УДК 351.77

А. О. Ляшук,
аспірант кафедри управління охороною здоров'я та публічного адміністрування,
Національний університет охорони здоров'я України імені П.Л. Шупика
ORCID ID: https://orcid.org/0000-0002-4206-3929
С. П. Кошова,
к. держ. упр., доцент, доцент кафедри управління
охороною здоров'я та публічного адміністрування,
Національний університет охорони здоров'я України імені П.Л. Шупика
ORCID ID: https://orcid.org/0000-0002-7637-4311

DOI: 10.32702/2306-6814.2023.6.194

ВДОСКОНАЛЕННЯ ДЕРЖАВНОГО МЕХАНІЗМУ КІБЕРБЕЗПЕКИ, МОНІТОРИНГУ, ЗАХИСТУ ТА АНАЛІЗУ МОЖЛИВИХ ВТРУЧАНЬ, ВТРАТ, ПОШКОДЖЕНЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА РЕЄСТРІВ СФЕРИ ОХОРОНИ ЗДОРОВ'Я

A. Liashuk,
Postgraduate student of the Department of Healthcare Management and Public Administration,
Shupyk National Healthcare University of UkraineKyiv, Ukraine
S. Koshova,
PhD in Public Administration, Associate Professor, Associate Professor of the Department of Healthcare Management and Public Administration, Shupyk National Healthcare University of Ukraine Kyiv, Ukraine

IMPROVEMENT OF THE STATE MECHANISM OF CYBERSECURITY, MONITORING, PROTECTION AND ANALYSIS OF POSSIBLE INTERVENTIONS, LOSSES, DAMAGES OF INFORMATION AND COMMUNICATION SYSTEMS AND REGISTERS OF THE HEALTHCARE SECTOR

Стаття присвячена удосконаленню державного механізму захисту електронної системи охорони здоров'я та її основних компонентів від кібератак. Актуальність дослідження обумовлена збільшенням кількості інформаційно-комунікаційних систем та медичних реєстрів, формуванням значних об'ємів медичних даних, які потребують захисту від можливих втручань, втрат та пошкоджень.

Мета статті — розроблення заходів з удосконалення державного механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів. Для досягнення мети в ході дослідження вирішено ряд завдань: визначено поняття електронної системи охорони здоров'я і її основних компонентів — інформаційно-комунікаційних систем та реєстрів, проаналізовано міжнародний досвід та висвітле-

но діяльність нашої держави щодо забезпечення кіберзахисту в сфері охорони здоров'я, визначено основні виклики, з якими зіткнулась зазначена сфера, та запропоновано шляхи їх вирішення. В ході дослідження використані загальнонаукові методи пізнання: метод критичного аналізу, синтезу, індукції та дедукції.

В умовах війни існує підвищена загроза кібератак зі сторони Російської Федерації, тому дотримання вимог безпеки є основним завданням електронної системи охорони здоров'я України. Разом з тим, медичні установи не в змозі самостійно впоратися з кібератаками, які постійно еволюціонують і несуть значні ризики для постачальників медичних послуг та їх пацієнтів. Саме тому вдосконалення механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів є пріоритетним напрямом діяльності держави в сфері охорони здоров'я.

За результатами дослідження встановлено, що інформаційно-комунікаційні системи та медичні реєстри eHealth надійно захищені від можливих втручань, втрат та пошкоджень. Однак у зв'язку з рядом невирішених проблем, медична галузь залишається основною мішенню для кіберзлочинців. До таких проблем необхідно віднести: відсутність кваліфікованого IT персоналу в медичних організаціях, нові виклики перед IT-спеціалістами у зв'язку з пандемією коронавірусу та війною в Україні, застарілу IT-інфраструктуру медичних закладів, невпорядкованість інформаційно-комунікаційних систем та реєстрів, вразливість хмарних технологій. Вирішення зазначених проблем потребує здійснення наступних заходів: удосконалення кримінального законодавства, прийняття локальних нормативних актів з правилами "цифрової гігієни", обмеження доступу до електронної системи охорони здоров'я, створення цілісної, стандартизованої та уніфікованої системи реєстрів, модернізація IT-інфраструктури медичних закладів, заходи інформаційно-освітнього характеру з медичним персоналом, розробка посібників з кібербезпеки. Практичне значення дослідження полягає в можливості використання отриманих результатів державними органами в процесі розроблення системи захисту медичних інформаційних систем та реєстрів від кібератак в галузі охорони здоров'я.

