МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ПРОТИДІЯ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ ПРОТИВНИКА У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ МЕДИЧНОЇ СИСТЕМИ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Вадим МАНГУБІ

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

APT – Advanced Persistent Threats, довготривалі цільові атаки

BC – Business Continuity, безперервність бізнесу

CERT-UA – Computer Emergency Response Team of Ukraine, Урядова команда реагування на комп'ютерні надзвичайні події України

CIA Triad – Confidentiality, Integrity, Availability Triad, тріада конфіденційності, цілісності та доступності

CSIRT – Computer Security Incident Response Team, команда реагування на інциденти комп'ютерної безпеки

CSIRT-M – Computer Security Incident Response Team for Medical facilities, команда реагування на кіберінциденти для медичних закладів

DDoS – Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»

DPIA – Data Protection Impact Assessment, оцінка впливу на захист даних

DR – Disaster Recovery, аварійне відновлення

DSSZZI – Державна служба спеціального зв'язку та захисту інформації України

EDR – Endpoint Detection and Response, виявлення та реагування на кінцевих пристроях

ePHI – electronic Protected Health Information, електронна медична інформація пацієнтів

ESCO – Energy Service Company, енергосервісна компанія

ESOZ (ЕСОЗ) – Електронна система охорони здоров'я

GDPR – General Data Protection Regulation, Загальний регламент захисту даних ЄС

Health-ISAC – Healthcare Information Sharing and Analysis Center, центр обміну інформацією та аналізу у сфері охорони здоров'я

HIPAA – Health Insurance Portability and Accountability Act, американський закон про переносимість і підзвітність медичного страхування

HL7 – Health Level 7, стандарт обміну медичними даними

ІВ (ІБ) – Інформаційна безпека

IDS/IPS – Intrusion Detection/Prevention Systems, системи виявлення та запобігання вторгненням

IoC – Indicators of Compromise, індикатори компрометації

IoMT – Internet of Medical Things, інтернет медичних речей

IS (ІС) – Інформаційна система

ISO – International Organization for Standardization, Міжнародна організація зі стандартизації

IT (ІТ) – Information Technology, інформаційні технології

КВ (КБ) – Кібернетична безпека

КВР (КБП) – Кіберпростір

KPI – Key Performance Indicators, ключові показники ефективності

MFA – Multi-Factor Authentication, багатофакторна автентифікація

MIC – Медична інформаційна система

МОЗ – Міністерство охорони здоров'я України

NATO (НАТО) – North Atlantic Treaty Organization, Організація Північноатлантичного договору

NGFW – Next-Generation Firewall, міжмережевий екран нового покоління

NIS2 – Network and Information Security Directive 2, Директива ЄС про мережеву та інформаційну безпеку (друга редакція)

NSZU (НСЗУ) – Національна служба здоров'я України

ОКІ (ОКІ) – Об'єкт критичної інфраструктури

OSINT – Open Source Intelligence, розвідка з відкритих джерел

OZ (ОЗ) – Охорона здоров'я

RBAC – Role-Based Access Control, контроль доступу на основі ролей

SBU (СБУ) – Служба безпеки України

SD – Соціальна інженерія (Social Engineering)

SIEM – Security Information and Event Management, управління інформацією та подіями безпеки

SLA – Service Level Agreement, угода про рівень обслуговування

SOC – Security Operations Center, центр операцій безпеки

SDP – Software-Defined Perimeter, програмно-визначений периметр

SSO – Single Sign-On, єдиний вхід

STANAG – Standardization Agreement, стандартизаційна угода НАТО

SUIB (СУІБ) – Система управління інформаційною безпекою

UIB (УІБ) – Управління інформаційною безпекою

US-CERT – United States Computer Emergency Readiness Team, Команда готовності до комп'ютерних надзвичайних ситуацій США

VLAN – Virtual Local Area Network, віртуальна локальна мережа

VMaaS – Vulnerability Management as a Service, управління вразливостями як сервіс

VPN – Virtual Private Network, віртуальна приватна мережа

XDR – Extended Detection and Response, розширене виявлення та реагування

ZTNA – Zero Trust Network Access, мережевий доступ з нульовою довірою

Zero-day – вразливість програмного забезпечення, невідома виробнику, для якої не існує оновлень безпеки

ВСТУП

Актуальність теми дослідження. В умовах повномасштабної війни система охорони здоров'я України перетворилася з соціальної сфери на об'єкт критичної інфраструктури, що зазнає систематичних інформаційних операцій та кібератак з боку агресора. Якщо до 2022 року вітчизняні медичні заклади стикалися переважно з випадковими кіберзлочинами фінансового характеру, то з початком повномасштабної агресії медична галузь стала ціллю координованих державних кібероперацї, що проводяться спецслужбами противника або підконтрольними їм хакерськими групами [2].

Цифрова трансформація медичної галузі останнього десятиліття, впровадження Електронної системи охорони здоров'я (ЕСОЗ), перехід на електронні медичні картки, цифровізація адміністративних процесів створили якісно нову інформаційну інфраструктуру. Водночас ці процеси сформували нові вразливості, які активно експлуатуються в рамках гібридної війни. За даними CERT-UA, кількість кібератак на медичну інфраструктуру зросла у десятки разів, а їхня складність та потенційний збиток істотно підвищилися [25].

Особлива небезпека полягає в тому, що інформаційні операції проти медичної системи мають подвійний вплив. Технічні кібератаки можуть безпосередньо загрожувати життю пацієнтів через порушення роботи критичних систем, а дезінформаційні кампанії підривають довіру населення до медичних інституцій, що має довгострокові наслідки для соціальної стабільності. В умовах війни, коли медична система функціонує на межі можливостей, такі атаки можуть призвести до критичної дезорганізації надання медичної допомоги.

Попри накопичення практичного досвіду протидії кіберзагрозам, вітчизняна система охорони здоров'я залишається вразливою через фрагментованість захисту, відсутність галузевих стандартів кібербезпеки, хронічний дефіцит кваліфікованих кадрів та технічну застарілість інфраструктури. Існуючі дослідження переважно фокусуються на технічних

аспектах кіберзахисту, тоді як комплексний підхід до протидії інформаційним операціям з позицій публічного управління залишається недостатньо розробленим [29].

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконано в рамках наукових інтересів кафедри та узгоджується з пріоритетними напрямами розвитку науки і техніки в Україні, зокрема з напрямом «Інформаційне суспільство» та Стратегією кібербезпеки України [49].

Мета і завдання дослідження. Метою роботи є розробка науково обґрунтованих рекомендацій щодо вдосконалення системи протидії інформаційним операціям у сфері охорони здоров'я України на основі комплексного аналізу сучасних загроз, існуючих механізмів захисту та міжнародного досвіду [15].

Для досягнення мети поставлено такі *завдання*:

– систематизувати теоретико-методологічні засади протидії інформаційним операціям у медичній сфері, визначити ключові концепції та проаналізувати структурні вразливості системи охорони здоров'я;

– дослідити сучасний ландшафт загроз для медичної інфраструктури, класифікувати типи кібератак та інформаційних операцій, проаналізувати гібридні сценарії їхньої координації;

– оцінити ефективність існуючих інституційних, технічних та організаційних механізмів протидії, виявити системні прогалини та критичні вразливості;

– провести компаративний аналіз моделей кібербезпеки медичної галузі у Європейському Союзі, країнах НАТО та Україні;

– розробити стратегічні напрями організаційно-інституційного розвитку, технологічної модернізації та розвитку людського капіталу для підвищення стійкості медичної системи до інформаційних операцій [6].

Об'єкт дослідження – процеси забезпечення інформаційної безпеки у сфері охорони здоров'я України в умовах гібридної війни.

Предмет дослідження – механізми публічного управління протидією

інформаційним операціям у медичній галузі [32].

Методи дослідження. У роботі використано комплекс загальнонаукових та спеціальних методів: системний підхід – для аналізу структури та взаємозв'язків елементів системи кібербезпеки медичної галузі; компаративний аналіз – для порівняння моделей кібербезпеки ЄС, НАТО та України; метод експертних оцінок – для оцінювання ефективності існуючих механізмів захисту; контент-аналіз – для дослідження дезінформаційних кампаній у соціальних мережах; структурно-функціональний метод – для визначення функцій та повноважень запропонованих організаційних структур [14].

Одержані результати дозволили сформувати комплексний міждисциплінарний підхід до протидії інформаційним операціям. Цей підхід інтегрує сучасні концепції кібербезпеки, реальний досвід боротьби з гібридними загрозами та стратегічне бачення подальшого розвитку галузі.

У роботі обґрунтовано модель багаторівневої системи кібербезпеки для медичної сфери, яка включає національний галузевий центр, регіональні центри компетенції та чіткі механізми координації. Автором здійснено синтез європейських регуляторних норм (GDPR/NIS2), натовської концепції проактивної оборони («Defend Forward») та унікального українського досвіду війни. Це дозволило створити гібридну модель безпеки, адаптовану саме до специфіки вітчизняної медицини. Крім того, запропоновано комплексну стратегію розвитку людського капіталу, що передбачає запуск спеціалізованих освітніх програм, систему галузевої сертифікації та заходи з формування культури безпеки [7].

Практичне значення одержаних результатів. Розроблені рекомендації мають прикладний характер та можуть бути використані:

– Міністерством охорони здоров'я України – при розробці галузевих стандартів кібербезпеки та створенні галузевого центру;

– Національною службою здоров'я України – для посилення захисту ЕСОЗ та встановлення вимог до кібербезпеки медичних закладів;

– регіональними управліннями охорони здоров'я – при організації

регіональних центрів компетенції;

– медичними закладами – для вдосконалення власних систем захисту та навчання персоналу [34].

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

1.1 Публічне управління та роль держави у протидії інформаційним операціям

Сучасний етап розвитку українського суспільства характеризується безпрецедентними викликами національної безпеки, спричиненими повномасштабною гібридною агресією російської федерації. У таких умовах система охорони здоров'я набула стратегічного значення, перетворившись із соціальної сфери на об'єкт критичної інфраструктури, що потребує комплексного захисту від різноманітних гібридних загроз.

Цифрова трансформація медичної галузі останнього десятиліття супроводжувалася масштабною інформатизацією усіх рівнів надання медичної допомоги. Впровадження Електронної системи охорони здоров'я (ЕСОЗ), перехід на електронні медичні картки пацієнтів, цифровізація адміністративних процесів і впровадження телемедицини створили якісно нову інформаційну інфраструктуру. Водночас ці процеси сформували нові вразливості, які активно експлуатуються противником у рамках інформаційних та кібероперацї [28].

Актуальність дослідження теоретико-методологічних засад протидії інформаційним операціям у сфері охорони здоров'я зумовлена кількома факторами. По-перше, медичні дані належать до найчутливіших категорій персональної інформації, а їх витік чи спотворення може мати критичні наслідки як для окремих громадян, так і для національної безпеки загалом. По-друге, інформаційні атаки на медичну інфраструктуру спрямовані не лише на технічне порушення функціонування систем, а й на підрив довіри населення до державних інституцій. По-третє, в умовах воєнного стану медична система виконує

подвійну роль – забезпечує цивільну охорону здоров'я та підтримує обороноздатність держави через систему військово-медичного забезпечення [23].

Цей розділ присвячений системному дослідженню та структуризації теоретико-методологічного фундаменту, необхідного для розуміння природи інформаційного протиборства у медичній сфері. Основна увага приділяється визначенню ключових концепцій інформаційної та кібернетичної безпеки, аналізу структурних вразливостей вітчизняної системи охорони здоров'я, систематизації міжнародного досвіду забезпечення кіберзахисту медичних закладів та обґрунтуванню організаційно-управлінських механізмів протидії гібридним загрозам. Теоретичне осмислення цих аспектів є необхідною передумовою для розробки практичних рекомендацій щодо підвищення стійкості медичної інфраструктури в умовах інформаційної війни [35].

Сучасна парадигма публічного управління розглядає протидію інформаційним операціям як невід'ємну стратегічну функцію держави, що безпосередньо впливає на забезпечення національної безпеки. Трансформація характеру збройних конфліктів XXI століття засвідчила, що інформаційне протиборство перетворилося на автономну складову військової кампанії, здатну системно виснажувати державність противника без застосування традиційних воєнних засобів.

Аналіз воєнних конфліктів останніх двох десятиліть демонструє принципову зміну пріоритетів у веденні бойових дій. Якщо у минулому столітті головною метою було фізичне знищення військового потенціалу супротивника, то сьогодні пріоритетом стає руйнування його інформаційної інфраструктури, дезорганізація систем управління та підрив морально-психологічного стану як армії, так і цивільного населення. Особливо яскраво ця тенденція проявилася під час російської агресії проти України, коли поряд із класичними військовими діями противник систематично здійснює масовані кібератаки на критичну інфраструктуру, поширює дезінформацію та проводить психологічні операції [3].

У цьому контексті ефективність публічного управління у сфері охорони здоров'я визначається не лише традиційними показниками функціональності системи – доступністю, якістю та своєчасністю медичної допомоги, – але й здатністю гарантувати її захищеність від цілеспрямованого гібридного впливу. Медична галузь стає об'єктом інформаційних операцій з кількох причин.

По-перше, порушення функціонування медичних закладів завдає прямої шкоди здоров'ю та життю громадян, що створює паніку у суспільстві та підриває довіру до влади. По-друге, медичні бази даних містять величезні масиви конфіденційної інформації, що може використовуватися для шантажу, маніпуляцій або розвідувальної діяльності. По-третє, дезінформаційні кампанії щодо епідеміологічної ситуації, якості медичної допомоги або безпеки вакцинації здатні спровокувати соціальну нестабільність та послабити обороноздатність країни.

Механізм забезпечення національної безпеки у критично важливій сфері охорони здоров'я ґрунтується на принципах комплексного управління ризиками. Цей підхід передбачає систематичну ідентифікацію потенційних загроз, оцінку їхньої ймовірності та можливих наслідків, розробку превентивних заходів і створення систем оперативного реагування. Водночас управління національною безпекою виконує подвійну функцію: з одного боку, воно спрямоване на блокування деструктивних зовнішніх впливів, а з іншого – на стимулювання внутрішніх процесів розвитку, що підвищують стійкість системи [13].

Державна політика у сфері протидії інформаційним операціям реалізується через систему органів виконавчої влади, кожен з яких має специфічні повноваження та зони відповідальності. Координація їхньої діяльності здійснюється на рівні Ради національної безпеки і оборони України, що визначає стратегічні пріоритети та контролює виконання ключових рішень. Міністерство охорони здоров'я України відповідає за формування галузевої політики інформаційної безпеки, розробку відповідних стандартів та методичних рекомендацій. Державна служба спеціального зв'язку та захисту інформації забезпечує технічний кіберзахист об'єктів критичної інфраструктури, до яких

належать медичні заклади. Служба безпеки України здійснює контррозвідувальні заходи, виявляє та нейтралізує спроби іноземних спецслужб проникнути до інформаційних систем медичної галузі [51].

Ефективність цієї багаторівневої системи безпеки залежить не лише від чіткого розподілу повноважень, а й від налагодженої міжвідомчої взаємодії, оперативного обміну інформацією про загрози та спільного планування заходів реагування. Досвід останніх років засвідчив, що найбільш вразливими виявилися ті ланки медичної системи, де координація між різними державними структурами була недостатньою або взагалі відсутньою.

Формування ефективної стратегії протидії інформаційним операціям вимагає чіткого розмежування ключових понять, що часто вживаються як взаємозамінні, хоча насправді відображають різні аспекти захисту інформаційного простору. Термінологічна плутанина у цій сфері може призвести до помилкового визначення пріоритетів, нераціонального розподілу ресурсів та, зрештою, до неефективності заходів безпеки.

Інформаційна безпека є найширшою концепцією, що охоплює увесь спектр заходів щодо захисту інформаційного простору держави. У сучасній науковій літературі інформаційна безпека трактується як стан захищеності національної інфосфери, що гарантує безперешкодне формування, використання та розвиток інформаційних ресурсів, необхідних для реалізації національних інтересів. Принципова відмінність цієї концепції полягає у її комплексності – інформаційна безпека орієнтована не лише на технічний захист даних, але й на захист свідомості персоналу та суспільства загалом від маніпулятивних впливів, дезінформації та психологічних операцій.

Класичною основою інформаційної безпеки є тріада CIA (Confidentiality, Integrity, Availability), що визначає три фундаментальні властивості інформації, які необхідно захищати. Конфіденційність означає обмеження доступу до інформації лише для авторизованих користувачів. У контексті охорони здоров'я це передусім стосується електронної медичної інформації пацієнтів (ePHI), яка містить діагнози, результати аналізів, відомості про лікування та іншу чутливу

інформацію. Порушення конфіденційності медичних даних може мати серйозні наслідки – від дискримінації пацієнтів на ринку праці чи страхування до шантажу та психологічного тиску [1].

Цілісність інформації гарантує, що дані не були несанкціоновано змінені або знищені у процесі зберігання чи передачі. У медичній практиці це має критичне значення, оскільки спотворення медичних записів може призвести до помилкової діагностики, призначення неадекватного лікування і, як наслідок, до загрози життю пацієнта. Доступність забезпечує своєчасний доступ авторизованих користувачів до необхідної інформації. Для медичних закладів це означає, що лікарі повинні мати можливість негайно отримати дані пацієнта для надання екстреної допомоги, незалежно від технічних збоїв чи кібератак.

Кібернетична безпека є більш вузькою, технологічно орієнтованою концепцією, що фокусується на захисті кіберпростору та окремих об'єктів інформаційної інфраструктури від зовнішнього кібервпливу. Якщо інформаційна безпека охоплює широкий спектр загроз, включаючи соціальні та психологічні аспекти, то кібербезпека зосереджена на технічних засобах захисту комп'ютерних систем, мереж і даних від кібератак, несанкціонованого доступу, вірусів та інших форм кіберзлочинності.

Об'єктами захисту у кібербезпеці є апаратні засоби (сервери, робочі станції, медичне обладнання, підключене до мережі), програмне забезпечення (операційні системи, медичні інформаційні системи, додатки), канали зв'язку (локальні та глобальні мережі, бездротові з'єднання) та бази даних. У сфері охорони здоров'я особливу увагу приділяють захисту медичних пристроїв Інтернету речей (IoMT – Internet of Medical Things), оскільки їхнє зламування може становити пряму загрозу життю пацієнтів, що використовують імплантовані або носимі медичні прилади [26].

Кіберпростір визначається як віртуальне комунікаційне середовище, утворене глобальною системою зв'язків між користувачами та об'єктами інформаційної інфраструктури. У сучасних стратегічних документах провідних держав світу кіберпростір розглядається як п'ятий вимір бойового простору

(поряд із сухопутним, морським, повітряним та космічним), що потребує особливих підходів до забезпечення безпеки. Теоретики кібербезпеки виділяють три рівні кіберпростору: фізичний (апаратні засоби та канали зв'язку), синтаксичний (програмне забезпечення та протоколи передачі даних) і семантичний (зміст інформації та її сприйняття користувачами). Для ефективного захисту необхідно забезпечити безпеку на всіх трьох рівнях одночасно [50].

В умовах гібридної війни концепції інформаційної та кібернетичної безпеки не можуть розглядатися ізольовано одна від одної. Сучасні інформаційні операції противника поєднують кібератаки на технічну інфраструктуру з психологічними операціями та дезінформаційними кампаніями. Наприклад, зламування медичної інформаційної системи може супроводжуватися витоком конфіденційних даних та їхнім використанням у пропагандистських цілях. Тому ефективна стратегія безпеки повинна органічно об'єднувати технічну оборону інфраструктури (кібербезпека) із захистом ментального простору (інформаційна безпека та психологічна стійкість персоналу і населення).

Окремої уваги заслуговує концепція стійкості (resilience), яка у сучасній теорії безпеки поступово витісняє традиційний підхід, орієнтований на пасивну оборону. Якщо класична модель безпеки передбачала створення «непробивного щита» проти відомих загроз, то концепція стійкості визнає неможливість абсолютного захисту і фокусується на здатності системи продовжувати функціонувати навіть під час атаки, швидко відновлюватися після інциденту та адаптуватися до нових викликів. У сфері охорони здоров'я це означає, що медичний заклад повинен не лише захистити електронні медичні дані, але й гарантувати безперервність надання медичної допомоги навіть у разі часткового або повного виходу з ладу інформаційних систем. Це досягається через резервування критично важливих компонентів інфраструктури, регулярне створення резервних копій даних, розробку детальних планів аварійного відновлення та проведення тренувань персоналу для дій в умовах кризових ситуацій.

Роль держави у протидії інформаційним операціям реалізується через комплексний державно-правовий механізм забезпечення національної безпеки, який являє собою динамічну систему взаємопов'язаних елементів. У сфері протидії інформаційним загрозам цей механізм функціонує через послідовні, хоча й частково паралельні стадії, що утворюють безперервний цикл управління безпекою.

Перша стадія – формулювання національних інтересів у сфері інформаційної безпеки охорони здоров'я. До таких інтересів належать: захист конфіденційності персональних медичних даних громадян від несанкціонованого доступу та витоків; забезпечення безперервного функціонування медичних інформаційних систем навіть в умовах кібератак; збереження та зміцнення довіри населення до системи охорони здоров'я та державних інституцій загалом; запобігання використанню медичної інформації у розвідувальних або диверсійних цілях противником.

Друга стадія передбачає виявлення та прогнозування загроз на основі постійного моніторингу внутрішнього та зовнішнього середовища. Ключовим суб'єктом на цій стадії виступає Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), яка відповідає за організацію кіберзахисту об'єктів критичної інфраструктури. ДССЗЗІ координує діяльність Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA), що здійснює цілодобовий моніторинг кіберпростору, аналізує індикатори компрометації та випускає оперативні попередження про нові загрози. Паралельно Служба безпеки України через свої підрозділи кіберзахисту виявляє спроби іноземних спецслужб впровадити агентурні мережі в медичних закладах або отримати несанкціонований доступ до стратегічно важливої медичної інформації [36].

Третя стадія – вироблення системи заходів протидії – передбачає розробку комплексу технічних, програмних, правових та організаційних заходів у відповідь на ідентифіковані загрози. Технічні заходи включають впровадження засобів криптографічного захисту інформації, системи виявлення і запобігання вторгненням (IDS/IPS), багатофакторної автентифікації користувачів.

Організаційні заходи охоплюють розробку політик безпеки, регламентацію процедур доступу до інформаційних ресурсів, проведення регулярних тренінгів для персоналу щодо інформаційної гігієни та протидії соціальній інженерії.

Четверта стадія – нейтралізація загроз – являє собою оперативне реагування на кіберінциденти та інформаційні операції у режимі реального часу. Це вимагає тісної координації між медичними закладами, CERT-UA та підрозділами СБУ. За діючою нормативною базою власники об'єктів критичної інфраструктури зобов'язані негайно повідомляти про кіберінциденти до CERT-UA та забезпечувати доступ фахівців до скомпрометованих систем для розслідування та ліквідації наслідків атаки.

П'ята стадія – здійснення заходів щодо відновлення – передбачає впровадження планів аварійного відновлення (Disaster Recovery Plans) та планів забезпечення безперервності роботи (Business Continuity Plans). Медичні заклади, що належать до критичної інфраструктури, зобов'язані розробляти та регулярно актуалізувати такі плани, а також проводити навчання для відпрацювання дій персоналу у кризових ситуаціях.

Нормативно-правова база кіберзахисту в Україні формувалася поступово, у відповідь на зростання кіберзагроз та під впливом процесу євроінтеграції. Фундаментом правового регулювання є Закон України «Про основні засади забезпечення кібербезпеки України» (2017), що визначив об'єкти кіберзахисту, суб'єктів забезпечення кібербезпеки та їхні повноваження, основні напрями державної політики у цій сфері. Цей закон запровадив поняття об'єктів критичної інфраструктури та встановив особливі вимоги до їхнього захисту [33].

Закон України «Про критичну інфраструктуру» (2021) конкретизував порядок віднесення об'єктів до критичної інфраструктури, установив процедури категоризації та сертифікації об'єктів за рівнем критичності. Медичні заклади, залежно від їхньої потужності, територіального значення та стратегічної важливості, можуть належати до різних категорій критичності, що визначає обсяг та строгість вимог щодо кіберзахисту [45].

