів. 5) Автоматизація керування доступами: інтегрувати створення і видалення користувачів з HR-процесами. Нового співробітника – створити акаунти за шаблоном посади; звільнився – одразу скриптом деактивувати у всіх системах. Таким чином уникнемо “забутих” активних акаунтів. Моніторинг доступів: включити механізми спостереження – наприклад, якщо акаунт лікаря раптом спробував зайти в 3 ночі з-за кордону, система блокує або принаймні сигналізує. Або якщо під одним акаунтом одночасно дві сесії – завершує одну (щоб обліковий не використовували двоє). Фізичний контроль доступу: синхронізувати з IT – наприклад, системи контролю дверей можуть бути пов’язані з IT-директорією (високий рівень інтеграції). Але якщо ні – хоча б відстежувати, щоб звільненим анулювали і фізичні пропуски. Привілейовані користувачі: адміністратори систем повинні мати два облікові записи – один зі звичайними правами для щоденної роботи (e-mail, офісні програми) і окремий – підвищений для адмін-завдань. Цей другий використовувати тільки коли треба конфіги міняти, і бажано входити під ним через окрему захищену станцію або через jump-server. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Управління ідентифікацією та доступом (PR.AA: Identity Management, Authentication and Access Control) – доступ до фізичних та інформаційних активів обмежено авторизованими користувачами, процесами і пристроями відповідно до принципу найменших привілеїв. | локального адміністратора). Сегментація мереж та доступів: розділити мережевий доступ за ролями – персонал адміністрації не повинен мати доступу до сегменту медичних даних, і навпаки (для цього – VLANи, правила брандмауера). Так навіть якщо користувач з однієї групи скомпрометований, зловмисник не одразу дістаться інших зон. Реалізація цих заходів забезпечує потужний бар'єр проти стороннього або надлишкового доступу до систем, мінімізуючи ризик внутрішніх зловживань і полегшуючи простежування дій у разі інциденту. |
| Обізнаність і навчання (PR.AT: Awareness and Training) – працівники організації та відповідні партнери отримують належну обізнаність щодо кібербезпеки та навчені виконувати свої обов'язки, беручи до уваги кіберризики. | Цей пункт вже широко описаний у HIPAA (Security Awareness Training) – тут лише підкреслимо деякі моменти і додамо: Різнорівневі тренінги: окрім базового для всіх, робити спеціалізовані для різних категорій. NIST CSF каже про рольову специфіку. Наприклад, для IT-адміністраторів – розширена програма з кібербезпеки (актуальні вектори атак на сервери, практики захисту, реагування); для лікарів – акцент на конфіденційність і фішинг, для молодшого медперсоналу – як захищати дані при спілкуванні (не називати в ліфті ім'я пацієнта з діагнозом при сторонніх). Регулярність: ми згадували – щорічно. Але можна дрібні активності робити частіше: щомісяця розсилати невеличкий бюлетень "Порада місяця з кібербезпеки" або постер змінювати |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Обізнаність і навчання (PR.AT: Awareness and Training) – працівники організації та відповідні партнери отримують належну обізнаність щодо кібербезпеки та навчені виконувати свої обов'язки, беручи до уваги кіберризики. | на дошці оголошень (напр. "Нагадування: не залишайте картки пацієнтів на столі"). Інтерактивність: краще засвоюється, коли це не просто лекція. Використовувати симуляції (наприклад, проходження модульних курсів із запитаннями, або настільні ігри на тему "знайди ризики в кабінеті"). Можна запросити експерта з кіберполіції для лекції – це додасть авторитетності. Оцінка знань: після навчання – тести або практичні перевірки (фішинг-тест, як згадували). Особливо з керівним складом варто пропрацювати – вони частіше ціль social engineering (так звані VIP-phishing, коли видають себе за директора і просять дані). Навчання партнерів: якщо є залучені підрядники, що працюють у наших системах (уборка, яка має доступ у приміщення з комп'ютерами, або аутсорсинг IT) – слід переконатися, що і вони пройшли базове навчання і розуміють вимоги. Можна включити у договір вимогу про проходження тренінгу з кібербезпеки. Кібергігієна вдома: корисно іноді давати поради, як захистити домашній комп'ютер, чи як дітям розказати про інтернет-безпеку. Це не прямо про роботу, але формує загальну культуру – працівник, який удома практикує безпеку, на роботі теж буде уважнішим. Відстеження участі: вести журнал, хто коли навчався, щоб не пропускати. Нового співробітника – в перші 1-2 тижні направити на курс, не допускати до систем без ознайомлення з правилами. Це |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Обізнаність і навчання (PR.AT: Awareness and Training) – працівники організації та відповідні партнери отримують належну обізнаність щодо кібербезпеки та навчені виконувати свої обов’язки, беручи до уваги кіберризики. | мотивує інших не ігнорувати безпеку. Навчений і обізнаний персонал – один з найкращих ресурсів проти атак: як показують дослідження, людська помилка є причиною до 95% інцидентів. Тому інвестиції в Awareness і Training повертаються зменшенням кількості інцидентів та збільшенням здатності швидко реагувати, якщо щось трапилось. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Безпека даних (PR.DS: Data Security) – дані керуються відповідно до стратегії ризиків організації для забезпечення конфіденційності, цілісності та доступності інформації. | Ця категорія концентрується на самих даних: засоби їх захисту протягом життєвого циклу. Частково це вже покрито в GDPR-технічних заходах та HIPAA Integrity/Transmission Security. Підсумуємо: Класифікація даних: визначити рівні чутливості. Ми це робили (медичні – висока, службові – середня...). Впровадити позначення: наприклад, на друкованих звітах ставити штамп “Конфіденційно”, на електронних – водяний знак або в метаданих classification label. Це підвищує усвідомлення. Шифрування даних у спокої: все, що можна, – шифрувати. Бази – або на рівні СУБД засобами Transparent Data Encryption, або хоча б на рівні дисків. Файлові сховища – шифровані диски. Резервні копії – перед записом архівувати з паролем/ключем. Особливо переносні носії – всі флешки, що використовуються, повинні бути апаратно чи програмно зашифровані (Bitlocker To Go, VeraCrypt). 3) Шифрування даних в транзиті: захищені протоколи для всіх з’єднань (SSH, TLS, VPN). Заборонити незашифровані підключення (на рівні брандмауера блокувати ftp/http). Використовувати сертифікати нестарі (TLS1.0 вже виключити). Цілісність даних: якщо є ресурси, розгортати системи контролю цілісності – наприклад, SIEM може відстежувати зміни критичних файлів; бази даних можуть мати вбудовані механізми аудиту змін. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Безпека платформ (PR.PS: Platform Security) – апаратне та програмне забезпечення і сервіси на фізичних та віртуальних платформах керуються відповідно до стратегії ризиків для захисту їх конфіденційності, цілісності та доступності. | Ця категорія з’явилась у CSF 2.0, фокусуючись на захисті середовища IT-платформ. Для медустанов це означає керування конфігураціями систем, регулярне обслуговування і контроль програм. Заходи: Управління конфігураціями: всі сервери і важливі робочі станції повинні мати стандарт конфігурації (secure baseline). Наприклад, Windows-сервер: прибрати непотрібні служби, встановити певні налаштування політик (через Group Policy) – блокувати старі протоколи (SMBv1, TLS1.0), увімкнути шифрування SMB, задати посилені параметри аудиту тощо. Те ж для робочих машин: вимкнути авторан USB, встановити firewall, заборонити встановлення програм звичайним користувачем. Документувати базові конфігурації і стежити за їх дотриманням (інструменти типу Microsoft SCT або аналоги можуть сканувати відхилення). Управління патчами та оновленнями: критично важливо для сучасних загроз. Налаштувати процес оновлень: використовувати WSUS для Windows чи альтернативи, мати графік – напр., щомісяця через тиждень після Patch Tuesday тестувати оновлення на парі машин, потім розгортати масово. Для серверів – мати відмовостійкість, щоб можна було перезавантажити по черзі. Не забувати оновлювати Linux-сервери, мережеве обладнання (прошивки), а також специфічні системи (PACS, лабораторне ПЗ – перевіряти у постачальників патчі). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Стійкість технологічної інфраструктури (PR.IR: Technology Infrastructure Resilience) – архітектури безпеки керуються відповідно до стратегії ризиків організації для захисту конфіденційності, цілісності, доступності активів і забезпечення організаційної стійкості. | Дана категорія трохи перекликається з раніше згаданими темами (резервування, запасні потужності) – під "інфраструктурою" маються на увазі мережі, середовища, архітектурні рішення, які роблять організацію більш стійкою. Заходи: Мережева сегментація і захищеність: (ми частково згадували) – розділити мережу на сегменти за призначенням (медичне обладнання в окремому VLAN з жорсткими правилами, офісні ПК – в іншому, гостьовий Wi-Fi – повністю ізольований). Встановити мережеві екрани (firewall) між сегментами з правилом "заборонено все, що не дозволено явно". Це локалізує потенційні інциденти. Захист периметру: як мінімум, один корпоративний фаєрвол на вихід в інтернет з вкл. функціями IPS/IDS (виявлення вторгнень). Регулярно оновлювати підписи IPS. Резервні канали зв'язку: якщо робота критично залежить від інтернету (скажімо, підключення до електронної системи МОЗ), мати два провайдери або 4G-резерв. Катастрофостійкість: для великих лікарень – розглядати відмовостійкий датацентр або хмару. Якщо клініка менша – принаймні резервні копії зберігати за межами основного приміщення (наприклад, в хмарі). План аварійного переключення: якщо впала база – чи є "гарячий" дубль? Якщо ні – "холодний" сервер готовий чи наявний Cloud-сервер, куди можна швидко розгорнути? Перевірити. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| Категорія DETECT | Рекомендації для реалізації |
|---|---|
| Безперервний моніторинг (DE.CM: Continuous Monitoring) – моніторинг мереж, систем, середовища, персоналу та постачальників для виявлення аномалій, індикаторів компрометації та потенційно шкідливих подій. | Для медичного закладу, де обмежений штат IT, continuous monitoring має бути максимально автоматизованим: Системи виявлення вторгнень (IDS/IPS): розгорнути мережеву IDS на межі між інтернетом і внутрішньою мережею. Вона аналізуватиме трафік на відомі сигнатури атак, аномалії. Такі рішення (Snort/Suricata, або модулі на фаєрволах) генерують алерти при підозрі на сканування портів, спроби експлойтів і т.д. Бажано мати IDS і на межі між сегментами (наприклад, між сегментом медобладнання і офісним – щоб побачити, якщо щось з офісу лізе до обладнання нестандартне). Системи моніторингу цілісності: як частину continuous monitoring – використати HIDS (хостова система виявлення) на ключових серверах. Вона може відстежувати зміни в критичних файлах, запуски незнайомих процесів тощо. Сучасні EDR (Endpoint Detection & Response) платформи виконують цю роль, вони ж можуть блокувати підозрілу активність. Наприклад, якщо процес Word раптом почне шифрувати десятки файлів – EDR це виявить як аномалію і зупинить. Аналіз журналів (логів): налаштувати агрегування логів у SIEM-систему. Вона в реальному часі співставлятиме події з різних джерел і шукатиме підозрілі шаблони. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Аналіз потенційних інцидентів (DE.AE: Adverse Event Analysis) – аномалії, індикатори компрометації та інші потенційно шкідливі події аналізуються для характеристики їх та визначення, чи є вони кіберінцидентами. | Ця категорія передбачає наявність процедур і можливостей проаналізувати зібрану інформацію і відфільтрувати справжні інциденти від фальшивих або незначних подій. Заходи: Процедура triage (сортування) інцидентів: встановити градацію – наприклад, рівень 1 (низький) – одинична підозріла подія (наприклад, один невдалий логін адміністратора – може, просто помилився), рівень 2 (середній) – сукупність подій або подія з потенційним впливом (наприклад, антивірус ізолював троян – інцидент, який варто розслідувати, але не аварійний), рівень 3 (високий) – підтверджений інцидент (кілька серверів зашифровано, витік даних, активна атака). Відповідно до рівня – різні дії: від запису в журнал і спостереження до скликання команди реагування і запуску плану реагування.<br>Інструменти аналізу: надати IT-фахівцям інструменти для розслідування: софт для аналізу логів (наприклад, Kibana/Elasticsearch для пошуку по логах), утиліти для форензік (Volatility, FTK Imager – щоб зняти дамп пам’яті або диска для аналізу). Якщо стався незрозумілий збій – мати можливість дослідити: зберігати копії логів, знати хеші важливих файлів (щоб порівняти, чи не підмінені). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| Категорія RESPOND | Рекомендації щодо реалізації |
|---|---|
| Управління інцидентами (RS.MA: Incident Management) – виконуються заходи відповідно до планів реагування, щоб запобігти розповсюдженню інциденту та пом’якшити його наслідки. | Це про наявність та реалізацію плану реагування на інциденти (Incident Response Plan, IRP). В контексті медзакладу:<br>Розробка IRP: ми вже наводили його ключові етапи (табл. 1, Security Incident Procedures). Важливо оформити це письмово як окремий документ або частину політики безпеки. План має охоплювати: ролі команди реагування (кому дзвонити при вірусі, при DDoS, при витоку?), які рішення хто приймає (наприклад, тільки директор може вирішити відключити всю лікарняну мережу, але IT-безпека може ізолювати окремий сегмент самостійно).<br>Наявність контактів: у IRP додати список актуальних контактів – від внутрішніх (директор, головлікар, керівники підрозділів) до зовнішніх (кіберполіція, експерти, постачальники, CERT). Регулярно оновлювати ці телефони/email. 3) Підготовка інструментів та доступів: заздалегідь забезпечити, щоб команда реагування мала необхідні привілеї (наприклад, адмін безпеки має логіни до всіх серверів, DPO має доступ до журналів), а також інструменти (завантажувальні антивірусні флешки, запасне серверне обладнання, чисті ноутбуки для розслідування). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Аналіз інцидентів (RS.AN: Incident Analysis) – проводиться детальний аналіз інциденту, щоб зрозуміти його масштаб, вплив, причини; інформація корелюється з різних джерел, встановлюється хронологія подій. | Під час реагування дуже важливо правильно оцінити ситуацію, щоб приймати адекватні рішення. Рекомендації:<br>Виділити окрему роль аналітика в команді реагування, який займеться збіркою даних, поки інші стримують. Це може бути той самий IT-безпековець, або зовнішній експерт.<br>Збір даних: аналітик бере лог-файли, знімає зразки шкідливого ПЗ (якщо є), опитує персонал, який першим помітив, дивиться на часову шкалу. Питання: коли почалося? які системи постраждали? який вектор атаки?<br>Використання форензік-методів: якщо підозрюємо серйозний злочин або треба зберегти докази – залучити спеціаліста з комп'ютерної криміналістики. Наприклад, зняти образ диска зламаного сервера для подальшого аналізу, і працювати вже на копії (щоб не зіпсувати докази). Використовувати Write-blockers, фіксувати хеші. У лікарні може не бути експертизи – варто мати контакти фірм, хто цим займається, на випадок критичного інциденту.<br>Оцінка впливу: швидко визначити, які дані або сервіси зачеплені. Якщо витік – що витекло (ПІБ, діагнози?), скількох пацієнтів? Якщо шифрування – які системи недоступні? Це потрібно і для комунікації керівництву, і для вирішення про повідомлення постраждалих (GDPR 72 години). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Комунікація та координація (RS.CO: Incident Response Communications & Coordination) – відбувається скоординована внутрішня і зовнішня комунікація під час або після інциденту; інформація ділиться з відповідними внутрішніми підрозділами, з керівництвом, з правоохоронцями, з постраждалими особами та з громадськістю, якщо потрібно. | У медичному закладі при серйозному інциденті може виникнути паніка або неправильні дії, якщо не налагоджена комунікація. Рекомендації:<br>Визначити спікера: хто від імені лікарні говорить із зовнішнім світом (зазвичай директор або PR-служба, якщо є). У плані реагування прописати: всі запити ЗМІ або клієнтів щодо інциденту – перенаправляти на визначеного спікера. Персонал не повинен на свій розсуд коментувати, щоб не поширювати неточну інформацію. Внутрішня комунікація: оповістити співробітників про те, що сталося і як діяти. Наприклад, "Увага, вірусна атака, не вмикайте комп'ютери, чекайте інструкцій". Для цього бажано мати альтернативні канали зв'язку – розсилку SMS або месенджер групу, на випадок якщо корпоративна мережа/пошта недоступна. Також, якщо інцидент впливає на роботу (наприклад, припинили прийом пацієнтів через IT-збій) – чітко довести персоналу, що казати пацієнтам (наприклад: "Вибачте, технічна перерва, ваші дані в безпеці, ми скоро відновимо роботу" – щоб не викликати паніки). Зовнішня комунікація (пацієнти, партнери): якщо стався витік даних, GDPR вимагає повідомляти постраждалих. Підготувати шаблони таких повідомлень: що сталося, які дані, що лікарня робить для виправлення, контакт для деталей. |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Пом’якшення (RS.MI: Mitigation) – здійснюються дії для запобігання поширенню інциденту та його ерадикації (усунення); інциденти локалізуються і ліквідовуються. | Пом’якшення – практично, це конкретні технічні кроки з ліквідації загрози. Частково вже описано у Incident Management (стримування, локалізація). Додамо:<br>Ерадикація (eradication): після локалізації (зупинення поширення) потрібно видалити причини. Напр., якщо це вірус – очистити або перевстановити всі заражені системи, видалити шкідливі файли. Якщо злом – закрити уразливість (поставити патч, змінити конфіг, оновити паролі). Важливо не повертати систему в роботу, поки не впевнені, що загроза усунена – інакше повториться.<br>Перевірка систем: після очищення – провести повний скан антивірусом, перевірку хешів критичних файлів (може, backdoor лишився). Можливо, запустити систему в ізольованому середовищі для моніторингу, чи не стучить нікуди. Якщо сумніви – краще повна перевстановлення ОС із чистого образу, ніж ризикувати. Інспекція сусідніх систем: якщо одна машина заражена, перевірити ті, що з нею взаємодіяли. Можливо, теж інфіковані. Пошук “залишків” атаки: зловмисники можуть залишити облікові записи, планувальники завдань, тощо. Переглянути користувачів, автозапуски, відкриті порти – чи все легітимне. Відновлення чистих даних: якщо дані пошкоджені (шифрування, видалення) – підняти з резервних копій. Переконатися, що резервні копії теж чисті (сканувати їх перед розгортанням). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| Категорія RECOVER | Рекомендації щодо реалізації |
|---|---|
| Виконання планів відновлення (RC.RP: Incident Recovery Plan Execution) – заходи з відновлення систем і послуг виконуються згідно з планом відновлення, щоб забезпечити оперативну доступність систем та сервісів, що постраждали. | Ця категорія відповідає на питання: як повернутись до нормальної роботи після інциденту. Багато з цього перекривається з планом аварійного відновлення (DRP) в рамках BCP, але з фокусом саме на кіберінциденти. Рекомендації: Мати заздалегідь розроблений план відновлення (Recovery Plan): описує кроки перезапуску систем, пріоритетність відновлення сервісів (наприклад, спочатку – реанімація IT-система моніторингу пацієнтів, потім – реєстратура, потім – другорядні). Цей план може бути частиною загального BCP. Резервні середовища: якщо є резервні майданчики або хмарні бекапи – в плані вказати, коли переключатись на них. Наприклад, якщо сервер з ЕМК знищено вірусом – чи є можливість підняти його образ на хмарі? План має містити інструкцію: де зберігаються образи, як розгорнути, які конфігурції внести (IP адреси, підключення). Пріоритет бізнес-функцій: тісно співвідноситься з кроком 1 – визначити, які функції відновлюємо першими. У медзакладі: можливо, критично запустити систему виписки рецептів, щоб пацієнти отримували ліки, навіть якщо доведеться відкласти відновлення системи статистики на тиждень. Часові рамки (RTO/RPO): для кожної ключової системи визначити цільовий час відновлення (RTO) і точку відновлення (RPO). |

