УДК 351:[681.51:614

DOI: https://doi.org/10.31470/2786-6246-2023-6-113-121

Ляшук Артем,
аспірант кафедри публічного управління, адміністрування та соціальної роботи Національного університету охорони здоров'я України імені П.Л. Шупика

Liashuk Artem,
Graduate student of the Department of Public Management, Administration and Social Work of Shupyk National Healthcare University of Ukraine

ORCID ID: https://orcid.org/0000-0002-4206-3929
✉ ernest-natan@ukr.net

ЗАГРОЗИ І ВИКЛИКИ ДЛЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ТА РЕЄСТРІВ СФЕРИ ОХОРОНИ ЗДОРОВ'Я

THREATS AND CHALLENGES TO THE CYBERSECURITY SYSTEM OF HEALTHCARE INFORMATION SYSTEMS AND REGISTRIES

Анотація. У статті розкрито ключові загрози та виклики для системи кібербезпеки інформаційних системи та реєстрів сфери охорони здоров'я. Розглянуто особливості Концепції електронної охорони здоров'я «e-Health» та з'ясовано, що щодо системи кібербезпеки нею передбачено інформатизацію закладів охорони здоров'я, затвердження концептуально-еталонної бази цифрових компетенцій медичних працівників, розвиток інформаційної культури та цифрової компетентності, кібербезпеки та кібергігієни медичного персоналу та пацієнтів. Відзначено шляхи забезпечення якості, безпечності та доступності електронної охорони здоров'я у напрямку кібербезпеки. Проаналізовано особливості Угоди про позику від 22.12.22 №9468-UA між Міністерством охорони здоров'я України та Світовим Банком в рамках проєкту «Зміцнення системи охорони здоров'я та збереження життя», якою передбачено щодо кібербезпеки розробку основних модулів системи електронної охорони здоров'я, включаючи реєстрацію медичних працівників, портал даних пацієнтів, модулі системи електронної охорони здоров'я для груп інвалідності та реабілітації, покращення кібербезпеки даних, пов'язаних зі здоров'ям, інтеграцію цифрових систем охорони здоров'я з пов'язаними системами в сусідніх країнах і зміцнення систем електронної охорони здоров'я в усіх закладах охорони здоров'я. З'ясовано, що повномасштабне вторгнення ворога на територію України принесло нові загрози та виклики, пов'язані з необхідністю підвищення рівня кіберзахисту інформаційних систем та реєстрів та розвитку електронної охорони здоров'я загалом. Відзначено ключові загрози та виклики, пов'язані з впливом війни на систему кібербезпеки сфери охорони здоров'я. Розкрито основні завдання робочої групи у контексті розробки та реалізації Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я. Представлено технічні та організаційні заходи щодо забезпечення належного рівня кібезбезпеки у сфері охорони здоров'я.

Ключові слова: кібербезпека, кіберзахист, кібератака, сфера охорони здоров'я, інформаційні системи та реєстри.

Abstract. The article reveals the key threats and challenges to the cybersecurity system of information systems and registries in the healthcare sector. The author

examines the features of the e-Health Concept and finds out that in terms of the cybersecurity system, it provides for the informatization of healthcare institutions, approval of the conceptual and reference base of digital competencies of healthcare professionals, development of information culture and digital competence, cybersecurity and cyberhygiene of medical staff and patients. The ways to ensure the quality, safety and accessibility of eHealth in the area of cybersecurity are highlighted. The features of the Loan Agreement dated 22.12.22 №9468-UA between the Ministry of Health of Ukraine and the World Bank under the project «Strengthening the Health System and Saving Lives» are analyzed, which provides for the development of the main modules of the eHealth system, including registration of healthcare professionals, patient data portal, eHealth modules for disability and rehabilitation groups, improvement of cybersecurity of health-related data, integration of digital health systems. It is found that the full-scale invasion of the enemy on the territory of Ukraine has brought new threats and challenges related to the need to increase the level of cybersecurity of information systems and registries and the development of eHealth in general. The key threats and challenges associated with the impact of the war on the healthcare cybersecurity system are noted. The main tasks of the working group in the context of the development and implementation of the Concept of Strategic Directions for the Development of Cybersecurity in the Field of Electronic Healthcare are revealed. Technical and organizational measures to ensure an adequate level of cybersecurity in the healthcare sector are presented.

Keywords: cybersecurity, cyber defense, cyber attack, healthcare, information systems and registries.

Постановка проблеми. Зі збільшенням використання цифрових технологій у сфері охорони здоров'я кібербезпека стала дуже важливою, оскільки конфіденційність медичної інформації та безпека інформаційних систем та реєстрів є складовою частиною сфери охорони здоров'я. Так, кібербезпека є важливим аспектом сфери охорони здоров'я, оскільки вона захищає конфіденційну медичну інформацію та запобігає втраті важливих даних. За останні роки цифрові технології революціонізували методи надання медичної допомоги та зберігання даних про здоров'я. З одного боку, покращилась якість та доступність медичних послуг. З іншого боку, це також створило нові загрози та виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я.