Постанова Кабінету Міністрів України №518 від 19 червня 2019 року «Про

затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» встановила базові технічні та організаційні стандарти, яких повинні дотримуватися власники та користувачі таких об'єктів. Ці вимоги охоплюють організацію системи управління кібербезпекою, контроль доступу до інформаційних ресурсів, захист від шкідливого програмного забезпечення, моніторинг подій безпеки, управління інцидентами та забезпечення безперервності роботи [40].

Постанова КМУ №1426 від 12 грудня 2022 року затвердила Положення про організаційно-технічну модель кіберзахисту об'єктів критичної інфраструктури, що деталізувала вимоги до побудови системи кіберзахисту на різних рівнях. Ця модель передбачає створення трирівневої архітектури захисту: на рівні окремого об'єкта, на галузевому рівні та на національному рівні [41].

Постанова КМУ №299 від 27 березня 2019 року «Деякі питання об'єктів критичної інфраструктури» регламентує порядок повідомлення про кіберінциденти, процедури розслідування та механізми міжвідомчої взаємодії під час реагування на кібератаки [42].

Наказ Адміністрації Держспецзв'язку №877 встановив уніфіковані форми Планів захисту об'єктів критичної інфраструктури, що значно спростило процес планування заходів безпеки та забезпечило можливість централізованого контролю за їхньою повнотою та актуальністю.

Слід зазначити, що українське законодавство у сфері кібербезпеки продовжує розвиватися під впливом імплементації європейських стандартів, зокрема Директиви NIS2, а також з урахуванням практичного досвіду протидії російським кібератакам у період повномасштабної агресії [47].

1.2 Організаційна структура медичної системи та її вразливості

Система охорони здоров'я України являє собою складну багаторівневу структуру, що об'єднує медичні заклади різних форм власності, рівнів підпорядкування та функціонального призначення. Реформування медичної галузі останніх років, спрямоване на підвищення доступності та якості медичних послуг, супроводжувалося глибокою цифровою трансформацією, що принципово змінило характер інформаційних потоків і створило нові виклики для безпеки.

Впровадження Електронної системи охорони здоров'я (ЕСОЗ) стало наріжним каменем цифровізації медичної галузі. ЕСОЗ об'єднала у єдиному інформаційному просторі первинну, вторинну та третинну ланки надання медичної допомоги, забезпечила електронний документообіг між медичними закладами, Національною службою здоров'я України та пацієнтами. У системі накопичуються величезні масиви електронної медичної інформації пацієнтів (ePHI – electronic Protected Health Information), що включає персональні дані, медичну історію, результати діагностичних досліджень, призначення та рецепти [30].

Саме ця концентрація чутливої інформації у цифровому форматі перетворила систему охорони здоров'я на привабливу ціль для кібератак та інформаційних операцій противника. На відміну від інших галузей критичної інфраструктури, де об'єктом атак є переважно технологічні процеси, у медичній сфері під загрозою опиняються безпосередньо життя та здоров'я людей. Блокування доступу до електронних медичних карток під час надання невідкладної допомоги, спотворення інформації про діагнози чи дозування ліків, витік конфіденційних медичних даних – усе це може мати фатальні наслідки.

Водночас медична система демонструє специфічні вразливості, що відрізняють її від інших об'єктів критичної інфраструктури. Ці вразливості мають комплексний характер і формуються на перетині організаційних,

технічних, кадрових та регуляторних проблем, які накопичувалися протягом років недофінансування та фрагментарного підходу до модернізації галузі.

Аналіз стану інформаційної безпеки у вітчизняній системі охорони здоров'я дозволяє виокремити кілька взаємопов'язаних системних проблем, що формують структурні вразливості перед зовнішніми інформаційними операціями.

Фрагментованість та децентралізованість інформаційного простору. Процес інформатизації медичної галузі відбувався без єдиної централізованої стратегії, що призвело до формування мозаїчного ІТ-ландшафту. Різні медичні заклади використовують різнорідні медичні інформаційні системи (МІС), які часто несумісні між собою або мають обмежену інтероперабельність. Регіональні та комунальні заклади охорони здоров'я самостійно обирали програмні рішення, керуючись переважно ціновими критеріями, без належної оцінки їхньої безпеки та відповідності національним стандартам.

Така фрагментованість створює низку проблем для забезпечення інформаційної безпеки. По-перше, вона ускладнює централізований моніторинг загроз та оперативне виявлення кіберінцидентів у режимі реального часу. По-друге, неможливість впровадження уніфікованих стандартів безпеки призводить до того, що різні сегменти медичної інфраструктури мають різний рівень захищеності, а найслабша ланка стає вразливістю для всієї системи. По-третє, обмін даними між різнорідними системами часто здійснюється через незахищені канали або з використанням застарілих протоколів, що створює додаткові точки вразливості.

Кадровий дефіцит та недостатня обізнаність персоналу. Однією з найсерйозніших проблем є гостра нестача кваліфікованого ІТ-персоналу, особливо фахівців з інформаційної безпеки, у медичних закладах. За оцінками експертів, більшість комунальних лікарень не мають у штаті спеціалізованих фахівців з кібербезпеки, а функції адміністрування інформаційних систем виконують ІТ-спеціалісти широкого профілю, які не завжди володіють необхідними компетенціями у сфері захисту інформації [21].

Ще більш критичною є проблема низького рівня інформаційної гігієни у медичного та адміністративного персоналу. Дослідження у сфері кібербезпеки стабільно демонструють, що до 70% порушень безпеки інформаційних систем пов'язані з людським фактором – ненавмисними помилками користувачів, недотриманням політик безпеки, успішними атаками соціальної інженерії. Медичні працівники, зосереджені на наданні допомоги пацієнтам, часто сприймають вимоги інформаційної безпеки як бюрократичні перешкоди, що заважають їхній основній роботі.

Типовими проявами недостатньої обізнаності є використання простих або повторюваних паролів, запис паролів на паперових стікерах, відкриття фішингових листів та завантаження вкладень з невідомих джерел, використання особистих пристроїв для доступу до робочих систем без належного захисту, ігнорування оновлень безпеки програмного забезпечення. Усе це робить медичні заклади особливо вразливими до атак соціальної інженерії, які не вимагають від зловмисників високої технічної кваліфікації, але дозволяють ефективно компрометувати навіть добре захищені технічно системи.

Технічна застарілість інфраструктури. Значна частина медичних закладів, особливо у регіонах, продовжує використовувати морально і фізично застаріле обладнання та програмне забезпечення. Сервери та робочі станції, що експлуатуються понад десять років, операційні системи, для яких припинено підтримку виробником (наприклад, Windows 7 або Windows Server 2008), медичні інформаційні системи, що не отримують регулярних оновлень безпеки – усе це створює критичні вразливості.

Особливу небезпеку становить медичне обладнання з вбудованими комп'ютерними системами, яке підключене до локальних мереж (Internet of Medical Things – IoMT). Томографи, апарати УЗД, системи моніторингу життєво важливих показників часто працюють на застарілих операційних системах, для яких не випускаються оновлення безпеки, а їхнє відключення для модернізації неможливе через критичну важливість для надання медичної допомоги. Зламування такого обладнання може не лише призвести до витоку даних, а й

становити пряму загрозу життю пацієнтів.

Не менш важливою проблемою є відсутність чітких регламентів та технічних можливостей для регулярного резервного копіювання (backup) критично важливих даних та їхнього швидкого відновлення (recovery) у разі інциденту. Багато медичних закладів не мають географічно розподілених резервних центрів зберігання даних, що робить їх вразливими до атак ransomware (шифрувальників), коли зловмисники блокують доступ до даних і вимагають викуп за їхнє відновлення [22].

Регуляторна невизначеність та недосконалість нормативної бази. Попри значний прогрес у розробці законодавства з кібербезпеки на загальнодержавному рівні, залишаються невирішеними питання галузевої специфіки регулювання процесів захисту інформації у сфері охорони здоров'я. В Україні досі відсутні гармонізовані стандарти, аналогічні американському HIPAA (Health Insurance Portability and Accountability Act), які б комплексно врегульовували питання конфіденційності, цілісності та доступності медичної інформації з урахуванням специфіки галузі [19].

Часто виникають колізії між вимогами забезпечення безпеки та необхідністю оперативного доступу до медичних даних. Наприклад, надмірно суворі процедури автентифікації можуть затримати доступ лікаря до електронної медичної картки пацієнта у критичній ситуації. З іншого боку, спрощення процедур безпеки заради зручності створює вразливості. Відсутність чітких галузевих стандартів призводить до того, що кожен медичний заклад вирішує цю дилему на власний розсуд, що зумовлює неоднорідність рівня безпеки у системі.

Крім того, недостатньо врегульованими залишаються питання юридичної відповідальності за витоки медичних даних. Якщо у фінансовій сфері існують чіткі санкції за порушення вимог захисту інформації, то у медичній галузі механізми притягнення до відповідальності керівників закладів за недотримання стандартів кібербезпеки залишаються недостатньо ефективними. Це знижує мотивацію адміністрації медичних закладів інвестувати обмежені ресурси у кіберзахист.

Розуміння природи загроз, що стоять перед медичними інформаційними системами, є необхідною умовою для розробки адекватної стратегії їхнього захисту. Систематизація загроз дозволяє визначити пріоритети у розподілі обмежених ресурсів та сфокусувати зусилля на найбільш критичних напрямах.

Класифікація загроз за походженням. У науковій літературі та практиці кібербезпеки прийнято класифікувати загрози медичним інформаційним системам за їхнім походженням на три основні категорії.

Перша категорія – людські загрози, які поділяються на навмисні та ненавмисні. Навмисні людські загрози включають дії інсайдерів – співробітників медичного закладу, які мають легітимний доступ до інформаційних систем, але зловживають своїми повноваженнями заради особистої вигоди, помсти або на замовлення третіх сторін. Інсайдерські загрози є особливо небезпечними, оскільки важко виявляються технічними засобами захисту – адже дії здійснюються від імені авторизованого користувача. До цієї ж підкатегорії належать зовнішні зловмисники – хакери, організовані злочинні групи, спецслужби іноземних держав, – які намагаються отримати несанкціонований доступ до медичних систем для крадіжки даних, вимагання викупу або саботажу.

Ненавмисні людські загрози пов'язані з помилками персоналу, які відбуваються через недостатню кваліфікацію, втому, неуважність або незнання правил інформаційної безпеки. Випадкове видалення важливих файлів, помилкове надання доступу сторонній особі, втрата носіїв інформації, розголошення паролів – усе це приклади ненавмисних загроз, які, за статистикою, становлять більшість інцидентів безпеки у медичних закладах [10].

Друга категорія – природні та екологічні загрози, що включають пожежі, повені, землетруси, перебої в електропостачанні, екстремальні температурні режими. Хоча ці загрози не є специфічними для інформаційних систем, вони можуть призвести до фізичного знищення обладнання та втрати даних. Особливу актуальність ці загрози набули в умовах війни, коли до природних факторів додалися обстріли та руйнування інфраструктури.

Третя категорія – технологічні несправності та збої, що виникають

внаслідок відмови апаратного або програмного забезпечення без зовнішнього втручання. Вихід з ладу серверів, жорстких дисків, мережевого обладнання, програмні помилки, що призводять до втрати або спотворення даних, – усе це загрози, ймовірність яких зростає при використанні застарілого обладнання без належного резервування.

Управлінська дилема «Безпека vs Доступність». Найбільш критичним управлінським викликом у сфері інформаційної безпеки медичних закладів є необхідність знаходити баланс між захистом інформації та збереженням її доступності для медичного персоналу. Ця дилема має фундаментальний характер і не може бути вирішена технічними засобами без урахування специфіки медичної діяльності.

З одного боку, медичні дані належать до найчутливішої категорії персональної інформації і потребують максимального захисту. Витік діагнозів, результатів генетичних тестів, інформації про психічні розлади або інфекційні захворювання може мати руйнівні наслідки для життя людини. Тому міжнародні стандарти, зокрема європейський GDPR, встановлюють найсуворіші вимоги до захисту медичних даних. Логіка безпеки вимагає багаторівневої автентифікації, шифрування даних при зберіганні та передачі, детального аудиту всіх дій з інформацією, обмеження доступу на основі принципу мінімальних необхідних привілеїв [24].

З іншого боку, медична допомога часто надається в умовах обмеженого часу, коли кожна секунда може бути критичною для порятунку життя пацієнта. Лікар швидкої допомоги, що прибув на виклик, повинен негайно отримати доступ до медичної історії пацієнта, щоб з'ясувати алергії, хронічні захворювання, протипоказання до певних препаратів. Якщо складні процедури автентифікації затримають цей доступ навіть на кілька хвилин, це може коштувати пацієнту життя. Аналогічна ситуація виникає у відділеннях інтенсивної терапії, операційних, приймальних відділеннях [48].

Така дилема посилюється в умовах воєнного стану, коли медичні заклади працюють у режимі масового надходження поранених, часто в умовах

відсутності електропостачання або інтернет-зв'язку. Надмірно суворі заходи безпеки можуть перешкодити ефективній роботі медиків, але їхнє послаблення створює вразливості.

Завдання управлінців медичних закладів – знайти розумний баланс, що забезпечує адекватний захист даних без критичного уповільнення оперативних процесів. Цей баланс не є універсальним і повинен визначатися індивідуально для кожного типу медичного закладу, відділення та навіть робочого місця, з урахуванням специфіки клінічних процесів, категорій користувачів та рівня загроз. Сучасні підходи до вирішення цієї дилеми включають впровадження контекстно-залежного контролю доступу, який автоматично адаптує рівень безпеки залежно від ситуації (наприклад, спрощує автентифікацію у режимі надзвичайної ситуації), використання біометричних методів автентифікації для поєднання безпеки та зручності, розробку чітких протоколів екстреного доступу до даних з обов'язковим постфактум аудитом.

Управління інформаційною безпекою у медичній сфері є комплексним багатовимірним процесом, що вимагає інтеграції технічних, організаційних та соціальних компонентів захисту. На відміну від інших галузей, де інформаційна безпека може розглядатися переважно як технічна проблема, у сфері охорони здоров'я вона нерозривно пов'язана з етичними принципами медичної діяльності, правами пацієнтів та безпосередньо впливає на якість медичної допомоги.

Сучасні теоретичні підходи до управління інформаційною безпекою ґрунтуються на визнанні того, що абсолютна безпека є недосяжною, а тому головним завданням стає не усунення всіх можливих загроз, а управління ризиками таким чином, щоб залишковий рівень ризику був прийнятним для організації. Цей підхід, закріплений у міжнародних стандартах серії ISO/IEC 27000, передбачає систематичний циклічний процес ідентифікації, оцінювання та обробки ризиків з постійним моніторингом їхньої динаміки [17].

Водночас специфіка медичної галузі вимагає врахування соціотехнічного виміру безпеки. Дослідження показують, що навіть найдосконаліші технічні засоби захисту виявляються неефективними, якщо персонал не дотримується

політик безпеки або стає жертвою маніпуляцій соціальної інженерії. Тому сучасне управління інформаційною безпекою повинно інтегрувати технологічний захист з формуванням культури безпеки, підвищенням обізнаності персоналу та створенням організаційних механізмів, що мінімізують людський фактор як джерело вразливостей.

У контексті євроінтеграції та адаптації до стандартів НАТО особливого значення набуває компаративний аналіз міжнародних моделей забезпечення кібербезпеки у сфері охорони здоров'я. Розуміння підходів, що застосовуються у Європейському Союзі та країнах-членах НАТО, дозволяє визначити напрями вдосконалення вітчизняної системи кіберзахисту медичної інфраструктури з урахуванням національної специфіки та наявних ресурсів.

Управління інформаційною безпекою є невід'ємною складовою Системи управління інформаційною безпекою (СУІБ), що представляє собою структурований підхід до систематичного управління чутливою корпоративною інформацією. Міжнародний стандарт ISO/IEC 27001 визначає вимоги до встановлення, впровадження, підтримування та постійного вдосконалення СУІБ, тоді як стандарт ISO/IEC 27005 конкретизує процеси управління ризиками інформаційної безпеки [12].

Концептуальна основа ризик-орієнтованого підходу. Фундаментальна ідея управління ризиками полягає у визнанні того, що жодна організація не має необмежених ресурсів для захисту від усіх можливих загроз. Тому необхідно раціонально розподіляти обмежені ресурси, зосереджуючи їх на найбільш критичних ризиках – тих, що мають високу ймовірність реалізації та можуть призвести до найсерйозніших наслідків. Для медичних закладів це означає, що пріоритетом захисту є системи та дані, що безпосередньо впливають на життя пацієнтів та забезпечують базові клінічні процеси.

Процес управління ризиками відповідно до ISO/IEC 27005 є циклічним і складається з кількох послідовних етапів.

Визначення контексту є підготовчим етапом, на якому формулюються цілі та межі процесу управління ризиками. Для медичного закладу це передбачає

визначення критичних інформаційних активів (електронні медичні картки, результати лабораторних досліджень, системи управління медичним обладнанням), ідентифікацію зацікавлених сторін (пацієнти, медичний персонал, регулятори, постачальники послуг), встановлення критеріїв прийнятності ризику та визначення методології оцінювання ризиків. На цьому етапі також формується команда управління ризиками, що включає представників різних підрозділів – IT, медичного персоналу, адміністрації, юридичної служби.

Ідентифікація ризиків полягає у систематичному виявленні всіх потенційних загроз інформаційній безпеці, вразливостей інформаційних систем та можливих інцидентів безпеки. Для медичних закладів типовими загрозами є кібератаки (ransomware, фішинг, DDoS-атаки), дії інсайдерів, помилки персоналу, технічні збої обладнання, стихійні лиха та умисне фізичне знищення інфраструктури. Вразливості можуть включати застаріле програмне забезпечення без оновлень безпеки, слабкі паролі, відсутність резервного копіювання, незахищені бездротові мережі, недостатню фізичну безпеку серверних приміщень.

Аналіз ризиків передбачає оцінювання ймовірності реалізації кожного ризику та величини потенційних наслідків. Існують різні методології аналізу ризиків – від якісних (експертні оцінки за шкалою «низький-середній-високий») до кількісних (розрахунок очікуваних фінансових втрат). Для медичних закладів при оцінюванні наслідків необхідно враховувати не лише фінансові втрати, а й можливий вплив на здоров'я та життя пацієнтів, репутаційні ризики, регуляторні санкції за порушення вимог захисту персональних даних.

Оцінювання ризиків – це порівняння результатів аналізу ризиків з попередньо встановленими критеріями прийнятності. Ризики класифікуються за пріоритетністю: критичні (потребують негайних дій), високі (потребують планових заходів у короткостроковій перспективі), середні (потребують моніторингу та планових заходів), низькі (можуть бути прийняті без додаткових заходів). Важливо, що критерії прийнятності для медичних закладів повинні бути суворішими, ніж для комерційних організацій, оскільки наслідки

інцидентів безпеки можуть включати загрозу життю.

Обробка ризиків передбачає вибір і впровадження заходів для зниження ризиків до прийнятного рівня. Існує чотири базові стратегії обробки ризиків: модифікація (зниження ризику через впровадження додаткових контрольних заходів – наприклад, встановлення антивірусного програмного забезпечення, впровадження багатофакторної автентифікації); уникнення (відмова від діяльності, що породжує неприйнятний ризик – наприклад, відмова від підключення критичного медичного обладнання до загальної мережі); передача (перенесення ризику на третю сторону – наприклад, через страхування або використання хмарних сервісів з SLA); прийняття (свідоме рішення не вживати додаткових заходів, якщо ризик знаходиться в межах прийнятного). Для кожного значущого ризику розробляється план обробки з конкретними заходами, відповідальними особами та термінами реалізації.

Моніторинг і перегляд є безперервним процесом відстеження ефективності впроваджених заходів, виявлення нових загроз і вразливостей, актуалізації оцінок ризиків. Ландшафт загроз постійно змінюється – з'являються нові типи кібератак, виявляються нові вразливості у програмному забезпеченні, змінюється регуляторне середовище. Тому управління ризиками не є одноразовим проєктом, а являє собою безперервний цикл, який зазвичай повторюється щонайменше щорічно, а для критичних систем – значно частіше.

Технічні засоби захисту, якими б досконалими вони не були, не можуть гарантувати безпеку, якщо не враховується людський фактор. Саме це усвідомлення лежить в основі соціотехнічного підходу до управління інформаційною безпекою, який розглядає організацію як складну систему взаємодії людей, технологій та організаційних процесів.

Феномен соціальної інженерії полягає у маніпулюванні людьми з метою змусити їх розголосити конфіденційну інформацію, надати несанкціонований доступ або вчинити дії, що порушують безпеку. На відміну від технічних атак, соціальна інженерія експлуатує психологічні вразливості – довіру, страх, бажання допомогти, повагу до авторитетів, поспіх. Статистика демонструє, що

соціальна інженерія залишається одним з найефективніших методів компрометації інформаційних систем, оскільки дозволяє обійти навіть найсучасніші технології безпеки.

Для медичних закладів соціальна інженерія становить особливу загрозу з кількох причин. По-перше, медичні працівники за своєю природою схильні допомагати людям і можуть бути легко маніпульованими через апеляцію до співчуття. По-друге, в медичних закладах часто панує атмосфера цейтноту та стресу, що знижує пильність персоналу. По-третє, культура відкритості та доступності медичних закладів для відвідувачів створює численні можливості для фізичного проникнення зловмисників.

Типові сценарії соціальної інженерії у медичних закладах включають фішингові електронні листи, що імітують повідомлення від керівництва, постачальників медичного обладнання або державних органів і містять шкідливі вкладення або посилання; телефонні дзвінки, коли зловмисник видає себе за співробітника IT-підтримки і просить надати паролі для «планового обслуговування системи»; претекстинг, коли зловмисник створює правдоподібну легенду (наприклад, представляється страховим агентом або працівником лабораторії) для отримання конфіденційної інформації; tailgating – фізичне проникнення у заборонені зони шляхом проходження слідом за авторизованим співробітником через двері контролю доступу; baiting – залишення інфікованих USB-накопичувачів у місцях, де їх можуть знайти співробітники медичного закладу, розраховуючи на їхню цікавість.

Основні напрями соціотехнічного захисту мають комплексний характер і включають технічні, організаційні та освітні компоненти.

Формування культури безпеки (Security Culture) є довгостроковим процесом, спрямованим на інтеграцію принципів інформаційної безпеки у повсякденну діяльність організації. Культура безпеки означає, що кожен співробітник усвідомлює свою особисту відповідальність за захист інформації, розуміє основні загрози та знає, як правильно реагувати на підозрілі ситуації. Формування такої культури вимагає підтримки з боку керівництва, яке має

демонструвати особистий приклад дотримання політик безпеки.

Регулярне навчання персоналу є критично важливим елементом соціотехнічного захисту. Тренінги з інформаційної безпеки не повинні обмежуватися одноразовими вступними інструктажами – вони мають проводитися систематично, з періодичністю щонайменше раз на рік, а для персоналу з підвищеними привілеями доступу – частіше. Ефективні програми навчання використовують інтерактивні методи, включаючи симуляції фішингових атак, рольові ігри, аналіз реальних інцидентів. Особливу увагу слід приділяти навчанню розпізнавання ознак соціальної інженерії: невідповідність відправника та змісту листа, створення штучного відчуття терміновості, запити конфіденційної інформації електронною поштою, помилки у адресах веб-сайтів або email.

Регламентація роботи з інформацією з обмеженим доступом передбачає розробку та впровадження чітких політик та процедур, що визначають: класифікацію інформації за рівнями конфіденційності; правила надання, зміни та скасування прав доступу на основі принципу мінімальних необхідних привілеїв; порядок зберігання, передачі та знищення конфіденційної інформації; процедури реагування на запити доступу до медичних даних від зовнішніх осіб (правоохоронні органи, страхові компанії); протоколи верифікації особи перед наданням доступу до інформації, особливо при телефонних або електронних запитах.

Критично важливим є створення механізмів звітування про підозрілі інциденти. Співробітники повинні мати чіткий та простий спосіб повідомити про підозрілий email, незвичайний запит інформації або будь-яку іншу ситуацію, що може свідчити про спробу соціальної інженерії. Організація має заохочувати таке звітування та ніколи не карати за помилкові тривоги – краще отримати десять хибних сигналів, ніж пропустити одну реальну атаку.