Продовження Додатку Б

Таблиця 3.3 Методичні рекомендації згідно NIST CSF 2.0

| | |
|---|---|
| Комунікації по відновленню (RC.CO: Recovery Communications) – внутрішні та зовнішні комунікації щодо статусу відновлення проводяться, за необхідності; зацікавлені сторони (керівництво, клієнти, партнери) проінформовані про оновлений статус. | Ця категорія доповнює комунікацію в Respond, акцентуючи на сповіщеннях під час саме фази відновлення. Рекомендації: Інформування керівництва про прогрес: поки IT працює над відновленням, керівництво (директор, головлікар) має отримувати регулярні оновлення: “Сервери розгорнуті, залишилось підключити базу, орієнтовно ще 1 година”, щоб вони могли планувати, коли відновити прийом пацієнтів, наприклад. Оновлення для персоналу: працівники мають знати, як йде процес. Наприклад, щогодини розсилати повідомлення: “Станом на 12:00 відновлено 3 з 5 модулів системи, очікуйте повного відновлення до 14:00, наразі продовжуйте працювати в паперовому режимі”. Це знижує напругу і допомагає уникнути дезінформації/чуток. Повідомлення пацієнтів: якщо інцидент був публічним (пацієнти про нього знали, бо, скажімо, прийом був зупинений або вони отримали повідомлення про витік), після відновлення корисно проінформувати їх: “Наші системи знову в строю, ви можете отримувати послуги в повному обсязі. Ми впровадили додаткові заходи захисту”. Це покаже, що ситуацію вирішено. |

**Додаток В**

**Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки**

| Етап / Завдання | Відповідальні | Термін виконання | Очікувані результати | Пріоритет |
|---|---|---|---|---|
| Етап І: Оцінка та підготовка (Start) | Керівництво закладу;<br>ІТ-відділ;<br>DPO/Юрист | 1-й місяць | Створено робочу групу з кібербезпеки;<br>Виконано базову оцінку ризиків та аудит поточної безпеки;<br>Визначено прогалини щодо HIPAA/GDPR/NIST;<br>Затверджено політику керівництва щодо підвищення кібербезпеки. | Високий (необхідна основа для інших етапів) |
| Провести інвентаризацію ІТ-активів та даних (Asset Inventory) | ІТ-адміністратори;<br>Завідувачі відділень | 1-й місяць | Складено повний реєстр апаратних і програмних активів, інформаційних систем та сховищ даних (включно з паперовими архівами); | Високий (основа для планування захисту) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Провести інвентаризацію IT-активів та даних (Asset Inventory) | IT-адміністратори;<br>Завідувачі відділень | 1-й місяць | Дані класифіковано за чутливістю (медичні, персональні, службові);<br>Виявлено застарілі та неавторизовані системи. | Високий (основа для планування захисту) |
| Призначити відповідальних осіб (CISO/безпека, DPO) | Головний лікар / Директор | 1-й місяць | Наказом призначено відповідального за інформаційну безпеку (CISO/ISO);<br>Призначено офіцера із захисту даних (DPO) (за потреби, суміщено з юристом);<br>Визначено склад комітету з кібербезпеки (IT, юридичний, клінічний представники). | Високий (необхідно для управління) |
| Розробити первинний план заходів та бюджет | Робоча група з кібербезпеки | 2-й місяць | Створено план дій на основі оцінки ризиків (що впровадити в | Високий (визначає подальші кроки) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Розробити первинний план заходів та бюджет | Робоча група з кібербезпеки | 2-й місяць | першу чергу: наприклад, резервне копіювання, MFA, навчання);<br>Підготовлено орієнтовний бюджет (ліцензії, обладнання, навчання);<br>Керівництво затвердило план і забезпечило ресурсами. | Високий (визначає подальші кроки) |
| Етап II: Політики, процедури та швидкі перемоги (Policies & Quick Wins) | Відповідальні | Термін виконання | Очікувані результати | Пріоритет |
| Розробити та затвердити комплекс політик безпеки | CISO / IT-безпека;<br>DPO;<br>Юридичний відділ | 2–3-й місяць | Створено політики: інформаційної безпеки, управління доступом, користування IT-ресурсами, | Високий (створює нормативну базу для змін) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Розробити та затвердити комплекс політик безпеки | CISO / IT-безпека;<br>DPO;<br>Юридичний відділ | 2–3-й місяць | реагування на інциденти, політика збереження даних тощо;<br>Політики узгоджені з вимогами HIPAA/GDPR (включно з конфіденційністю пацієнтів, правами суб'єктів);<br>Наказом керівника політики введені в дію і розіслані персоналу. | Високий (створює нормативну базу для змін) |
| Налаштувати резервне копіювання критичних даних (Quick Win) | IT-адміністратор систем;<br>Зав.відділом IT | 2-й місяць | Реалізовано щоденне резервне копіювання баз даних пацієнтів на віддалений носій або в хмару;<br>Перевірено відновлення з бекапу на тестовому сервері (успішно); | Високий (негайно знижує ризик катастрофічної втрати даних) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Налаштувати резервне копіювання критичних даних (Quick Win) | IT-адміністратор систем;<br>Зав.відділом IT | 2-й місяць | Встановлено процедуру зберігання резервних копій поза основним приміщенням (наприклад, в іншій локації). | Високий (негайно знижує ризик катастрофічної втрати даних) |
| Впровадити контроль фізичного доступу до серверної і архівів | Служба безпеки закладу;<br>Системний адміністратор | 2–4-й місяць | Встановлено замки/систему карткового доступу до серверної;<br>Складено список осіб з дозволом доступу, доступ сторонніх заборонено;<br>Журнал відвідувань серверної ведеться охороною;- Архіви з паперовими картами переміщено в кімнату, що замикається, доступ лише уповноваженим. | Високий (швидко вирішує фізичні уразливості) |

| | | | | |
|---|---|---|---|---|
| Налаштувати базові засоби мережевої безпеки (Quick Win) | Мережевий інженер;<br>Адмін систем | 3-й місяць | Оновлено конфігурацію міжмережевого екрану: закрито несанкціоновані порти, дозволено лише необхідні з’єднання;<br>Впроваджено розділення Wi-Fi: гостьовий Wi-Fi ізольовано від внутрішньої мережі;<br>Установлено та налаштовано базову IDS (наприклад, включено функції в наявному фаєрволі) для моніторингу трафіку на периметрі. | Високий (захищає від зовнішніх атак з мінімальними витратами) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Запровадити багатофакторну автентифікацію (MFA) на віддалений доступ та ключові системи | IT-адмін систем;<br>Керівники підрозділів | 3–5-й місяць | Налаштовано MFA для VPN-доступу до мережі лікарні;<br>MFA ввімкнено для облікових записів адміністраторів та лікарів у системі електронних медичних записів (використання мобільного додатку або апаратного токена);<br>Проведено інструктаж персоналу щодо використання MFA токенів/додатків. | Високий (суттєво підвищує захист облікових записів) |
| Провести первинне навчання персоналу з кібербезпеки | DPO / Юрист;<br>CISO / IT-безпека;<br>Відділ кадрів | 4-й місяць | 100% співробітників, що працюють з даними, пройшли тренінг: основи захисту даних пацієнтів, правила користування | Високий (адресує людський фактор) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Провести первинне навчання персоналу з кібербезпеки | DPO / Юрист;<br>CISO / IT-безпека;<br>Відділ кадрів | 4-й місяць | комп’ютером (паролі, USB, email-фішинг);<br>Зібрано підписи/тести, що підтверджують засвоєння матеріалу;<br>Нові працівники включені в програму навчання (вступний інструктаж). | Високий (адресує людський фактор) |
| Етап III: Технічна модернізація та впровадження контролів (Implement Controls) | Відповідальні | Термін виконання | Очікувані результати | Пріоритет |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Впровадити систему керування логами та моніторинг (SIEM) | IT-адмін безпеки;<br>Системний адміністратор | 4–6-й місяць | Розгорнуто SIEM-платформу (або центральний syslog-сервер);<br>Налаштовано збір журналів з серверів, мережевого обладнання, баз даних;<br>Встановлено базові кореляційні правила (спроби входу, аномалії трафіку);<br>Відповідальний спеціаліст проходить навчання роботі з SIEM (або підключено MSSP – зовнішній SOC). | Середній (після базових заходів, щоб не перевантажити до готовності) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Удосконалити контроль доступу та управління обліковками | Системний адміністратор (AD);<br>Відділ кадрів | 5–6-й місяць | Впроваджено централізоване управління обліковими записами (Active Directory) для всіх користувачів;<br>Налаштовано політики паролів (мін. довжина 10, складність, зміна кожні 180 днів);<br>Створено процедуру негайної деактивації обліковки при звільненні співробітника (HR повідомляє IT в день звільнення);<br>Проведено чистку “старих” акаунтів (видалено або відключено невикористовувані облікові записи). | Високий (завершує налаштування доступів, критично для безпеки) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Модернізувати антивірусний захист (Endpoint Security) | CISO / IT-безпека;<br>Адмін робочих станцій | 5–7-й місяць | Встановлено сучасне антивірусне ПЗ (або EDR) на всі сервери і робочі станції (замінено застаріле, якщо було);<br>Налаштовано централізовану консоль моніторингу вірусних інцидентів;<br>Включено автоматичне оновлення антивірусних баз та сканування за розкладом;<br>Проведено навчання IT-персоналу щодо реагування на виявлення (ізоляція хоста, аналіз карантину). | Середній (важливо, але базовий антивірус напевно вже був; EDR – покращення) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Відокремити та захистити медичне обладнання в мережі | Мережевий інженер;<br>Біомед. інженер | 6–8-й місяць | Медичні прилади (МРТ, КТ, монітори) винесені в окремий VLAN з мінімально необхідним доступом;- На мережевому рівні застосовано фільтрацію: обладнання не має доступу до інтернету, тільки до потрібних серверів;<br>Впроваджено регулярний аудит конфігурації цих пристроїв, перевірено наявність оновлень прошивки від виробників;<br>Для пристроїв без оновлень впроваджено компенсуючі заходи (ізоляція, моніторинг трафіку). | Середній (закриває потенційно уразливий напрямок – IoT/медобладнання) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Реалізувати шифрування даних і носіїв | Системний адміністратор;<br>CISO / IT-безпека | 6–8-й місяць | Увімкнено шифрування дисків на серверних масивах з базами даних (BitLocker, LUKS або СУБД-рівень);<br>Робочі ноутбуки лікарів/керівництва зашифровані (BitLocker з TPM);<br>Визначено правило: всі резервні копії на знімних носіях зберігаються тільки у зашифрованому вигляді;<br>Портативні носії (USB) заблоковані політикою або дозволені тільки з апаратним шифруванням. | Середній (підвищує захищеність, але потребує підготовки користувачів і IT) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| Етап IV: Тестування, навчання, відповідність нормативам (Test & Compliance) | Відповідальні | Термін виконання | Очікувані результати | Пріоритет |
|---|---|---|---|---|
| Провести планове тестування планів реагування та відновлення | CISO / ІБ;<br>Команда реагування (ІТ, безпека, управлінці) | 8-й місяць | Проведено імітацію інциденту (наприклад, вірус-шифрувальник) в форматі настільного навчання: команда зібралась і відпрацювала дії за Incident Response Plan;<br>Виявлено та задокументовано вдосконалення в план реагування (оновлено контакти, уточнено ролі). Також проведено тест відновлення: взято резервну копію ключової системи. | Середній (важливо для готовності, після впровадження основних технологій) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Актуалізувати та протестувати процедури виконання прав суб’єктів (GDPR) | DPO;<br>Відділ кадрів;<br>IT-адмін БД | 8–9-й місяць | Перевірено на практиці: пацієнт подав запит на доступ до своїх даних – протягом 5 днів сформовано повний витяг з ЕМК;<br>Випадок запиту на виправлення: протестовано процес коригування запису і логування змін;<br>DPO оновив реєстр обробок даних із урахуванням нових IT-систем (з’явились підсистеми) та впроваджених заходів безпеки;<br>Персонал проінформований, як реагувати на запити пацієнтів (кого інформувати – DPO). | Середній (для відповідності GDPR та кращого сервісу пацієнтам) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Здійснити внутрішній аудит відповідності HIPAA/GDPR/NIST | Внутрішній аудитор (або зовнішній консультант);<br>DPO;<br>CISO | 9-й місяць | Проведено аудит: переглянуто політики, журнали, налаштування систем на відповідність вимогам (чи виконуються Safeguards HIPAA, статті GDPR);<br>Відзначено суттєвий прогрес: більшість контролів впроваджено;- Складено перелік невеликих невідповідностей або зон для покращення (наприклад, необхідність оновити договір з одним із постачальників під GDPR Art.28);<br>Керівництву представлено звіт з оцінкою рівня захищеності “до/після”. | Високий (для оцінки результатів проекту, підготовка до зовн.перевірок) |