Аналіз останніх досліджень і публікацій. Проблемі кібербезпеки у сфері охорони здоров'я присвячено багато праць вчених. Зокрема, колектив науковців під керівництвом О. Трофименко пропонують під кібербезпекою у сфері охорони здоров'я розуміти важливу складову державної політики, спрямовану на контроль поточного стану інформаційних систем критичної інфраструктури, підвищення обізнаності та кіберграмотності співробітників, підготовку кваліфікованих фахівців у сфері кібербезпеки та отримання успішного світового досвіду в цій сфері. На думку вчених, важливими засобами забезпечення безпеки віддаленої підтримки пацієнтів є надійні електронні бази медичних даних, механізми реєстрації та керування доступом до медичних даних, що передаються між пацієнтами та постачальниками медичних послуг. Водночас до забезпечення надійного захисту медичних комп'ютерних систем необхідно підходити з найбільшою ретельністю, враховуючи програмні, апаратні та організаційні аспекти [1, с. 31-32; 36].

І. Волинець зазначає, що захист від кіберзлочинності у сфері охорони здоров'я потребує врахування усталеної міжнародної практики та сучасних

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

технологічних досягнень у сфері протидії злочинності в електронних мережах, що здійснюють зберігання, обробку, збір та використання медичної інформації [2, с. 118].

А. Стрєлкіна та Д. Узун надають такі рекомендації щодо забезпечення кібербезпеки системи охорони здоров'я в контексті Інтернету речей, які складаються, серед іншого, з таких компонентів: 1) забезпечити наявність і готовність, оскільки за своєю конструкцією медичні пристрої мають обмежені ресурси, обмежене обладнання, включаючи батареї, і термін служби в кілька років; 2) механізм контролю доступу необхідний для, щоб гарантувати, що довірені пристрої включені в систему охорони здоров'я та що ці пристрої можуть довіряти брокеру або програмі, яка надсилає команди керування; 3) відповідність моделі OSI, оскільки взаємодія між компонентами в мережі фізичних об'єктів повинна здійснюватися за допомогою протоколів прикладного рівня; 4) дотримуватись вимог безпеки нормативних документів; 5) регулярний моніторинг та управління безпекою, що включає збір інформації, дослідження побічних ефектів, а також активне виявлення, дослідження та запобігання проблемам безпеки, які можуть виникнути під час використання пристрою; 6) кваліфікаційні вимоги до обслуговуючого персоналу, що передбачає регулярне проведення різноманітних навчальних курсів, зустрічей та консультацій з експертами з кібербезпеки для всіх співробітників [3, с. 47–48].

Водночас Б. Коваль, Л. Коваль та С. Пойда зазначають, що вивчення основ медіаграмотності та кібербезпеки допоможе майбутнім лікарям ефективно захищати конфіденційність своїх пацієнтів і запобігати розголошенню конфіденційної медичної інформації. З позиції вчених, захист від кібератак має вирішальне значення у сфері охорони здоров'я, оскільки помилки в цьому питанні можуть мати серйозні наслідки для здоров'я та життя пацієнта. Крім того, розголошення особистої інформації може призвести до величезних втрат для людей поза медичною спільнотою [4, с. 181].

Враховуючи дослідження науковців, зазначимо, що питання висвітлення особливостей кібербезпеки у сфері охорони здоров'я у контексті оперативного реагування на загрози та виклики інформаційних системи та реєстрів потребує більш поглибленого обговорення та, зокрема, доцільно показати практичні аспекти питання з урахуванням реалій сьогодення.

Метою статті передбачено розкрити ключові загрози та виклики для системи кібербезпеки інформаційних системи та реєстрів сфери охорони здоров'я.

Виклад основного матеріалу. Кібербезпека у сфері охорони здоров'я стала ключовою проблемою для медичних установ і країни. Для розвитку електронної системи охорони здоров'я та активної цифровізації процесів медичній спільноті потрібні не лише цифрові знання та навички, а й базові знання та навички з кібербезпеки для захисту власних даних і даних пацієнтів у цифровому просторі. З огляду на те, кіберзахист забезпечує такі заходи, як захист від вірусів, хакерських атак, фальсифікації даних та інших дій, які можуть призвести до видалення чи крадіжки даних, а також потенційно згубного впливу на роботу та продуктивність працівників, використання незаконно отриманої інформації про лікувальні установи, фізичних чи юридичних осіб або з метою зриву процесу надання медичних та супутніх послуг у цілому.