Посилений кадровий контроль спрямований на мінімізацію інсайдерських загроз – навмисних або ненавмисних порушень безпеки з боку співробітників організації. Інсайдери є особливо небезпечними, оскільки мають легітимний

доступ до інформаційних систем та знають їхні вразливості. Заходи протидії інсайдерським загрозам включають перевірку благонадійності кандидатів при прийомі на роботу (background check), що є обов'язковою для посад з доступом до критичної інформації; впровадження системи моніторингу дій користувачів (User Behavior Analytics), що дозволяє виявляти аномальну поведінку – наприклад, масове копіювання файлів, доступ до незвичних ресурсів, робота в нетипові години; розділення обов'язків (segregation of duties), при якому критичні операції вимагають участі кількох осіб, що ускладнює зловживання повноваженнями; процедури офбордингу при звільненні співробітників, що включають негайне блокування всіх облікових записів, вилучення доступу до приміщень та повернення обладнання.

Розбудова ефективної системи кіберзахисту у вітчизняній охороні здоров'я потребує критичного осмислення міжнародного досвіду з урахуванням національної специфіки та викликів, що постали перед Україною в умовах повномасштабної війни. Компаративний аналіз підходів Європейського Союзу, НАТО та України дозволяє виявити як універсальні принципи ефективного кіберзахисту, так і контекстуально зумовлені особливості, що вимагають адаптації при імплементації.

Модель Європейського Союзу – GDPR та NIS2 Directive характеризується комплексністю регулювання, що поєднує захист персональних даних з вимогами до стійкості критичної інфраструктури.

Загальний регламент захисту даних (GDPR), що набув чинності у 2018 році, хоча формально не є актом про кібербезпеку, встановив найсуворіші у світі вимоги до захисту персональних даних, включаючи медичну інформацію, яка належить до «особливих категорій даних». GDPR запровадив концепцію «захисту даних за замовчуванням та за дизайном» (privacy by design and by default), що вимагає врахування питань захисту даних на всіх етапах розробки та впровадження інформаційних систем, а не як доповнення після факту [20].

Для медичних закладів GDPR встановлює обов'язок проводити Оцінку впливу на захист даних (Data Protection Impact Assessment – DPIA) перед

впровадженням нових інформаційних систем або технологій, що можуть створювати високі ризики для прав і свобод фізичних осіб. Ця процедура вимагає систематичного аналізу всіх потоків даних, оцінювання ризиків несанкціонованого доступу, визначення заходів мінімізації ризиків. GDPR також встановлює суворі вимоги щодо повідомлення про порушення захисту даних – контролюючий орган має бути сповіщений протягом 72 годин з моменту виявлення інциденту, а у випадках високого ризику для прав громадян необхідно також повідомити безпосередньо постраждалих осіб.

Санкційний механізм GDPR є найсуворішим у світі – штрафи можуть досягати 20 мільйонів євро або 4% річного глобального обороту організації. Ця загроза значних фінансових санкцій стала потужним стимулом для медичних закладів інвестувати у кіберзахист та дотримуватися найвищих стандартів захисту даних.

Директива NIS2 (Directive on measures for a high common level of cybersecurity across the Union), що була прийнята у 2022 році на заміну початковій Директиві NIS, посилила вимоги до кіберзахисту операторів критичної інфраструктури, до яких прямо належать заклади охорони здоров'я. NIS2 розширила коло підпадаючих під регулювання суб'єктів, включивши не лише великі лікарні, а й середні медичні заклади, а також лабораторії та постачальників медичних послуг [18].

Ключовими вимогами NIS2 є запровадження систем управління ризиками кібербезпеки на основі міжнародних стандартів; впровадження заходів управління інцидентами, включаючи детектування, реагування та відновлення; забезпечення безперервності бізнесу через резервне копіювання та плани аварійного відновлення; безпека ланцюгів постачання, що вимагає оцінювання кіберризиків від постачальників IT-послуг та програмного забезпечення; навчання персоналу з питань кібербезпеки.

NIS2 також встановлює жорсткі вимоги щодо звітності про інциденти – попереднє повідомлення має бути надане протягом 24 годин, детальний звіт протягом 72 годин, а остаточний звіт з результатами розслідування – протягом

одного місяця. Директива також передбачає персональну відповідальність керівників організацій за дотримання вимог кібербезпеки.

Європейська модель характеризується сильною регуляторною складовою, що поєднує жорсткі обов'язкові вимоги з значними санкціями за їхнє недотримання. Це створює потужні стимули для інвестицій у кіберзахист, але водночас вимагає значних адміністративних ресурсів для забезпечення комплаєнсу.

Модель НАТО – стандартизація та концепція «Defend Forward формувалася у контексті колективної оборони та військової співпраці, що визначило його специфічні характеристики. Для України, яка прагне членства в Альянсі та активно співпрацює з НАТО у військовій сфері, розуміння цих підходів має стратегічне значення [39].

Принцип стандартизації є основою функціонування НАТО (STANAG – Standardization Agreements) визначають єдині вимоги до технічних систем, процедур та протоколів, що забезпечує сумісність та взаємодію збройних сил країн-членів. У контексті медичного забезпечення це означає необхідність уніфікації форматів медичних даних, протоколів їхнього обміну, систем ідентифікації пацієнтів між військово-медичними підрозділами різних країн.

Стандартизація медичних інформаційних систем дозволяє забезпечити безперервність медичної допомоги військовослужбовцям під час міжнародних операцій, коли пацієнт може послідовно лікуватися у медичних закладах різних країн. Вона також критично важлива для координації медичної евакуації та обміну інформацією під час спільних навчань або операцій.

Концепція «Defend Forward» (захист шляхом просування вперед) є відносно новим підходом у кіберстратегії НАТО, що передбачає проактивну протидію загрозам. На відміну від традиційного підходу пасивної оборони, коли організація очікує на атаку і потім реагує, концепція Defend Forward передбачає активне виявлення загроз у кіберпросторі противника, моніторинг його активності та, де можливо, превентивні дії для нейтралізації загроз до того, як вони досягнуть критичної інфраструктури.

Для сфери охорони здоров'я це трансформується у створення високопрофесійних команд реагування на кіберінциденти (CSIRT-M – Computer Security Incident Response Team for Medical facilities), здатних не лише пасивно захищатися, а й швидко аналізувати вектори атак, виявляти індикатори компрометації, обмінюватися інформацією про загрози з іншими медичними закладами та координувати спільну відповідь на масштабні кібератаки. Проактивний підхід також включає регулярне проведення пентестів (тестів на проникнення) та навчань типу «red team / blue team», коли одна команда імітує дії зловмисників, а інша відпрацьовує захист.

Важливим елементом натовської моделі є концепція колективної кіберзахисту. Стаття 5 Вашингтонського договору, що визначає принцип колективної оборони, була поширена і на кіберпростір. Це означає, що кібератака на критичну інфраструктуру однієї країни-члена може розглядатися як напад на весь Альянс, що активізує механізми взаємодопомоги. Для медичної сфери це може означати надання технічної експертизи, обміну інформацією про загрози та методи захисту, спільні навчання та сертифікацію персоналу.

Ключовий висновок щодо моделі НАТО полягає у наголосі на оперативній сумісності систем, колективній обороні та проактивній протидії загрозам через розвиток високопрофесійних команд реагування.

Модель України – адаптація та регулювання в умовах війни, це модель кібербезпеки охорони здоров'я є перехідною та формується у надзвичайно складних умовах повномасштабної війни, що одночасно створює як критичні виклики, так і унікальні можливості для швидкої модернізації.

Принципова відмінність української моделі полягає у пріоритеті національної безпеки над індивідуальними правами у екстремальних ситуаціях. Якщо європейська модель GDPR вибудована навколо захисту прав громадянина, а модель НАТО орієнтована на військову ефективність, то українська модель змушена балансувати між цими підходами в умовах активних бойових дій. Закони України «Про критичну інфраструктуру» та «Про основні засади забезпечення кібербезпеки України» надають пріоритет забезпеченню стійкості

критичної інфраструктури та безперервності життєво важливих сервісів, навіть якщо це вимагає тимчасових обмежень окремих процедур [46].

Система реагування на кіберінциденти в Україні є більш централізованою порівняно з європейською моделлю. Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) під егідою Державної служби спеціального зв'язку та захисту інформації виконує координуючу роль для всіх секторів критичної інфраструктури, включаючи охорону здоров'я. CERT-UA здійснює цілодобовий моніторинг кіберпростору, аналізує індикатори компрометації, випускає оперативні попередження про нові загрози та надає методичну підтримку при реагуванні на інциденти [31].

Така централізація має свої переваги в умовах війни – вона дозволяє швидко мобілізувати ресурси для захисту найбільш атакованих об'єктів, координувати відповідь на масштабні кібератаки національного рівня, ефективно обмінюватися інформацією між різними секторами. Водночас вона створює ризик перевантаження центральних структур та можливого single point of failure.

Основний виклик української моделі полягає у проблемі імплементації регуляторних вимог на рівні регіональних та первинних медичних закладів. Якщо великі обласні лікарні та національні медичні центри мають ресурси для впровадження сучасних систем кіберзахисту, то комунальні заклади охорони здоров'я у малих містах та селах часто не мають ні кваліфікованого персоналу, ні фінансових можливостей для виконання встановлених вимог. Ця фрагментованість впровадження створює вразливості на рівні всієї системи.

Війна також виявила специфічну проблему кіберзахисту мобільних медичних підрозділів та польових госпіталів, що працюють в умовах відсутності стабільного інтернет-зв'язку та електропостачання. Традиційні моделі кібербезпеки, що передбачають постійний моніторинг та оновлення захисту в режимі онлайн, виявилися неадекватними для таких умов. Це стимулювало розробку гібридних рішень, що поєднують онлайн та офлайн режими захисту.

Позитивним аспектом української моделі є накопичення унікального

практичного досвіду протидії масштабним, добре організованим кібератакам з боку державного противника. Цей досвід включає методи швидкого відновлення після атак шифрувальників, захист від DDoS-атак критичної інфраструктури, виявлення та нейтралізацію APT (Advanced Persistent Threats) груп. Українські фахівці з кібербезпеки набули компетенцій, які важко отримати в мирних умовах, і цей досвід активно вивчається міжнародними партнерами. Аналіз трьох моделей дозволяє сформулювати стратегічні напрями розвитку системи кібербезпеки української охорони здоров'я.

По-перше, необхідна адаптація високих регуляторних стандартів ЄС (GDPR/NIS2) з урахуванням реалій воєнного стану. Це означає впровадження суворих вимог до захисту персональних медичних даних, але з гнучкими механізмами для екстремальних ситуацій. Важливо розробити галузеві стандарти, аналогічні американському HIPAA, що враховують специфіку медичної діяльності та встановлюють чіткі процедури балансу між безпекою і доступністю даних.

По-друге, доцільне впровадження принципів стандартизації та оперативної сумісності з систем НАТО, особливо у військово-медичній сфері. Україна вже розпочала процес адаптації натовських стандартів у військовій сфері, і система військово-медичного забезпечення має стати пріоритетом цього процесу. Це включає уніфікацію форматів медичних даних, протоколів обміну інформацією, систем ідентифікації постраждалих.

По-третє, необхідно зберегти переваги централізованої моделі реагування через CERT-UA, але при цьому розвивати галузеві та регіональні центри компетенції з кібербезпеки у медичній сфері. Створення мережі CSIRT-M (медичних команд реагування на кіберінциденти) при обласних та великих міських медичних закладах дозволить поєднати переваги централізованої координації з оперативністю локального реагування.

По-четверте, критично важливим є вирішення проблеми кадрового дефіциту через створення спеціалізованих програм підготовки фахівців з кібербезпеки для медичної галузі. Це може включати введення відповідних

спеціалізацій у медичних та технічних університетах, програми перепідготовки ІТ-спеціалістів, залучення міжнародної технічної допомоги для навчання персоналу.

По-п'яте, необхідно розробити диференційовані вимоги до кіберзахисту залежно від категорії медичного закладу, його розміру та наявних ресурсів. Встановлення однакових вимог для національного медичного центру та сільської амбулаторії є нереалістичним і контрпродуктивним. Потрібна багаторівнева система стандартів з базовими вимогами для всіх закладів та посиленими вимогами для критичних об'єктів. Інтеграція кращих практик європейської регуляторної моделі, натовської оперативної сумісності та проактивного підходу до захисту з урахуванням специфіки української реальності може створити унікальну модель кіберстійкої системи охорони здоров'я, здатної функціонувати навіть в екстремальних умовах гібридної війни.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ТА МЕХАНІЗМІВ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ У СИСТЕМІ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

2.1 Характеристика сучасного ландшафту загроз для системи охорони здоров'я

Теоретико-методологічний аналіз засад протидії інформаційним операціям у сфері охорони здоров'я дозволив сформулювати низку принципових положень, що формують концептуальну основу дослідження.

Інформаційне протиборство у медичній сфері є складним багатовимірним феноменом, що вимагає чіткого розмежування понять інформаційної та кібернетичної безпеки при їхній одночасній інтеграції. Інформаційна безпека як стратегічна концепція охоплює захист інформаційного простору, свідомості персоналу та суспільства, базуючись на тріаді конфіденційності, цілісності та доступності даних. Кібернетична безпека фокусується на технологічному захисті кіберпростору та окремих об'єктів інфраструктури від кібервтручання. В умовах гібридної війни ці два виміри не можуть розглядатися ізольовано і вимагають комплексного підходу.

Сучасна парадигма безпеки базується на концепції стійкості (resilience), що передбачає не лише захист від загроз, а й здатність системи функціонувати під час атаки та швидко відновлюватися після інцидентів. Для медичної сфери це означає гарантію безперервності надання медичної допомоги навіть у разі часткового порушення роботи інформаційних систем.

Державно-правовий механізм забезпечення національної безпеки у сфері протидії інформаційним операціям включає п'ять послідовних стадій: формулювання інтересів, виявлення та прогнозування загроз, вироблення

системи заходів протидії, нейтралізацію загроз та заходи відновлення. Українська нормативно-правова база у цій сфері активно розвивається, хоча й потребує подальшого вдосконалення щодо галузевої специфіки медицини.

Структурні вразливості вітчизняної системи охорони здоров'я мають системний характер і формуються на перетині організаційних, технічних, кадрових та регуляторних проблем. Фрагментованість інформаційного простору, кадровий дефіцит, технічна застарілість інфраструктури та регуляторна невизначеність створюють комплекс взаємопов'язаних вразливостей, що не можуть бути усунені виключно технічними засобами.

Управлінська дилема «Безпека vs Доступність» є фундаментальним викликом для медичної сфери, що не має універсального рішення. Баланс між захистом конфіденційності медичних даних та забезпеченням їхньої оперативної доступності для надання допомоги повинен визначатися індивідуально з урахуванням специфіки медичного закладу, типу відділення та характеру клінічних процесів.

Компаративний аналіз міжнародних моделей кібербезпеки (ЄС, НАТО, Україна) продемонстрував відсутність єдиного оптимального підходу. Європейська модель наголошує на захисті прав громадян через GDPR та регуляторному примусі через NIS2, натовська – на оперативній сумісності та проактивній обороні «Defend Forward», українська формується в умовах війни з пріоритетом національної безпеки. Ефективна національна модель має інтегрувати високі регуляторні стандарти ЄС з проактивною централізованою моделлю реагування НАТО, фокусуючись на розвитку кадрового потенціалу та стандартизації.

Повномасштабна російська агресія проти України докорінно змінила характер і масштаб загроз інформаційній безпеці медичної галузі. Якщо до 24 лютого 2022 року вітчизняні медичні заклади переважно стикалися з випадковими кібератаками з боку кіберзлочинців, що діяли заради фінансової наживи, то з початком повномасштабної війни медична сфера перетворилася на об'єкт систематичних, цілеспрямованих кібероперацій, координованих

спецслужбами держави-агресора або підконтрольними їй хакерськими угрупованнями.

Трансформація ландшафту загроз відбулася одночасно у кількох вимірах. По-перше, різко зросла інтенсивність атак – якщо у довоєнний період Урядова команда реагування на комп'ютерні надзвичайні події (CERT-UA) фіксувала окремі інциденти з медичними закладами, то з початку повномасштабної війни кількість спроб кібератак на об'єкти медичної інфраструктури збільшилася у десятки разів. По-друге, змінилася мотивація зловмисників – від фінансової вигоди до стратегічних цілей дестабілізації держави, підриву довіри населення до влади, створення гуманітарної кризи. По-третє, значно підвищився рівень технічної складності атак – противник використовує передові інструменти кібервійни, включаючи zero-day вразливості (невідомі раніше уразливості програмного забезпечення), custom malware (спеціально розроблені шкідливі програми) та методи довготривалого прихованого проникнення до мереж (Advanced Persistent Threats) [27].

Аналіз інцидентів, зафіксованих CERT-UA та Службою безпеки України протягом 2022-2024 років, дозволяє виокремити основні категорії загроз, з якими стикається система охорони здоров'я в умовах війни. Ці загрози мають комплексний характер і часто реалізуються у координованому режимі, коли кібератаки поєднуються з фізичними ударами по медичній інфраструктурі, дезінформаційними кампаніями та психологічними операціями.

Систематизація кіберзагроз для медичної інфраструктури вимагає чіткої класифікації, що враховує як технічні характеристики атак, так і їхні стратегічні цілі. Сучасна практика кібербезпеки виокремлює кілька основних типів атак, кожен з яких має специфічні механізми реалізації та потенційні наслідки для функціонування медичних закладів.

Ransomware-атаки (атаки шифрувальників) залишаються однією з найбільш небезпечних і поширених загроз для медичних закладів по всьому світу. Механізм таких атак полягає у несанкціонованому проникненні до інформаційної системи медичного закладу, шифруванні критично важливих

даних (електронних медичних карток, результатів досліджень, баз даних пацієнтів, адміністративних документів) і вимаганні викупу за надання ключів дешифрування. Особлива небезпека ransomware для медичної сфери полягає у тому, що блокування доступу до медичних даних може безпосередньо загрожувати життю пацієнтів – лікарі втрачають доступ до історії хвороби, результатів алергопроб, переліку медикаментів, що приймає пацієнт.

Аналіз реальних інцидентів демонструє різноманітність сценаріїв проникнення ransomware до медичних мереж. Найпоширенішим вектором залишається фішинг – співробітники отримують електронні листи, що імітують легітимну кореспонденцію від постачальників медичного обладнання, страхових компаній, державних органів або навіть від колег з інших відділень. Лист містить вкладення (зазвичай документ Office з макросами або архів) або посилання на зовнішній ресурс, відкриття якого запускає завантаження та виконання шкідливого коду.

Іншим поширеним вектором є експлуатація вразливостей у публічно доступних сервісах медичного закладу – веб-порталах для онлайн-запису, системах телемедицини, застарілих версіях програмного забезпечення на серверах, що мають доступ до інтернету. Зловмисники систематично сканують інтернет у пошуках систем з відомими вразливостями, для яких не були встановлені оновлення безпеки. Після отримання початкового доступу до одного сервера атакуючі здійснюють lateral movement – поступове розширення контролю на інші системи у локальній мережі, використовуючи вкрадені облікові записи, експлуатацію вразливостей внутрішньої мережі або соціальну інженерію.

Сучасні ransomware-операції часто використовують тактику подвійного вимагання (double extortion): перед шифруванням даних зловмисники копіюють конфіденційну інформацію на свої сервери і загрожують опублікувати її у відкритому доступі, якщо викуп не буде сплачено. Для медичних закладів це створює додатковий тиск, оскільки публікація медичних даних пацієнтів не лише порушує законодавство про захист персональних даних, а й може призвести до

величезних репутаційних втрат і регуляторних санкцій [43].

Особливу категорію становлять ransomware-атаки, мотивовані не фінансово, а політично. Під час війни зафіксовані випадки, коли атакуючі не вимагали викуп, а просто знищували дані або блокували системи з метою максимального збитку критичній інфраструктурі. У таких випадках метою є не збагачення, а дестабілізація роботи медичної системи у критичний момент.

DDoS-атаки (Distributed Denial of Service – розподілена атака типу «відмова в обслуговуванні») спрямовані на перевантаження інформаційних ресурсів медичного закладу величезним потоком запитів, що робить їх недоступними для легітимних користувачів. Механізм DDoS-атаки полягає у використанні ботнету – мережі заражених комп'ютерів по всьому світу, які одночасно надсилають запити на цільовий сервер, вичерпуючи його обчислювальні ресурси, пропускну здатність каналу зв'язку або ліміти одночасних з'єднань.

Для медичних закладів DDoS-атаки можуть паралізувати роботу веб-порталів для онлайн-запису до лікарів, систем телемедичних консультацій, електронних черг у поліклініках, інформаційних ресурсів, через які населення отримує важливу інформацію про роботу медичних закладів. Під час пандемії COVID-19 зафіксовані DDoS-атаки на сайти вакцинації, що перешкоджали громадянам записатися на щеплення. В умовах війни DDoS-атаки на медичні ресурси можуть координуватися з фізичними обстрілами для посилення хаосу та ускладнення координації надання допомоги постраждалим [4].

Особливо небезпечними є DDoS-атаки на критичні елементи інфраструктури Електронної системи охорони здоров'я (ЕСОЗ). Тимчасова недоступність центральних компонентів ЕСОЗ може паралізувати роботу медичних закладів по всій країні, оскільки лікарі втрачають доступ до електронних медичних карток пацієнтів, не можуть виписувати електронні рецепти, створювати направлення на обстеження. Хоча самі дані при DDoS-атаці не компрометуються і не знищуються, тимчасова недоступність критичних систем у медичній сфері може мати серйозні наслідки для здоров'я та життя

пацієнтів.

Атаки на медичне обладнання, підключене до мережі (IoMT – Internet of Medical Things) представляють особливо небезпечну категорію загроз, оскільки можуть безпосередньо впливати на процес лікування та життєво важливі функції пацієнтів. До IoMT належать різноманітні пристрої: системи моніторингу життєво важливих показників пацієнтів у відділеннях інтенсивної терапії, інфузійні помпи для дозованого введення ліків, апарати штучної вентиляції легень, імплантовані кардіостимулятори та дефібрилятори з можливістю віддаленого налаштування, комп'ютерні томографи, МРТ-сканери та іншу діагностичну техніку з мережевим підключенням.

Вразливість IoMT зумовлена кількома факторами. По-перше, медичне обладнання має тривалий життєвий цикл – пристрої експлуатуються 10-15 років, і їхнє програмне забезпечення часто не оновлюється протягом цього періоду. Виробники медичного обладнання не завжди своєчасно випускають оновлення безпеки, а навіть коли вони доступні, медичні заклади часто уникають їхнього встановлення, побоюючись порушити стабільність роботи критично важливого обладнання або втратити сертифікацію регуляторних органів.

По-друге, багато медичних пристроїв розроблялися в епоху, коли питання кібербезпеки не були пріоритетними, і містять фундаментальні архітектурні вразливості – відсутність шифрування даних, використання стандартних паролів, що не можуть бути змінені, відкриті мережеві порти для сервісного обслуговування, відсутність механізмів автентифікації. По-третє, медичне обладнання часто підключається до тієї ж локальної мережі, що й адміністративні комп'ютери і сервери, що створює можливість для lateral movement після компрометації будь-якого вузла мережі.

Теоретична можливість кібератак на імплантовані медичні пристрої (кардіостимулятори, інсулінові помпи) була продемонстрована дослідниками безпеки ще в 2010-х роках. Хоча масштабні реальні атаки на такі пристрої поки не зафіксовані, сам факт їхньої потенційної вразливості створює серйозні ризики у контексті цілеспрямованих атак на конкретних осіб – високопоставлених

чиновників, військових, громадських діячів.