The article is devoted to the improvement of the state mechanism for protecting the electronic healthcare system and its main components from cyberattacks. The relevance of the study is due to the increase in the number of information and communication systems and medical registers, the formation of significant amounts of medical data that need protection from possible interference, loss and damage.

The purpose of the article is to develop measures to improve the state mechanism of cybersecurity, monitoring, protection and analysis of possible interference, loss, damage to information and communication systems and registers. To achieve this goal, the study solved a number of tasks: defined the concept of electronic healthcare system and its main components — information and communication systems and registries, analyzed international experience and highlighted the activities of our state to ensure cybersecurity in the healthcare sector, identified the main challenges faced by this area, and proposed ways to solve them. The study used general scientific methods of cognition: the method of critical analysis, synthesis, induction and deduction.

In the conditions of war, there is an increased threat of cyberattacks from the Russian Federation, therefore compliance with security requirements is the main task of the electronic health care system of Ukraine. At the same time, healthcare institutions are unable to deal with cyberattacks on their own, which are constantly evolving and pose significant risks to healthcare providers and their patients. That is why the improvement of the mechanism of cyber security, monitoring, protection and analysis of possible interventions, losses, damages of information and communication systems and registers is a priority direction of the state's activity in the field of health care.

According to the results of the study, it was found that information and communication systems and medical registers eHealth are reliably protected from possible interference, loss and damage. However, due to a number of unresolved problems, the healthcare industry remains a major target for cybercriminals. Such problems include: lack of qualified IT personnel in medical organizations, new challenges for IT specialists due to the coronavirus pandemic and the war in Ukraine, outdated IT infrastructure of medical institutions, disorganization of information and communication systems and registers, vulnerability of cloud technologies. The solution to these problems requires the implementation of the following measures: improvement of criminal legislation, adoption of local regulations with the rules of "digital hygiene", restriction of access to the electronic healthcare

system, creation of a holistic, standardized and unified system of registers, modernization of the IT infrastructure of medical institutions, information and educational activities with medical staff, development of cybersecurity guidelines. The practical significance of the study lies in the possibility of using the results obtained by state bodies in the process of developing a system of protection of medical information systems and registers from cyberattacks in the healthcare sector.

Ключові слова: державний механізм, кібербезпека, електронна система охорони здоров'я, медичні реєстри, інформаційно-комунікаційні системи.

Key words: state mechanism, cybersecurity, electronic healthcare system, medical registers, information and communication systems.

ПОСТАНОВКА ПРОБЛЕМИ

Діджиталізація — невід'ємна складова сьогодення. Не виключенням є медична галузь, цифрова трансформація якої дозволяє здійснювати передачу медичних даних між пацієнтами і постачальниками медичних послуг та надавати медичні послуги дистанційно. Важливою частиною такої трансформації є впровадження електронної системи охорони здоров'я (eHealth), яка складається з низки інформаційно-комунікаційних систем та реєстрів у сфері охорони здоров'я. З розвитком eHealth кількість таких систем та реєстрів збільшується. Відповідно, зростає обсяг даних, які в них формуються та циркулюють. Підвищеної уваги потребує безпека даних в інформаційно-комунікаційних системах і реєстрах та їх захист від можливих кібератак.