Концепція електронної охорони здоров'я «e-Health» є природною еволюцією стратегічного плану дій щодо вдосконалення національної системи охорони здоров'я. Електронна охорона здоров'я означає використання інформаційно-

комунікаційних технологій у системі охорони здоров'я. Зараз цей напрямок вважається одним з найбільш перспективних і швидко розвивається. Однак у реаліях вітчизняної системи впровадження «e-Health» стикається зі значною кількістю перешкод різного походження, які певною мірою затримують перехід усієї системи охорони здоров'я на новий рівень. Тому належне управління ресурсами сфери охорони здоров'я здійснюється без достатньої функціональності, надійності та своєчасної інформації. Зрештою, інформація формує основу процесу управління, оскільки вона містить дані, необхідні для оцінки ситуації та прийняття управлінських рішень. Без економічних, технологічних, соціально-психологічних та адміністративних методів управління, за допомогою яких система управління безпосередньо впливає на цілі управління, неможливо приймати оптимальні управлінські рішення. Важливу роль у цьому процесі відіграє підвищення якості інформаційного забезпечення процесів управління шляхом впровадження інформаційних комп'ютерних технологій.

У Концепції розвитку електронної охорони здоров'я [1] щодо системи кібербезпеки передбачено інформатизацію закладів охорони здоров'я, затвердження концептуально-еталонної бази цифрових компетенцій медичних працівників, розвиток інформаційної культури та цифрової компетентності, кібербезпеки та кібергігієни медичного персоналу та пацієнтів.

Водночас для забезпечення якості, безпечності та доступності електронної охорони здоров'я у напрямку кібербезпеки передбачено:

1) забезпечити кібербезпеку, відстежувати, захищати та аналізувати можливі вторгнення, втрати та пошкодження;
2) реалізувати функції програм і платформ, необхідних для пошуку вразливостей у системах, програмах, реєстрах тощо та, за необхідності, проводити постійний моніторинг кіберзагроз за участю «етичних хакерів»;
3) впроваджувати програми з кібербезпеки та кібергігієни та навчати користувачів електронної системи охорони здоров'я, щоб забезпечити відповідність вимогам і стандартам захисту персональної інформації [5].

Міністерство охорони здоров'я України спільно зі Світовим Банком в рамках проєкту «Зміцнення системи охорони здоров'я та збереження життя» (HEAL Ukraine) ухвалило Угоду про позику від 22.12.22 р. №9468-UA [6], якою передбачено створити єдиний Галузевий Центр кібербезпеки в галузі охорони здоров'я, щоб забезпечити належний рівень інформаційної безпеки у цій сфері та суспільстві в цілому.

Так, положеннями Угоди передбачено розвиток потенціалу, цифровізацію та підтримку інновацій, зокрема розробку основних модулів системи електронної охорони здоров'я, включаючи реєстрацію медичних працівників, портал даних пацієнтів, модулі системи електронної охорони здоров'я для груп інвалідності та реабілітації, покращення кібербезпеки даних, пов'язаних зі здоров'ям, інтеграцію цифрових систем охорони здоров'я з пов'язаними системами в сусідніх країнах і зміцнення систем електронної охорони здоров'я в усіх закладах охорони здоров'я [6].

Кількість кібератак на критично важливу інфраструктуру, в тому числі на заклади охорони здоров'я, значно зросла з початку повномасштабної російсько-української війни. Такі кібератаки націлені на те, щоб перервати роботу, викрасти та використати медичні дані населення України. Тому захист особистої та медичної інформації є дуже важливим. Особливо це актуально, коли Україна

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

перебуває у воєнному стані, де хакери країни-агресора постійно намагаються викрасти дані населення України для кібератак і дезінформаційних кампаній. Тому, враховуючи такі проблеми, потрібно приділити особливу увагу питанням кібербезпеки на стратегічному, організаційному та технічному рівнях.

З огляду на те, зауважимо, що повномасштабне вторгнення ворога на територію України принесло нові загрози та виклики, пов'язані з необхідністю підвищення рівня кіберзахисту інформаційних систем та реєстрів та розвитку електронної охорони здоров'я загалом.

Так, ключові загрози та виклики, пов'язані з впливом війни на систему кібербезпеки сфери охорони здоров'я, в основному зумовлені тим, що:

1. з розвитком електронної медицини збільшується кількість інформаційних систем та реєстрів, кількість даних, а разом з цим і кількість кібератак;
2. підвищується ризик втрати або пошкодження особистої та медичної інформації про пацієнта;
3. у міру розвитку війни були вжиті агресивні заходи проти критичної інформаційної інфраструктури;
4. кіберзлочинці використовують складні та різноманітні кібератаки, причому останнім часом найпоширенішими є кібератаки з використанням вірусів-вимагачів та атаки через постачальників IT-послуг.