Фішингові кампанії та соціальна інженерія залишаються найефективнішим методом початкового проникнення до корпоративних мереж медичних закладів. За різними оцінками, від 70% до 90% успішних кібератак розпочинаються саме з фішингу – обману користувача з метою змусити його виконати дію, що компрометує безпеку. Фішингові атаки на медичні заклади мають свою специфіку і часто використовують контекст, релевантний для медичної сфери. Типові сценарії включають: листи, що нібито надіслані від Міністерства охорони здоров'я з термінов ими вказівками щодо зміни процедур звітності або оновлення реєстраційних даних в ЕСОЗ; повідомлення від постачальників медичного обладнання або фармацевтичних компаній з інформацією про критичні оновлення безпеки або відкликання препаратів; листи від страхових компаній з проханням підтвердити дані пацієнтів для обробки страхових випадків; фальшиві повідомлення від ІТ-відділу про необхідність змінити пароль або підтвердити облікові дані через зовнішнє посилання; імітація кореспонденції від колег з інших відділень або медичних закладів з проханням переглянути «термінову медичну консультацію» у вкладеному документі. В умовах війни фішингові кампанії активно експлуатують емоційний стан медичного персоналу, використовуючи теми пов'язані з військовими подіями, гуманітарною допомогою, евакуацією, інформацією про поранених. Зловмисники розуміють, що медичні працівники перебувають у стані постійного стресу та перевантаження, що знижує їхню пильність і критичність при оцінюванні підозрілих повідомлень.

Особливо небезпечними є spear phishing attacks – цільові фішингові атаки на конкретних осіб з використанням персоналізованої інформації про них. Атакуючі попередньо збирають відкриту інформацію про ціль через соціальні мережі, професійні профілі, публічні виступи, а потім використовують ці дані для створення надзвичайно правдоподібних повідомлень. Наприклад, лист може посилатися на недавню конференцію, в якій брав участь адресат, або містити інформацію про його професійні інтереси. Такі персоналізовані атаки мають

значно вищий рівень успішності порівняно з масовими фішинговими розсилками.

APT (Advanced Persistent Threats) – довготривалі цільові атаки представляють найбільш складну та небезпечну категорію загроз. На відміну від opportunistic attacks, що мають на меті швидке отримання вигоди, APT-операції характеризуються тривалим плануванням, значними ресурсами, використанням передових технологій і спрямовані на досягнення стратегічних цілей.

Типовий життєвий цикл APT-атаки включає кілька послідовних фаз. На етапі розвідки зловмисники збирають інформацію про цільову організацію – її інформаційну інфраструктуру, співробітників, партнерів, використовуване програмне забезпечення. Ця інформація збирається з відкритих джерел (OSINT – Open Source Intelligence), через соціальну інженерію, а також технічними методами – сканування мережі, аналіз DNS-записів, виявлення публічно доступних сервісів.

Етап початкового проникнення часто здійснюється через фішинг, експлуатацію вразливостей у публічних сервісах або компрометацію облікових записів через витік паролів з інших джерел (credential stuffing). Після отримання початкового доступу атакуючі встановлюють backdoor – прихований канал віддаленого доступу, що дозволяє їм повертатися до системи навіть після виявлення і ліквідації початкової точки входу.

На етапі закріплення зловмисники підвищують свої привілеї у системі (privilege escalation), створюють додаткові облікові записи, модифікують систему для забезпечення persistence – здатності зберігати доступ навіть після перезавантаження системи або встановлення оновлень. Використовуються різноманітні техніки приховування присутності – rootkits, що маскують процеси та файли, модифікація системних журналів для видалення слідів активності.

Етап lateral movement передбачає поступове розширення контролю на інші системи у мережі організації. Атакуючі використовують вкрадені облікові записи, експлуатують вразливості внутрішньої мережі, підбирають паролі адміністраторів. Метою є досягнення найбільш цінних активів організації – баз

даних з медичними записами, серверів електронної пошти, систем фінансового обліку.

На фінальному етапі виконання місії (mission execution) зловмисники реалізують свою початкову мету – масове викрадення конфіденційних даних (data exfiltration), шифрування систем, саботаж критичної інфраструктури або встановлення механізмів довгострокового шпигунства. У контексті війни APT-групи, що працюють на користь держави-агресора, можуть збирати інформацію про стан медичної системи, наявність ресурсів, евакуаційні плани, дані про поранених військовослужбовців.

Виявлення APT-атак є надзвичайно складним завданням, оскільки атакуючі використовують передові техніки ухилення від детектування, включаючи zero-day вразливості (невідомі раніше вразливості програмного забезпечення, для яких не існує оновлень), custom malware (шкідливе програмне забезпечення, розроблене спеціально для цієї операції і невідоме антивірусним системам), living-off-the-land techniques (використання легітимних системних утиліт для виконання зловмисних дій, що ускладнює їхнє виявлення).

Атаки на ланцюги постачання (Supply Chain Attacks) стали одним з найбільш ефективних методів компрометації великої кількості організацій одночасно. Замість атаки на кожну цільову організацію окремо, зловмисники компрометують спільного постачальника програмного забезпечення або послуг, через якого потім отримують доступ до всіх його клієнтів.

Для медичної сфери особливо актуальними є атаки на постачальників медичних інформаційних систем (MIC). Якщо зловмисникам вдається впровадити шкідливий код у оновлення MIC, яка використовується десятками або сотнями медичних закладів, вони автоматично отримують доступ до всіх цих закладів після встановлення скомпрометованого оновлення. Аналогічну загрозу становлять компрометовані оновлення операційних систем, антивірусного програмного забезпечення, системних утиліт.

Іншим вектором атак на ланцюги постачання є компрометація провайдерів хмарних сервісів або аутсорсингових компаній, що надають послуги з

обслуговування ІТ-інфраструктури медичних закладів. Якщо атакуючі отримують доступ до систем такого провайдера, вони автоматично отримують доступ до даних і систем усіх його клієнтів. Це особливо небезпечно для малих медичних закладів, що повністю покладаються на зовнішніх підрядників для обслуговування своєї ІТ-інфраструктури.

Поряд з технічними кібератаками медична сфера є об'єктом систематичних інформаційних операцій, спрямованих на маніпулювання суспільною свідомістю, підрив довіри до медичних інституцій та створення соціальної напруженості. Якщо кібератаки спрямовані на технічні системи, то інформаційні операції націлені на людей – пацієнтів, медичних працівників, адміністрацію медичних закладів, широку громадськість.

Дезінформація щодо епідеміологічної ситуації є одним з найнебезпечніших напрямів інформаційних операцій, оскільки може спровокувати паніку, неадекватну поведінку населення та перевантаження медичної системи. Під час пандемії COVID-19 спостерігалася безпрецедентна за масштабами дезінформаційна кампанія, що включала: поширення конспірологічних теорій про штучне походження вірусу, нібито створеного у біологічних лабораторіях; фейки про неефективність або небезпеку вакцин, що призвело до зниження рівня вакцинації та подовження пандемії; маніпуляції зі статистикою захворюваності та смертності для створення хибного уявлення про масштаб проблеми; поширення небезпечних «народних методів лікування», що не мають наукового обґрунтування і можуть завдати шкоди здоров'ю.

В умовах війни дезінформація щодо епідеміологічної ситуації набула нових форм. Противник систематично поширює фейки про нібито спалахи небезпечних інфекційних захворювань на територіях, контрольованих Україною, про біологічну зброю, що нібито розробляється у військових лабораторіях, про масове зараження води та продуктів харчування. Такі фейки мають на меті створити атмосферу страху, спровокувати масові евакуації, перевантажити медичну систему зверненнями панікуючих громадян.

Дискредитація медичної системи та окремих медичних закладів є ще

одним важливим напрямом інформаційних операцій. Ця діяльність включає поширення неправдивих або перебільшених повідомлень про нібито масові випадки лікарських помилок, низьку кваліфікацію медичного персоналу, корупцію в медичних закладах, нестачу ліків і обладнання. Особливо активно такі фейки поширюються після резонансних медичних інцидентів, коли емоційний фон суспільства є підвищеним і люди схильні вірити негативній інформації.

Механізм дискредитації часто використовує реальні проблеми медичної системи, але перебільшує їхній масштаб або подає їх у викривленому контексті. Наприклад, окремий випадок лікарської помилки може бути представлений як системна проблема, що свідчить про катастрофічний стан усієї медичної галузі. Інформація про тимчасову нестачу певного препарату в одному медичному закладі може бути трансформована у фейк про повну відсутність ліків у всій країні.

Під час війни особливо активно дискредитуються медичні заклади, що надають допомогу пораненим військовослужбовцям. Поширюються фейки про нібито жахливі умови лікування, про те, що поранених залишають без допомоги, що відбувається розкрадання гуманітарної медичної допомоги. Метою таких інформаційних операцій є підрив морального духу військовослужбовців, зниження довіри до держави та її інституцій, провокування соціального невдоволення серед родичів військових.

Цілеспрямовані атаки на репутацію окремих лікарів та керівників медичних закладів використовують різноманітні технології інформаційної агресії. Створюються фейкові аккаунти у соціальних мережах, з яких публікуються наклепницькі повідомлення про конкретних медичних працівників. Виготовляються і поширюються компрометуючі відео або аудіозаписи, часто створені з використанням технологій deepfake – штучного інтелекту, що дозволяє створювати реалістичні фальшиві відео або аудіо з обличчям чи голосом реальної людини.

Організовуються координовані кампанії негативних відгуків на медичні

заклади у Google Maps, медичних порталах, соціальних мережах. Сотні або тисячі фейкових акаунтів одночасно публікують однотипні негативні відгуки, що різко знижує рейтинг медичного закладу і підриває довіру потенційних пацієнтів. Такі кампанії особливо ефективні проти приватних медичних клінік, для яких репутація є критично важливим бізнес-активом.

Маніпулювання інформацією про доступність медичної допомоги включає поширення фейків про нібито масове закриття медичних закладів, про неможливість отримати медичну допомогу без хабарів, про величезні черги та багатомісячне очікування на прийом до фахівців. В умовах війни активно поширюється дезінформація про евакуацію медичних закладів, про припинення роботи швидкої допомоги у певних регіонах, про відсутність місць у лікарнях для прийому поранених цивільних.

Особливо небезпечними є фейки, що поширюються через месенджери у групах жителів певних населених пунктів. Такі повідомлення часто мають вигляд приватної інформації «від знайомого, який працює у лікарні» і тому сприймаються як достовірні. Люди поширюють їх далі своїм знайомим, створюючи ефект снігової кулі. До моменту спростування фейку офіційними джерелами він вже встигає охопити значну аудиторію.

Використання ботів та тролів у соціальних мережах є важливим інструментом інформаційних операцій. Боти – це автоматизовані акаунти, керовані програмами, що можуть масово публікувати однотипні повідомлення, ставити лайки, робити репости. Тролі – це реальні люди (часто наймані або ідеологічно мотивовані), що систематично публікують провокаційні коментарі, розпалюють конфлікти, поширюють дезінформацію.

У контексті медичної тематики боти і тролі активізуються навколо резонансних тем – реформування медицини, вакцинація, фінансування охорони здоров'я, окремі гучні медичні інциденти. Вони формують хибне уявлення про масштаби невдоволення населення, створюють враження, що «всі проти» певної ініціативи, провокують конфлікти між різними групами користувачів. Координовані кампанії у соціальних мережах можуть штучно вивести певну

тему в топ обговорень, створюючи хибне уявлення про її актуальність для широких мас.

Сучасні технології дозволяють створювати складні мережі синтетичних акаунтів, що імітують поведінку реальних користувачів – публікують різноманітний контент, взаємодіють між собою, мають фотографії та особисту інформацію. Виявлення таких синтетичних мереж є складним технічним завданням, що вимагає аналізу великих масивів даних та використання алгоритмів машинного навчання. Платформи соціальних мереж постійно удосконалюють алгоритми детектування ботів, але зловмисники так само постійно адаптують свої методи для обходу захисту.

Експлуатація емоційних тригерів та когнітивних упереджень є психологічною основою ефективних інформаційних операцій. Дезінформація конструюється таким чином, щоб максимально резонувати з існуючими страхами, упередженнями та емоційними станами цільової аудиторії. У медичній тематиці найпотужнішими емоційними тригерами є страх за здоров'я та життя – своє і близьких людей, недовіра до влади та експертів, конспірологічне мислення, бажання знайти прості пояснення складним проблемам.

Інформаційні операції активно використовують когнітивні упередження – систематичні помилки мислення, властиві всім людям. Ефект підтвердження (confirmation bias) змушує людей шукати та надавати більшої ваги інформації, що підтверджує їхні існуючі переконання, ігноруючи суперечливі факти. Наприклад, людина, що недовіряє вакцинації, буде активно шукати і поширювати інформацію про нібито негативні наслідки вакцин, ігноруючи наукові дослідження про їхню ефективність і безпеку.

Ефект доступності (availability heuristic) змушує переоцінювати ймовірність подій, про які часто згадується у ЗМІ. Якщо медіа активно висвітлюють окремі випадки лікарських помилок, люди починають вважати їх масовим явищем, навіть якщо статистично вони є рідкісними. Ефект «хибного консенсусу» створює враження, що більшість людей поділяє певну думку, навіть якщо це не відповідає дійсності. Масові публікації ботів та тролів формують

ілюзію загального невдоволення певною політикою або медичним закладом.

Особливо ефективним є використання наративів про змову (conspiracy narratives), що апелюють до природного бажання людей знайти простий і зрозумілий сюжет, що пояснює складні події. Медична тематика є особливо сприйнятливою до конспірологічних теорій через свою технічну складність, яка робить важким для пересічної людини самостійне оцінювання достовірності інформації. Тези про «фармацевтичних магнатів, що приховують дешеві методи лікування», «лікарів, що навмисно призначають шкідливі ліки», «владу, що експериментує на громадянах» знаходять благодатний ґрунт у суспільстві з низьким рівнем медичної грамотності та високим рівнем недовіри до інституцій.

Таргетування різних сегментів аудиторії дозволяє підвищити ефективність інформаційних операцій. Для кожної цільової групи розробляються специфічні наративи та канали поширення. Для медичного персоналу використовуються професійні форуми, закриті групи у соціальних мережах, месенджери. Повідомлення акцентують на темах низької оплати праці, важких умов роботи, нестачі обладнання, конфліктів з адміністрацією. Метою є посилення професійного вигорання, провокування трудових конфліктів, стимулювання міграції кваліфікованих кадрів за кордон.

Для пацієнтів використовуються масові медіа, популярні соціальні мережі, месенджери. Наративи фокусуються на недоступності медичної допомоги, корупції, низькій якості лікування, небезпеці нових методів діагностики або лікування. Для батьків дітей активно експлуатується тема безпеки вакцинації, якості дитячого харчування, екологічних загроз здоров'ю.

Для осіб похилого віку, які менш критично оцінюють інформацію з інтернету і частіше довіряють сенсаційним повідомленням, використовуються месенджери та класичні ЗМІ. Повідомлення часто мають форму «порад від лікаря» або «інформації, яку приховують», що експлуатує недовіру до офіційної медицини та бажання отримати «секретні знання».

Використання deepfake технологій відкриває нові можливості для дезінформації у медичній сфері. Технології генеративного штучного інтелекту

дозволяють створювати реалістичні відео або аудіозаписи, на яких конкретна людина нібито говорить або робить те, чого насправді ніколи не було. Це може бути використано для компрометації керівників медичних закладів, створення фейкових заяв від міністра охорони здоров'я, імітації медичних експертів, що дають небезпечні поради.

Хоча високоякісні deepfake все ще вимагають значних технічних ресурсів і експертизи, базові технології стають дедалі доступнішими. Існують онлайн-сервіси, що дозволяють створювати прості deepfake відео навіть користувачам без технічних навичок. У майбутньому можна очікувати зростання використання таких технологій в інформаційних операціях проти медичної сфери.

Найбільш небезпечними є гібридні сценарії, коли фізичні удари по медичній інфраструктурі координуються з кібератаками та інформаційними операціями для досягнення синергетичного ефекту максимальної дестабілізації.

Координація часових рамок є ключовим елементом гібридних операцій. Кібератака може здійснюватися безпосередньо перед або одночасно з фізичним ударом по медичному закладу, щоб паралізувати системи зв'язку та координації, ускладнити надання допомоги постраждалим, створити максимальний хаос. Наприклад, DDoS-атака на сервери швидкої медичної допомоги під час масованого обстрілу міста може критично уповільнити реагування на численні виклики від постраждалих.

Інформаційна операція може розпочатися одразу після фізичного удару або кібератаки для посилення їхнього психологічного ефекту. Поширюються фейки про значно більшу кількість жертв, про нездатність медичної системи впоратися з потоком постраждалих, про відсутність необхідних ресурсів для надання допомоги. Метою є створення атмосфери безнадійності та паніки, підрив довіри до спроможності держави захистити своїх громадян.

Ешелонування атак передбачає проведення серії послідовних атак різного характеру. Наприклад, початкова кібератака може скомпрометувати систему відеоспостереження та контролю доступу медичного закладу, після чого здійснюється фізичне проникнення для встановлення додаткових пристроїв

прослуховування або викрадення обладнання. Альтернативно, кібератака може бути використана для отримання інформації про розташування критичних елементів інфраструктури, систем резервного живлення, серверних приміщень, що потім використовується для планування більш ефективного фізичного удару.

Атаки на ланцюги реагування та відновлення спрямовані не лише на саму критичну інфраструктуру, а й на системи, що забезпечують реагування на інциденти та відновлення після атак. Компрометація систем резервного копіювання паралельно з основною ransomware-атакою робить неможливим швидке відновлення даних. Атаки на канали зв'язку між медичними закладами та командами реагування на надзвичайні ситуації ускладнюють координацію під час масових надходжень постраждалих.

Використання «вікон вразливості» – періодів підвищеної навантаги на медичну систему або зниженої готовності до протидії загрозам. Кібератаки можуть бути приурочені до періодів масових захворювань (епідемії грипу, COVID-19), святкових днів, коли частина персоналу відсутня, періодів після природних катастроф або техногенних аварій, коли медична система вже перевантажена. В умовах війни «вікнами вразливості» є періоди масованих обстрілів, коли система працює на межі своїх можливостей.

2.2 Існуючі механізми протидії інформаційним операціям та їхня ефективність

Аналіз ландшафту загроз, представлений у попередньому пункті, демонструє масштаб і складність викликів, що постали перед системою охорони здоров'я України. Водночас за роки після початку повномасштабної агресії вітчизняна медична інфраструктура накопичила значний досвід протидії гібридним загрозам, розробила та впровадила низку організаційних, технічних і нормативних механізмів захисту. Критичний аналіз ефективності цих механізмів

є необхідним для визначення напрямів їхнього вдосконалення.

Система протидії інформаційним операціям у медичній сфері має багаторівневий характер і включає національний рівень (загальнодержавні інституції та регуляторні органи), галузевий рівень (профільні департаменти МОЗ, галузеві центри кібербезпеки), регіональний рівень (обласні управління охорони здоров'я, регіональні медичні заклади) та локальний рівень (окремі медичні заклади, їхні підрозділи інформаційної безпеки). Ефективність системи залежить від того, наскільки добре координується робота між цими рівнями і наскільки швидко інформація про загрози передається від національного рівня до окремих медичних закладів і навпаки.

Організаційна структура протидії кіберзагрозам у медичній сфері формувалася поступово, адаптуючись до нових викликів і враховуючи міжнародний досвід. Центральним елементом цієї структури є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), яка відповідає за загальнодержавну політику кібербезпеки та координацію захисту об'єктів критичної інфраструктури, до яких належать медичні заклади.

Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) функціонує у складі ДССЗЗІ і виконує роль національного центру кіберзахисту. CERT-UA здійснює цілодобовий моніторинг кіберпростору України, аналізує індикатори компрометації (IoC – Indicators of Compromise), виявляє нові типи кіберзагроз та шкідливого програмного забезпечення, випускає оперативні попередження про активні кампанії атак, надає методичну та технічну підтримку організаціям при реагуванні на кіберінциденти, координує взаємодію з міжнародними центрами реагування.

Для медичної сфери CERT-UA розробляє специфічні рекомендації з урахуванням галузевої специфіки, аналізує тренди атак на медичні заклади, забезпечує обмін інформацією про загрози між різними медичними організаціями. Після виявлення нової кіберзагрози, що становить ризик для медичної інфраструктури, CERT-UA негайно інформує МОЗ та ключові медичні заклади, надаючи технічні деталі атаки та рекомендації щодо захисту.

Ефективність роботи CERT-UA значно зросла за роки війни. Якщо у довоєнний період середній час від виявлення кіберзагрози до повідомлення зацікавлених сторін міг сягати кількох днів, то зараз критична інформація поширюється протягом годин. CERT-UA активно співпрацює з міжнародними партнерами – CERT-EU (європейська команда реагування), US-CERT (американська команда), командами реагування країн НАТО, що дозволяє швидше виявляти глобальні кампанії атак та обмінюватися інформацією про нові техніки зловмисників.

Водночас існують об'єктивні обмеження можливостей CERT-UA. По-перше, команда не може фізично моніторити мережі всіх медичних закладів – вона покладається на те, що самі організації виявлять інциденти і повідомлять про них. По-друге, CERT-UA надає переважно методичну підтримку, а безпосереднє реагування на інцидент повинен здійснювати сам медичний заклад, що вимагає наявності у нього відповідних компетенцій. По-третє, пріоритети CERT-UA визначаються на національному рівні, і не завжди окремий інцидент у регіональному медичному закладі отримує негайну увагу, якщо паралельно відбуваються масштабніші атаки на іншу критичну інфраструктуру.

Служба безпеки України (СБУ) через свої профільні підрозділи здійснює контррозвідувальну діяльність у кіберпросторі, виявляє та нейтралізує кібероперації іноземних спецслужб, розслідує кіберзлочини з ознаками загрози національній безпеці, проводить оперативні заходи щодо ідентифікації та затримання організаторів кібератак. У контексті медичної сфери СБУ особливу увагу приділяє виявленню інсайдерських загроз – випадків, коли співробітники медичних закладів співпрацюють з іноземними розвідками або організованими злочинними групами.

СБУ також відповідає за протидію інформаційним операціям противника, включаючи виявлення та блокування дезінформаційних кампаній, координованих ботнетів у соціальних мережах, фейкових новинних ресурсів. У співпраці з адміністраторами соціальних мереж та месенджерів СБУ ініціює блокування акаунтів, що систематично поширюють дезінформацію про медичну

систему України.

Проте ефективність протидії інформаційним операціям обмежена складністю виявлення та доведення координованого характеру дезінформаційних кампаній. Відмінність між genuine criticism (справжньою критикою) та coordinated information operation (координованою інформаційною операцією) не завжди є очевидною. Надмірно агресивне блокування критичних повідомлень може сприйматися як цензура і само по собі підривати довіру до влади.

Міністерство охорони здоров'я України виконує роль галузевого координатора у сфері інформаційної безпеки медичних закладів. МОЗ розробляє галузеві стандарти та методичні рекомендації з кібербезпеки, визначає вимоги до медичних інформаційних систем з точки зору безпеки, координує заходи щодо підвищення кваліфікації персоналу медичних закладів у питаннях інформаційної безпеки, забезпечує захист центральних компонентів Електронної системи охорони здоров'я (ЕСОЗ) [37].

МОЗ створило спеціалізований підрозділ, відповідальний за питання кібербезпеки у медичній галузі, який взаємодіє з CERT-UA, СБУ та міжнародними партнерами. Цей підрозділ відіграє роль галузевої точки контакту (healthcare sector POC – Point of Contact) для питань кібербезпеки – саме до нього надходить від CERT-UA інформація про загрози, специфічні для медичної сфери, і саме він забезпечує її подальше поширення до регіональних управлінь охорони здоров'я та окремих медичних закладів.

Водночас МОЗ стикається з проблемою обмежених повноважень щодо примусового впровадження стандартів безпеки у комунальних медичних закладах, які перебувають у підпорядкуванні місцевих органів влади. МОЗ може розробляти рекомендації та стандарти, але не завжди може забезпечити їхнє обов'язкове виконання, особливо якщо це вимагає значних фінансових інвестицій від медичних закладів з обмеженими бюджетами.

Національна служба здоров'я України (НСЗУ), як оператор ЕСОЗ та адміністратор програми медичних гарантій, також відіграє важливу роль у

забезпеченні кібербезпеки. НСЗУ відповідає за захист центральних компонентів ЕСОЗ, що містять медичні дані мільйонів українців. Організація створила власний підрозділ кібербезпеки, впровадила міжнародні стандарти захисту інформації, регулярно проходить незалежні аудити безпеки [38].