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Підвищити рівень обізнаності: фішинг-симуляція, додаткові тренінги | CISO / ІБ;<br>Відділ кадрів;<br>DPO | 9–10-й місяць | Проведено несподіваний тест-фішинг для персоналу: розіслано навчальні листи-імітації, ~X% співробітників "попалися" – з ними проведено додаткову сесію навчання;<br>Розроблено пам’ятку для лікарів щодо захисту конфіденційності пацієнтів (роздано і вивішено у відділеннях);<br>На регулярних зборах медперсоналу включена 5-хвилинка про кібергігієну (раз на місяць). | Середній (закріплює культуру безпеки, безперервний процес) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| Етап V: Безперервне вдосконалення та підтримка (Continuous Improvement) | Відповідальні | Термін виконання | Очікувані результати | Пріоритет |
|---|---|---|---|---|
| Впровадити процес перегляду інцидентів та оновлення заходів | Комітет з кібербезпеки (CISO, DPO, IT, керівництво) | Постійно (з 10-го місяця – далі щокварталу) | Створено постійну комісію (зустріч щокварталу) для аналізу безпеки: розглядаються події минулого кварталу, виконання політик, нові ризики;<br>За підсумками кожної зустрічі – коригування: напр. “оновити ПО X до останньої версії”, “провести позаплановий тренінг через новий тип шахрайства”. Керівництву надається щоквартальний звіт з показниками. | Середній (забезпечує підтримку досягнутого рівня і рух вперед) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Отримати сертифікацію або провести зовнішній аудит (опц.) | Керівництво;<br>DPO;<br>CISO | ~12-й місяць (або пізніше) | (Опціонально, якщо потрібно) Пройдено зовнішній аудит/сертифікація на відповідність, наприклад, вимогам ISO 27001 / "Додатку з охорони здоров'я" або отримано лист-висновок від незалежних експертів про дотримання HIPAA Security Rule та основних положень GDPR;<br>Це підтвердило високий рівень захисту даних у закладі і підвищило довіру партнерів. | Середній/Низький (не обов'язково, залежно від стратегічних цілей) |
| Підготовка підсумкового звіту та плану на наступний період | CISO;<br>DPO;<br>Внутрішній аудит | 12-й місяць | Підготовлено детальний звіт про реалізацію проекту кібербезпеки: виконані заходи, порівняння стану | Середній (закріплює результати, планує наступні кроки) |

Додаток В

Таблиця 3.5 Дорожня карта впровадження заходів кібербезпеки

| | | | | |
|---|---|---|---|---|
| Підготовка підсумкового звіту та плану на наступний період | CISO;<br>DPO;<br>Внутрішній аудит | 12-й місяць | "До і Після" (в т.ч. результати аудиту, показники);<br>Оновлено документи: реєстр ризиків (більшість ризиків знижено), реєстр активів (доповнено новим обладнанням, встановленим для безпеки, напр. фаєрвол), політики (актуалізовані за рік);<br>Розроблено новий план удосконалень на наступний рік (наприклад, впровадження DLP, розширене резервування, участь у галузевих кібервченнях тощо). | Середній (закріплює результати, планує наступні кроки) |

## Додаток Г

**Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження**

| Адміністративна вимога HIPAA | Рекомендації щодо впровадження в медзакладі |
|---|---|
| Аналіз та управління ризиками – провести точну і повну оцінку ризиків для всіх систем, що містять ePHI; впровадити заходи для зменшення ризиків до прийнятного рівня. | Створити робочу групу з кібербезпеки (залучити IT-фахівців, клінічних інженерів, адміністрацію). Провести початковий аналіз ризиків: виявити всі джерела та носії ePHI (медичні інформаційні системи, бази даних, паперові архіви, мобільні пристрої тощо), оцінити потенційні загрози (кібератаки, віруси, витоки через помилки персоналу) і вразливості. На основі аналізу сформувати перелік ризиків з оцінкою їхньої ймовірності та впливу. Далі розробити план обробки ризиків – визначити, які заходи потрібно реалізувати першочергово (наприклад, резервне копіювання для критичних систем, усунення застарілого програмного забезпечення, посилення захисту мережі). Регулярно (наприклад, щорічно) переглядати та оновлювати оцінку ризиків з урахуванням змін (впровадження нових IT-систем, поява нових кіберзагроз). |
| Призначення відповідального за безпеку – визначити посадову особу, відповідальну за розвиток і впровадження заходів безпеки (Security Officer). | Офіційно призначити відповідального за інформаційну безпека закладу. На цю роль підходить керівник IT-відділу або окремий фахівець із кібербезпеки. В його посадовій інструкції прописати повноваження: розробка політик безпеки, контроль їх виконання, моніторинг подій, реагування на інциденти. Забезпечити пряме підпорядкування цього спеціаліста керівнику закладу для належного рівня впливу. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Контроль кадрового доступу (Workforce Security) – забезпечити, щоб доступ до ePHI мали лише уповноважені працівники; налаштувати процеси авторизації, нагляду та усунення доступу при звільненні. | Запровадити політику розмежування доступу персоналу: визначити, які категорії співробітників до яких даних можуть доступатися відповідно до їхніх службових обов'язків (принцип мінімально необхідних привілеїв). Для нового працівника передбачити процедуру надання доступів: лише після тренінгу з безпеки та дозволу керівника підрозділу. Для звільнених або переведених співробітників – негайне скасування доступу (деактивація облікових записів у системах, вилучення ключів/карт доступу тощо). Встановити журнал перевірки актуальності прав доступу щоквартально: адміністратор IT переглядає списки активних облікових записів і підтверджує з керівниками відділів, що доступи є обґрунтованими. |
| Управління доступом до інформації – реалізувати політики та процедури авторизації доступу до ePHI відповідно до ролей і службових обов'язків (принцип "мінімально необхідного"). | Документувати матрицю доступу для всіх IT-систем: які ролі (лікарі, медсестри, реєстратори, технічний персонал) які дії можуть виконувати в медичних системах (читати дані, редагувати, видаляти). Налаштувати рольовий доступ у програмному забезпеченні: наприклад, лікар бачить дані тільки своїх пацієнтів, а не всіх; лабораторія може вносити результати аналізів, але не змінювати діагнози тощо. Заборонити спільне використання облікових записів – у кожного користувача має бути свій унікальний логін. Забезпечити автентифікацію користувачів (паролі, апаратні токени або двофакторна авторизація – детальніше у технічних заходах нижче). |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Програма навчання з безпеки – навчати весь персонал політикам та процедурам безпеки; передбачити санкції за порушення. | Розробити та проводити регулярні тренінги з інформаційної безпеки для співробітників. При прийомі на роботу – вступний курс, що охоплює основи захисту даних, правила використання інформаційних систем, заборону розголошення конфіденційної інформації (підписати угоду про нерозголошення). Після цього – щорічно обов'язкове навчання/атестація (онлайн-тести або семінари) щодо актуальних політик і нових загроз (фішинг, соціальна інженерія тощо). Включити спеціальні модулі для медичного |

| | |
|---|---|
| | персоналу про важливість конфіденційності (наприклад, нагадати про випадки, коли за розголошення PHI працівників звільняли). Встановити дисциплінарні заходи за порушення політик безпеки: від догани до звільнення залежно від тяжкості (як-от неправомірний доступ до чужих записів, публікація конфіденційних даних пацієнта тощо – це тягне негайне звільнення). Керівництву слід демонструвати приклад прихильності до принципів безпеки, формувати культуру захисту даних. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Процедури реагування на інциденти – виявляти та реагувати на підозрілі або відомі інциденти безпеки, пом'якшувати їх наслідки; документувати інциденти та результати розслідування. | Розробити формальний План реагування на інциденти (Incident Response Plan). Призначити команду реагування (включаючи IT-фахівця, представника керівництва, юридичного консультанта, якщо є). Описати кроки при виявленні інциденту: Виявлення та повідомлення – співробітники мають негайно повідомити IT-відділ про підозрілі події (вірус на комп'ютері, втрата ноутбука з даними, несанкціонований вхід у систему тощо). Утримання і аналіз – IT-відділ ізолює уражене обладнання або акаунт, збирає журнали, визначає масштаб проблеми. 3) Пом'якшення – вжити заходів для зупинення або обмеження інциденту (відключити заражений сегмент мережі, відкликати скомпрометовані облікові записи, застосувати патчі). Відновлення – відновити системи з резервних копій (якщо було пошкодження даних), перевірити цілісність ePHI. 5) Повідомлення – якщо стався значний витік персональних даних, підготувати офіційні повідомлення керівництву, пацієнтам і, за потреби, регуляторам (враховуючи вимоги українського законодавства та GDPR щодо повідомлення про витоки протягом 72 годин). Документування – фіксувати кожен інцидент в журналі: дата, суть, які дії вжито, результати розслідування, уроки на майбутнє. Після ліквідації – провести аналіз першопричин і впровадити заходи, щоб подібне не повторилося (модифікувати політики, навчити персонал, посилити контроль). |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Планування на випадок надзвичайних ситуацій (Contingency Plan) – мати плани резервного копіювання, відновлення даних та | Розробити план забезпечення безперервності діяльності (BCP) і план відновлення після збою (DRP) спеціально для IT-систем з пацієнтськими даними. Основні компоненти: Резервне копіювання даних – налаштувати регулярне автоматичне резервне копіювання баз даних електронних медичних записів на захищений сервер чи хмарне сховище. Перевіряти відновлюваність резервних копій (тестове відновлення хоча б раз на квартал). |