Значне збільшення кібератак на критичну інформаційну інфраструктуру фіксується у всьому світі. Зокрема, відомо про велику кількість випадків, коли інформаційні системи організацій та установ медичного сектору атакувалися вірусами-здирниками (RoT — Ransomware of Things). Такі віруси потрапляють на комп'ютери, шифрують наявну в ньому інформацію й виводять з ладу базову інфраструктуру. Отримавши доступ до керування пристроями в системі, зловмисники вимагають викуп за відновлення її роботи. Подібний випадок трапився у 2020 році в США. Вірус-здирник атакував загальнонаціональну мережу лікарень Universal Health Services, що спричинило відмову її інформаційної системи. Відбувалися широкомасштабні відключення, затримувалися лабораторні аналізи, а пацієнти, які потребували медичної допомоги, направлялися в інші лікарні. Аналогічний випадок був зафіксований в грудні 2020 року. В результаті кібератаки віруса-здирника на мережу косметологічних клінік Transform Hospital Group у Великій Британії, зловмисники заволоділи даними на 900 Гб та погрожували опублікувати фотографії пацієнтів до та після операції. Цього ж року програми-здирники атакували сервери інших медичних установ: університетської лікарні в Нью-Джерсі, дитячої лікарні Бостона та лікарні Дюссельдорфського університету [1].

В умовах війни існує підвищена загроза кібератак зі сторони Російської Федерації, тому дотримання вимог безпеки є основним завданням електронної системи охорони здоров'я України. Разом з тим, медичні установи не в змозі самостійно впоратися з кібератаками, які постійно еволюціонують і несуть значні ризики для постачальників медичних послуг та їх пацієнтів. Саме тому вдосконалення механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів є пріоритетним напрямом діяльності держави в сфері охорони здоров'я.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання безпеки медичних даних розглядається в роботах багатьох вітчизняних та зарубіжних науковців: Seals T. [1], Москаленко Ю. [2], Черниша Д. [4], Burt T. [6], Савченко-Галушко Т. [7]. Однак недостатньо дослідженим на сьогоднішній день залишається питання вдосконалення державного механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів, які є основними складовими електронної системи охорони здоров'я.

МЕТА СТАТТІ

Мета статті — розроблення заходів з удосконалення державного механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Запровадження електронної системи охорони здоров'я (ЕСОЗ) — важливий крок в реформуванні медичної галузі. З кінця 2022 року всі без виключення заклади охорони здоров'я та фізичні особи-підприємці, які здійснюють господарську діяльність з медичної практики, зобов'язані працювати в цій системі. Станом на жовтень 2022 року, з ЕСОЗ працює понад 7 тис приватних та комунальних закладів охорони здоров'я [2].

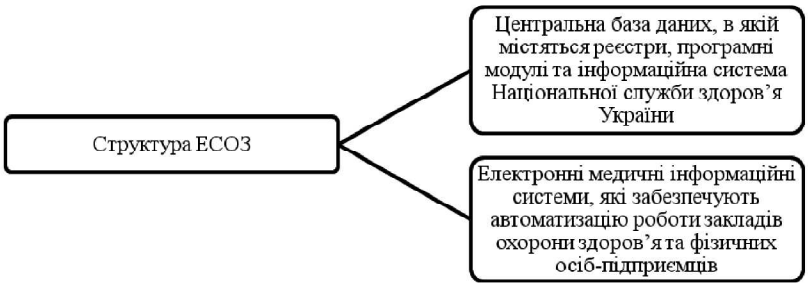

Рис. 1. Структура ЕСОЗ [3]

Примітка: систематизовано автором.

Згідно з положеннями Закону України "Основи законодавства України про охорону здоров'я", під електронною системою охорони здоров'я слід розуміти інформаційно-комунікаційну систему, яка забезпечує облік медичних послуг та управління медичними даними шляхом їх автоматизованого формування, перегляду та обміну з центральною базою даних [3]. Основні компоненти електронної системи охорони здоров'я наведені на рис. 1.

Обмін даними та документацією між центральною базою даних та медичними інформаційними системами здійснюється в автоматичному режимі.