НСЗУ також встановлює мінімальні вимоги до інформаційної безпеки для медичних закладів, що укладають договори про надання медичних послуг у рамках програми медичних гарантій. Це створює економічний стимул для медичних закладів інвестувати у кібербезпеку – без відповідності мінімальним вимогам заклад не може працювати в системі державного фінансування.

Регіональні та локальні механізми координації мають критичне значення для оперативного реагування на інциденти. Обласні управління охорони здоров'я виконують роль посередника між національним рівнем та окремими медичними закладами, забезпечують поширення інформації про загрози, координують заходи підвищення кваліфікації персоналу, організовують спільні навчання для відпрацювання реагування на кіберінциденти.

Великі медичні заклади – обласні лікарні, спеціалізовані національні центри – створюють власні підрозділи інформаційної безпеки або призначають відповідальних осіб. Вони розробляють локальні політики безпеки, плани реагування на інциденти, проводять регулярні навчання персоналу. Проте значна частина малих та середніх медичних закладів, особливо у сільській місцевості, не має спеціалізованого персоналу з кібербезпеки, а функції забезпечення безпеки виконують ІТ-адміністратори широкого профілю, які часто не мають відповідних компетенцій.

Технічний захист медичної інфраструктури базується на класичних принципах defense in depth – багаторівневого ешелонованого захисту, коли компрометація одного рівня безпеки не призводить до компрометації всієї системи. Сучасні медичні заклади впроваджують різноманітні технічні засоби, кожен з яких адресує специфічні типи загроз.

Мережева безпека є першою лінією оборони, що запобігає несанкціонованому доступу до внутрішніх мереж медичного закладу з інтернету.

Ключовими компонентами мережевої безпеки є міжмережеві екрани (firewalls), що фільтрують мережевий трафік згідно з визначеними правилами, блокують підозрілі з'єднання та обмежують доступ до критичних систем.

Сучасні медичні заклади впроваджують next-generation firewalls (NGFW), що здійснюють не лише базову фільтрацію пакетів, а й глибоку інспекцію трафіку (deep packet inspection), виявлення і блокування шкідливих програм, контроль додатків, інтеграцію з системами threat intelligence для блокування відомих джерел загроз. NGFW дозволяють гранулярно контролювати, які саме додатки можуть використовувати мережеве з'єднання, що критично важливо для запобігання витоку даних через несанкціоновані канали.

Системи виявлення та запобігання вторгненням (IDS/IPS – Intrusion Detection/Prevention Systems) аналізують мережевий трафік на предмет ознак атак – сканування портів, експлуатації вразливостей, спроб несанкціонованого доступу. IDS виявляє підозрілу активність і генерує сповіщення адміністраторам, тоді як IPS автоматично блокує шкідливий трафік у режимі реального часу.

Для медичних закладів особливо важливою є сегментація мережі – розділення єдиної мережі на ізольовані сегменти (VLAN – Virtual Local Area Networks) залежно від призначення систем та рівня конфіденційності даних. Типова архітектура передбачає окремі сегменти для: медичних інформаційних систем з електронними картками пацієнтів; адміністративних систем (бухгалтерія, HR, електронна пошта); медичного обладнання (IoMT); гостьової мережі WiFi для відвідувачів; системи відеоспостереження та контролю доступу. Сегментація забезпечує, що навіть якщо зловмисники компрометують один сегмент (наприклад, через підключення до гостьової WiFi), вони не отримають автоматичного доступу до критичних систем в інших сегментах.

Захист від шкідливого програмного забезпечення базується на багаторівневому підході, що включає традиційні антивіруси, системи поведінкового аналізу та пісочниці. Класичні антивірусні рішення використовують сигнатурний метод виявлення – порівняння файлів з базою відомих шкідливих програм. Хоча цей метод ефективний проти відомих загроз,

він безсилий проти zero-day malware (нових шкідливих програм, для яких ще не створено сигнатури). Тому сучасні медичні заклади впроваджують endpoint detection and response (EDR) системи, що використовують поведінковий аналіз для виявлення підозрілої активності навіть від невідомого шкідливого ПЗ. EDR моніторить процеси на робочих станціях та серверах, аналізує їхню поведінку (які файли відкриваються, які мережеві з'єднання встановлюються, які зміни вносяться до системного реєстру) і виявляє аномалії, характерні для зловмисної активності. Наприклад, масове шифрування файлів, характерне для ransomware, буде виявлено навіть якщо конкретний зразок шифрувальника невідомий антивірусу. Пісочниці (sandboxes) дозволяють безпечно перевіряти підозрілі файли, запускаючи їх у ізольованому віртуальному середовищі і спостерігаючи за поведінкою. Якщо файл демонструє зловмисну активність у пісочниці, він блокується до того, як потрапить до реальної системи. Це особливо важливо для захисту від складних targeted attacks, що використовують custom malware.

Управління доступом та автентифікація є критично важливими для медичних систем, оскільки дані пацієнтів повинні бути доступні авторизованому персоналу, але надійно захищені від несанкціонованого доступу. Сучасні медичні заклади відходять від традиційної моделі «логін-пароль» до багатофакторної автентифікації (MFA – Multi-Factor Authentication), що вимагає двох або більше незалежних факторів підтвердження особи: щось, що користувач знає (пароль або PIN-код); щось, що користувач має (смарт-карта, token, смартфон з додатком автентифікації); щось, чим користувач є (біометрія – відбитки пальців, розпізнавання обличчя).

Впровадження MFA значно підвищує безпеку, оскільки навіть якщо зловмисники вкрадуть пароль користувача через фішинг або витік бази даних, вони не зможуть увійти до системи без другого фактору автентифікації. Для медичних працівників, що працюють у екстрених ситуаціях, розробляються балансовані підходи – MFA для доступу до адміністративних функцій, але спрощена автентифікація для екстреного перегляду медичних карток у критичних ситуаціях з обов'язковим аудитом таких доступів.

Рольова модель доступу (RBAC – Role-Based Access Control) передбачає, що права доступу надаються не індивідуально кожному користувачу, а на основі його ролі в організації. Наприклад, роль «лікар-терапевт» має доступ до перегляду медичних карток пацієнтів терапевтичного відділення та створення записів у них, але не має доступу до фінансових даних або адміністративних налаштувань системи. Це реалізує принцип least privilege – мінімальних необхідних привілеїв, коли кожен користувач має лише той рівень доступу, який необхідний для виконання його службових обов'язків.

Шифрування даних захищає конфіденційність медичної інформації як при зберіганні (encryption at rest), так і при передачі (encryption in transit). Шифрування при зберіганні гарантує, що навіть якщо зловмисники фізично викрадуть жорсткий диск або створять резервну копію бази даних, вони не зможуть прочитати інформацію без ключів дешифрування. Це особливо важливо для мобільних пристроїв медичного персоналу (ноутбуки, планшети), що можуть бути загублені або вкрадені.

Шифрування при передачі захищає дані, що передаються мережею. Усі з'єднання до медичних веб-порталів, систем телемедицини, ЕСОЗ повинні використовувати протокол HTTPS (HTTP over TLS/SSL), що забезпечує шифрування трафіку між браузером користувача та сервером. Це запобігає перехопленню конфіденційної інформації при передачі через незахищені WiFi мережі або компрометовані мережеві вузли.

Для організації безпечних з'єднань між віддаленими локаціями (наприклад, між центральною лікарнею та філіями у різних районах) використовуються VPN (Virtual Private Networks) – віртуальні приватні мережі, що створюють шифровані тунелі через публічний інтернет.

Резервне копіювання та відновлення даних є критично важливими для забезпечення безперервності роботи медичного закладу після кіберінцидентів. Стратегія резервного копіювання повинна відповідати правилу 3-2-1: три копії даних (оригінал плюс дві резервні); дві різні технології зберігання (наприклад, жорсткі диски та стрічки); одна копія за межами основної локації (offsite backup).

Особливо важливою є концепція immutable backups – незмінних резервних копій, які не можуть бути змінені або видалені навіть адміністратором системи протягом визначеного періоду. Це захищає від ransomware-атак, коли зловмисники намагаються знищити або зашифрувати резервні копії перед шифруванням основних даних. Якщо резервні копії є незмінними, їх неможливо скомпрометувати, і дані завжди можна відновити.

Air-gapped backups – резервні копії на носіях, фізично відключених від мережі, забезпечують найвищий рівень захисту. Періодично створюються копії критичних даних на зовнішні жорсткі диски або стрічки, які потім відключаються від усіх систем і зберігаються у безпечному місці. Навіть якщо зловмисники отримають повний контроль над усією IT-інфраструктурою медичного закладу, вони фізично не зможуть досягти air-gapped копій.

Моніторинг та аналіз подій безпеки здійснюється через SIEM (Security Information and Event Management) системи, що збирають логи з усіх компонентів інфраструктури – серверів, робочих станцій, мережевого обладнання, систем безпеки – і аналізують їх у режимі реального часу для виявлення потенційних інцидентів безпеки. SIEM використовує правила кореляції, що дозволяють виявляти складні багатоетапні атаки, окремі елементи яких можуть виглядати безневинно, але в сукупності свідчать про зловмисну активність.

Наприклад, поодинока невдала спроба входу до системи є нормальною подією (користувач помилився у паролі), але сотні невдалих спроб входу з різних IP-адрес протягом короткого часу свідчать про brute-force атаку. Доступ користувача до файлів, з якими він зазвичай не працює, може бути легітимним, але масове копіювання великої кількості файлів на зовнішній носій о третій годині ночі викликає підозру і може свідчити про інсайдерську загрозу або компрометацію облікового запису.

Технічні засоби, якими б досконалими вони не були, не можуть гарантувати безпеку без відповідного організаційного забезпечення та чітких процедур. Організаційна складова включає політики, стандарти, процедури, навчання персоналу та механізми контролю їхнього дотримання.

Політики інформаційної безпеки є фундаментальними документами, що визначають принципи, цілі та загальні вимоги до забезпечення безпеки інформації в медичному закладі. Політика інформаційної безпеки зазвичай затверджується керівником закладу і є обов'язковою для виконання всіма співробітниками. Вона встановлює відповідальність різних рівнів керівництва за безпеку, визначає класифікацію інформації за рівнями конфіденційності, встановлює загальні принципи управління доступом, вимоги до паролів, правила використання робочого обладнання.

На основі загальної політики розробляються більш детальні стандарти та процедури для специфічних аспектів безпеки: стандарт управління обліковими записами користувачів (порядок створення, зміни, видалення облікових записів); процедура реагування на кіберінциденти (покрокові дії при виявленні різних типів інцидентів); політика прийнятного використання (що дозволено і заборонено робити з робочими комп'ютерами та системами); процедура резервного копіювання та відновлення даних; політика роботи з мобільними пристроями та віддаленого доступу.

Критично важливим є не лише наявність цих документів, а й забезпечення їхнього дотримання на практиці. Дослідження демонструють, що у багатьох організаціях політики безпеки існують лише формально, на папері, але не виконуються співробітниками через їхню складність, непрактичність або відсутність контролю. Тому політики повинні бути реалістичними, зрозумілими для персоналу та підкріплені механізмами контролю і відповідальності за їхнє порушення.

Навчання та підвищення обізнаності персоналу є, можливо, найефективнішим організаційним заходом безпеки, враховуючи, що більшість інцидентів пов'язана з людським фактором. Програма навчання повинна бути багаторівневою та систематичною, а не обмежуватися одноразовим вступним інструктажем при прийомі на роботу.

Базове навчання для всього персоналу має охоплювати: основи інформаційної гігієни – створення надійних паролів, розпізнавання фішингових

листів, безпечну роботу з електронною поштою та інтернетом; правила роботи з конфіденційною інформацією пацієнтів – що можна і чого не можна робити з медичними даними; процедури звітування про підозрілі інциденти – до кого звертатися при виявленні підозрілої активності; відповідальність за порушення політик безпеки – як дисциплінарну, так і кримінальну.

Поглиблене навчання для окремих категорій персоналу включає спеціалізовані курси для адміністраторів інформаційних систем з технічних аспектів кібербезпеки, для керівників відділень – з управління ризиками інформаційної безпеки, для працівників, що мають підвищені привілеї доступу – з особливої відповідальності та загроз, пов'язаних з їхніми повноваженнями.

Особливо ефективними є інтерактивні методи навчання. Симуляції фішингових атак, коли співробітники отримують тестові фішингові листи і їхня реакція аналізується, дозволяють виявити найбільш вразливих користувачів та надати їм додаткове навчання. Такі симуляції створюють реальний досвід без реальних ризиків – співробітник, який один раз «потрапився» на тестовий фішинг і отримав зворотній зв'язок, значно менш ймовірно піддасться реальній атаці у майбутньому.

Tabletop exercises (настільні навчання) для команд реагування відпрацьовують сценарії кіберінцидентів без фактичного втручання у роботу систем. Учасники обговорюють гіпотетичний сценарій атаки і визначають, які дії повинні бути вжиті на кожному етапі, хто відповідальний за кожну дію, які ресурси потрібні. Це дозволяє виявити прогалини у планах реагування та покращити координацію між різними підрозділами.

Управління інцидентами безпеки вимагає наявності формалізованого процесу та спеціалізованої команди. Incident Response Team (команда реагування на інциденти) повинна включати представників різних підрозділів – IT, безпеки, юридичної служби, зв'язків з громадськістю, керівництва. Кожен член команди має чітко визначену роль і відповідальність у разі інциденту.

План реагування на інциденти (Incident Response Plan) описує покрокові дії для різних типів інцидентів. Типовий процес реагування включає фази:

виявлення та аналіз – визначення факту інциденту, його типу та масштабу; стримування – обмеження поширення інциденту, ізоляція скомпрометованих систем; викорінення – видалення шкідливого ПЗ, закриття вразливостей, що були експлуатовані; відновлення – повернення систем до нормального функціонування, відновлення даних з резервних копій; post-incident activity – аналіз причин інциденту, документування lessons learned, внесення змін до процедур для запобігання подібним інцидентам у майбутньому.

Критично важливим є регулярне тестування планів реагування через проведення навчань та drill exercises. План, що існує лише на папері, але ніколи не тестувався, майже напевно виявиться неефективним у реальній кризовій ситуації. Навчання виявляють практичні проблеми – наприклад, що контактна особа з CERT-UA вказана невірно, що процедура відключення скомпрометованого сервера не враховує залежності інших систем, що команда реагування не має необхідних технічних інструментів.

Управління вразливостями є проактивним підходом до безпеки, що передбачає систематичне виявлення та усунення слабких місць в інформаційній інфраструктурі до того, як їх експлуатують зловмисники. Процес включає регулярне сканування вразливостей за допомогою автоматизованих інструментів, що перевіряють системи на наявність відомих вразливостей програмного забезпечення, неправильних конфігурацій, слабких паролів.

Vulnerability management повинен включати пріоритизацію виявлених вразливостей на основі їхньої критичності та ймовірності експлуатації. Не всі вразливості однаково небезпечні – критична вразливість у публічно доступному веб-сервері, що містить медичні дані, вимагає негайного усунення, тоді як незначна вразливість в ізольованій системі може бути виправлена під час планового обслуговування.

Patch management (управління оновленнями) є ключовим елементом управління вразливостями. Більшість успішних кібератак експлуатують відомі вразливості, для яких виробники вже випустили оновлення безпеки, але ці оновлення не були встановлені. Медичні заклади повинні мати чіткий процес

тестування та встановлення оновлень безпеки протягом визначеного часу після їхнього випуску.

Водночас встановлення оновлень у медичній сфері є складнішим, ніж у багатьох інших галузях, через критичну важливість безперервності роботи. Оновлення не можна встановлювати під час операції або коли система моніторингу пацієнтів у реанімації не може бути вимкнена. Тому необхідні process windows – заплановані періоди обслуговування, коли оновлення можуть бути встановлені з мінімальним впливом на надання медичної допомоги.

Управління доступом третіх сторін є специфічним викликом для медичних закладів, що активно співпрацюють з зовнішніми підрядниками – постачальниками медичних інформаційних систем, компаніями з обслуговування медичного обладнання, аутсорсинговими IT-провайдерами. Ці треті сторони часто потребують доступу до внутрішніх систем для виконання своїх функцій, що створює додаткові вектори атаки.

Vendor risk management (управління ризиками постачальників) повинно включати: due diligence при виборі постачальника – оцінювання його практик кібербезпеки, наявності сертифікатів (ISO 27001), історії інцидентів безпеки; контрактні вимоги щодо безпеки – включення у договори чітких вимог до захисту даних, зобов'язань негайно повідомляти про інциденти безпеки, права на аудит; обмеження доступу – надання постачальникам лише мінімально необхідного доступу, використання окремих облікових записів для зовнішніх користувачів, моніторинг їхньої активності; регулярний перегляд доступів – періодична верифікація, що всі активні облікові записи третіх сторін є обґрунтованими і необхідними.

Фізична безпека залишається важливою складовою захисту інформаційних активів, оскільки найсучасніші кіберзахисти можуть бути обійдені через фізичний доступ до обладнання. Серверні приміщення повинні мати обмежений доступ з системами контролю входу (електронні замки з картками доступу, біометричні сканери), відеоспостереження з записом та зберіганням архіву, сигналізацію несанкціонованого проникнення.

Робочі станції у загальнодоступних зонах (реєстратури, коридори) повинні бути фізично захищені від несанкціонованого доступу – автоматичне блокування екрану при відсутності активності, неможливість підключення зовнішніх USB-пристроїв без авторизації. Практика clean desk policy (політика чистого столу) вимагає, щоб співробітники не залишали конфіденційні документи або незаблоковані комп'ютери без нагляду.

Утилізація застарілого обладнання та носіїв інформації також є важливим аспектом фізичної безпеки. Жорсткі диски, що виводяться з експлуатації, повинні бути безпечно знищені (фізичне руйнування або криптографічне стирання), а не просто відформатовані, оскільки стандартне форматування не гарантує неможливості відновлення даних спеціалізованими інструментами.

Оцінювання ефективності існуючих механізмів протидії інформаційним операціям у медичній сфері вимагає балансованого підходу, що враховує як досягнення, так і наявні проблеми. За три роки повномасштабної війни українська система охорони здоров'я продемонструвала значну стійкість до кіберзагроз, але водночас виявилися системні вразливості, що потребують термінового вирішення.

Позитивні досягнення включають суттєве підвищення рівня обізнаності про кіберзагрози серед керівництва медичних закладів. Якщо до 2022 року кібербезпека часто сприймалася як другорядне питання, то зараз більшість керівників усвідомлюють критичну важливість захисту інформаційних систем. Це призвело до збільшення інвестицій у технічні засоби захисту та найм спеціалізованого персоналу, принаймні у великих медичних закладах.

Покращилася координація між державними інституціями – CERT-UA, СБУ, МОЗ, НСЗУ. Створено механізми оперативного обміну інформацією про загрози, що дозволяє швидше поширювати попередження та рекомендації. Час реагування на критичні інциденти значно скоротився порівняно з довоєнним періодом.

Впровадження міжнародних стандартів та best practices прискорилося завдяки підтримці міжнародних партнерів. Багато медичних закладів отримали

технічну допомогу від організацій-донорів, що дозволило модернізувати інфраструктуру та впровадити сучасні системи захисту. Міжнародна співпраця також забезпечила доступ до threat intelligence – інформації про нові загрози та методи атак, що використовуються проти медичних закладів у інших країнах.

Накопичено унікальний практичний досвід протидії масштабним державним кібератакам. Українські фахівці з кібербезпеки розробили ефективні методи швидкого реагування на ransomware-атаки, захисту від DDoS, виявлення APT-груп. Цей досвід активно вивчається міжнародними експертами і може бути корисним для інших країн.

Критичні прогалини та системні проблеми, водночас, залишаються значними і потребують термінового вирішення. Найсерйознішою проблемою є величезна нерівність у рівні кібербезпеки між великими міськими медичними центрами та малими регіональними закладами. Якщо обласні клінічні лікарні та національні медичні центри мають спеціалізований персонал з кібербезпеки, сучасне обладнання захисту та регулярно проходять аудити безпеки, то сільські амбулаторії та районні лікарні часто не мають навіть базових засобів захисту.

Ця нерівність створює ефект «найслабшої ланки» – зловмисники можуть спочатку скомпрометувати слабо захищений малий медичний заклад, а потім використати його як плацдарм для атаки на більш захищені системи через довірені канали зв'язку між медичними закладами. Наприклад, якщо районна лікарня інтегрована з обласною клінікою для обміну медичними даними, компрометація районної лікарні може надати доступ до мережі обласного центру.

Кадровий дефіцит залишається гострою проблемою на всіх рівнях. За оцінками експертів, українська медична система потребує щонайменше кілька сотень спеціалістів з кібербезпеки, але фактично їх значно менше. Конкуренція за таланти з приватним сектором, особливо з IT-індустрією, є дуже жорсткою – заробітні плати у комерційних компаніях значно перевищують те, що можуть запропонувати бюджетні медичні заклади. Еміграція кваліфікованих кадрів за кордон посилює проблему.

Навіть там, де є IT-персонал, часто бракує саме компетенцій з кібербезпеки. Системний адміністратор може бути кваліфікованим у підтримці серверів та мереж, але не мати достатніх знань про специфічні загрози, методи атак, техніки захисту. Спеціалізовані тренінги з кібербезпеки є дорогими і не завжди доступними для персоналу бюджетних закладів.

Застаріла інфраструктура продовжує бути джерелом критичних вразливостей. Повна модернізація IT-інфраструктури медичної галузі потребувала б величезних інвестицій, яких немає у бюджеті в умовах війни. Багато медичних закладів продовжують використовувати операційні системи, для яких припинено підтримку (Windows 7, Windows Server 2008), застаріле медичне обладнання з відомими вразливостями, що не можуть бути виправлені.

Особливо проблемною є ситуація з legacy systems – критично важливими системами, що працюють на застарілих технологіях, але не можуть бути оновлені через відсутність сумісних нових версій або через надзвичайно високу вартість заміни. Наприклад, дороге діагностичне обладнання, придбане 10-15 років тому, може працювати лише під управлінням застарілої версії Windows і не має оновлень від виробника, який, можливо, вже не існує на ринку.

Фрагментованість та відсутність уніфікації створюють складнощі для централізованого управління безпекою. Різні медичні заклади використовують різні медичні інформаційні системи від різних постачальників, що ускладнює впровадження єдиних стандартів безпеки, централізований моніторинг загроз, обмін інформацією між системами. Відсутність єдиної точки контролю означає, що національні органи не мають повної картини стану кібербезпеки у медичній галузі.

Спроби впровадження централізованих систем моніторингу та управління стикаються з опором на місцевому рівні через побоювання втрати автономії, недовіру до центральних органів, небажання ділитися інформацією про інциденти (через страх репутаційних втрат або санкцій). Медичні заклади часто приховують інциденти безпеки, сподіваючись вирішити проблему самостійно, що позбавляє систему можливості раннього попередження інших закладів про

нові загрози.

Недосконаліть правового регулювання проявляється у кількох аспектах. По-перше, відсутні галузеві стандарти кібербезпеки, специфічні для медичної сфери та адаптовані до її особливостей. Загальнодержавні вимоги до кіберзахисту критичної інфраструктури є універсальними, але не враховують специфіку медичної діяльності – необхідність балансу між безпекою та доступністю даних, особливості роботи з медичним обладнанням, етичні аспекти роботи з конфіденційною медичною інформацією.

По-друге, механізми відповідальності за порушення вимог кібербезпеки є недостатньо ефективними. Якщо у фінансовому секторі регулятор (Національний банк) має потужні інструменти примусу – від штрафів до відкликання ліцензій, то у медичній сфері санкції за недотримання вимог безпеки є символічними і рідко застосовуються на практиці. Це знижує мотивацію керівників медичних закладів інвестувати обмежені ресурси саме у кібербезпеку, а не в інші потреби.

По-третє, відсутня чітка регламентація взаємодії між різними державними органами при реагуванні на кіберінциденти у медичній сфері. Розподіл повноважень між ДССЗЗІ, СБУ, МОЗ, поліцією не завжди є чітким, що може призводити до дублювання зусиль або, навпаки, до ситуацій, коли кожен вважає, що відповідальність лежить на іншому.