| | |
|---|---|
| функціонування в надзвичайному режимі для захисту ePHI. | План аварійного відновлення – прописати, як діяти у разі збою основної інформаційної системи: хто відповідає за запуск резервних серверів, як перемикнути користувачів на резервну систему чи журналювання на папері.<br>Екстрений режим роботи – визначити, як буде надаватися медична допомога, якщо IT-системи недоступні (наприклад, використання паперових форм для запису даних з наступним їх внесенням після відновлення систем). Забезпечити наявність необхідного обладнання (резервні джерела живлення для серверів, дублюючі мережеві канали).<br>Відповідальні особи та контакти – список ключових працівників (IT-інженери, постачальники програмного забезпечення) з телефонами для екстреного зв'язку. Регулярно актуалізувати цей план та проводити навчання персоналу щодо дій за надзвичайних ситуацій. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Періодична оцінка ефективності заходів (Evaluation) – періодично проводити технічну та нетехнічну переоцінку, наскільки реалізовані політики та заходи відповідають вимогам HIPAA. | Встановити процес внутрішнього аудиту безпеки. Щонайменше раз на рік аудиторська група (внутрішня або із залученням зовнішніх експертів) перевіряє відповідність практик закладу вимогам політик та стандартів (HIPAA, GDPR, локальні інструкції). Аудит включає: аналіз актуальності політик, перевірку журналів доступу та подій безпеки, опитування співробітників щодо знання процедур, тестування вибіркових контрольних точок (наприклад, спроба зайти під нечинним акаунтом має бути заблокована, резервні копії відновлюються за нормований час тощо). За результатами оцінки готується звіт з переліком невідповідностей та рекомендаціями. Керівництво затверджує план коригувальних дій та виділяє ресурси на усунення недоліків. Крім планових оцінок, слід проводити позапланові – після серйозних змін (впровадження нового ПО, інфраструктури) або значних інцидентів – аби перевірити, чи не з'явилися нові ризики. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Угоди з постачальниками (Business Associate Agreements) – перед передачею чи наданням доступу до ePHI стороннім особам/організаціям необхідно укласти письмову угоду, що зобов'язує їх забезпечувати захист інформації згідно з вимогами HIPAA. | Визначити коло сторонніх організацій (контрагентів), які отримують або обробляють дані пацієнтів: наприклад, хмарні провайдери для зберігання даних, сторонні лабораторії, страхові компанії, IT-підрядники, що обслуговують медичне ПО. З кожним таким партнером необхідно підписати договір про конфіденційність та захист даних (аналог Business Associate Agreement). В угоді прописати: допустимі цілі використання даних, заходи безпеки, яких має дотримуватись партнер (включно з вимогами HIPAA/GDPR щодо збереження даних, повідомлення про інциденти не пізніше X годин після виявлення тощо), відповідальність за порушення. Переконатися, що контрагент розуміє свої зобов'язання і також дотримується принципу мінімізації (отримує лише необхідний обсяг даних). Вести реєстр таких угод, переглядати їх при оновленні нормативних вимог або зміні умов співпраці. |
| Політики, процедури та документація – розробити письмові політики й процедури з безпеки, забезпечити їх дотримання та зберігання | Створити пакет внутрішніх політик інформаційної безпеки: політика класифікації інформації, політика керування доступом, політика використання електронної пошти та інтернету, політика реагування на інциденти, політика зберігання та знищення даних тощо. Кожна політика повинна бути затверджена керівництвом і доведена до відома співробітників (під підпис або електронне підтвердження). Також оформити операційні процедури (стандартні операційні інструкції) для IT-персоналу: наприклад, порядок |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| документації не менше 6 років (вимога HIPAA). | створення облікового запису для нового співробітника, процедура резервного копіювання, порядок встановлення патчів. Документувати всі дії, пов'язані з безпекою: звіти аналізу ризиків, результати навчань, журнали інцидентів, акти знищення носіїв – і зберігати ці записи у визначеному архіві. HIPAA вимагає зберігати документацію не менше 6 років, тому слід завести як електронний, так і паперовий архів політик та |

| | |
|---|---|
| | записів аудиту. Це також стане в нагоді у разі перевірок або розслідувань інцидентів – наявність належної документації демонструє проактивність закладу у захисті даних. |
| Фізичний захід HIPAA | Рекомендації щодо реалізації |
| Контроль фізичного доступу (Facility Access Control) – обмежити фізичний доступ до інформаційних систем і приміщень, де вони знаходяться, тільки уповноваженим особам. | Переглянути захищені зони закладу: серверні, архіви з паперовими картками, кабінети лікарів, де є комп'ютери з чутливими даними. Забезпечити систему контролю доступу – магнітні картки або ключі для входу до серверної/архіву лише відповідальному IT-персоналу або завідувачу. На reception та інших зонах – режим пропускної системи для відвідувачів: журнали реєстрації, бейджі для гостей у відділеннях. Встановити камери відеоспостереження у ключових зонах (серверна, коридори біля архіву) – зберігати записи, перевіряти їх при інцидентах. Забезпечити, щоб двері до серверної завжди були зачинені, а доступ мав обмежене коло осіб. Періодично перевіряти журнали доступу (хто заходив і коли) та ревізувати списки допущених осіб. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Безпечне використання робочих місць (Workstation Use & Security) – встановити правила належного використання і розміщення робочих станцій, що мають доступ до ePHI. | Розробити інструкції для співробітників щодо безпечної роботи з комп'ютерами та іншими пристроями: 1) Розташування екранів – монітори на робочих місцях пацієнтоорієнтованого персоналу (реєстратура, пост медсестер) слід повертати так, щоб екран не був видимий пацієнтам чи відвідувачам за спиною. Використати захисні екрани-фільтри (privacy filters) на моніторах, якщо є ризик підглядання через плече. 2) Автоматичне блокування – налаштувати, щоб кожна робоча станція автоматично блокувалася через короткий проміжок неактивності (наприклад, 5-10 хвилин). Навчити персонал блокувати екран вручну щоразу, коли він відходить від ПК (комбінація клавіш або кнопка). 3) Вхід до систем за паролем – впровадити політику сильних паролів для входу в операційну систему. Фізично закріпити робочі комп'ютери, якщо вони знаходяться у зонах доступних пацієнтам (наприклад, прикріпленням до столу, щоб унеможливити крадіжку пристрою). 4) Чистий стіл – заборонити залишати на столі паперові медичні документи чи записи, що містять персональні дані, після закінчення роботи; вони мають зберігатися в закритих шухлядах або знищуватися. Провести |

| | |
|---|---|
| | довідники для пацієнтів у зоні очікування, щоб пояснювали політику конфіденційності, аби пацієнти теж розуміли, чому, наприклад, їх можуть попросити відійти, поки медсестра працює з комп’ютером. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Контроль пристроїв та носіїв (Device & Media Controls) – політики поводження з апаратним забезпеченням та електронними носіями, що містять ePHI: отримання, переміщення, знищення носіїв, утилізація або повторне використання після очищення. | Скласти реєстр всіх пристроїв, де зберігаються або можуть зберігатися медичні дані: сервери, системні блоки, ноутбуки лікарів, зовнішні жорсткі диски для резервних копій, флешки, планшети з медсистемами, навіть смартфони, якщо на них є службова поштова скринька з даними пацієнтів. Отримання і інвентаризація – при надходженні нового обладнання вносити його до реєстру, присвоювати інвентарний номер; зафіксувати відповідальну особу (наприклад, ноутбук №5 – закріплений за завідуючим відділення). Переміщення – регламентувати винос пристроїв за межі закладу: заборонити без дозволу виносити ноутбуки чи паперові архіви додому; якщо дозволено, то лише за письмовим погодженням і з шифруванням даних. Зберігання носіїв – всі резервні копії на фізичних носіях (стрічки, диски) зберігати у сейфах або в охоронюваних приміщеннях. Обмежити коло осіб, що мають доступ до них. Утилізація та повторне використання – впровадити процедуру безпечного знищення носіїв, що містили ePHI. Наприклад, жорсткі диски перед списанням – або апаратно знищувати (дроблення, шредер для дисків), або проводити багаторазове перезаписування даних спеціальними утилітами (wipe). Те ж саме для паперових носіїв – обладнати шредери в усіх відділеннях і вимагати знищення документів, а не викидання у смітник. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| Технічний контроль HIPAA | Рекомендації з реалізації |
|---|---|
| Контроль доступу (Access Control) – технічні засоби, що дозволяють доступ до ePHI лише авторизованим особам. HIPAA вимагає унікальних користувацьких ID, екстреного доступу, автоматичного завершення сесії та шифрування даних, коли це доцільно (addressable). | Реалізувати багаторівневу систему керування доступом до електронних медичних систем: 1) Унікальні облікові записи – кожен співробітник має свій логін і надійний пароль. Використовувати централізовану директорію (напр. Active Directory) для керування обліковими записами і правами. 2) Розмежування прав – інтегрувати налаштування ролей (див. вище про матрицю доступу). 3) Мультифакторна автентифікація (MFA) – запровадити MFA для віддаленого доступу до систем (VPN, доступ до електронної медичної системи з дому) або для привілейованих акаунтів адміністраторів. Це суттєво знизить ризик компрометації облікових записів. 4) Автоматичне завершення сеансу – налаштувати інформаційні системи так, щоб після визначеного періоду бездіяльності користувача сеанс завершувався (користувача викидало із системи, і потрібно увійти знову). Також реалізувати політику "один сеанс": користувач не може бути одночасно залогований в системі з двох різних пристроїв. 5) Шифрування даних – увімкнути шифрування баз даних та файлів, що містять ePHI, на рівні серверів (або принаймні шифрувати диски серверів). На робочих станціях лікарів використовувати шифрування дисків (BitLocker або аналог) – це захистить дані у разі крадіжки пристрою. При передаванні даних між сервером і клієнтом – використовувати |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| | тільки захищені протоколи (HTTPS, TLS1.2+). Таким чином, навіть якщо зловмисник перехопить трафік чи отримає доступ до диску, дані будуть у зашифрованому вигляді. Для надзвичайних ситуацій налаштувати екстрений доступ: наприклад, створити зарезервований обліковий запис адміністратора, пароль до якого зберігати в запечатаному конверті у сейфі – для використання лише у випадку, коли звичайні механізми автентифікації не працюють. |

| | |
|---|---|
| Аудит-логування (Audit Controls) – апаратні чи програмні механізми для запису та перегляду активності систем, що містять ePHI. | Увімкнути журнали аудиту в усіх критичних системах: електронна медична інформаційна система (EMIC), система лабораторних інформацій, сервери баз даних, файлові сховища. Логувати принаймні: спроби входу (успішні і невдалі) із зазначенням користувача, час і IP-адреси; доступ до записів пацієнтів (хто переглядав чи змінював); дії адміністраторів (створення/видалення користувачів, зміна прав, видалення даних). Централізувати збір логів за допомогою SIEM-системи (Security Information and Event Management) – така система збирає журнали з різних джерел і аналізує на предмет аномалій. Налаштувати оповіщення для IT-безпеки: наприклад, якщо до медичних даних звертається нетиповий користувач або масово експортуються дані, або відбулося 10 невдалих спроб входу підряд – система генерує попередження. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Цілісність даних (Integrity) – забезпечити, щоб ePHI не була неправомірно змінена або знищена; впровадити електронні механізми підтвердження цілісності. | Для захисту цілісності медичних даних реалізувати декілька рівнів контролю. По-перше, обмежити коло осіб, що мають право редагувати чи видаляти записи (це вже досягається розмежуванням доступів). По-друге, увімкнути журналювання версій або архівування змін: щоб будь-яке редагування запису пацієнта фіксувалося (хто змінив і що було до зміни). Якщо програмне забезпечення дозволяє, налаштувати контрольні суми або хешування важливих файлів/записів – щоб потім можна було перевірити, чи файл не було таємно змінено. Наприклад, для образів з медичними знімками зберігати їх хеш SHA-256 у базі; при завантаженні знімку для перегляду обчислювати хеш і порівнювати. На серверних базах даних – налаштувати реплікацію в режимі лише для читання на резервний сервер: це не лише забезпечить резерв, а й ускладнить непомітну зміну даних (будуть розбіжності при реплікації, якщо щось змінено поза транзакціями). Проводити контрольні перевірки цілісності: наприклад, щомісяця вибірково перевіряти важливі таблиці на предмет невідповідностей (кількість записів, цілісність посилань). Використовувати технології невідкидного журналу (immutable log) там, де можливо, щоб запис раз внесений не міг бути змінений без сліду. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Перевірка автентичності (Person/Entity Authentication) – впровадити процедури перевірки особи, що намагається отримати доступ до ePHI, тобто гарантувати, що користувач є тим, за кого себе видає. | Основний спосіб автентифікації – логін+пароль, але його потрібно посилити політикою складності паролів: мінімум 8-10 символів, з буквами різного регістру, цифрами, спеціальними знаками; заборона на типові паролі; регулярна примусова зміна (наприклад, кожні 6 місяців). Налаштувати для критичних систем двохфакторну автентифікацію: окрім пароля, користувач вводить одноразовий код із SMS або застосунку, або використовує апаратний токен/смарт-картку. Для внутрішніх систем у межах захищеної мережі MFA може бути опційною, але для будь-якого віддаленого доступу (через інтернет) – обов'язкова. Персонал має бути проінструктований ні в якому разі не передавати свої облікові дані іншим. Використовувати автентифікацію пристроїв: наприклад, VPN-доступ до лікарняної мережі дозволяти тільки з корпоративних ноутбуків, які мають цифрові сертифікати. Так ми впевнимося, що підключився саме лікар на виданому йому ноутбуці, а не хтось інший. У фізичних межах – запровадити системи контролю біометричної автентифікації або смарт-картки для доступу до робочих станцій у відділеннях з підвищеною конфіденційністю (наприклад, центр лікування ВІЛ, психіатричне відділення) – щоб виключити доступ сторонніх. |

Продовження Додатку Г

Таблиця 3.1 Вимоги HIPAA та рекомендації щодо впровадження

| | |
|---|---|
| Захист під час передачі даних (Transmission Security) – застосувати технічні засоби для захисту ePHI, що передається електронними мережами, від перехоплення та несанкціонованого доступу. | Усі мережеві з'єднання, де проходять персональні дані пацієнтів, повинні бути зашифровані. Забезпечити використання протоколів HTTPS/TLS для веб-доступу до медичних систем, SSL/TLS для поштових серверів (шифрування пошти). Якщо співробітники обмінюються електронними листами з даними пацієнтів – впровадити шифрування електронної пошти (S/MIME або PGP) або, як мінімум, захищені вкладення з паролями, переданими окремо. Для внутрішньої мережі лікарні – сегментувати її: відокремити сегмент з медичними системами від загальнодоступного Wi-Fi для відвідувачів. На мережевому рівні використовувати VPN для з'єднання філій або віддалених користувачів із головним центром – щоб дані подорожували захищеним тунелем. Розгорнути систему виявлення вторгнень (IDS) на периферії мережі, щоб відстежувати підозрілий трафік (наприклад, великі обсяги даних, що надсилаються назовні не в робочий час). Заборонити використання незашифрованих протоколів передачі (FTP, Telnet) – замінити їх на захищені (SFTP, SSH). Особливу увагу приділити переносним носіям: якщо треба передати дані на зовнішньому носії, перед копіюванням зашифрувати файли (архів з паролем або програми шифрування). Також домовитися з партнерами про безпечні методи обміну (наприклад, через захищене хмарне сховище з двофакторним доступом). |