З розвитком електронної системи охорони здоров'я збільшується кількість реєстрів та медичних інформаційних систем. Так, на сьогоднішній день нараховується більше десяти реєстрів (Реєстр пацієнтів, Реєстр декларацій, Реєстр медичних працівників, Реєстр медичних записів тощо). Варто зазначити й те, що крім державних інформаційних систем, в Україні працюють приватні системи. За допомогою таких систем приватні медичні заклади передають інформацію до центральної бази [4].

Отже, на сьогоднішній день E-health є найбільшою електронною системою в медичній галузі та в країні загалом. ЕСОЗ постійно розвивається та вдосконалюється. В ній формуються величезні масиви медичних даних, більшість з яких належать до специфічної категорії персональних даних. Такі дані повинні бути надійно захищеними та недоступними для сторонніх осіб. Разом з тим, медичні установи не в змозі самостійно впоратися з втручаннями, втратами, пошкодженнями інформаційно-комунікаційних систем та реєстрів. Саме тому пріоритетним напрямом діяльності держави в сфері охорони здоров'я має стати вдосконалення механізму кібербезпеки, моніторингу, захисту та аналізу таких втручань, втрат та пошкоджень. Перед тим, як висвітлити діяльність нашої держави щодо забезпечення кіберзахисту в сфері охорони здоров'я, проаналізуємо міжнародний досвід.

Протягом останніх років спостерігається збільшення кількості кібератак на сектор охорони здоров'я в усьому світі. З початком пандемії у квітні 2020 року число кіберпосягань на медичні організації зросло ще більше.

Зростання кількості загроз кібербезпеці системи охорони здоров'я підтверджується результатами опитування фахівців з кібербезпеки, проведеного американською неурядовою організацією Healthcare Information and Management Systems Society (HIMSS) у 2022 році. Згідно з результатами опитування, більшість організацій вже стикалися з серйозними посяганнями на інформаційно-комунікаційні системи та реєстри, скоєні шляхом віддаленого доступу. Основними способами атак був фішинг, вимагання та використання засобів соціальної інженерії (зловживання довірою чи обман з метою отримання інформації). Наслідками атак стали збої у роботі інформаційних систем постраждалих організацій та порушення у наданні медичних послуг [5].

Серед найбільш серйозних кібератак, які зазнали організації охорони здоров'я по всьому світу в останні роки, необхідно відмітити атаки хакерів-вимагачів на госпіталь у Брно (Чехія), паризьку госпітальну систему, лікарні в Іспанії та Таїланді, клініки в різних штатах США. Атак зазнав департамент охорони здоров'я штату Іллінойс та навіть ВООЗ. Однак найбільш трагічним став хакерський напад на госпіталь у Дюссельдорфі, який спричинив смерть пацієнтки [6].

Кібератакам піддаються наукові центри та лабораторії. Згідно з даними IBM, сім провідних компаній в Канаді, Франції, Індії, Південній Кореї та США, які займаються створенням вакцин та проведенням клінічних випробувань, стали мішенями для цифрових атак [6].

Постійна загроза в сфері охорони здоров'я та інших сферах діяльності змушує співпрацювати між собою різні країни. Основоположними документами у боротьбі з кіберзлочинністю, прийнятими в результаті такої співпраці, є "Конвенція про злочинність у сфері комп'ютерної інформації" Ради Європи та "Резолюція боротьби зі злочинним використанням інформаційних технологій", прийнята країнами-учасницями ООН у 2001 році. Згідно з Резолюцією, основними заходами у боротьбі з кіберзлочинністю є:

— законодавче закріплення відповідальності за кіберзлочини;

— міждержавна взаємодія правоохоронних органів, їх відповідна підготовка в умовах інформаційного суспільства;

— обмін інформацією щодо проблем кіберзлочинів;

— забезпечення достатнього рівня захисту інформаційних систем від незаконного втручання;

— своєчасний збір доказів під час розслідування скоєних кіберзлочинів.