Недостатня протидія інформаційним операціям (на відміну від технічних кібератак) залишається слабким місцем системи. Якщо механізми захисту від технічних кіберзагроз поступово розвиваються і вдосконалюються, то протидія дезінформаційним кампаніям, маніпуляціям у соціальних мережах, психологічним операціям проти медичної сфери є значно менш ефективною [16].

Відсутня систематична робота з моніторингу інформаційного простору для раннього виявлення дезінформаційних кампаній проти медичної системи. Реагування на фейки часто відбувається з запізненням, коли неправдива інформація вже широко розповсюдилася. Механізми спростування дезінформації є недосконалими – офіційні спростування часто не досягають тієї

ж аудиторії, що була охоплена фейком, або подаються у формі, що не є переконливою для скептично налаштованих громадян.

Медичні заклади та їхній персонал не мають достатніх компетенцій та інструментів для самостійної протидії інформаційним атакам на їхню репутацію. Координовані кампанії негативних відгуків, фейкові звинувачення у соціальних мережах часто залишаються без адекватної відповіді, оскільки у медичних закладів немає фахівців з комунікацій та управління репутацією у цифровому просторі.

Відсутність культури кібербезпеки на рівні медичного персоналу залишається фундаментальною проблемою. Попри проведення тренінгів та інформаційних кампаній, значна частина медичних працівників продовжує сприймати вимоги кібербезпеки як бюрократичні перешкоди, що заважають їхній основній роботі. Складні паролі забуваються і записуються на папері, багатофакторна автентифікація викликає роздратування через додаткові кроки, попередження системи безпеки ігноруються.

Ця проблема має глибші корені – медичний персонал перебуває у стані хронічного стресу та перевантаження, особливо в умовах війни. Коли лікар працює по 12-14 годин без перерви, необхідність витрачати додаткову хвилину на складну процедуру входу до системи сприймається як неприйнятна. Тому будь-які заходи безпеки, що значно уповільнюють робочі процеси, будуть саботуватися персоналом, який шукатиме обхідні шляхи.

Недостатня інтеграція з міжнародними системами захисту обмежує доступ до глобального threat intelligence та best practices. Хоча співпраця з міжнародними партнерами посилилася, українські медичні заклади ще не є повноправними учасниками глобальних мереж обміну інформацією про кіберзагрози у медичній сфері. Багато міжнародних баз даних про індикатори компрометації, шкідливе програмне забезпечення, техніки атак є платними або обмеженими для країн-членів певних організацій.

Мовний бар'єр також відіграє роль – більшість міжнародних ресурсів з кібербезпеки є англомовними, що обмежує їхню доступність для персоналу

регіональних медичних закладів. Адаптація міжнародних стандартів та методичних матеріалів до українського контексту відбувається повільно через брак ресурсів та експертизи.

Узагальнюючи аналіз ефективності існуючих механізмів, можна констатувати, що українська система охорони здоров'я знаходиться у перехідному стані. Створено базові організаційні та технічні механізми протидії кіберзагрозам, накопичено практичний досвід, встановлено міжнародну співпрацю. Водночас залишаються системні проблеми, що не можуть бути вирішені лише еволюційним шляхом і потребують стратегічних рішень на державному рівні – масштабних інвестицій у модернізацію інфраструктури, системної підготовки кадрів, вдосконалення правового регулювання, створення галузевих стандартів та механізмів їхнього впровадження.

Аналіз сучасного ландшафту загроз та ефективності існуючих механізмів протидії виявив драматичну трансформацію характеру інформаційного протиборства у медичній сфері та системні проблеми у організації захисту.

Повномасштабна агресія російської федерації радикально змінила природу загроз для медичної інфраструктури. Якщо до 2022 року домінували opportunistic attacks з фінансовою мотивацією, то зараз медична сфера стала об'єктом цілеспрямованих державних кібероперацї, координованих спецслужбами противника. Інтенсивність атак зросла у десятки разів, рівень їхньої технічної складності підвищився (використання zero-day вразливостей, custom malware, APT-технік), а мотивація змістилася до стратегічних цілей дестабілізації держави.

Систематизація кіберзагроз виявила основні типи атак: ransomware з подвійним вимаганням та політичною мотивацією, DDoS-атаки на критичні сервіси для створення хаосу під час масових надходжень постраждалих, компрометація медичного обладнання IoMT з потенційною загрозою життю пацієнтів, складні APT-операції з довготривалим прихованим проникненням, атаки на ланцюги постачання програмного забезпечення та послуг. Особливу небезпеку становлять гібридні сценарії, коли технічні кібератаки координуються

з фізичними ударами та інформаційними операціями.

Інформаційні операції проти медичної сфери виявилися не менш небезпечними за технічні кібератаки. Систематична дезінформація щодо епідеміологічної ситуації, дискредитація медичних закладів та персоналу, координовані кампанії у соціальних мережах з використанням ботів і тролів, експлуатація емоційних тригерів та когнітивних упереджень створюють довгострокові репутаційні збитки та підривають довіру населення до медичної системи.

Аналіз існуючих механізмів протидії виявив як досягнення, так і критичні прогалини. Позитивними є створення базової координації між CERT-UA, СБУ, МОЗ та НСЗУ, накопичення унікального практичного досвіду протидії масштабним атакам, впровадження міжнародних стандартів за підтримки партнерів, підвищення обізнаності керівництва про важливість кібербезпеки.

Водночас виявлені системні проблеми, що потребують термінового вирішення. Найсерйознішою є величезна нерівність у рівні кібербезпеки між великими міськими медичними центрами та малими регіональними закладами, що створює ефект «найслабшої ланки».

Хронічний кадровий дефіцит фахівців з кібербезпеки посилюється конкуренцією з приватним сектором та еміграцією. Застаріла інфраструктура продовжує бути джерелом критичних вразливостей при відсутності ресурсів для швидкої модернізації.

Фрагментованість систем ускладнює централізований моніторинг та впровадження уніфікованих стандартів.

Недосконалість правового регулювання проявляється у відсутності галузевих стандартів кібербезпеки для медичної сфери, недостатньо ефективних механізмах відповідальності за порушення вимог безпеки, нечіткій регламентації взаємодії між державними органами при реагуванні на інциденти.

Найбільшою вразливістю залишається людський фактор – до 70% інцидентів пов'язані з помилками або недостатньою обізнаністю персоналу при відсутності системної культури кібербезпеки.

Медичний персонал у стані хронічного стресу сприймає вимоги безпеки як бюрократичні перешкоди, що призводить до саботажу навіть обґрунтованих заходів захисту.

РОЗДІЛ 3
СТРАТЕГІЧНІ НАПРЯМИ ВДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

3.1 Організаційно-інституційний розвиток системи кібербезпеки медичної галузі

Критична оцінка ефективності існуючих механізмів захисту, представлені у попередньому розділі, дозволяють перейти до формулювання стратегічних напрямів вдосконалення системи протидії інформаційним операціям у вітчизняній медичній сфері. Цей розділ присвячений розробці конкретних рекомендацій, що базуються на виявлених проблемах і прогалинах, враховують міжнародний досвід та адаптовані до специфічних умов функціонування української системи охорони здоров'я.

Ключовий принцип запропонованого підходу полягає у визнанні того, що ефективна протидія інформаційним операціям вимагає комплексної трансформації, а не окремих точкових заходів. Необхідна координована робота на всіх рівнях – від національної стратегії до конкретних технічних рішень у кожному медичному закладі, від удосконалення законодавства до зміни корпоративної культури медичного персоналу. Водночас важливо враховувати обмеженість наявних ресурсів та необхідність пріоритизації заходів за критеріями їхньої критичності, вартості впровадження та очікуваного ефекту.

Запропоновані рекомендації структуровані за трьома основними напрямами, що відповідають виявленим системним проблемам: організаційно-інституційний розвиток (створення ефективних структур управління кібербезпекою на національному та галузевому рівнях), технологічна модернізація (впровадження сучасних технічних засобів захисту з урахуванням специфіки медичної галузі), розвиток людського капіталу (системна підготовка

кадрів та формування культури кібербезпеки). Кожен з цих напрямів є необхідним, але недостатнім сам по собі – лише їхня синергетична взаємодія може забезпечити фундаментальне підвищення стійкості медичної інфраструктури до гібридних загроз.

Ефективна протидія інформаційним операціям вимагає, насамперед, створення чіткої організаційної структури з визначеними повноваженнями, зонами відповідальності та механізмами координації між різними рівнями та суб'єктами. Аналіз міжнародного досвіду та вітчизняної практики демонструє, що технічні засоби захисту самі по собі не можуть компенсувати організаційний хаос та відсутність стратегічного керівництва.

Однією з найбільш критичних прогалин у сучасній системі є відсутність спеціалізованого галузевого органу, що відповідав би виключно за питання кібербезпеки у медичній сфері. Хоча загальне керівництво здійснює ДССЗЗІ через CERT-UA, а галузеву координацію намагається забезпечити МОЗ, жодна з цих структур не має достатніх ресурсів, повноважень та експертизи для системної роботи саме у медичній специфіці.

Концепція галузевого центру кібербезпеки базується на успішному міжнародному досвіді створення sectoral CSIRT (галузевих команд реагування на комп'ютерні інциденти) у критичних секторах економіки. Такі спеціалізовані центри функціонують у фінансовому секторі (Financial CERT), енергетиці (Energy CERT), телекомунікаціях. Медична сфера, враховуючи її критичну важливість та специфічні виклики, потребує аналогічної структури – Healthcare CERT або Healthcare Cybersecurity Center.

Основними функціями галузевого центру мають бути: моніторинг кіберзагроз, специфічних для медичної інфраструктури – відстеження активності APT-груп, що спеціалізуються на атаках медичних закладів, аналіз нових типів ransomware та методів атак на медичні інформаційні системи; координація реагування на інциденти – центр повинен виступати першою точкою контакту для медичних закладів при виявленні кіберінциденту, забезпечувати триаж інцидентів за рівнем критичності, координувати залучення спеціалістів CERT-

UA або СБУ для найсерйозніших випадків; розробка галузевих стандартів та методичних рекомендацій – на основі аналізу інцидентів та кращих практик центр повинен формулювати специфічні вимоги до кібербезпеки медичних закладів різних типів та категорій; проведення аудитів та оцінок відповідності – систематична перевірка медичних закладів на відповідність встановленим стандартам, виявлення вразливостей та рекомендації щодо їхнього усунення; навчання та сертифікація персоналу – розробка та впровадження програм підготовки фахівців з кібербезпеки для медичної галузі, сертифікація відповідальних осіб у медичних закладах; міжнародна співпраця – взаємодія з аналогічними центрами інших країн, участь у міжнародних мережах обміну інформацією про загрози (Health-ISAC) [8].

Організаційна структура центру повинна забезпечувати баланс між технічною експертизою та розумінням специфіки медичної галузі. До складу центру мають входити: технічні експерти з кібербезпеки – фахівці з пентестингу, форензики, аналізу шкідливого ПЗ, архітектури безпеки; медичні ІТ-експерти – фахівці, що розуміють специфіку медичних інформаційних систем, медичного обладнання, клінічних процесів; аналітики загроз – спеціалісти з моніторингу кіберпростору, аналізу індикаторів компрометації, прогнозування трендів; юристи – експерти з регуляторних вимог, захисту персональних даних, міжнародного законодавства; фахівці з комунікацій – для роботи з медичними закладами, поширення інформації про загрози, управління кризовими комунікаціями під час інцидентів.

Правовий статус центру потребує ретельного опрацювання. Оптимальним варіантом видається створення центру як державної установи при МОЗ з частковим фінансуванням через НСЗУ (оскільки забезпечення кібербезпеки є необхідною умовою якісного надання медичних послуг за програмою медичних гарантій). Альтернативно можна розглянути модель публічно-приватного партнерства, коли центр утворюється як незалежна організація з державним фінансуванням, але з залученням експертизи приватного сектору – вітчизняних та міжнародних компаній з кібербезпеки, постачальників медичних

інформаційних систем.

Критично важливим є наділення центру достатніми повноваженнями. Він не повинен бути лише консультативним органом – центр має мати право проводити обов'язкові перевірки медичних закладів, що є об'єктами критичної інфраструктури, вимагати усунення виявлених критичних вразливостей у визначені терміни, застосовувати санкції (або ініціювати їхнє застосування іншими органами) за систематичне недотримання вимог кібербезпеки. Водночас центр повинен діяти не як каральний орган, а як партнер медичних закладів, надаючи їм необхідну методичну та технічну підтримку для досягнення відповідності стандартам.

Фінансування центру має бути стабільним та достатнім для залучення висококваліфікованих фахівців. Орієнтовний бюджет на створення та перший рік функціонування (включаючи зарплати 20-30 співробітників, технічне обладнання, програмне забезпечення, навчання) може становити 50-100 млн грн. Це значні кошти, але порівняно з потенційними збитками від масштабних кіберінцидентів (як фінансовими, так і у вигляді загроз життю пацієнтів) ці інвестиції є цілком виправданими.

Джерела фінансування можуть включати: державний бюджет (МОЗ); частку від бюджету НСЗУ (як необхідна інфраструктура для функціонування системи медичних гарантій); міжнародну технічну допомогу (багато міжнародних організацій готові підтримувати проєкти зміцнення кібербезпеки критичної інфраструктури); частково – платні послуги для приватних медичних закладів (аудити безпеки, консультації, навчання).

Етапність створення центру має бути реалістичною з урахуванням обмежених ресурсів та необхідності поступового нарощування спроможностей. На першому етапі (6-12 місяців) доцільно створити невелику базову команду (5-10 осіб) при МОЗ, яка зосередиться на найкритичніших функціях – моніторингу загроз та координації реагування на найсерйозніші інциденти. Цей етап може фінансуватися за рахунок міжнародної допомоги та перерозподілу існуючих бюджетних ресурсів. На другому етапі (12-24 місяці) відбувається розширення

функціоналу – розробка галузевих стандартів, запуск програм навчання, створення системи моніторингу стану кібербезпеки у медичних закладах. Команда розширюється до 15-20 осіб, залучаються зовнішні експерти та консультанти. На третьому етапі (24-36 місяців) центр досягає повної операційної спроможності – впроваджується комплексна система аудитів, запускаються спеціалізовані сервіси для медичних закладів (threat intelligence feed, incident response support, vulnerability scanning as a service), встановлюється повноцінна міжнародна співпраця. Центр стає визнаним національним та міжнародним центром експертизи з кібербезпеки медичної галузі.

Централізований галузевий центр, хоч і необхідний для стратегічного керівництва та координації, не може фізично забезпечити оперативне реагування на інциденти в усіх медичних закладах по всій країні. Тому паралельно з створенням національного центру необхідно розвивати мережу регіональних центрів компетенції, що забезпечать наближення експертизи до безпосередніх користувачів.

Концепція регіональних центрів компетенції базується на принципі розподіленої відповідальності та використання наявних ресурсів. Замість створення повністю нових структур з нуля, доцільно визначити anchor institutions – опорні медичні заклади у кожній області (зазвичай це обласні клінічні лікарні або найбільші міські медичні центри), які мають відносно розвинуті IT-підрозділи та певну експертизу з кібербезпеки, і надати їм додаткові ресурси та повноваження для виконання функцій регіонального центру компетенції.

Основні функції регіонального центру включають: надання первинної технічної підтримки медичним закладам області при виявленні кіберінцидентів – консультації по телефону або онлайн, віддалена діагностика проблеми, рекомендації щодо першочергових дій; проведення базових аудитів безпеки для малих та середніх медичних закладів області, що не мають власних фахівців з кібербезпеки; організацію регіональних тренінгів та навчань для персоналу медичних закладів; моніторинг стану кібербезпеки у медичних закладах регіону та звітування до національного центру; координацію з регіональними

підрозділами ДССЗЗІ та СБУ при розслідуванні серйозних інцидентів.

Організаційна модель регіонального центру може бути гнучкою залежно від специфіки регіону. У великих областях з кількома потужними медичними закладами доцільно створити окремий підрозділ кібербезпеки при обласному управлінні охорони здоров'я, який координуватиме роботу спеціалістів з різних медичних закладів. У менших регіонах функції центру може виконувати розширений відділ інформаційної безпеки обласної лікарні.

Мінімальна команда регіонального центру повинна включати 3-5 фахівців: керівника центру (має досвід як у кібербезпеці, так і у медичній ІТ); технічного експерта з кібербезпеки (спеціалізація на виявленні та реагуванні на інциденти); адміністратора безпеки (відповідає за аудити, перевірку дотримання політик); тренера (проводить навчання персоналу медичних закладів). Для регіонів з великою кількістю медичних закладів команда може бути розширена.

Механізми координації між рівнями – національним центром та регіональними центрами – мають бути формалізовані та технологічно забезпечені. Національний центр повинен надавати регіональним центрам: оперативну інформацію про нові загрози та вразливості; методичні рекомендації та готові процедури реагування; технічні інструменти для моніторингу та аналізу (системи сканування вразливостей, SIEM, sandbox для аналізу підозрілих файлів); навчання та сертифікацію персоналу регіональних центрів; підтримку при складних інцидентах, що перевищують можливості регіонального центру.

Регіональні центри, у свою чергу, повинні звітувати національному центру про: всі виявлені кіберінциденти у регіоні (із зазначенням деталей атаки, постраждалих систем, заходів реагування); виявлені системні вразливості, що характерні для багатьох медичних закладів регіону; проблеми впровадження стандартів та рекомендацій національного центру; потреби у додатковій підтримці або ресурсах.

Фінансова модель регіональних центрів має поєднувати різні джерела. Базове фінансування може здійснюватися через обласні бюджети (управління охорони здоров'я), додаткова підтримка – від національного центру у формі

грантів на конкретні проєкти, технічного обладнання, ліцензій на програмне забезпечення. Частина коштів може генеруватися через надання платних послуг приватним медичним закладам регіону.

Орієнтовний бюджет на створення та річне утримання одного регіонального центру може становити 5-10 млн грн залежно від розміру регіону. Для 24 областей України (включаючи окреме фінансування для Києва) загальна потреба становитиме 120-240 млн грн на рік. Це значні кошти, але вони можуть бути частково компенсовані через перерозподіл існуючих бюджетів обласних медичних закладів та залучення міжнародної допомоги.

Мережева модель взаємодії між медичними закладами у межах регіону може значно підвищити ефективність використання обмежених ресурсів. Замість того, щоб кожен медичний заклад намагався самостійно вирішувати всі питання кібербезпеки, створюється модель shared services – спільних сервісів, коли регіональний центр надає централізовані послуги, доступні всім медичним закладам області.

Такі централізовані сервіси можуть включати: Security Operations Center (SOC) – централізований моніторинг подій безпеки з усіх медичних закладів регіону в режимі 24/7; централізовану систему резервного копіювання – регіональний data center, що зберігає резервні копії критичних даних усіх медичних закладів; централізовану систему управління оновленнями – тестування оновлень безпеки на стенді регіонального центру перед розгортанням у медичних закладах; threat intelligence feed – підписка на комерційні бази даних про загрози з розповсюдженням інформації всім медичним закладам регіону; incident response team – команда експертів, готова оперативно виїхати на місце серйозного інциденту у будь-якому медичному закладі області.

Пілотний проєкт доцільно розпочати у 2-3 пілотних регіонах, що відрізняються за характеристиками – наприклад, у великій області з розвиненою медичною інфраструктурою (Дніпропетровська, Харківська), у середній області (Вінницька, Чернігівська) та у невеликій прикордонній області, що зазнає підвищених кіберзагроз (Сумська, Херсонська). Результати пілотного проєкту

дозволять відкоригувати модель перед масштабуванням на всі регіони.

Тривалість пілотного проєкту має становити 12-18 місяців, протягом яких будуть відпрацьовані процедури взаємодії, протестовані технічні рішення, оцінена реальна вартість та ефективність моделі. Після успішного завершення пілоту розгортання мережі регіональних центрів може відбуватися поетапно – по 6-8 нових центрів щороку протягом 3-4 років.

Ефективність організаційних структур значною мірою залежить від якості правового регулювання, що визначає їхні повноваження, зони відповідальності та механізми примусу. Сучасна нормативно-правова база у сфері кібербезпеки медичної галузі має суттєві прогалини, що потребують термінового усунення.

Розробка галузевих стандартів кібербезпеки для медичної сфери є пріоритетним завданням. На відміну від загальних вимог до кіберзахисту критичної інфраструктури, галузеві стандарти повинні враховувати специфіку медичної діяльності – необхідність балансу між безпекою та доступністю даних для екстреної допомоги, особливості захисту медичного обладнання з вбудованими комп'ютерними системами, етичні аспекти роботи з конфіденційною медичною інформацією.

За основу можна взяти американський стандарт HIPAA Security Rule, але адаптувати його до українського контексту та доповнити з урахуванням досвіду протидії кіберзагрозам в умовах війни. Галузевий стандарт має встановлювати: класифікацію медичних закладів за категоріями критичності (національні медичні центри, обласні лікарні, районні лікарні, амбулаторії) з диференційованими вимогами до кібербезпеки; обов'язкові технічні контрольні заходи (шифрування даних, багатофакторна автентифікація, системи виявлення вторгнень) з конкретними технічними специфікаціями; організаційні вимоги (політики безпеки, плани реагування на інциденти, програми навчання персоналу); процедури аудиту та сертифікації відповідності стандарту; санкції за недотримання вимог.

Розробка регламенту реагування на кіберінциденти у медичній сфері має формалізувати процедури взаємодії між різними органами. Регламент повинен

чітко визначати: критерії класифікації інцидентів за рівнями серйозності (критичні, високі, середні, низькі); процедури повідомлення про інциденти – до кого, у які терміни, в якому форматі повинен звітувати медичний заклад при виявленні інциденту; розподіл відповідальності між галузевим центром, CERT-UA, СБУ, поліцією при розслідуванні різних типів інцидентів; процедури координації реагування – хто очолює реагування, як координується робота різних органів, як приймаються рішення про залучення додаткових ресурсів; вимоги до документування інцидентів та post-incident analysis.

Особливу увагу слід приділити процедурам реагування на масштабні інциденти, що одночасно впливають на багато медичних закладів (наприклад, масована ransomware-кампанія або DDoS-атака на центральні компоненти ЕСОЗ). Регламент повинен передбачати механізм активації crisis response mode, коли всі доступні ресурси мобілізуються для локалізації загрози та мінімізації збитків.

Удосконалення механізмів відповідальності за порушення вимог кібербезпеки має включати як адміністративну, так і кримінальну складові. Необхідно внести зміни до Кодексу України про адміністративні правопорушення, встановивши конкретні штрафи за: недотримання обов'язкових вимог галузевого стандарту кібербезпеки для медичних закладів критичної інфраструктури; несвоєчасне повідомлення про кіберінциденти до відповідних органів; відмову надати доступ представникам галузевого центру або CERT-UA при розслідуванні інциденту; експлуатацію медичних інформаційних систем без дотримання базових вимог безпеки, що призвело до витоку конфіденційної інформації пацієнтів.

Розмір штрафів має бути достатнім для створення реального стимулу дотримуватися вимог. Орієнтовно, для керівників медичних закладів штрафи можуть становити від 50 до 200 неоподатковуваних мінімумів доходів громадян (від 850 до 3400 грн), а для юридичних осіб – від 500 до 2000 неоподатковуваних мінімумів (від 8500 до 34000 грн) залежно від серйозності порушення. Водночас механізм штрафів має бути справедливим – малі медичні заклади з обмеженими

бюджетами не повинні каратися за неможливість виконати вимоги через об'єктивну відсутність ресурсів.

Кримінальна відповідальність має застосовуватися у випадках умисних дій або грубої недбалості керівництва, що призвели до критичних наслідків – загрози життю пацієнтів, масового витоку конфіденційної інформації. Доцільно доповнити Кримінальний кодекс України статтею про відповідальність керівників критичної інфраструктури за ненадання належного захисту, якщо це призвело до тяжких наслідків.

Гармонізація з європейським законодавством є важливою в контексті євроінтеграції України. Процес імплементації Директиви NIS2 має бути прискорений, а вимоги цієї директиви адаптовані до специфіки вітчизняної медичної системи. Зокрема, необхідно: визначити чіткі критерії віднесення медичних закладів до категорії essential entities (ключові суб'єкти) та important entities (важливі суб'єкти) з відповідними рівнями вимог; встановити процедури обов'язкової звітності про інциденти з терміном 24 години для попереднього повідомлення та 72 години для детального звіту; запровадити вимогу про оцінку кіберризиків у ланцюгах постачання; встановити персональну відповідальність керівників медичних закладів за дотримання вимог кібербезпеки [5].