**Додаток Д**

**Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження**

| Принцип GDPR | Реалізація в медичному закладі |
|---|---|
| Законність, справедливість і прозорість – дані повинні оброблятися законно, чесно і прозоро для пацієнта. Це означає наявність правової підстави для | Переконатися, що кожна операція з персональними даними пацієнтів має законну підставу. Основні підстави за GDPR для медицини: згода пацієнта; виконання медичного контракту (надання послуг); виконання законного обов'язку (ведення меддокументації за наказами МОЗ); захист життєво важливих інтересів (екстрена допомога непритомному пацієнту); публічний інтерес у сфері охорони здоров'я. Для звичайних медичних послуг |

| | |
|---|---|
| кожної операції з даними та інформування пацієнтів про те, як їхні дані використовуються. | достатньо нормативної бази України (пацієнт дає інформовану згоду на лікування, що включає обробку даних). Проте на практиці варто отримувати письмову згоду пацієнта на обробку його персональних даних під час первинного звернення – окремим пунктом у формі згоди на медичне втручання або як окремий документ. У згоді чітко вказати, які дані збираються і для чого (наприклад: для діагностики і лікування, для ведення електронної медичної картки, для передачі в страхову компанію за потреби). Для вторинних цілей (наукові дослідження, маркетинг) – отримувати окрему згоду або деперсоніфікувати дані. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Обмеження мети – збір даних лише для конкретних, явних та законних цілей і недопущення їх подальшої обробки несумісно з цими цілями. | Описати цілі обробки у внутрішній документації та доводити їх до відома пацієнтів. Для медзакладу типовими цілями є: ведення медичної картки для лікування; забезпечення безперервності лікування (передача епікризів іншим лікарям); розрахунки зі страховими; виконання вимог МОЗ зі статистики; покращення якості послуг (внутрішній аналіз). Заборонено використовувати зібрані медичні дані для інших несумісних цілей – наприклад, передавати контактні дані пацієнтів фармкомпаніям для реклами без окремої згоди. Якщо лікарня хоче використовувати історії хвороби для наукових публікацій – слід або отримати згоду пацієнтів, або знеособити дані (псевдонімізувати). Внести до реєстру операцій з даними (див. нижче) чіткий перелік цілей. Періодично переглядати, чи не використовується деінде інформація поза заявленими цілями. Якщо виникає нова мета (наприклад, планують впровадити систему розсилки повідомлень пацієнтам про акції клініки) – перевірити її сумісність з первинною метою лікування; швидше за все, потрібна окрема згода на маркетингову розсилку. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Мінімізація даних – збирати лише ті персональні дані, що потрібні для заявлених цілей (“не більше, ніж потрібно”). | Провести ревізію форм і полів, які заповнюються про пацієнта. Вилучити зайве: не питати в анкетах дані, не критично потрібні для лікування. Наприклад, якщо послуга не потребує інформації про родинний стан чи місце роботи – не збирати їх “про всяк випадок”. В електронній медсистемі налаштувати обов’язкові поля мінімально необхідними (ім’я, контакти, дані для анамнезу) – інші робити опціональними. Проводити регулярне очищення: видаляти застарілі записи, які більше не потрібні (наприклад, резюме кандидатів на роботу, якщо з моменту збору пройшло 2-3 роки). Мінімізація також стосується доступів: як згадано вище, персонал повинен бачити лише необхідні їм дані. Реалізувати псевдонімізацію там, де можливо – напряму визначальні дані (ім’я, номер паспорта) зберігати окремо від медичних показників, пов’язуючи їх через ідентифікатор. У разі досліджень чи телемедицини, де повне ім’я не потрібне, використовувати код пацієнта замість персональних даних. Це дозволить зменшити обсяг конфіденційної інформації, доступної на кожному етапі. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Точність – персональні дані повинні бути точними і актуальними; вживати заходів для виправлення неточностей. | Забезпечити механізми актуалізації даних: при кожному відвідуванні пацієнта уточнювати ключову інформацію (адресу, контакти, алергії тощо). Якщо пацієнт помітив помилку в своїх даних або звернувся з проханням виправити – реалізувати процедуру швидкого виправлення: визначити відповідального (наприклад, працівник реєстратури або IT-адміністратор для електронних даних), який внесе правки в систему. Логувати виправлення (що було змінено, ким і коли).<br>Неактуальні або помилкові дані, які не підлягають оновленню, – видаляти або архівувати. Наприклад, якщо пацієнт змінив прізвище, старе прізвище варто зберегти в історії змін, але у поточному профайлі відображати лише актуальне.<br>Переконатися, що дані з зовнішніх джерел (лабораторні аналізи, направлення) правильно внесені до картки – медсестра чи лікар повинні перевіряти відповідність результати-пацієнт. В рамках внутрішнього аудиту періодично вибірково перевіряти записи на точність та повноту. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Обмеження зберігання – зберігати персональні дані не довше, ніж це потрібно для цілей обробки. | Встановити політику зберігання даних: скільки часу різні категорії інформації тримаються в системі. В Україні є мінімальні терміни зберігання медичних документів (наприклад, форми облікові – 5-25 років, архів – 25 років чи довічно для історій пологів). GDPR же вимагає не тримати довше, ніж потрібно. Тож після закінчення обов'язкових термінів варто видаляти або архівувати дані. Наприклад, електронні записи про давно невідвідувавших пацієнтів перевести в архівну базу, від'єднану від основної системи, або повністю знеособити (прибрати імена, залишивши тільки знеособлену статистику). Розробити графік перевірки і зачистки даних: раз на рік адміністратор бази переглядає записи, старші певного порогу (скажімо, 8-10 років після останнього візиту) і приймає рішення – видалити чи архівувати. При цьому врахувати можливі юридичні вимоги (наприклад, дані про щеплення можливо слід зберігати довше для довідок). Якщо пацієнт відгук відкликав згоду і немає іншої законної підстави зберігати його дані – їх теж слід видалити (крім хіба що мінімальної інформації про надані послуги, потрібної для фінансової звітності). Документуйте усі такі операції видалення на випадок перевірки регулятора. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Цілісність і конфіденційність – гарантувати належну безпеку персональних даних, включно із захистом від несанкціонованого чи незаконного оброблення, випадкової втрати, знищення чи пошкодження (впровадити відповідні технічні й організаційні заходи). | Цей принцип безпосередньо апелює до інформаційної безпеки. Його реалізація багато в чому збігається з вимогами HIPAA, описаними вище, та з заходами NIST CSF (див. наступні розділи). Стисло: потрібно забезпечити конфіденційність (щоб дані не потрапили стороннім – через контроль доступу, шифрування, навчання персоналу), цілісність (щоб дані не були спотворені – через обмеження прав, резервні копії, журнали змін) та доступність (щоб дані були доступні, коли потрібні – через резервування систем, відмовостійкість, плани відновлення). GDPR у ст.32 наводить приклади заходів: шифрування та псевдонімізація; здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем; можливість вчасно відновити доступ до даних після інциденту; регулярне тестування ефективності заходів безпеки. У контексті лікарні це означає: шифрувати персональні дані пацієнтів в базах і при передачі (SSL, VPN); підтримувати стійкість роботи IT-систем (джерела безперебійного живлення, резервні сервери, кластери); регулярно тестувати плани відновлення (наприклад, імітація відмови сервера і відпрацювання перемикання на резервний). Організаційно – призначити відповідального за захист даних (DPO або відповідальний, див. нижче), проводити тренінги, контролювати дотримання політик. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| Організаційний контроль GDPR | Рекомендації щодо впровадження |
|---|---|
| Відповідальний за захист даних (Data Protection Officer, DPO) – GDPR вимагає призначити DPO, якщо діяльність установи пов’язана з масштабною обробкою чутливих даних (наприклад, даних про здоров’я). DPO контролює дотримання GDPR і консультує організацію. | Оцінити, чи потрібен формально DPO. За GDPR, лікарня або велика приватна клініка, що обробляє значний обсяг даних про здоров’я, повинна мати DPO. Навіть якщо закон прямо не зобов’язує, рекомендується призначити таку особу для координації відповідності. DPO може бути: штатний співробітник (юрист або спеціаліст з IT безпеки, обізнаний у захисті даних) або залучений на аутсорсі. Важливо: DPO має бути незалежним – підпорядковуватись вищому керівництву, не отримувати вказівок щодо виконання своїх завдань. Завдання DPO: моніторити дотримання GDPR, проводити аудит, навчати персонал, надавати рекомендації щодо DPIA, бути контактною особою для регулятора та пацієнтів з питань даних. У структурі клініки може бути призначено, наприклад, юрисконсульта як DPO, якщо він має достатню експертизу, або керівника відділу якості. Видати наказ про призначення, оприлюднити контакт DPO (email) для звернень пацієнтів. Якщо DPO відсутній, призначити хоча б відповідального за виконання вимог захисту даних (може суміщатися з роллю відповідального за ІБ або начальника канцелярії). |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Реєстр операцій з персональними даними – GDPR (ст.30) зобов'язує кожного контролера вести облік всіх категорій операцій з персональними даними: які дані, з якою метою, хто отримує, строки зберігання тощо. | Створити Реєстр обробки даних для закладу. Це може бути таблиця або документ, де перечислено: категорії суб'єктів (пацієнти, працівники); категорії даних (паспортні дані, дані про стан здоров'я, результати аналізів тощо); цілі обробки для кожної категорії; правова підстава (згода, договір, закон); отримувачі даних (наприклад: МОЗ – для звітності, страхові – для страхових випадків, лабораторії – для аналізів, IT-підрядники); міжнародні передачі (якщо є – наприклад, хмарне зберігання за межами України/EU, тоді які захисні заходи – стандартні договірні положення); строки зберігання по кожній категорії; засоби захисту (коротко: шифрування, контроль доступу, тощо).<br>Цей реєстр можна скласти за шаблонами, доступними в інтернеті, або звернутися до DPO. Він не обов'язково подається кудись, але має бути готовий на випадок перевірки регулятора і в цілому допомагає структуровано бачити всі дані та процеси.<br>Переглядати реєстр при появі нових процесів або зміні існуючих. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Data Protection Impact Assessment (DPIA) – оцінка впливу на захист даних. Проводиться, якщо обробка може мати високий ризик для прав людей (обробка великого обсягу здоров'я, нові технології, відеоспостереження тощо). | Визначити, які процеси в закладі потребують DPIA. Зазвичай DPIA потрібна при: впровадженні нової електронної медичної системи, що містить усі дані пацієнтів; запуску телемедицини з передачою даних онлайн; установці системи відеоспостереження в публічних зонах; передачі даних на аутсорсинг (хмарне сховище). Наприклад, якщо лікарня планує перейти з паперових карток на EMR (electronic medical record), слід провести DPIA: описати процес, оцінити, які ризики для приватності виникають (витік через хакерів, помилки, нецільове використання), оцінити ймовірність і серйозність цих ризиків для пацієнтів (зважаючи на чутливість даних про здоров'я, ризики високі), визначити заходи для зниження ризиків (шифрування, доступ за картками, навчання персоналу, DLP-системи). Результати DPIA задокументувати. Залучити DPO до цього аналізу. Якщо ризик залишається високим навіть після заходів – консультатуватися з регулятором (в Україні – Уповноважений ВРУ). На практиці, DPIA можна оформити як документ Word 10-15 сторінок або форму з питаннями (багато шаблонів доступні). Важливо мати DPIA до впровадження нового процесу, а не після. Зберігати DPIA результати, оновлювати при зміні умов. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Політики захисту даних та конфіденційності – GDPR вимагає, щоб організація впровадила політики, які забезпечують відповідність (наприклад, політика зберігання даних, політика реагування на витоки, політика використання пристроїв тощо). | Розробити внутрішні регламенти та політики по роботі з персональними даними. Частково вони перетинаються з політиками ІБ (HIPAA), але акцент на приватність: 1) Політика захисту персональних даних пацієнтів – загальні принципи, посилання на закон, відповідальність співробітників, порядок дій при запитах пацієнтів, при інцидентах. 2) Політика зберігання та видалення даних – як довго зберігаємо медичні записи, коли архівуємо, як видаляємо, хто санкціонує. 3) Інструкція щодо реагування на запити суб'єктів – як працівники мають перенаправити запит DPO, які строки. 4) Політика щодо передачі даних третім сторонам – наприклад, заборона передавати дані без угоди (Business Associate Agreement / договір про конфіденційність). 5) Конфіденційність працівників – окремо, адже лікарня також має дані співробітників (досьє, медогляди). Слід регламентувати, хто має доступ до цих даних (тільки відділ кадрів, лікарі-профпатологи) і що вони під захистом. Включити положення про конфіденційність у трудові договори: кожен співробітник підписує зобов'язання нерозголошувати персональні дані пацієнтів, які він дізнався під час роботи. Проводити тренінги з GDPR для відповідального персоналу (реєстратори, адміністратори даних) – пояснити їх обов'язки та відповідальність. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Контракти з обробниками даних – якщо клініка залучає сторонніх обробників (IT-сервіси, лабораторії, бухгалтерію), GDPR вимагає укладення договорів, що зобов’язують цих обробників дотримуватися GDPR (ст.28). | Інвентаризувати всіх контрагентів, які отримують персональні дані пацієнтів чи працівників: IT-компанія, що підтримує софт і має доступ до БД; хмарний провайдер для резервних копій; стороння лабораторія, яка отримує направлення з даними пацієнта; кол-центр, якщо зовнішній; страхові компанії (вони самі контролери, тут скоріше спільні контролери). З кожним потрібно мати договір про обробку даних (Data Processing Agreement). У договорі прописати: предмет і тривалість обробки, характер і ціль, тип даних (медичні, ідентифікаційні) і категорії суб’єктів (пацієнти); обов’язки і права контролера (клініки); обов’язки обробника – діяти тільки за інструкцією контролера, забезпечувати конфіденційність (всі працівники під NDA), вживати належних заходів безпеки (вказати, яких саме – наприклад, шифрування, сертифікація ISO 27001), допомагати контролеру виконувати запити суб’єктів та вимоги ст.32-36 GDPR (безпека, повідомлення про витоки, DPIA), після завершення послуг видалити або повернути всі дані; дозволяти аудит; не залучати інші суб-обробники без дозволу. Багато компаній вже мають типові DPA, але їх варто перевірити. Якщо контрагент за межами ЄЕЗ, потрібно забезпечити правовий механізм передачі даних (стандартні контрактні положення, або він сертифікований, тощо). |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Управління інцидентами та повідомлення – GDPR вимагає повідомляти регулятора (на території ЄС) про витік персональних даних протягом 72 годин, а суб'єктів – без зволікань, якщо витік може зашкодити їм (ст.33, 34). Медзакладу потрібно мати процес виявлення та оповіщення про такі випадки. | Детально цей аспект розглядається у розділі про реагування на інциденти (нижче). В контексті GDPR організаційно треба: 1) Процедура повідомлення: DPO або відповідальний за безпеку оцінює інцидент (напр. зламано сервер, вкрадено ноутбук з базою) і визначає, чи був витік персональних даних і наскільки серйозний. 2) Якщо витік може призвести до ризику для прав і свобод людей (наприклад, розкрито медичні діагнози) – повідомити Уповноваженого ВРУ (в Україні, або інший наглядовий орган, коли буде) протягом 72 годин з моменту виявлення витоку. Повідомлення містить: скільки суб'єктів і записів постраждало, характер даних, ймовірні наслідки, вжиті заходи. 3) Якщо ризик високий – повідомити самих пацієнтів (через телефон, email або лист) про те, що сталося, які дані розкрито і що їм робити (наприклад, змінити паролі, стежити за рахунками тощо). Це потрібно зробити невідкладно, бажано індивідуально кожному. 4) Документувати всі інциденти безпеки, навіть дрібні, і аналізувати їх. Внести в політику безпеки пункт про повідомлення: персонал повинен негайно інформувати керівництво про будь-які підозри на витік; DPO/безпековець вирішує про зовнішнє повідомлення. Відпрацювати шаблони листів для таких повідомлень, щоб у стресовий момент діяти швидко. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Сертифікації та найкращі практики – хоча не пряма вимога, GDPR заохочує впровадження кодексів поведінки, сертифікацій (ст.40-42) як доказ відповідності. | Розглянути можливість добровільної сертифікації в сфері захисту даних. Наприклад, міжнародні стандарти ISO/IEC 27001 (система управління інформаційною безпекою) та ISO/IEC 27701 (розширення для приватності, сумісне з GDPR). Медичний заклад, сертифікований за цими стандартами, продемонструє високий рівень зрілості системи безпеки і приватності. Це також допоможе впорядкувати процеси – адже стандарти вимагають наявності політик, оцінки ризиків, контролю доступу тощо, що ми і так впроваджуємо. Якщо повна сертифікація не по силах, слід хоча б запозичити кращі практики: проводити тренінги, внутрішні аудити, складати плани вдосконалення безпеки. Можна долучитися до галузевих ініціатив – наприклад, в ЄС є Кодекси поведінки для охорони здоров'я, які роз'яснюють застосування GDPR у цій сфері. Дотримання таких кодексів (навіть без формальної сертифікації) покаже, що заклад рухається у правильному напрямку. |
| Технічний захід (ст.32 GDPR) | Рекомендації щодо реалізації в медзакладі |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Шифрування та псевдонімізація даних – перетворення даних у форму, що ускладнює ідентифікацію особи без додаткової інформації. | Шифрування: застосувати сучасні алгоритми шифрування для даних як "у спокої", так і "в русі". Як зазначено в HIPAA секції, слід шифрувати диски серверів з базами даних (AES-256), резервні копії (якщо зберігаються в хмарі – покладатися на cloud encryption плюс власне шифрування файлів), ноутбуки лікарів (повне шифрування диска). Для передачі – SSL/TLS, VPN тощо. Це гарантує, що у випадку компрометації носія чи перехоплення трафіку зловмисник не прочитає дані. Псевдонімізація: у медичному контексті – відділення особистої інформації (ПІБ, контакти) від медичних даних. Практичний підхід: створити окрему таблицю “Пацієнти” з ID, ім’ям, адресою і т.д., а медичні записи посилатися лише на ID пацієнта. У повсякденній роботі це прозоро, але якщо витікнуть медичні записи без таблиці відповідності – вони не будуть прив’язані до конкретних осіб без цієї “ключової” інформації. Звісно, псевдонімізація не заміняє повного шифрування або контролю доступу, але зменшує обсяг даних, що розкриваються при витоку. Також можна псевдонімізувати дані для вторинних цілей: для статистики по лікарні замінити особові дані кодами. Важливо безпечно зберігати “ключ” (таблицю відповідності) – з обмеженим доступом і бажано теж шифрувати. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Забезпечення стійкості та доступності систем – здатність систем і послуг з обробки даних залишатися конфіденційними, цілісними та доступними, навіть при збої чи інциденті. | Стійкість (resilience) означає, що системи спроєктовано з урахуванням відмов: якщо одна компонента виходить з ладу, інша перебирає функції. Для лікарні критично, щоб інформаційна система була доступною 24/7, особливо стаціонару. Рекомендації:<br>Резервне обладнання: мати дублюючий сервер на випадок виходу з ладу основного (бажано з реплікацією даних в реальному часі). Або використовувати хмарні рішення з гарантованим uptime.<br>Живлення: встановити джерела безперебійного живлення (UPS) для серверів і мережевого обладнання, генератор для лікарні, щоб короткочасні відключення електрики не спричинили недоступність даних. Сегментація мережі: злам чи зараження однієї частини мережі не повинен паралізувати всю систему – розділити VLAN для різних підсистем (адміністрація, діагностичне обладнання, публічний Wi-Fi).<br>Тестування на відмову: періодично імітувати відмову компонент – напр. відключити один з серверів кластеру – і перевіряти, чи система продовжує працювати на резервному.<br>Моніторинг доступності: налаштувати інструменти, які сповістять IT-персонал про збій (Zabbix, Nagios тощо) щоб швидко відреагувати. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Здатність вчасно відновити доступ до даних після інциденту – тобто наявність резервного копіювання та планів відновлення. | Як вже описувалося у HIPAA Contingency Plan, необхідно мати чітку систему резервного копіювання і відновлення. На рівні GDPR варто перевірити, що: Резервні копії охоплюють всі критичні дані: бази даних пацієнтів, документообіг, системи обліку. Частота бекапів відповідає потребам (в ідеалі щоденно інкрементально, а повний – щотижня; якщо клініка велика – то і частіше).<br>Відокремлення: хоча б одна копія зберігається офлайн або в іншому середовищі (проти ризику ransomware, коли онлайн-копії теж шифруються). Наприклад, щотижневий бекап на зовнішній носій, відключений від мережі.<br>Регулярне тестування відновлення – принаймні раз на квартал обирати кілька резервних копій і пробувати розгорнути на тестовому сервері, переконатися, що дані цілі. Відновлення після інциденту: розробити покрокову інструкцію для IT-персоналу, як розгортати новий сервер з бекапу, скільки часу це займає, кого повідомити про перерву в роботі. Прагнути до мінімального часу простою (RTO) – наприклад, не більше 4-6 годин. Якщо треба швидше – розглядати реплікацію в режимі реального часу. |