Міжнародну протидію кіберзлочинності, в тому числі, у сфері охорони здоров'я, проводить НАТО. В 2013 року була розроблена єдина система з реагування на атаки в кіберпросторі. Постійно ведуться роботи з оцінки ефективності цієї системи та її вдосконалення.

Рис. 2. Мета кібератак, кількість випадків [7]

Примітка: систематизовано автором.

Зокрема, кожен рік проводяться навчання "Кіберкоаліція" та "Захисний шар".

В 2013 році у Гаазі був створений Європейський центр, який займається збором та аналізом даних з кіберзлочинів, розробленням заходів щодо їх розслідування, обміном досвідом у боротьбі та попередженні кібератак з іншими країнами.

Враховуючи вищезазначене, можна зробити висновок про активну міжнародну протидію кіберзлочинності. Участь у розробці заходів щодо запобігання кіберзлочинам в сфері охорони здоров'я приймає й Україна. Досвід нашої держави в боротьбі з кібератаками російського агресора допомагає іншим країнам та міжнародним організаціям у побудові дієвих національних та міжнародних систем кіберзахисту.

Згідно з даними CERT-UA, з 24 лютого 2022 року по 24 серпня 2022 року було зареєстровано 1123 кібератаки на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури [7]. Значна частина кібератак здійснювалася на сектор охорони здоров'я, зокрема, на інформаційно-комунікаційні системи та реєстри ЕСОЗ. Основною метою таких кібератак став несанкціонований збір інформації, розміщення шкідливого програмного коду та втручання у роботу ресурсів (рис. 2).

Не дивлячись на постійні кібератаки з боку російських хакерів, інформаційно-комунікаційні системи та реєстри сфери охорони здоров'я залишаються неушкодженими. Цього вдалося досягти завдяки надійному захисту ЕСОЗ.

Електронна система охорони здоров'я розроблена відповідно з вимогами діючого законодавства України до захисту інформації та кіберзахисту. Основними законами, які регулюють питання забезпечення захисту медичних даних, що формуються та циркулюють в цій системі, є Закон України "Основи законодавства України про охорону здоров'я" та Закон України "Про захист персональних даних".

На сьогоднішній день медичними інформаційними системами E-health користуються українські лікарні, аптеки та, безпосередньо, пацієнти, які з їх допомогою передають інформацію до центральної бази. За безпеку даних відповідає держава, якій і належить ця база. Саме в базі зберігаються реєстри з даними про пацієнтів, укладені декларації, медичні висновки, медичні записи тощо. За захист даних відповідає НСЗУ, яка є власником електронної системи. Також відповідальність несуть медпрацівники, які здійснюють їх обробку під час прийому пацієнтів, консультування, проведення процедур, діагностики, призначення лікування тощо.

Захист даних інформаційно-комунікаційних систем та реєстрів ЕСОЗ в Україні забезпечується шляхом таких заходів:

— втілення заходів безпеки та постійна робота над її посиленням НСЗУ та державним підприємством "Електронне здоров'я", яке є адміністратором eHealth;

— залучення експертів міжнародних аудиторських компаній до моніторингу безпеки медичних інформаційних систем;

— обов'язкове проходження сертифікації та отримання атестату відповідності всіх інформаційних систем, які обмінюються інформацією з центральною базою даних;

— реалізація принципів GDPR (регламенту по захисту даних, General Data Protection Regulation) і міжнародних стандартів захисту інформації. ЕСОЗ має таку структуру, яка дозволяє зберігати персональні дані людини окремо від її медичних даних. Завдяки цьому, у разі втручань, втрат або пошкоджень медичних інформаційно-комунікаційних систем чи реєстрів отримати медичні дані конкретної особи неможливо;

— забезпечення обмеженого доступу до даних електронної системи охорони здоров'я. Доступ повинні мати виключно ідентифіковані та автентифіковані користувачі. При вході в систему такі користувачі повинні авторизуватися в МІС та ЕСОЗ. Дані пацієнта доступні сімейному лікарю, з яким укладена декларація, та лікарю-спеціалісту за згодою пацієнта;