Паралельно з імплементацією NIS2 доцільно адаптувати окремі положення GDPR, що стосуються технічних та організаційних заходів захисту персональних даних. Хоча Україна має власний Закон про захист персональних даних, його вимоги є менш деталізованими порівняно з GDPR, особливо щодо обов'язку проведення Data Protection Impact Assessment для нових інформаційних систем.

Стимулювання добровільного дотримання стандартів через економічні механізми може бути ефективнішим за примусові заходи. НСЗУ може диференціювати розміри фінансування медичних закладів залежно від рівня їхньої кібербезпеки – заклади, що пройшли сертифікацію відповідності галузевому стандарту, отримують додатковий коефіцієнт при розрахунку тарифів на медичні послуги. Це створить економічний стимул інвестувати у кібербезпеку.

Альтернативно можна запровадити програму грантової підтримки для медичних закладів, що демонструють прогрес у підвищенні рівня кібербезпеки. Заклади подають заявки на гранти для придбання засобів захисту, навчання персоналу, проведення аудитів безпеки. Пріоритет надається закладам, що обслуговують вразливі категорії населення, розташовані у зонах підвищеного ризику, демонструють реальне прагнення покращити свою безпеку.

Міжнародні угоди та меморандуми про співпрацю у сфері кібербезпеки медичної галузі мають бути укладені з країнами-партнерами. Такі угоди можуть передбачати: обмін інформацією про кіберзагрози, специфічні для медичної інфраструктури; взаємну технічну допомогу при розслідуванні транснаціональних кіберзлочинів проти медичних закладів; спільні навчання та тренінги для персоналу; обмін кращими практиками та методичними матеріалами; можливість звернення за експертною допомогою у випадку масштабних інцидентів.

Особливо важливою є формалізація співпраці з Health-ISAC (Healthcare Information Sharing and Analysis Center) – міжнародною організацією, що координує обмін інформацією про кіберзагрози у медичній сфері між членами з різних країн. Членство українського галузевого центру у Health-ISAC забезпечить доступ до глобальної бази даних про загрози, методичних матеріалів, можливість консультацій з міжнародними експертами [9].

3.2 Технологічна модернізація та впровадження передових рішень кібербезпеки

Організаційно-інституційний розвиток має супроводжуватися технологічною модернізацією медичної інфраструктури. Застаріле обладнання, програмне забезпечення без підтримки, фрагментовані інформаційні системи створюють фундаментальні вразливості, які неможливо усунути виключно

організаційними заходами.

Повна заміна всього застарілого обладнання та програмного забезпечення у медичній галузі потребувала б величезних інвестицій, яких реально немає. Тому необхідна прагматична стратегія, що базується на пріоритизації – визначенні найкритичніших систем, модернізація яких дасть найбільший ефект з точки зору безпеки, та поетапному плані оновлення протягом 5-7 років.

Інвентаризація та категоризація активів є першим необхідним кроком. Кожен медичний заклад повинен створити повний реєстр своїх інформаційних активів – серверів, робочих станцій, медичного обладнання з комп'ютерними системами, мережевого обладнання, програмного забезпечення. Для кожного активу фіксуються: тип та модель обладнання/ПЗ; версія операційної системи та прошивки; дата останнього оновлення; статус підтримки виробником (чи випускаються оновлення безпеки); критичність для функціонування медичного закладу; категорія даних, що обробляються (чи містить ePHI).

На основі цієї інформації активи класифікуються за рівнем ризику. Найвищий ризик становлять системи, що одночасно: обробляють критично важливі або конфіденційні дані; використовують застаріле ПЗ без підтримки; мають мережеве підключення; критично важливі для надання медичної допомоги. Такі системи потребують пріоритетної модернізації або компенсаційних заходів захисту.

Стратегія заміни legacy systems має бути диференційованою. Для систем, що більше не підтримуються виробником і не можуть бути оновлені, але критично важливі для роботи, можливі кілька підходів: ізоляція у окремому мережевому сегменті без прямого доступу до інтернету та з суворим контролем з'єднань з іншими системами; впровадження додаткових компенсаційних контролів – application whitelisting (дозвіл на виконання лише затверджених програм), мережевий моніторинг на предмет аномальної активності, посилена фізична безпека; планування поступової заміни – розробка бізнес-кейсу, пошук фінансування, вибір альтернативних рішень.

Для медичного обладнання з вбудованими комп'ютерними системами, що

працюють на застарілих ОС, рекомендується: узгодження з виробником можливості оновлення прошивки або ОС без втрати сертифікації обладнання; якщо оновлення неможливе – ізоляція обладнання у окремій VLAN з обмеженим доступом; впровадження network segmentation – розділення мережі таким чином, щоб компрометація застарілого обладнання не дала доступу до інших систем.

Програма поетапної модернізації повинна мати реалістичний часовий горизонт 5-7 років з чіткими проміжними цілями. Перший етап (1-2 роки) фокусується на найкритичніших системах – серверах, що зберігають ePHI, системах, що безпосередньо впливають на життя пацієнтів (системи моніторингу у реанімаціях, системи управління інфузійними помпами). Другий етап (3-4 роки) охоплює модернізацію робочих станцій медичного персоналу, мережевої інфраструктури, систем резервного копіювання. Третій етап (5-7 років) передбачає заміну менш критичних систем та планове оновлення систем, модернізованих на першому етапі.

Фінансування програми модернізації може здійснюватися через: державний бюджет – цільові програми модернізації медичної інфраструктури; міжнародну технічну допомогу – багато донорів готові фінансувати проєкти цифровізації медицини; модель ESCO (Energy Service Company), адаптовану для IT – коли компанія-підрядник фінансує модернізацію, а медичний заклад виплачує кошти з економії операційних витрат протягом кількох років; лізинг обладнання замість придбання – розподіл платежів у часі, що знижує одномоментне навантаження на бюджет.

Паралельно з модернізацією застарілих систем необхідно впроваджувати сучасні архітектурні підходи до побудови безпечної інфраструктури, що базуються на принципах defense in depth (ешелонована оборона) та zero trust (нульова довіра). Архітектура zero trust передбачає відмову від традиційної моделі «периметр безпеки», коли все, що знаходиться всередині корпоративної мережі, вважається довіреним. Натомість кожен запит на доступ до ресурсів, незалежно від його походження (зсередини чи ззовні мережі), має бути автентифікований, авторизований та верифікований. Це особливо актуально для

медичної сфери, де співробітники часто працюють з різних локацій – з дому, з мобільних медичних пунктів, під час виїздів до пацієнтів. Для медичних закладів впровадження концепції zero trust має включати кілька ключових компонентів.

По-перше, це відмова від традиційних VPN-рішень на користь більш сучасних технологій Zero Trust Network Access (ZTNA), що надають доступ не до всієї корпоративної мережі, а лише до конкретних додатків та ресурсів, необхідних конкретному користувачу для виконання його функцій. Якщо лікар-терапевт має доступ лише до електронних медичних карток пацієнтів свого відділення, навіть компрометація його облікового запису не дасть зловмисникам доступу до фінансових систем або даних інших відділень.

По-друге, необхідна мікросегментація мережі – розділення єдиної корпоративної мережі на безліч ізольованих сегментів з чітко визначеними правилами комунікації між ними. Це дозволяє радикально обмежити lateral movement – можливість зловмисників переміщуватися між системами після початкового проникнення. Навіть якщо атакуючі скомпрометують робочу станцію у реєстратурі, вони не зможуть звідти потрапити до серверів з медичними даними або до систем управління медичним обладнанням, оскільки ці сегменти ізольовані один від одного.

По-третє, концепція continuous verification – постійної верифікації довіри протягом усієї сесії користувача. На відміну від традиційного підходу, коли автентифікація відбувається лише при вході до системи, а далі користувач вважається довіреним до кінця сесії, zero trust передбачає постійний аналіз поведінки. Якщо система виявляє аномалії – користувач раптом починає завантажувати величезні обсяги даних, звертатися до ресурсів, з якими зазвичай не працює, або активність походить з незвичайної географічної локації – може бути автоматично запитана додаткова автентифікація або обмежено доступ до найбільш чутливих ресурсів.

Впровадження повноцінної архітектури zero trust є складним багаторічним процесом, що вимагає не лише технологічних змін, а й організаційної трансформації. Тому доцільно розпочати з пілотних проєктів на найкритичніших

сегментах інфраструктури. Наприклад, можна почати з захисту доступу до центральних компонентів ЕСОЗ або до систем психіатричних клінік, де конфіденційність даних є особливо критичною. Успішний досвід пілотних проєктів може бути згодом масштабований на інші сегменти медичної інфраструктури.

Extended Detection and Response (XDR) представляє еволюцію традиційних систем виявлення загроз, інтегруючи дані з усіх рівнів інфраструктури – кінцевих пристроїв (робочі станції, сервери, мобільні пристрої), мережевого рівня, хмарних сервісів, систем електронної пошти. На відміну від традиційних SIEM-систем, що переважно збирають та зберігають логи для подальшого аналізу, XDR активно аналізує події у режимі реального часу, використовуючи алгоритми машинного навчання для виявлення складних багатоетапних атак. Ключова перевага XDR полягає у можливості виявляти зв'язки між подіями на різних рівнях інфраструктури, що окремо виглядають безневинно, але разом формують картину атаки. Наприклад, XDR може зв'язати факт отримання підозрілого email конкретним користувачем, відкриття вкладення, встановлення нового процесу на його комп'ютері, незвичайні мережеві з'єднання до зовнішніх IP-адрес і автоматично класифікувати це як ймовірну ransomware-атаку на початковій стадії. Для медичної галузі впровадження XDR має відбуватися централізовано через галузевий або регіональні центри кібербезпеки. Індивідуальні медичні заклади, особливо малі та середні, не мають ні фінансових ресурсів для придбання дорогих XDR-платформ, ні експертизи для їхньої налаштування та експлуатації. Натомість регіональний центр може розгорнути єдину XDR-платформу та підключити до неї всі медичні заклади області, забезпечуючи централізований моніторинг безпеки 24/7 та швидке реагування на виявлені загрози.

Системи автоматизованого управління вразливостями є критично важливими для систематичного виявлення та усунення слабких місць в інфраструктурі ще до того, як їх експлуатують зловмисники. Сучасні рішення класу Vulnerability Management as a Service (VMaaS) дозволяють автоматизувати

весь цикл управління вразливостями – від їхнього виявлення до усунення. Система регулярно (щотижня або навіть щоденно) сканує всі компоненти інфраструктури медичного закладу, ідентифікує вразливості програмного забезпечення, неправильні конфігурації, слабкі паролі. Кожна виявлена вразливість автоматично класифікується за рівнем критичності з урахуванням кількох факторів: технічної серйозності самої вразливості (чи дозволяє вона віддалене виконання коду, підвищення привілеїв, витік даних); експозиції системи (чи доступна вразлива система з інтернету, чи лише з внутрішньої мережі); критичності системи для роботи медичного закладу; наявності публічних експлойтів (чи активно експлуатується вразливість у реальних атаках). На основі цієї пріоритизації система автоматично генерує plan remediation – план усунення вразливостей, де найкритичніші позначаються для негайного виправлення, менш критичні – для планового оновлення під час наступного вікна обслуговування. Для некритичних систем оновлення можуть встановлюватися автоматично після тестування на спеціальному стенді, тоді як для критичних систем (сервери з ePHI, медичне обладнання) генеруються детальні інструкції для ручного встановлення оновлень з мінімальним ризиком порушення роботи.

Захист від DDoS-атак для публічних онлайн-сервісів медичної галузі повинен поєднувати локальні засоби захисту з хмарними сервісами mitigation. Локальні засоби (спеціалізовані апаратні пристрої або програмні рішення на периметрі мережі) ефективні проти невеликих та середніх атак, але масовані DDoS-атаки сучасності, що можуть досягати сотень гігабіт трафіку на секунду, здатні перевантажити навіть потужні локальні системи захисту. Тому для захисту найкритичніших сервісів – порталів ЕСОЗ, систем онлайн-запису до лікарів, телемедичних платформ – необхідно використовувати хмарні сервіси захисту від DDoS провідних міжнародних провайдерів (Cloudflare, Akamai, AWS Shield). Ці сервіси мають величезні розподілені потужності по всьому світу і можуть поглинати навіть найпотужніші атаки, фільтруючи шкідливий трафік ще до того, як він досягне інфраструктури медичного закладу. Легітимний трафік

при цьому проходить без затримок, забезпечуючи безперебійний доступ користувачів до сервісів. НСЗУ як оператор центральних компонентів ЕСОЗ, від яких залежить робота всієї медичної системи країни, повинна забезпечити захист від DDoS найвищого рівня, здатний протистояти атакам державного масштабу потужністю понад 100 Gbps. Це вимагає комбінації найкращих хмарних сервісів mitigation, резервування через географічно розподілені дата-центри та можливості швидкого перемикання трафіку у разі атаки на один з центрів.

Захист електронної пошти залишається критично важливим напрямом, оскільки email продовжує бути найпоширенішим вектором початкового проникнення у корпоративні мережі. Сучасні системи захисту електронної пошти мають виходити далеко за межі традиційних антиспам-фільтрів.

Advanced email filtering з використанням машинного навчання дозволяє виявляти складні фішингові атаки, включаючи targeted spear phishing, що імітують листи від довірених відправників та містять персоналізовану інформацію про адресата. Система аналізує не лише текст та вкладення, а й metadata листа, історію комунікацій користувача, поведінкові патерни для виявлення аномалій.

Sandbox для вкладень – технологія автоматичного відкриття всіх вкладень у ізольованому віртуальному середовищі перед доставкою користувачу. Якщо вкладення демонструє зловмисну поведінку у sandbox (намагається завантажити додаткові файли з інтернету, шифрує файли, встановлює backdoor), воно блокується і не доставляється користувачу.

URL rewriting – технологія автоматичної заміни всіх посилань у вхідних листах на захищені посилання через проксі-сервіс. Коли користувач клікає на посилання, спочатку воно перевіряється системою безпеки у реальному часі (чи не веде воно на фішинговий сайт, чи не містить malware), і лише якщо перевірка пройшла успішно, користувач перенаправляється на цільовий сайт.

Для медичної галузі доцільно впровадити централізований захист електронної пошти на рівні галузевого або регіональних центрів. Замість того, щоб кожен медичний заклад окремо купував та налаштовував систему захисту

email, всі заклади регіону можуть використовувати єдину централізовану платформу. Це забезпечує економію коштів через bulk licensing, єдиний високий рівень захисту для всіх, централізоване управління політиками безпеки та можливість швидко поширювати інформацію про нові типи фішингових атак, виявлені в одному закладі, на всі інші заклади регіону.

Найдосконаліші технічні рішення та найкраще організовані структури управління виявляться неефективними без кваліфікованих людських ресурсів та культури безпеки, що пронизує всі рівні медичної системи. Статистика незмінно демонструє, що людський фактор залишається як найбільшою вразливістю (до 70-90% успішних атак використовують помилки або недостатню обізнаність персоналу), так і найпотужнішим ресурсом захисту (пильний та навчений персонал може виявити та зупинити атаку на ранніх стадіях).

Хронічний дефіцит кваліфікованих фахівців з кібербезпеки у медичній сфері не може бути вирішений виключно підвищенням зарплат та переманюванням спеціалістів з інших галузей. Необхідна системна довгострокова програма підготовки кадрів, що враховує унікальну специфіку медичної галузі та формує покоління фахівців, які володіють як глибокими технічними компетенціями у кібербезпеці, так і розумінням медичних процесів, етичних аспектів роботи з даними пацієнтів, регуляторних вимог медичної сфери.

Спеціалізовані освітні програми мають стати фундаментом довгострокового вирішення кадрової проблеми. Доцільно ініціювати створення спеціалізованих магістерських програм «Кібербезпека в охороні здоров'я» або «Медична інформаційна безпека» у провідних медичних та технічних університетах країни. Оптимальна модель передбачає співпрацю медичного та технічного університету у одному місті, що дозволяє поєднати їхню експертизу.

Навчальна програма має бути збалансованою та включати кілька блоків дисциплін. Технічний блок охоплює фундаментальні компетенції кібербезпеки – мережеву безпеку та архітектуру захищених мереж, криптографію та технології шифрування, цифрову форензику та розслідування кіберінцидентів, етичний

хакінг та пентестинг, аналіз аналіз шкідливого програмного забезпечення та техніки реверс-інжинірингу.

Медично-технологічний блок фокусується на специфіці медичної інформатики – архітектурі медичних інформаційних систем та їхніх вразливостях, стандартах обміну медичними даними (HL7, FHIR, DICOM), безпеці медичного обладнання з комп'ютерними компонентами (IoMT), специфіці телемедицини та мобільних медичних додатків, технологіях Big Data та штучного інтелекту у медицині з точки зору безпеки [11].

Регуляторно-правовий блок включає законодавство України про захист персональних даних та інформаційну безпеку, міжнародні стандарти та регуляції (GDPR, HIPAA, ISO 27799), етичні аспекти роботи з медичною інформацією, юридичну відповідальність за витоки даних та порушення безпеки [44].

Управлінський блок розвиває компетенції з управління ризиками інформаційної безпеки, організації реагування на кіберінциденти та бізнес-континуїті, комунікації з нетехнічними стейкхолдерами (медичне керівництво, пацієнти, регулятори), управління командами та проєктами у сфері кібербезпеки.

Критично важливим елементом програми є практична складова – обов'язкові практики та стажування у реальних медичних закладах, у галузевому центрі кібербезпеки, участь у реальних проєктах з аудиту безпеки, реагування на інциденти, впровадження систем захисту. Випускники таких програм будуть мати унікальну комбінацію компетенцій, що робить їх природними кандидатами на позиції у галузевому та регіональних центрах кібербезпеки, у великих медичних закладах, у компаніях-розробниках медичних інформаційних систем.

Програми перепідготовки та професійного розвитку дозволяють швидше заповнити кадровий дефіцит, перенавчивши фахівців суміжних спеціальностей. Цільовими аудиторіями для таких програм є: IT-фахівці з медичних закладів, що вже мають практичний досвід роботи з медичними системами та розуміють специфіку галузі, але потребують поглиблених знань саме з кібербезпеки; фахівці з кібербезпеки з інших галузей (фінанси, телеком, державний сектор), що мають глибокі технічні компетенції, але потребують навчання специфіці

медичної сфери; медичні працівники з технічною освітою (медична інформатика, біомедична інженерія), зацікавлені у кар'єрному переході до IT-безпеки.

Програми перепідготовки мають бути інтенсивними (від 3 до 6 місяців залежно від базової підготовки слухачів), максимально практико-орієнтованими з великою кількістю лабораторних робіт, кейс-стаді, симуляцій. Важливою є можливість навчання без повного відриву від роботи – вечірні програми, онлайн-формати з періодичними очними сесіями, модульна структура з можливістю поетапного проходження.

Фінансування програм перепідготовки може здійснюватися через різні канали: державні програми професійного розвитку та перекваліфікації; міжнародну технічну допомогу (багато донорів підтримують ініціативи з розвитку цифрових компетенцій); корпоративні програми навчання великих медичних закладів, що інвестують у розвиток власного персоналу; індивідуальне навчання за кошти слухачів з можливістю розстрочки або освітніх кредитів.

Система галузевої сертифікації фахівців з кібербезпеки в охороні здоров'я має встановлювати єдині стандарти компетенції та забезпечувати визнання кваліфікації. Галузевий центр кібербезпеки може виступити розробником та оператором такої системи сертифікації, можливо у партнерстві з професійними асоціаціями та університетами.

Сертифікація може мати кілька рівнів складності: базовий рівень (Healthcare Security Associate) – для IT-персоналу медичних закладів, що відповідає за базові функції безпеки; професійний рівень (Healthcare Security Professional) – для фахівців регіональних центрів компетенції, відповідальних за безпеку у великих медичних закладах; експертний рівень (Healthcare Security Expert) – для персоналу галузевого центру, консультантів, архітекторів безпеки для медичної галузі.

Сертифікація повинна включати як теоретичний іспит, що перевіряє знання стандартів, технологій, процедур, так і практичну частину – розв'язання реальних кейсів, симуляцію реагування на інцидент, аудит безпеки тестового

середовища. Сертифікат має обмежений термін дії (наприклад, 3 роки) з обов'язковим проходженням ресертифікації, що включає підтвердження професійного розвитку (участь у тренінгах, конференціях) та актуальності знань.

Механізми утримання кадрів мають виходити за межі простого підвищення зарплат, хоча конкурентна компенсація безумовно важлива. Комплексна стратегія утримання має включати: можливості постійного професійного розвитку – регулярні тренінги за рахунок роботодавця, оплата участі у профільних конференціях, підтримка отримання міжнародних сертифікацій (CISSP, CISM, CEH та інших), що підвищують ринкову вартість фахівця; цікаву та змістовну роботу – робота у кібербезпеці медичної галузі в умовах реальних активних загроз надає унікальний практичний досвід, недоступний у багатьох інших галузях; соціальну місію та значущість – усвідомлення, що твоя робота безпосередньо захищає здоров'я та життя тисяч людей, є потужним нематеріальним мотиватором для багатьох фахівців; гнучкі умови праці – можливість частково віддаленої роботи, гнучкий графік, що особливо цінується IT-фахівцями; кар'єрне зростання – чітко визначені кар'єрні траєкторії від junior до senior позицій, можливості горизонтального росту (поглиблення експертизи у вузькій галузі) та вертикального (перехід до управлінських позицій).

Навіть якщо вдасться підготувати достатню кількість висококваліфікованих фахівців з кібербезпеки, це вирішить лише частину проблеми. Більшість кіберінцидентів відбувається не через недоліки технічного захисту, а через дії або бездіяльність звичайного персоналу – лікарів, медсестер, адміністраторів. Тому систематична робота з підвищення обізнаності та формування культури безпеки на всіх рівнях медичної організації є не менш важливою, ніж технічні заходи.

Багаторівнева диференційована програма навчання має враховувати різні ролі, рівні технічної грамотності та специфічні потреби різних категорій персоналу. Базовий рівень навчання для всього персоналу без винятку (лікарі, медсестри, реєстратори, адміністратори, технічний персонал) включає короткий

онлайн-курс тривалістю 2-3 години з інтерактивними елементами, обов'язковий при прийомі на роботу та з щорічним оновленням.

Цей базовий курс має охоплювати фундаментальні теми: основи інформаційної гігієни – як створювати надійні паролі, чому не можна їх записувати на стікерах або ділитися з колегами, важливість блокування комп'ютера при відході від робочого місця; розпізнавання фішингу – практичні вправи на виявлення ознак фішингових email (підозрілі адреси відправників, орфографічні помилки, створення штучного відчуття терміновості, запити конфіденційної інформації), підозрілих посилань та вкладень; конфіденційність медичних даних – що дозволено і заборонено робити з інформацією пацієнтів, кому і за яких умов можна надавати доступ, відповідальність за несанкціоноване розголошення; безпечне використання особистих пристроїв – чому небезпечно читати робочу пошту на особистому смартфоні без захисту, ризики використання публічних WiFi-мереж; процедури звітування – до кого і як швидко звертатися при виявленні підозрілого email, втраті носія інформації, будь-якій іншій підозрілій ситуації.

Розширений рівень навчання призначений для персоналу з підвищеними привілеями доступу – завідувачів відділень, старших медсестер, адміністраторів реєстратур, керівників структурних підрозділів. Ці категорії мають більший доступ до конфіденційної інформації та можливість надавати доступ іншим, тому потребують поглибленого навчання.

Розширений курс включає: управління доступом – відповідальність за надання та своєчасне відкликання прав доступу підлеглим при звільненні або зміні посади, принцип мінімальних необхідних привілеїв; соціальну інженерію у глибокому розумінні – як розпізнати спроби маніпуляції не лише через email, а й через телефонні дзвінки (vishing), особисті контакти, використання поведінкових тригерів (апеляція до авторитету, страх покарання, бажання допомогти); інсайдерські загрози – як виявити ознаки потенційно небезпечної поведінки колег (незвичайний інтерес до систем, до яких немає робочої необхідності, копіювання великих обсягів даних, робота в незвичайний час), як діяти у таких

ситуаціях; безпечну роботу з зовнішніми підрядниками – процедури надання тимчасового доступу третім особам, необхідність супроводу та контролю їхніх дій.