Продовження Додатку Д

Таблиця 3.2 Вимоги GDPR та рекомендації щодо впровадження

| | |
|---|---|
| Регулярне тестування, оцінка та вимірювання ефективності заходів безпеки – постійний процес перевірки того, наскільки добре заходи працюють. | GDPR наголошує на цикл PDCA (Plan-Do-Check-Act) у безпеці. Медичному закладу слід запровадити: 1) Періодичні аудити та перевірки: як згадано, внутрішній аудит політик щороку, сканування уразливостей мережі щокварталу, тестування відновлення резервних копій, імітація сценаріїв витоку (table-top exercise: збирається команда і програє ситуацію “що робимо, якщо знайшли флешку з даними на парковці”). 2) Пентестування: за можливості замовляти зовнішнє тестування на проникнення в мережу і веб-сайти лікарні – щоб виявити слабкі місця до реальних хакерів. 3) Оцінка відповідності: DPO або зовнішні консультанти можуть щорічно оцінювати відповідність вимогам GDPR і локального закону, надавати звіт керівництву. 4) Опитування персоналу: оцінювати обізнаність – проводити сюрпризні фішингові тестування (розіслати підробні фішинг-листи і подивитися, скільки людей клікне, з подальшим навчанням), або короткі опитування знань політик. 5) Метрики безпеки: розробити KPI – наприклад, кількість інцидентів на квартал, середній час реагування, відсоток пройдених тренінгів персоналом, відсоток систем з актуальними патчами. Ці метрики обговорювати на нарадах керівництва. |

## Додаток Е

**Таблиця 2.1 Модель загроз для медичних IT-систем**

| Загроза | Опис | Джерело загрози | Вектор атаки | Цільовий компонент |
|---|---|---|---|---|
| Фішинг (шахрайські електронні листи) | Атаки соціальної інженерії, в яких зловмисник надсилає правдоподібні повідомлення співробітникам медзакладу, щоб виманити облікові дані або змусити встановити шкідливе ПЗ. Фішинг залишається найпоширенішим методом компрометації медичних організацій. Успішний фішинг може надати атакувальнику доступ до системи та даних пацієнтів. | Зовнішній атакувальник (кіберзлочинець) | Електронна пошта, повідомлення (social engineering) | Користувач (персонал, що відкриває лист) |

Продовження Додатку Е

Таблиця 2.1 Модель загроз для медичних ІТ-систем

| | | | | |
|---|---|---|---|---|
| Програма-вимагач (ransomware) | Шкідливе програмне забезпечення, що шифрує медичні дані і вимагає викуп. Сучасні програми-вимагачі часто також викрадають копії даних перед шифруванням, загрожуючи їх оприлюдненням. Для лікарень атаки ransomware особливо небезпечні, адже блокування медичних записів може ставити під загрозу життя пацієнтів. | Зовнішній атакувальник (кіберзлочинець або група) | Фішингові листи з вкладенням, експлойти у вразливостях, заражені веб-сайти | Сервери та бази даних (медичні записи), мережа установи |
| Шкідливе ПЗ (трояни, шпигунське ПЗ) | Програми, що потай виконують несанкціоновані дії: крадуть конфіденційні дані (номери карток, дані пацієнтів) або відкривають “бекдор” для зовнішнього доступу. Таке ПЗ може потрапити через інфіковані файли, підробні програми чи зовнішні носії. Результатом може бути непомітний витік великих обсягів даних назовні. | Зовнішній атакувальник (хакерські групи, кіберзлочинці) | Заражені файли, шкідливі програми на носіях, завантаження з інтернету | Клієнтські комп’ютери, робочі станції, мобільні пристрої |

Продовження Додатку Е

Таблиця 2.1 Модель загроз для медичних ІТ-систем

| | | | | |
|---|---|---|---|---|
| Атака через вразливість системи | Експлуатація невиправлених вразливостей у програмному забезпеченні медичних систем (наприклад, у веб-додатках електронних медичних записів або PACS-системах). Атакувальник може отримати несанкціонований доступ до БД пацієнтів | Зовнішній атакувальник | Мережевий (через Internet) – віддалена експлойтація вразливостей, SQL-ін’єкція через веб-форми | Веб-додаток, база даних (сервер застосунку або СУБД) |

| | | | | |
|---|---|---|---|---|
| | шляхом SQL-ін’єкції або інших експлойтів. Уразливі веб-системи часто стають шлюзом для крадіжки даних пацієнтів. | | | |
| Атака методом підбору паролів | Спроби отримати доступ до облікових записів медичної системи шляхом перебору слабких паролів або використання злитих облікових даних. Якщо облікові записи працівників або адміністраторів захищені слабо, зловмисник може отримати привілейований доступ і вивантажити конфіденційні дані. | Зовнішній атакувальник | Brute-force атаки, використання викрадених паролів з інших витоків (credential stuffing) | Системи автентифікації, облікові записи користувачів (EHR, мережеві сервіси) |

Продовження Додатку Е

Таблиця 2.1 Модель загроз для медичних IT-систем

| | | | | |
|---|---|---|---|---|
| Зловмисний інсайдер | Співробітник медичного закладу, який навмисно викрадає або розголошує дані. Такий інсайдер вже має законний доступ до медичних систем, що ускладнює виявлення витоку. Мотив може бути фінансовим (продаж даних на чорному ринку) або особистим. Витік внутрішнім порушником – друга за частотою причина медичних витоків після хакерських атак, адже дані пацієнтів дуже цінні для зловмисників. | Внутрішній порушник (співробітник, інсайдер) | Внутрішня мережа або системи – зловживання наданими привілеями, копіювання даних на зовнішні носії або знімки екрану | Бази даних пацієнтів, системи ЕМК (EMR), медична інформація на носіях |
| Ненавмисне розголошення (помилка персоналу) | Витік інформації через людський фактор без злого умислу. Приклади: відправка електронного листа з даними пацієнта не тому адресату; публікація медичних даних у відкритий доступ через помилкові | Внутрішній (персонал, що припустився помилки) | Помилкові дії: неправильно налаштовані права доступу, помилкова відправка даних | Будь-який компонент (електронна пошта, база даних |

| | | | | |
|---|---|---|---|---|
| | налаштування; випадкова втрата документів чи носія з інформацією. | | | |

Продовження Додатку Е

Таблиця 2.1 Модель загроз для медичних IT-систем

| | | | | |
|---|---|---|---|---|
| Втрата або крадіжка пристрою | Фізична втрата ноутбука, зовнішнього диска, смартфона чи іншого носія, що містить медичні дані. Якщо пристрій не зашифрований, зловмисник, що його отримає, може отримати доступ до конфіденційної інформації (наприклад, база пацієнтів на ноутбуці лікаря). Такі випадки особливо небезпечні при наявності ПІІ/ЕМЗ на пристроях без захисту. | Внутрішній (через недбалість) або зовнішній (крадіжка) | Фізичний – крадіжка пристрою, втрата у громадських місцях | Клієнтські пристрої (ноутбуки, планшети, портативні носії з даними) |
| Компрометація стороннього підрядника | Витік даних через злам або недбалість сторонньої організації, що має доступ до медичної інформації (наприклад, IT-підрядник, лабораторія, страхова компанія). Зловмисник може атакувати менш захищеного партнера, щоб отримати доступ до даних лікарні. | Зовнішній (через уразливого партнера) | Мережевий (атака на підрядника), соціальна інженерія або зловживання довіреним доступом | Сторонні системи, інтеграційні інтерфейси (обмін даними між лікарнею та партнером) |

**Додаток Є**

**Таблиця 2.2 Модель порушника (типи зловмисників)**

| Тип порушника | Мотивація | Технічні можливості | Рівень привілеїв | Типові дії |
|---|---|---|---|---|
| Зовнішній атакуючий (кіберзлочинець) | Фінансова вигода (крадіжка даних для продажу, вимагання викупу за розшифрування тощо) є основним мотивом таких зловмисників. Також можливі мотиви шантажу, промислового шпигунства або дискредитації медзакладу. | Зазвичай середні або високі: володіє навичками зламу систем, створення фішингових кампаній, розробки або використання шкідливого ПЗ. Може залучати інструменти з даркнету чи готові експлойти. | Низький на початку (не має легітимного доступу). Намагається отримати привілеї шляхом злому (наприклад, адміністраторські права після атаки). | Сканування мереж на вразливості, розсилка фішингових листів, запуск експлойтів, використання вкрадених облікових даних, встановлення бекдорів, ексфільтрація (вивантаження) даних назовні. |

Продовження Додатку Є

Таблиця 2.2 Модель порушника (типи зловмисників)

| | | | | |
|---|---|---|---|---|
| Внутрішній привілейований порушник (системний адміністратор або IT-персонал) | Може бути мотивований образами, конфліктами на роботі або зовнішнім підкупом. Також можлива мотивація ідеологічна або зловмисна цікавість. У випадку підкупу з боку третіх осіб мотивом знову ж таки стає фінансова вигода. | Високі технічні можливості: добре знає внутрішні системи, мережу, має навички адміністрування. Здатен обійти багато засобів захисту або вимкнути їх. | Високий (широкі права доступу до систем, баз даних, серверів). Може мати доступ до привілейованих облікових записів, конфіденційних даних і налаштувань систем безпеки. | Зловживання адмінправами для доступу до конфіденційних БД, відключення журналювання чи засобів захисту, копіювання великих масивів даних, зміна прав доступу для приховування слідів. |