— співпраця з міжнародними партнерами в сфері кіберзахисту. Міжнародна спільнота використовує інформацію від українських фахівців на міжнародних заходах, присвячених питанням кібербезпеки. Прикладом такого заходу є міжнародна конференція з кібербезпеки HAT-2022 та міжнародна конференція FIRST. В липні-серпні 2022 року був підписаний "Меморандум про взаєморозуміння у сфері кіберзахисту" зі Словенією та Польщею. Також була налагоджена співпраця з Агентством із кібербезпеки та безпеки інфраструктури Департаменту нацбезпеки США. Варто відзначити підписання меморандуму про співпрацю Міністерства цифрової трансформації з провідною організацією з кібербезпеки США та Австралії "Інтернет 2.0" [8].

Табл. 1. Заходи з удосконалення державного механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів ЕСОЗ [11]

Заходи	Пояснення
Правові	Удосконалення кримінального законодавства як на національному, так і на міжнародному рівні, включаючи укладання відповідних угод з іншими державами та міжнародними організаціями Введення до закону нових обставин, що обтяжують покарання, та формування спеціальних норм про відповідальність за кіберзлочини у сфері охорони здоров'я Прийняття локальних нормативних актів в конкретній медичній чи іншій організації, з правилами «цифрової гігієни» для співробітників
Технічні	Застосування підходу «нульової довіри», відповідно до якого кожен доступ до даних та програм повинен підтверджуватися. Користувачам таких програм необхідно надавати мінімально необхідні права Створення цілісної, стандартизованої та уніфікованої системи реєстрів ЕСОЗ шляхом інвентаризації та формування переліку таких реєстрів Модернізація ІТ-інфраструктури медичних закладів та обладнання, яке використовується в закладах охорони здоров'я
Освітні	Регулярні заходи інформаційно-освітнього характеру з медичним персоналом та іншими співробітниками медичних організацій, які використовують у своїй діяльності цифрові технології Розробка посібників з кібербезпеки для охорони здоров'я

Примітка: систематизовано автором.

— тимчасове зберігання даних за кордоном. Напередодні повномасштабної війни українською владою було ухвалено рішення про тимчасове зберігання державних реєстрів за кордоном. Згідно з даними Ukrinform, в перші тижні війни було перенесено більше 60 критичних реєстрів та систем на ресурси компанії Амазон. Пропозицією цієї компанії скористалось Міністерство охорони здоров'я [9].

Таким чином, інформаційно-комунікаційні системи та реєстри сфери охорони здоров'я України надійно захищені від можливих втручань, втрат та пошкоджень. Однак у зв'язку з рядом невирішених проблем, медична галузь залишається основною мішенню для кіберзлочинців. До таких проблем необхідно віднести наступні:

— відсутність кваліфікованого ІТ персоналу в медичних організаціях, що пояснюється низькими заробітними платами в сфері охорони здоров'я;

— нові виклики перед ІТ-спеціалістами у зв'язку з пандемією коронавірусу та війною в Україні;

— застаріла ІТ-інфраструктура медичних закладів, яка не відповідає сучасним вимогам;

— невпорядкованість інформаційно-комунікаційних систем та реєстрів сфери охорони здоров'я;

— вразливість хмарних технологій, які використовуються більшістю медичних організацій до кібератак та обмежені можливості персоналізації;

— застарілі підключені пристрої, які використовуються в лікарнях: рентгенівські апарати, сканери МРТ тощо [10].

Вирішення зазначених проблем сприятиме вдосконаленню державного механізму кібербезпеки, моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень інформаційно-комунікаційних систем та реєстрів ЕСОЗ. Для цього МОН та інші центральні органи виконавчої влади спільно з Міністерством цифрової трансформації, Держспецзв'язком та підпорядкованим йому Державним центром кіберзахисту повинні здійснити ряд заходів — правових, технічних та освітніх (табл. 1).