Спеціалізований рівень для керівництва медичних закладів (директори, заступники, головні лікарі) має фокусуватися не на технічних деталях, а на стратегічних та управлінських аспектах: розуміння ландшафту загроз – які основні типи кібератак загрожують медичним закладам, які можуть бути наслідки успішної атаки (фінансові, репутаційні, юридичні, загроза життю пацієнтів); управління ризиками – як оцінювати кіберризики у контексті інших ризиків організації, як приймати обґрунтовані рішення про інвестиції у безпеку; юридична та персональна відповідальність – які санкції передбачені законодавством за витоки даних, порушення вимог кібербезпеки, чи може керівник нести персональну відповідальність; кризові комунікації – як правильно комунікувати з персоналом, пацієнтами, ЗМІ, регуляторами у разі кіберінциденту; безперервність роботи – як забезпечити продовження надання медичної допомоги під час або після кіберінциденту, коли інформаційні системи частково або повністю недоступні.

Симуляції фішингових атак визнані найефективнішим методом практичного навчання розпізнаванню загроз. Галузевий або регіональні центри можуть надавати сервіс симуляцій як централізовану послугу для всіх медичних закладів. Регулярно (наприклад, щомісяця) персоналу надсилаються тестові фішингові листи різного рівня складності – від очевидних з множинними помилками до складних targeted spear phishing, що імітують листи від реальних відправників з персоналізованою інформацією.

Співробітники, що «потрапляють у пастку фішинга « на тесті (клікають на посилання або відкривають вкладення), замість доступу до шкідливого контенту отримують короткий навчальний модуль на 5-10 хвилин, що пояснює, на які саме ознаки треба було звернути увагу, чому цей лист є підозрілим, як правильно діяти у подібних ситуаціях. Такий just-in-time learning – навчання в момент помилки – є надзвичайно ефективним, оскільки людина емоційно залучена і

максимально мотивована зрозуміти, де саме вона помилилася.

Детальна статистика результатів симуляцій (хто і коли потрапився, на які типи фішингу, як змінюються результати з часом) дозволяє виявляти найбільш вразливих користувачів для надання їм персоналізованого додаткового навчання, підрозділи з низьким рівнем обізнаності для проведення цільових тренінгів, найбільш ефективні типи фішингу для розробки спеціалізованих навчальних модулів. Важливо також відстежувати позитивну динаміку – якщо phishing click rate (відсоток користувачів, що клікають на фішинг) знижується з часом, це свідчить про ефективність програми навчання.

Геймифікація процесу навчання може драматично підвищити залученість персоналу та зробити навчання з кібербезпеки не нудним обов'язком, а цікавим досвідом. Традиційні презентації та тести викликають опір та швидко забуваються. Натомість інтерактивні сценарії, квести, змагання між відділеннями створюють позитивні емоції та краще запам'ятовування матеріалу.

Приклади геймифікованих форматів включають: escape room з кібербезпеки – команда має «втекти» з віртуальної кімнати, розв'язуючи загадки та завдання про інформаційну безпеку; інтерактивні сценарії з розгалуженим сюжетом – користувач приймає рішення у різних ситуаціях (чи відкрити підозрілий email, чи надати доступ незнайомцю), і бачить наслідки своїх рішень; симулятори інцидентів – відтворення реального кіберінциденту, де учасники грають різні ролі (IT-адміністратор, керівник, офіцер зв'язків з громадськістю) та відпрацьовують взаємодію; змагання між відділеннями – який відділ покаже найкращі результати у симуляціях фішингу, тестах з безпеки, дотриманні політик, отримує визнання та символічні призи.

Security Champions Program – програма формування «чемпіонів безпеки» у кожному структурному підрозділі медичного закладу. Це не обов'язково IT-фахівці, а ентузіасти з числа медичного персоналу, які цікавляться питаннями кібербезпеки, готові витратити додатковий час на навчання та стати неформальними лідерами у своїх підрозділах. Чемпіони проходять поглиблене навчання, регулярно отримують інформацію про нові загрози від відділу

безпеки, а потім неформально поширюють знання серед колег – нагадують про правила, допомагають з питаннями, заохочують правильну поведінку.

Культурна трансформація на рівні всієї організації вимагає не лише навчання рядового персоналу, а й активної підтримки та особистого прикладу з боку керівництва. Культура безпеки не може бути нав'язана згори наказами – вона формується через цінності, поведінкові норми, що демонструються лідерами організації. Якщо директор медичного закладу систематично порушує політики безпеки (просить ІТ-відділ «зробити виняток для нього», записує паролі на стікерах, грубо поводиться з персоналом, що звітує про інциденти), це транслює сигнал всій організації, що безпека насправді не є пріоритетом. Навпаки, коли керівництво публічно підтримує ініціативи з безпеки, регулярно включає питання кібербезпеки до порядку денного нарад, виділяє адекватний бюджет, визнає та нагороджує співробітників за правильну поведінку, це формує organizational culture де безпека сприймається як спільна відповідальність кожного, а не як обов'язок виключно ІТ-відділу.

Інтеграція безпеки у повсякденні робочі процеси має зробити безпечну поведінку природною, зручною та неподільною від основної роботи. Якщо вимоги безпеки створюють значні незручності та заважають медичному персоналу виконувати їхні прямі обов'язки, люди природно шукатимуть способи обійти ці вимоги. Тому при розробці політик та процедур безпеки критично важливо враховувати реальні робочі процеси, особливо в умовах екстрених ситуацій.

Приклади user-friendly підходів до безпеки включають: Single Sign-On (SSO) – користувач один раз автентифікується зранку і автоматично має доступ до всіх необхідних систем без повторного введення паролів для кожної; passwordless authentication через біометрію (відбиток пальця, розпізнавання обличчя) або смарт-карти – взагалі усуває необхідність запам'ятовувати та вводити паролі; context-aware access control – система автоматично адаптує рівень безпеки залежно від контексту (у звичайній ситуації вимагає стандартну автентифікацію, але у режимі надзвичайної ситуації спрощує доступ до

критичних даних з обов'язковим постфактум аудитом); автоматичне шифрування даних без додаткових дій користувача – дані шифруються прозоро у фоновому режимі.

Постійний моніторинг та вдосконалення програми обізнаності через систему числових показників та KPI (Key Performance Indicators). Ефективність програми має вимірюватися об'єктивними показниками, а не суб'єктивними враженнями. Ключові показники включають: completion rate – відсоток персоналу, що завершив обов'язкове навчання протягом визначеного терміну (ціль: 100% протягом першого місяця роботи, 95%+ для щорічного оновлення); test scores – середній бал тестів після навчання (ціль: 80%+ правильних відповідей); phishing simulation results – відсоток користувачів, що клікають на тестові фішингові посилання (початковий baseline зазвичай 20-40%, ціль після року навчання: під 10%, довгострокова ціль: під 5%); time to report – середній час від отримання підозрілого email до його звітування (ціль: зниження з годин до хвилин); incident metrics – кількість інцидентів, спричинених людським фактором (ціль: зниження на 50% протягом року).

Ці дані мають регулярно (щоквартально) аналізуватися командою, відповідальною за програму обізнаності, і програма коригуватися на основі даних. Якщо певна категорія персоналу показує стабільно гірші результати, розробляються спеціалізовані інтервенції для цієї групи. Якщо певний тип фішингу виявляється особливо ефективним, створюється додатковий навчальний модуль саме про цей тип атак. Якщо результати симуляцій погіршуються після тривалого періоду без навчання, це сигналізує про необхідність частіших refresher trainings.

Мотивація та заохочення правильної поведінки доповнює навчання та контроль позитивним підкріпленням. Програма recognition and rewards визнає та нагороджує співробітників за внесок у безпеку організації. Наприклад, «Працівник місяця з кібербезпеки» – співробітник, що виявив та повідомив про реальний фішинг або іншу загрозу, що могла призвести до серйозного інциденту, публічно визнається на загальних зборах та отримує символічну нагороду

(сертифікат, невелика премія, додатковий день відпустки).

Колективні нагороди для підрозділів, що демонструють найкращі результати, створюють здорову конкуренцію та командний дух. Відділ з найнижчим phishing click rate протягом кварталу, найвищим completion rate обов'язкового навчання, найкращим дотриманням політик безпеки може отримати корпоративний захід, визнання керівництва, символічний трофей, що переходить від переможця до переможця.

Важливо, що recognition має бути публічним та своєчасним – нагородження через кілька місяців після події втрачає свій мотиваційний ефект. Швидке визнання правильної поведінки (виявлення загрози, звітування про інцидент) підкріплює бажану поведінку та заохочує інших діяти аналогічно.

Комплексна реалізація всіх трьох стратегічних напрямів – організаційно-інституційного розвитку через створення галузевих та регіональних центрів компетенції, технологічної модернізації через впровадження сучасних архітектурних рішень та засобів захисту, розвитку людського капіталу через системну підготовку фахівців та формування культури безпеки – створює синергетичний ефект, де кожен елемент посилює та підтримує інші. Лише такий цілісний системний підхід здатний забезпечити фундаментальне підвищення стійкості медичної інфраструктури України до інформаційних операцій та кіберзагроз в умовах тривалого гібридного протистояння.

На основі виявлених теоретико-методологічних засад та критичного аналізу існуючої ситуації сформульовані три взаємопов'язані стратегічні напрями вдосконалення системи протидії інформаційним операціям у медичній сфері, що мають комплексний та системний характер.

Організаційно-інституційний розвиток передбачає створення дворівневої структури управління кібербезпекою. На національному рівні необхідне створення галузевого центру кібербезпеки охорони здоров'я як спеціалізованого органу з повноваженнями моніторингу загроз, координації реагування на інциденти, розробки галузевих стандартів, проведення аудитів та сертифікації, навчання персоналу та міжнародної співпраці. На регіональному рівні доцільно

розвивати мережу центрів компетенції на базі опорних медичних закладів для забезпечення наближеної підтримки та впровадження моделі shared services.

Удосконалення нормативно-правової бази має включати розробку галузевих стандартів кібербезпеки для медичної сфери з урахуванням специфіки балансу між безпекою та доступністю даних, регламенту реагування на кіберінциденти з чітким розподілом відповідальності між органами, ефективних механізмів адміністративної та кримінальної відповідальності, гармонізації з європейським законодавством через імплементацію NIS2 та окремих положень GDPR.

Технологічна модернізація має здійснюватися через прагматичну стратегію пріоритизації найкритичніших систем протягом 5-7 років. Інвентаризація та категоризація активів за рівнем ризику дозволяє сфокусувати обмежені ресурси на системах, що одночасно обробляють критичні дані, використовують застаріле ПЗ, мають мережеве підключення та є критичними для надання допомоги. Програма поетапної модернізації має чіткі проміжні цілі та різноманітні джерела фінансування.

Впровадження сучасних архітектурних рішень включає концепцію zero trust з відмовою від моделі периметру безпеки, XDR-платформи для інтегрованого виявлення загроз через централізовані центри, автоматизоване управління вразливостями, захист від DDoS промислового рівня для критичних сервісів, advanced email filtering для протидії фішингу як найпоширенішому вектору атак.

Розвиток людського капіталу є найбільш критичним напрямом, оскільки людський фактор залишається як найбільшою вразливістю, так і найпотужнішим потенційним ресурсом захисту. Системна програма підготовки кадрів має включати спеціалізовані магістерські програми «Кібербезпека в охороні здоров'я», програми перепідготовки фахівців суміжних спеціальностей, систему галузевої сертифікації та комплексні механізми утримання кадрів через професійний розвиток, цікаву роботу, соціальну місію та гнучкі умови праці.

Формування культури безпеки вимагає багаторівневої диференційованої

програми навчання для різних категорій персоналу, симуляцій фішингових атак як найефективнішого методу практичного навчання, геймифікації для підвищення залученості, активної підтримки та особистого прикладу керівництва, інтеграції безпеки у повсякденні процеси для забезпечення зручності, постійного моніторингу ефективності через об'єктивні метрики та систему recognition and rewards для мотивації правильної поведінки.

Запропоновані рекомендації мають прикладний характер та можуть бути впроваджені поетапно з урахуванням обмежених ресурсів. Пріоритетними першими кроками є створення базової команди галузевого центру протягом 6-12 місяців, запуск пілотних проєктів у 2-3 регіонах, розробка проєкту галузевого стандарту, започаткування освітніх програм у провідних університетах.

Комплексна реалізація всіх трьох стратегічних напрямів створює синергетичний ефект, де організаційні структури розробляють стандарти та надають підтримку, сучасні технології автоматизують захист та спрощують дотримання політик, а кваліфіковані кадри та культура безпеки перетворюють персонал з найбільшої вразливості на найпотужніший захисний ресурс. Лише такий цілісний системний підхід здатен забезпечити фундаментальне підвищення стійкості медичної інфраструктури України до інформаційних операцій та кіберзагроз в умовах тривалого гібридного протистояння.

ВИСНОВКИ

Проведене дослідження проблеми протидії інформаційним операціям у сфері охорони здоров'я України дозволяє констатувати, що ця сфера перебуває на критичному етапі трансформації від традиційної моделі реактивного захисту до проактивної стійкої системи, здатної функціонувати в умовах перманентного гібридного протистояння.

1. Запропоновано цілісну модель багаторівневої системи кібербезпеки медичної галузі, що поєднує національний галузевий центр, регіональні центри компетенції та локальні підрозділи безпеки у медичних закладах з чіткими механізмами координації та розподілу відповідальності та сформовано методологічний внесок дослідження, який полягає у синтезі європейської регуляторної моделі (GDPR/NIS2), натовської концепції проактивної оборони («Defend Forward») та українського досвіду реагування на державні кібератаки в умовах війни. Цей синтез формує унікальну гібридну модель, адаптовану до специфіки вітчизняної медичної системи – необхідності балансу між високими стандартами захисту даних та реаліями обмежених ресурсів, між централізованою координацією та збереженням автономії регіональних закладів, між жорсткими вимогами безпеки та оперативною доступністю даних для надання невідкладної допомоги.

2. За допомогою емпіричний аналізу виявлено парадоксальну ситуацію: попри накопичення значного практичного досвіду протидії масштабним атакам та створення базових організаційних структур, система залишається фрагментованою та вразливою через відсутність системної інтеграції окремих елементів. Технічні засоби захисту існують, але не координуються; нормативна база розвивається, але не адаптована до медичної специфіки; фахівці працюють, але їх критично бракує і вони діють ізольовано; персонал навчається, але культура безпеки не формується системно. Запропоновано підходи до системної трансформації, що охоплює одночасно

організаційний, технологічний та людський виміри. Створення галузевого центру без модернізації застарілої інфраструктури буде неефективним. Впровадження сучасних технологій без підготовки кваліфікованих кадрів для їхньої експлуатації не дасть результату. Навчання персоналу без зміни організаційної культури та підтримки керівництва не змінить поведінку. Лише синергетична взаємодія всіх трьох напрямів може забезпечити якісний прорив.

3. Розроблено деталі конкретного плану дій з чіткою пріоритизацією, етапністю впровадження та оцінкою необхідних ресурсів. На відміну від абстрактних рекомендацій «необхідно покращити», «слід посилити», запропоновані заходи мають конкретні параметри – розмір команди галузевого центру (20-30 осіб), орієнтовний бюджет (50-100 млн грн на перший рік), термін реалізації пілотного проєкту (12-18 місяців), метрики успішності (зниження phishing click rate до 5%, completion rate навчання 95%+, зниження інцидентів людського фактору на 50%). Приділено особлива увага дослідженні проблемі людського фактору як найбільшої вразливості системи. Статистика демонструє, що 70-90% успішних атак використовують помилки персоналу, і жодні технічні засоби не можуть це компенсувати.

4. Запропонована багаторівнева програма формування культури безпеки виходить за межі традиційного навчання, інтегруючи симуляції, геймифікацію, систему мотивації та, критично важливо, підтримку керівництва та інтеграцію безпеки у повсякденні процеси. Безпека має стати не обтяжливим обов'язком, а природною частиною професійної діяльності медичного працівника. Сформульоване стратегічне бачення, яке передбачає поетапну трансформацію протягом 5-7 років від фрагментованої системи із значною нерівністю рівня захисту до інтегрованої мережевої моделі з високим baseline рівнем безпеки у всіх медичних закладах незалежно від їхнього розміру та розташування. Це амбітна, але досяжна мета за умови політичної волі, адекватного фінансування та послідовного впровадження запропонованих заходів.

Дослідження також виявило важливу тенденцію зміщення акцентів від

виключно технічного кіберзахисту до комплексної протидії інформаційним операціям, що включає дезінформацію, маніпуляції у соціальних мережах, психологічний вплив. Якщо технічна кібербезпека в Україні поступово розвивається і досягла певного рівня зрілості, то протидія інформаційним операціям залишається значно менш розвиненою. Це створює асиметричну вразливість – противник може досягати стратегічних цілей дестабілізації та підриву довіри до медичної системи навіть без технічних кібератак, виключно через інформаційні маніпуляції. Подальші дослідження мають бути спрямовані на деталізацію окремих аспектів запропонованої системи – розробку конкретних галузевих стандартів кібербезпеки з технічними специфікаціями, методик оцінювання рівня зрілості кібербезпеки медичних закладів, програм навчання з детальними навчальними планами, економічних моделей фінансування модернізації. Також перспективним є дослідження міжнародного досвіду інших країн, що стикалися з масштабними кібератаками на медичну інфраструктуру, для екстракції lessons learned та адаптації успішних практик.

Загальний висновок. Український досвід протидії інформаційним операціям у медичній сфері в умовах повномасштабної війни є унікальним і цінним для міжнародної спільноти. Жодна інша країна не стикалася з такою інтенсивністю та різноманітністю гібридних загроз при необхідності одночасно підтримувати функціонування медичної системи для цивільного населення та військово-медичне забезпечення. Систематизація та поширення цього досвіду може стати вкладом України у глобальну систему кібербезпеки охорони здоров'я та основою для міжнародної співпраці у цій сфері

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020. 1232 p.

2. CISA Healthcare and Public Health Sector. URL: https://www.cisa.gov/healthcare-and-public-health-sector (last accessed: 03.12.2025).

3. Coventry L., Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. 2018. Vol. 113. P. 48-52. DOI: 10.1016/j.maturitas.2018.04.008.

4. Cyber Attacks on Healthcare Sector During COVID-19 Pandemic. Interpol, 2021. URL: https://www.interpol.int (last accessed: 03.12.2025).

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (last accessed: 03.12.2025).

6. ENISA Threat Landscape for the Healthcare Sector. European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-the-healthcare-sector (last accessed: 03.12.2025).

7. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu (last accessed: 03.12.2025).

8. Healthcare Cybersecurity Report: Recent Attacks and Lessons Learned. Health-ISAC, 2023. URL: https://h-isac.org (last accessed: 03.12.2025).

9. Healthcare Information Sharing and Analysis Center (Health-ISAC). URL: https://h-isac.org (last accessed: 03.12.2025).

10. IBM Security X-Force Threat Intelligence Index 2024. IBM Corporation, 2024. URL: https://www.ibm.com/security/data-breach/threat-intelligence (last accessed: 03.12.2025).

11. ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002. Geneva: ISO, 2016.

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022.

13. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: ISO, 2022.

14. Jalali M. S., Kaiser J. P. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*. 2018. Vol. 20(5). e10059. DOI: 10.2196/10059.

15. Kruse C. S., Frederick B., Jacobson T., Monticone D. K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*. 2017. Vol. 25(1). P. 1-10. DOI: 10.3233/THC-161263

16. Luna R., Rhine E., Myhra M., Sullivan R., Kruse C. S. Cyber threats to health information systems: A systematic review. *Technology and Health Care*. 2016. Vol. 24(1). P. 1-9. DOI: 10.3233/THC-151102

17. Martins N., Marques de Sá J. Healthcare cybersecurity: a systematic mapping. *Journal of Medical Systems*. 2023. Vol. 47. Article 36. DOI: 10.1007/s10916-023-01932-4.

18. NIST Cybersecurity Framework Version 1.1. National Institute of Standards and Technology, 2018. URL: https://www.nist.gov/cyberframework (last accessed: 03.12.2025).

19. NIST Special Publication 800-66 Rev. 2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. NIST, 2023. URL: https://csrc.nist.gov/publications/detail/sp/800-66/rev-2/final (last accessed: 03.12.2025).

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (last accessed: 03.12.2025).

21. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Company, 2018. 288 p.

22. The State of Ransomware in Healthcare 2023. Sophos, 2023. URL: https://www.sophos.com/en-us/content/state-of-ransomware (last accessed: 03.12.2025).

23. Verizon 2024 Data Breach Investigations Report. Verizon, 2024. URL: https://www.verizon.com/business/resources/reports/dbir (last accessed: 03.12.2025).

24. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2021. 784 p.

25. WHO Global Strategy on Digital Health 2020-2025. World Health Organization, 2021. URL: https://www.who.int/publications/i/item/9789240020924 (last accessed: 03.12.2025).

26. Williams P. A., Woodward A. J. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*. 2015. Vol. 8. P. 305-316. DOI: 10.2147/MDER.S50048

27. Бакуменко В. Д., Безносенко Д. О. Державне управління в умовах кризових ситуацій: навч. посіб. Київ: НАДУ, 2011. 252 с.

28. Васюк Н. О. Запровадження електронної системи охорони здоров'я (e-health) як важливий напрям трансформації медичної галузі. *Державне управління: удосконалення та розвиток*. 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2609 (дата звернення: 03.12.2025).

29. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.

30. Електронна система охорони здоров'я. URL: https://ehealth.gov.ua (дата звернення: 03.12.2025).

31. Звіти CERT-UA. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cert.gov.ua (дата звернення: 03.12.2025).

32. Конах В. К. Механізми публічного управління охороною здоров'я на регіональному рівні: монографія. Запоріжжя: КПУ, 2018. 464 с.

33. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/

254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 03.12.2025).

34. Ліпкан В. А. Національна безпека України: навч. посіб. Київ: КНТ, 2009. 576 с.

35. Основи кібербезпеки, кіберзахисту та кібергігієни. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/news/osnovi-kiberbezpeki-2 (дата звернення: 03.12.2025).

36. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua (дата звернення: 03.12.2025).

37. Офіційний веб-сайт Міністерства охорони здоров'я України. URL: https://moz.gov.ua (дата звернення: 03.12.2025).

38. Офіційний веб-сайт Національної служби здоров'я України. URL: https://nszu.gov.ua (дата звернення: 03.12.2025).

39. Офіційний портал НАТО з кібербезпеки. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 03.12.2025).

40. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2021 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2021-%D0%BF (дата звернення: 03.12.2025).

41. Про затвердження Положення про організаційно-технічну модель кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 17 листопада 2022 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2022-%D0%BF (дата звернення: 03.12.2025).

42. Про затвердження Порядку повідомлення про кіберінциденти: Постанова Кабінету Міністрів України від 16 березня 2022 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2022-%D0%BF (дата звернення: 03.12.2025).

43. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 03.12.2025).

44. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII.

URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 03.12.2025).

45. Про критичну інфраструктуру: Закон України від 16 листопада 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 03.12.2025).

46. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 03.12.2025).

47. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.12.2025).

48. Солоненко І. М. Державне управління у сфері охорони здоров'я в Україні: генезис і перспективи розвитку: монографія. Київ: НАДУ, 2013. 404 с.

49. Стратегія кібербезпеки України: затв. Указом Президента України від 14 вересня 2023 р. № 573/2023. URL: https://www.president.gov.ua/documents/5732023-46973 (дата звернення: 03.12.2025).

50. Центр стратегічних комунікацій та інформаційної безпеки. URL: https://spravdi.gov.ua (дата звернення: 03.12.2025).

51. Шаблони для впровадження кіберстандартів у медичних закладах. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/shabloni-dlja-vprovadzhennja-kiberstandartiv-u-medichnih-zakladah (дата звернення: 03.12.2025).