Продовження Додатку Є

Таблиця 2.2 Модель порушника (типи зловмисників)

| | | | | |
|---|---|---|---|---|
| Інсайдер (рядовий співробітник зі зловмисним наміром) | Особиста вигода (продаж даних, фінансова винагорода) – одна з головних причин, чому працівники навмисно порушують конфіденційність. Інші мотиви: помста роботодавцю, передача даних конкурентам, цікавість чи шантаж. | Середні: знає, як користуватися корпоративними системами, може розуміти базові засоби обходу контролю (наприклад, зробити скриншоти екрана, якщо заборонено експорт даних). Не обов'язково володіє глибокими IT-навичками. | Середній (звичайний рівень доступу відповідно до ролі – наприклад, лікар має доступ до ЕМЗ своїх пацієнтів). Привілеї обмежені посадовими обов'язками, але інсайдер використовує їх для витоку. | Несанкціоноване копіювання інформації (друк, фото екрану, експорт у файли), передача даних третім особам, обхід DLP (наприклад, перейменування файлів, шифрування перед відправкою), викрадення паперових документів. |

Продовження Додатку Є

Таблиця 2.2 Модель порушника (типи зловмисників)

| | | | | |
|---|---|---|---|---|
| Випадковий порушник (недбалий персонал) | Відсутня зла умисна мотивація. Причиною порушень є необережність, неуважність або недостатня обізнаність. Наприклад, співробітник може помилково надіслати дані не тому адресату або налаштувати публічний доступ до записів, не розуміючи ризиків. | Низькі: технічно такі працівники часто не володіють специфічними навичками кібербезпеки. Порушення відбуваються через брак знань (наприклад, використання слабких паролів, незнання політик безпеки). | Середній або низький (звичайний доступ відповідно до посади). Може не мати доступу до великого обсягу даних, але навіть на своєму рівні здатен спричинити витік помилково (наприклад, медсестра розкрила дані одного пацієнта). | Ненавмисні дії: відкриття фішингового листа, перехід за шкідливим посиланням, завантаження невідомого файлу, неправильне налаштування прав доступу, втрата незашифрованого ноутбука чи паперових документів, порушення протоколів безпеки |
| Сторонній підрядник/партнер (третя сторона) | Зазвичай прямої зловмисної мотивації немає (партнери – наприклад, IT-компанія чи лабораторія – зацікавлені у співпраці). Однак їх співробітники можуть бути мотивовані фінансово (продати доступ або дані) чи діяти недбало. Також | Залежить від компанії: технічні можливості середні. Якщо це IT-партнер – він технічно підкований, але може мати уразливі системи. Інші партнери (лабораторії, страхові) можуть не | Зазвичай обмежений до необхідних систем (принцип найменших привілеїв за договором). Проте партнер може мати доступ до певних даних пацієнтів чи | Помилкове поводження з даними (витік через необачність), зберігання медичних даних на недостатньо захищених системах, ненавмисне |

| | | | | |
|---|---|---|---|---|
| | зовнішній хакер може використати підрядника як шлях атаки, знаючи про довірчі зв’язки. | мати сильного кіберзахисту. | інтерфейсів системи (API). | розголошення або пропуск фішингової атаки. У гіршому разі – змова окремого співробітника підрядника із зловмисниками або компрометація його облікових даних. |

**Додаток Ж**

**Таблиця 2.3 Матриця ризиків для загроз витоку даних**

| Загроза | Компонент | Наслідки (опис) | Рівень ризику | Рекомендовані заходи реагування |
|---|---|---|---|---|
| Фішинг-атака | Користувач (облікові записи) | Зловмисник отримує облікові дані співробітника та доступ до внутрішніх систем. Наслідок – компрометація облікового запису і несанкціонований доступ до даних пацієнтів. Може статися масштабний витік даних (один успішний фішинг здатен скомпрометувати всю базу). | Високий (ймовірність висока; вплив високий) | Навчання персоналу кібергігієні (тренінги з розпізнавання фішингу), фішинг-симуляції; впровадження багатофакторної автентифікації, щоб вкрадені паролі були не достатні для доступу; фільтрація електронної пошти та веб-трафіку для блокування шахрайських листів. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Атака програми-вимагача (ransomware) | Сервери, база даних, мережа | Шифрування баз даних та критичних систем, блокування доступу до електронних медичних записів. Можлива крадіжка даних перед шифруванням з подальшим шантажем. Вплив – повна зупинка роботи лікарні, відмова у наданні медичних послуг, ризик для життя пацієнтів (відомі випадки затримки операцій через кібератаки). Потенційний витік тисяч записів, фінансові збитки та штрафи. | Високий (ймовірність середня; вплив дуже високий) | Регулярне резервне копіювання даних і перевірка відновлення; сегментування мережі, щоб обмежити поширення зараження; сучасні антивірусні засоби та EDR-системи; оперативне встановлення оновлень безпеки; навчання персоналу не відкривати підозрілі файли. Розробка плану реагування на інцидент (IRP) на випадок ransomware-атаки. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Експлуатація вразливості | Веб-додатки, сервери | Атакувальник через мережу використовує уразливість (наприклад, відсутній патч чи SQL-ін’єкцію) і отримує прямий доступ до бази даних з медичною інформацією. Наслідки – непомітне витікання великих обсягів даних (тисячі записів пацієнтів) без авторизації. Вплив високий: порушення конфіденційності, можливі штрафні санкції. Ймовірність залежить від наявності невиправлених вразливостей (за відсутності належного менеджменту оновлень – висока). | Середній/Високий (ймовірність середня; вплив високий) | Регулярний аналіз вразливостей та встановлення оновлень (патч-менеджмент); проведення пен-тестів і аудитів безпеки застосунків; використання Web Application Firewall (WAF) для захисту від веб-атак; мінімізація відкритих сервісів, строгий контроль конфігурацій. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Зловмисний інсайдер | База даних, внутрішні системи | Співробітник навмисно витягає конфіденційні дані (наприклад, повний реєстр пацієнтів) і передає їх стороннім. Наслідки – масштабний витік зсередини, який важко виявити одразу. | Високий (ймовірність нижча за зовнішні атаки, але вплив дуже високий) | Розмежування доступу за принципом необхідності (least privilege) – жоден співробітник не має зайвих прав; впровадження систем DLP для контролю витоку (моніторинг |

| | | | | |
|---|---|---|---|---|
| | | Вплив високий: компрометація довіри, юридичні наслідки (порушення законів про захист даних), фінансові втрати. Хоча ймовірність навмисних дій одного співробітника невисока, такі інциденти трапляються і складають значну частку витоків. | | пересилання файлів, друку, USB); журналювання доступу до важливих даних та регулярний аналіз логів; політика двох осіб для критичних операцій; ретельна перевірка персоналу при наймі, робота зі співробітниками (етичний кодекс. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Помилка персоналу (витік з необережності) | Електронна пошта, документи, хмарні сховища | Ненавмисне розголошення окремих записів або невеликих масивів даних: наприклад, медпрацівник відправив виписку не тому пацієнту, або помилково виклав файл з даними у публічний доступ. Наслідки – обмежений витік даних (одиничного пацієнта чи групи), але все одно порушення конфіденційності та можливі санкції. Вплив середній (локалізований витік), ймовірність висока (людський фактор присутній постійно). | Середній (ймовірність висока; вплив низький/середній) | Навчання та підвищення обізнаності персоналу щодо безпечного поводження з даними; впровадження політик класифікації інформації (помітки “для службового користування” тощо); налаштування DLP для контролю вихідної пошти (пошук номерів карток, персональних даних у вкладеннях); перевірка налаштувань доступу до загальних папок і хмарних сховищ; регулярні інструктажі щодо нових загроз соціальної інженерії. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Компрометація підрядника | Сторонні інтеграції, API | Зовнішній партнер (наприклад, провайдер IT-послуг або лабораторія) зламаний хакерами, що призводить до витоку медичних даних, якими партнер оперує. Наслідки – | Середній (ймовірність середня; вплив високий) | Укладення строгих договорів з вимогами з кібербезпеки для третіх сторін (BAA, NDA); аудит безпеки підрядників, вимога дотримання стандартів (наприклад, ISO 27001, HIPAA |

| | | | | |
|---|---|---|---|---|
| | | витік даних пацієнтів за межами основної організації, причому лікарня може навіть не відразу дізнатися про інцидент. Вплив високий (значний обсяг даних, порушення регуляторних вимог), ймовірність середня (цільові атаки на ланцюг постачання почастішали). | | для тих, хто працює з PHI); обмеження обсягу даних, доступного стороннім (мінімізація даних, необхідних для роботи); моніторинг аномальної активності на інтеграційних точках; плани реагування на інциденти, що включають третіх осіб. |

Продовження Додатку Ж

Таблиця 2.3 Матриця ризиків для загроз витоку даних

| | | | | |
|---|---|---|---|---|
| Втрата/крадіжка пристрою | Ноутбук, носій інформації | Пристрій із незашифрованими даними потрапляє до рук сторонніх осіб. Наслідки – можливий доступ до медичної інформації на пристрої, що порушує конфіденційність пацієнтів. Обсяг витоку залежить від даних на носії (наприклад, база на тисячі пацієнтів на жорсткому диску). Вплив середній (локальний характер, але може бути значним, якщо багато даних на пристрої); ймовірність середня (випадки втрати пристроїв трапляються). | Середній (ймовірність середня; вплив середній) | Шифрування дисків ноутбуків та мобільних пристроїв; використання засобів MDM (Mobile Device Management) для дистанційного очищення втрачених пристроїв; політика заборони зберігати дані локально без необхідності (використовувати захищені сервери); фізичний контроль доступу до пристроїв, маркування та інвентаризація носіїв; навчання персоналу не залишати пристрої без нагляду. |

**Додаток З**

**Таблиця 3.4 HLD-рішення до впровадження**

| Компонент | Призначення | Рекомендоване рішення / постачальник | Орієнтовна ціна | Примітки (інтеграція, відповідність GDPR/HIPAA/NIST) |
|---|---|---|---|---|
| Електронна медична картка (ЕМК / EHR) | Центральна МІС для ведення електронних медичних записів пацієнтів, розкладу прийому, рецептів, звітності. | МІС “Доктор Елекс” (визнана одна з найкращих в Україні для клінік) або аналогічна, сертифікована для eHealth. Забезпечує ведення картки пацієнта, історії хвороби, шаблони документів тощо. | ~500 000 – 1 000 000 грн на рік (залежно від розміру закладу). Напр., річна підтримка “Доктор Елекс” закуповувалася за ~995 тис. грн. Альтернатива SaaS: ~150 $/міс на лікаря. | Інтегрується з національною системою eHealth (через захищене API) – автоматично передає дані пацієнтів, декларацій, е-рецептів до ЦБД НСЗУ. Підтримує стандарти HL7/FHIR для обміну даними. Відповідає вимогам GDPR/HIPAA: налаштовуються ролі доступу, логування дій, шифрування даних на сервері. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| PACS (система архівування і передавання зображень) | Зберігання медичних зображень (рентген, КТ, МРТ), управління дослідженнями, надання доступу до знімків і описів. | Orthanc PACS сервер – легкий відкритий PACS/DICOM-сервер з веб-інтерфейсом; або комерційне PACS-рішення (напр. AGFA Impax, GE Centricity – за потреби). Orthanc як VNA (vendor-neutral archive) сумісний зі стандартом DICOM. | Ліцензія Orthanc – безкоштовна (open-source). Витрати – на серверне обладнання та дискові сховища (оцінково від 100 000 грн одноразово для сервера з RAID-масивом). Комерційні PACS: від кількох тисяч доларів за інсталяцію + підтримка. | Інтегрується з EHR: лікарі переглядають зображення через посилання/вьювер PACS із картки пацієнта. Всі зображення та DICOM-дані зберігаються локально; передача досліджень – за протоколом DICOM (можливе використання DICOMweb для веб-доступу). Необхідне налаштування доступу по HTTPS/VPN для віддаленого перегляду (щоб відповідати HIPAA). Дотримання GDPR: зображення – персоніфіковані дані, тому зберігання в захищеному середовищі, контроль доступу. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Лабораторна інформаційна система (LIS) | Управління лабораторними дослідженнями: направлення на аналізи, облік проб, автоматичне | OpenELIS або еквівалентна відкрита LIS (відсутність ліцензійного збору). Може | Open-source LIS – безкоштовно. Витрати – впровадження та підтримка (адміністрування, | Інтеграція з обладнанням лабораторії: LIS приймає дані від аналізаторів напряму або через проміжне ПЗ, що значно економить час лаборантів. Результати автоматично |

| | | | | |
|---|---|---|---|---|
| | отримання результатів та передача їх лікарям. | бути реалізована як модуль MIC (“Доктор Елекс” має модуль лабораторії, що інтегрується з аналізаторами). | інтеграція) ~50 000–100 000 грн. Комерційні LIS (як частина MIC) можуть входити в загальну вартість ліцензії. | завантажуються в EHR пацієнта. Забезпечено контроль доступу (тільки лаборанти/лікарі бачать сирі результати), ведеться аудит дій користувачів (вимога HIPAA). Дані лабораторії шифруються в базі або на рівні диску. Стандарти GDPR дотримані – чутлива інформація про здоров’я захищена. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| CRM система (для адміністрування та відносин з пацієнтами) | Управління записом пацієнтів, роботою контакт-центру, нагадуваннями, маркетингом послуг. Модуль фінансового обліку (рахунки, оплати), робота зі страховими. | Вбудований CRM-модуль МІС (як у “Доктор Елекс”) – покриває реєстратуру, контакт-центр, маркетинг. Альтернативно – Medcenter+ CRM (хмарна МІС для клінік) або інтеграція з загальним CRM (наприклад, Bitrix24) з доопрацюваннями під медицину. | Якщо CRM є частиною МІС – в ціні EHR. Окремий хмарний CRM Medcenter+ – ліцензія ~$150/лікар + $50/немедперсонал на місяць (понад 30 лікарів – індивідуальний тариф). Інтеграція з телефонією (Binotel та ін.) – ~350 грн/міс. | CRM синхронізовано з EHR: єдиний довідник пацієнтів, планування прийомів, відкриття картки пацієнта при дзвінку. Забезпечує розсилання нагадувань (SMS/Email) – потрібно отримувати згоду пацієнтів (GDPR). Контакт-центр автоматично фіксує звернення, оператори бачать історію пацієнта. Дані CRM (контакти, платежі) захищені відповідно до GDPR: шифрування каналу (HTTPS), обмеження на доступ до маркетингових даних. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| DICOM-сервер | Прийом та зберігання медичних зображень у форматі DICOM, обслуговування запитів Worklist та передачі | Orthanc DICOM Server – легковагий сервер, що підтримує повний стек DICOM-протоколів. Може працювати як | Безкоштовно (open-source). Закупівля серверів і СГД під образи – основна стаття | Інтеграція: всі модальності (УЗД, рентген апарати тощо) надсилають зображення на DICOM-сервер по мережі. Сервер веде Modality Worklist (список запланованих |

| | | | | |
|---|---|---|---|---|
| | знімків. Фактично, “серце” PACS. | VNA і як сервер для PACS/Workstations. Альтернатива – dcm4chee VNA (Java-базований, відкритий). | витрат. Для середньої установи (наприклад, 50 000 досліджень на рік) потрібно ~20 TB сховища; це ~$5 000 вартості обладнання. | досліджень) – отримує дані від EHR (через HL7/DICOM MWL). PACS-станції лікарів-рентгенологів підключаються до DICOM-сервера для отримання знімків. Забезпечено сумісність зі стандартом DICOM 3.0 та DICOMweb (за потреби веб-доступ). |