ВИСНОВКИ

Організації охорони здоров'я у всьому світі піддаються та будуть піддаватися кібератакам, які посягають на громадську безпеку, власність, життя та здоров'я, конституційні права громадян, безпеку збору, зберігання та передання медичної інформації. В зв'язку з цим приорітетним напрямом діяльності держави повинно стати вдосконалення механізму кібербезпеки, моніторингу, захисту та аналізу втручань, втрат та пошкоджень інформаційно-комунікаційних систем та медичних реєстрів електронної системи охорони здоров'я України.

E-health є надійно захищеною від кіберзлочинців, однак у зв'язку з рядом невирішених проблем в медичній галузі, ця система залишається основною мішенню для кіберзлочинців. На сьогоднішній день такими проблемами є: відсутність кваліфікованого ІТ персоналу в медичних організаціях, нові виклики перед ІТ-спеціалістами у зв'язку з пандемією коронавірусу та війною в Україні, застаріла ІТ-інфраструктура медичних закладів, невпорядкованість інформаційно-комунікаційних систем та реєстрів, вразливість хмарних технологій. Для вирішення зазначених проблем пропонується здійснення наступних заходів: удосконалення кримінального законодавства, прийняття локальних нормативних актів з правилами "цифрової гігієни", обмеження доступу до електронної системи охорони здоров'я, створення цілісної, стандартизованої та уніфікованої системи реєстрів, модернізація ІТ-інфраструктури медичних закладів, заходи

інформаційно-освітнього характеру з медичним персоналом, розробка посібників з кібербезпеки.

Практичне значення дослідження полягає в можливості використання отриманих результатів державними органами в процесі розроблення механізму захисту медичних інформаційних систем та реєстрів від кібератак в галузі охорони здоров'я.

Література:

1. Seals T. Misery of Ransomware Hits Hospitals the Hardest. Threatpost, 2020. URL: https://threatpost.com/ransomware-hits-hospitals-hardest/162096/

2. Москаленко Ю. Електронна система охорони здоров'я під час війни: як зараз працює одна з найбільших IT-систем в Україні. Zn.ua, 2022. URL: https://zn.ua/ukr/UKRAINE/elektronna-sistema-okhoroni-zdorovja-pid-chas-vijni-jak-zaraz-pratsjuje-odna-z-najbilshikh-it-sistem-v-ukrajini.html

3. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 року № 2801-XII. zakon.rada.gov.ua, 2022. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text

4. Черниш Д. В Україні працює кілька приватних медичних інформаційних систем. Як там захищені дані українців. Forbes.ua, 2022. URL: https://forbes.ua/innovations/v-ukraini-pratsyue-kilka-privatnikh-medichnikh-informatsiynikh-sistem-yak-tam-zakhishcheni-dani-ukraintsiv-08092022-8211

5. 2022 HIMSS Cybersecurity Survey Collecting Responses from Healthcare Professionals. HIMSS, 2022. URL: https://www.himss.org/news/2022-himss-cybersecurity-survey-collecting-responses-healthcare-professionals

6. Burt T. Cyberattacks targeting health care must stop. Microsoft, 2020. URL: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

7. Савченко-Галушко Т. Як забезпечити захист кіберпростору України на тлі збройної агресії рф. Armyinform, 2022. URL: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/

8. Посилюємо кіберзахист: Мінцифри підписало Меморандум з міжнародною компанією "Інтернет 2.0". Урядовий портал, 2022. URL: https://www.kmu.gov.ua/news/posyliuiemo-kiberzakhyst-mintsyfry-pidpysalo-memorandum-z-mizhnarodnoiu-kompaniieiu-internet-20

9. Українські сайти витримали найпотужніші кібератаки ворога — Зеленський. Укрінформ, 2022. URL: https://www.ukrinform.ua/rubric-technology/3565926-ukrainski-sajti-vitrimali-najpotuznisi-kiberataki-voroga-zelenskij.html