Продовження Додатку З

Таблиця 3.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Хмарні сервіси | Додаткові обчислювальні ресурси і сховища “в хмарі”. Використовуються для розміщення окремих підсистем (за потреби) або резервного копіювання/відновлення після збою (DR). | Microsoft Azure / Amazon AWS (EU Region) – для розгортання віртуальних серверів або зберігання резервних копій. Або локальні хмарні провайдери (наприклад, De Novo, GigaCloud в Україні) для | Залежить від споживаних ресурсів. Наприклад, резервне сховище на Azure для 5 TB даних – ~200 $/міс. Розгортання цілої MIC в хмарі – ~1000 $/міс (під середнє навантаження). | Розміщення MIC у хмарі: можливе для зменшення навантаження на IT-інфраструктуру клініки. Сервери MIC можуть знаходитися у захищеному хмарному центрі обробки даних – доступ через інтернет (HTTPS + VPN). ВВсі передані в хмару дані шифруються (наприклад, на рівні S3/Azure Blob налаштовується encryption-at-rest і передача по HTTPS). |

| | | | | |
|---|---|---|---|---|
| | | зберігання даних в юрисдикції України. | | |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Дата-центр (локальний) | Власна IT-інфраструктура лікарні: серверне обладнання, мережеве обладнання, СГД. Розміщення основних сервісів на території закладу. | Віртуалізована серверна ферма (2–3 фізичних сервери x86 з VMware vSphere або Hyper-V, Сховище SAN/NAS для даних). Сервери від HPE, Dell або Cisco UCS – із підтримкою відмовостійких компонентів (RAID, резервне живлення). | ~20 000 $ (≈ 740 тис. грн) капітальні витрати на обладнання середнього рівня. Вартість залежить від потужності: наприклад, 2 сервери по 64 GB RAM + дискова полиця на 50 TB. Щорічно ~10–15% на обслуговування (IT-персонал, гарантія). | Локальний дата-центр забезпечує зберігання даних *on-premises*, що спрощує контроль відповідності законодавству (дані не виходять за межі установи). Фізична безпека: серверна кімната з контролем доступу, UPS/генератор (NIST CSF *Protect*). Всі критичні системи (EHR, PACS, LIS) розгорнуті в локальній мережі під захистом міжмережевого екрану. Для відмовостійкості – налаштовано кластеризацію або резервні сервери, регулярне резервування. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Резервне копіювання (Backup) | Створення резервних копій баз даних EHR, знімків PACS, критичних віртуальних машин – для відновлення у разі збою, атак (наприклад, ransomware) або стихійного лиха. | Veeam Backup & Replication – рішення для резервування, популярне в охороні здоров'я (Windows/Linux VM, підтримка образів і журналів транзакцій). Альтернатива: Nakivo (бюджетніше), або open-source Bacula/Restic | Ліцензія Veeam: від ~$2000 (≈74 тис. грн) на рік для середньої клініки – залежно від кількості серверів/VM. Додатково – вартість носіїв: стрічковий стример LTO (~100 тис. грн) або хмарне сховище (~5 грн/GB щомісяця). | Інтеграція: резервні копії робляться щоденно (інкрементальні) з локальних серверів на резервний сервер/сховище. Налаштовано off-site копіювання до хмари (для географічного резерву) – ці копії позначаються як *immutable* (незмінні) для захисту від шифрувальників. Перевірка відновлюваності (SureBackup тестування) – раз на тиждень. Відповідність NIST CSF: реалізує *Recover*-функцію (швидке відновлення даних) та частково *Detect* (сповіщення про збої/цілісність). |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Мобільні додатки | Мобільний доступ до сервісів клініки. Додаток пацієнта: перегляд власної електронної картки, результатів аналізів, | Пацієнтський мобільний додаток від постачальника MIC. Наприклад, "Доктор Елекс" надає пацієнту мобільний застосунок | Входить у вартість MIC (для комерційних систем, що пропонують | Інтеграція: мобільний додаток пацієнта підключається до серверу EHR через захищене API (HTTPS + OAuth2 автентифікація). Пацієнт може переглядати результати, |

| | | | | |
|---|---|---|---|---|
| | запис на прийом, відеоконсультації з лікарем. Додаток лікаря: доступ до розкладу, перегляд історії хвороби, введення даних при виїздах. | з усією медичною історією, онлайн-записом, онлайн-оплатами і консультаціями. Для лікарів – веб-додаток або окремий мобільний застосунок, що підключається | мобільний портал). При розробці під замовлення – від 300 тис. грн. | призначення, спілкуватися з лікарем у чаті. Записи на прийом із мобільного синхронізуються з розкладом CRM в реальному часі. Безпека: відповідність GDPR – користувач дає згоду на отримання своїх даних; застосунок не зберігає персональні дані локально без шифрування. Передача даних – лише в зашифрованому вигляді |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| | | через VPN до внутрішньої системи. | | (TLS). Для телемедицини відеозв’язок реалізовано через безпечний канал (наприклад, WebRTC з шифруванням). HIPAA: мобільний доступ до PHI (Protected Health Information) захищений паролем, бажано MFA; лог дій (перегляд/завантаження даних) відправляється в центральний журнал. NIST CSF: мобільні клієнти враховані у політиках безпеки (керування пристроями, контроль сесій). |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| API інтеграція з eHealth (ЕСОЗ України) | Обмін даними з Центральною базою даних електронної системи охорони здоров'я (НСЗУ). Передача необхідних даних про пацієнтів, послуги, рецепти для державних реєстрів. | Модуль інтеграції eHealth у складі МІС. Усі сертифіковані МІС мають реалізовані API-виклики до ЦБД. З боку держави надається захищене REST API (HTTPS) + електронний підпис для автентифікації. | Включено у вартість МІС. Додатково – вартість КЕП (кваліфікований електронний підпис) для відповідальних осіб та захищений інтернет-канал. | МІС автоматично надсилає необхідні дані до eHealth: укладені декларації, направлення, інформацію для електронних лікарняних та рецептів. Інтеграція двостороння: отримання ID пацієнтів з центрального MPI (Master Patient Index), перевірка права на послуги, тощо. Безпека: передача даних по API здійснюється через шифроване з'єднання HTTPS з використанням TLS 1.2+; дані підписуються/шифруються згідно вимог НСЗУ. |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Телемедицина | Проведення дистанційних консультацій лікар-пацієнт, телеконсиліуми. Забезпечує відеозв’язок, передачу медичних даних (витягів, зображень) онлайн. | Інтегрована телемедична платформа в МІС (в “Доктор Елекс” є модуль онлайн-консультацій через мобільний додаток). Або сторонній сервіс: Zoom for Healthcare, Microsoft Teams (Healthcare) – з укладанням BAA для HIPAA. | Вбудована у МІС – без додаткової оплати (як правило, оплачується через загальну ліцензію). Zoom: ~$200/місяць за медичний тариф. Розгортання власного відеосервера (Jitsi) – ~50 000 грн одноразово + підтримка. | Інтеграція: телемедичний модуль пов’язаний з EHR – призначення телеприйомів видно в розкладі, після консультації лікар вносить запис у електронну картку. Пацієнт підключається до сеансу через мобільний додаток або веб-портал, лікар – зі свого ПК. Обмін відео/аудіо – через захищений канал (WebRTC, шифрування end-to-end). Відповідність стандартам: платформа відповідає вимогам HIPAA (шифрування даних, автентифікація учасників). |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| VPN (Virtual Private Network) | Захищений канал для віддаленого підключення до внутрішніх ресурсів лікарні. Забезпечує шифрування трафіку через недовірені мережі (інтернет). Використовується лікарями для віддаленої роботи, підключення філій, а також для безпечної передачі даних між клінікою і хмарою. | OpenVPN (програмний VPN, з підтримкою SSL/TLS). Апаратні реалізації: VPN-сервер на базі MikroTik або інтегрований в міжмережевий екран (напр. Fortinet FortiGate має IPSec/SSL VPN). | OpenVPN – безкоштовно (потрібен лише сервер). Апаратний VPN-шлюз (середній) – ~$1000. Витрати включають налаштування та підтримку. | Інтеграція: VPN-шлюз встановлено на межі мережі (як правило, на міжмережевому екрані). Лікарі та адмінперсонал можуть підключатися зі своїх домашніх ПК/ноутбуків через VPN-клієнт, отримуючи доступ до EHR, PACS та інших систем так, ніби вони в локальній мережі. Дані в тунелі шифруються (AES-256 або подібним алгоритмом). Безпека: доступ видається лише уповноваженим користувачам, використовується двофакторна автентифікація . |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Міжмережевий екран (Firewall) | Захист периметру мережі клініки від несанкціонованого доступу, фільтрація трафіку, розмежування сегментів мережі (медична мережа, гостьова, зовнішні підключення). | NGFW (Next-Generation Firewall) – напр. *Fortinet FortiGate*, *Palo Alto*, *Cisco Secure Firewall*. Або програмно-апаратний комплекс на базі pfSense (open-source) для менших бюджетів. | Середній NGFW для клініки: ~3000 $ (≈111 тис. грн) за пристрій + підписка на оновлення сигнатур (UTM-функції) ~$500/рік. pfSense на власному сервері – ~30 тис. грн (сервер) + трудовитрати. | Інтеграція і функції: брандмауер встановлено на стику між локальною мережею лікарні та інтернетом. Налаштовано правила, що дозволяють лише потрібний трафік: VPN-з'єднання, запити до API eHealth, веб-доступ пацієнтів до порталу тощо – все інше блокується. Впроваджено сегментацію: окремо мережа медичних приладів/PACS, офісна мережа, гостьовий WiFi – між ними VLAN і фільтрація. Безпека: NGFW забезпечує виявлення та запобігання вторгнень (IDS/IPS), веб-фільтрацію, антивірус на |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| Міжмережевий екран (Firewall) | Захист периметру мережі клініки від несанкціонованого доступу, фільтрація трафіку, розмежування | NGFW (Next-Generation Firewall) – напр. *Fortinet FortiGate*, *Palo* | Середній NGFW для клініки: ~3000 $ (≈111 тис. грн) за пристрій + підписка на оновлення | шлюзі. Це відповідає вимогам NIST CSF щодо функцій *Protect* і *Detect*. Журнали firewall (всі підозрілі пакети, спроби доступу) передаються в систему |

| | | | | |
|---|---|---|---|---|
| | сегментів мережі (медична мережа, гостьова, зовнішні підключення). | *Alto*, *Cisco Secure Firewall*. Або програмно-апаратний комплекс на базі pfSense (open-source) для менших бюджетів. | сигнатур (UTM-функції) ~$500/рік. pfSense на власному сервері – ~30 тис. грн (сервер) + трудовитрати. | моніторингу безпеки (SIEM) для аналізу. GDPR/HIPAA: міжмережевий екран запобігає неавторизованому доступу до персональних даних через інтернет, що є обов'язковою технічної мірою безпеки. Регулярно оновлюються сигнатури атак та прошивка (вимога стандартів кібербезпеки). |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| SIEM (Security Information and Event Management) | Система моніторингу безпеки, що збирає та аналізує журнали подій з усіх компонентів: серверів EHR/LIS/PACS, мережевого обладнання, ОС користувачів. Дозволяє виявляти атаки та інциденти інформаційної безпеки. | OSSIM/AT&T Cybersecurity (open-source SIEM, основана на AlienVault) або Wazuh (відкритий SIEM на базі ElasticStack). Для більшого закладу – Splunk Enterprise Security, IBM QRadar (потужні, але дорогі). Можливий аутсорсинг у вигляді MSSP/SOC послуг. | Open-source SIEM: безкоштовно, але потрібен сервер (~20 тис. грн) і спеціаліст для підтримки. Комерційні: від $10 000 на рік (залежно від обсягу логів). | Інтеграція: всі системи налаштовано на надсилання логів на SIEM у режимі реального часу. Наприклад, журнали доступу до EHR, аудиту дій з медичними даними, логи VPN підключень, спрацьовування firewall IPS – агрегуються та корелюються. SIEM містить правила виявлення підозрілої активності: спроби підбору паролів, доступ до медзапису поза робочим часом, масове копіювання даних тощо. При виявленні інциденту – автоматичне сповіщення ІБ-персоналу (email/SMS). Відповідність NIST CSF: реалізує |

Продовження Додатку З

Таблиця З.4 HLD-рішення до впровадження

| | | | | |
|---|---|---|---|---|
| SIEM (Security Information and Event Management) | Система моніторингу безпеки, що збирає та аналізує журнали подій з усіх компонентів: серверів EHR/LIS/PACS, мережевого обладнання, | OSSIM/AT&T Cybersecurity (open-source SIEM, основана на AlienVault) або Wazuh (відкритий | Open-source SIEM: безкоштовно, але потрібен сервер (~20 тис. грн) і спеціаліст для | функції *Detect* та *Respond* – дозволяє швидко виявити кібератаку і вжити заходів. GDPR: допомагає виконати вимогу про здатність виявляти факти порушення захисту |

| | | | | |
|---|---|---|---|---|
| | ОС користувачів. Дозволяє виявляти атаки та інциденти інформаційної безпеки. | SIEM на базі ElasticStack). Для більшого закладу – Splunk Enterprise Security, IBM QRadar (потужні, але дорогі). Можливий аутсорсинг у вигляді MSSP/SOC послуг. | підтримки. Комерційні: від $10 000 на рік (залежно від обсягу логів). | персональних даних (і повідомляти про витоки протягом 72 год). HIPAA: забезпечує аудит і протоколювання доступів до PHI, що вимагається Правилом Безпеки. Логи зберігаються тривалий час у захищеному вигляді (що також відповідає принципам непідробності і цілісності даних). |