10. Небезпека кібератак на сектор охорони здоров'я: як справитися з новим викликом. Eset, 2022. URL: https://eset.ua/ua/news/view/952/opasnost-kiberatak-na-sektor-zdravookhraneniya-kak-spravitsya-s-novymi-vyzovami

11. МОЗ розпочало роботу з оптимізації та систематизації реєстрів сфери охорони здоров'я. Урядовий портал, 2022. URL: https://www.kmu.gov.ua/news/moz-rozpochalo-robotu-z-optymizatsii-ta-systematyzatsii-reiestriv-sfery-okhorony-zdorovia

References:

1. Seals, T. (2020), "Misery of Ransomware Hits Hospitals the Hardest", Threatpost, available at: https://threatpost.com/ransomware-hits-hospitals-hardest/162096/ (Accessed 05 March 2023).

2. Moskalenko, Yu. (2022), "The electronic health care system during the war: how one of the largest IT systems in Ukraine currently works", Zn.ua, available at: https://zn.ua/ukr/UKRAINE/elektronna-sistema-okhoroni-zdorovja-pid-chas-vijni-jak-zaraz-pratsjuje-odna-z-najbilshikh-it-sistem-v-ukrajini.html (Accessed 05 March 2023).

3. Verkhovna Rada of Ukraine (1992), The Law of Ukraine "Fundamentals of the Legislation of Ukraine on Health Care", available at: https://zakon.rada.gov.ua/laws/show/2801-12#Text (Accessed 05 March 2023).

4. Chernysh, D.V (2022), "Several private medical information systems operate in Ukraine. How is the data of Ukrainians protected there?", Forbes.ua, available at: https://forbes.ua/innovations/v-ukraini-pratsyue-kilka-privatnikh-medichnikh-informatsiynikh-sistem-yak-tam-zakhishcheni-dani-ukraintsiv-08092022-8211 (Accessed 05 March 2023).

5. HIMSS (2022), "HIMSS Cybersecurity Survey Collecting Responses from Healthcare Professionals", available at: https://www.himss.org/news/2022-himss-cybersecurity-survey-collecting-responses-healthcare-professionals (Accessed 05 March 2023).

6. Burt, T. (2020), "Cyberattacks targeting health care must stop", Microsoft, available at: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (Accessed 05 March 2023).

7. Savchenko-Halushko, T. (2022), "How to ensure the protection of the cyberspace of Ukraine against the background of the armed aggression of the Russian Federation", Armyinform, available at: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/ (Accessed 05 March 2023).

8. Government portal (2022), "We are strengthening cyber protection: the Ministry of Digital Affairs signed a Memorandum with the international company "Internet 2.0"", available at: https://www.kmu.gov.ua/news/posyliuiemo-kiberzakhyst-mintsyfry-pidpysalo-memorandum-z-mizhnarodnoiu-kompaniieiu-internet-20 (Accessed 05 March 2023).

9. Ukrinform (2022), "Ukrainian sites have withstood the most powerful cyberattacks of the enemy — Zelenskyi", available at: https://www.ukrinform.ua/rubric-technology/3565926-ukrainski-sajti-vitrimali-najpotuznisi-kiberataki-voroga-zelenskij.html (Accessed 05 March 2023).

10. Eset (2022), "The danger of cyberattacks on the healthcare sector: how to cope with the new challenge", available at: https://eset.ua/ua/news/view/952/opasnost-kiberatak-na-sektor-zdravookhraneniya-kak-spravitsya-s-novymi-vyzovami (Accessed 05 March 2023).

11. Government portal (2022), "The Ministry of Health has started work on the optimization and systematization of health care registers", available at: https://www.kmu.gov.ua/news/moz-rozpochalo-robotu-z-optymizatsii-ta-systematyzatsii-reiestriv-sfery-okhorony-zdorovia (Accessed 05 March 2023).

Стаття надійшла до редакції 11.03.2023 р.