Створення єдиного інформаційного простору охорони здоров'я з наскрізними процесами та послугами та взаємодією між країнами та кордонами є важливою складовою для розвитку електронної охорони здоров'я та посилення кібербезпеки. Водночас забезпечення інфраструктурних та технічних умов для надання якісних медичних послуг з використанням інформаційних систем та реєстрів усіх рівнів та створення зручного і прозорого механізму для доступу користувачів і керування даними про здоров'я виступають також ключовими засадами ефективності системи кібербезпеки.

Доцільно також відзначити, що Наказом Міністерства охорони здоров'я України від 15.06.2022 р. №1034 затверджено склад Робочої групи з питань розробки та реалізації Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я, а також положення про основні завдання діяльності цієї групи [7].

Основними завданнями робочої групи у контексті розробки та реалізації Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я є:

1. проведення аналізу поточного стану кібербезпеки в сфері електронної охорони здоров'я;
2. встановлення шляхів розв'язання проблем, які виникають під час забезпечення кібербезпеки у сфері електронної охорони здоров'я;
3. підтримка забезпечення скоординованих дій державних органів влади у визначенні пріоритетів для розвитку галузевих систем кібербезпеки в секторі електронної охорони здоров'я;
4. розробка пропозиції щодо Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я;
5. розробка пропозицій щодо впровадження заходів із впровадження стандартів кібербезпеки на основі стратегічного напряму розвитку кібербезпеки у сфері електронної охорони здоров'я, включаючи моніторинг та аналіз рівня захисту стану інформаційної безпеки, електронних можливостей вторгнення, втрати або пошкодження даних з

телекомунікаційних, інформаційно-комунікаційних систем, баз даних, електронних реєстрів та інших інформаційних ресурсів у сфері охорони здоров'я;
6. розробка рекомендацій щодо організаційних, технічних та інших рішень для забезпечення кібербезпеки у сфері електронної охорони здоров'я;
7. забезпечення міжвідомчої взаємодії та організація діяльності усіх учасників, залучених до виконання роботи робочої групи;
8. опрацювання інших питань, що пов'язані із забезпеченням кібербезпеки у сфері електронної охорони здоров'я [7].

Важливим документом у контексті реагування на загрози та виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я є Наказ Міністерства охорони здоров'я України «Про затвердження Протоколу кризових комунікацій під час реагування на кібератаки та кіберінциденти» від 06.12.2013 р. №2076 [8]. Цим документом затверджено протокол кризових комунікацій під час реагування на кібератаки та кіберінциденти, який надає шаблони та процедури для обміну інформацією, координації та спільних дій у відповідь на кібератаки та кіберінциденти в Міністерстві охорони здоров'я, Національній службі здоров'я України, Центрі громадського здоров'я України, Державному підприємстві «Електронне здоров'я». Послідовність взаємодії органів кібербезпеки при реагуванні на кіберінциденти та кібератаки встановлює вимоги до обміну інформацією, координації та спільних дій органів кібербезпеки при реагуванні на кіберінциденти та кібератаки.

З метою збереження конфіденційності інформації, пов'язаної з персональною медичною інформацією та персональними даними пацієнтів, Міністерством охорони здоров'я України спільно з проєктом USAID «Підтримка реформи охорони здоров'я» розроблено методичні рекомендації щодо кіберзахисту закладів охорони здоров'я. Обізнаність користувачів інформаційної системи про ризики кібербезпеки та заходи захисту від загроз відіграє важливу роль у підвищенні кіберстійкості сфери охорони здоров'я. Для забезпечення належного рівня кібербезпеки суб'єкти охорони здоров'я повинні дотримуватися наступних технічних та організаційних заходів:

1. Конфіденційність. Усі працівники повинні знати про конфіденційність медичної та особистої інформації, отриманої під час роботи закладу, і повинні розуміти та дотримуватися правил поводження з конфіденційною інформацією. Вони не мають права поширювати таку інформацію. Для досягнення цієї мети необхідне регулярне навчання всіх працівників, принаймні раз на рік. Під час службових справ конфіденційна інформація передається від однієї особи до іншої. Особи, які отримали конфіденційну інформацію, повинні забезпечити зберігання та обробку цієї інформації на умовах, встановлених особами, які надали згоду на обробку своїх персональних даних.
2. Шифрування даних з обмеженим доступом. Зберігання та передача персональних даних має бути зашифрованою. Ця інформація включає будь-яку інформацію, яка може бути використана для ідентифікації особи та медичну інформацію пацієнта. Алгоритми та засоби шифрування мають відповідати вимогам, встановленим Державною службою спеціального зв'язку та захисту інформації України.
3. Ідентифікація користувачів інформаційних систем. Кожен користувач медичної інформаційної системи повинен мати унікальний ідентифікатор (акаунт, логін) та пароль для доступу до системи.

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

4. Контроль доступу до інформації. Інформаційні ресурси повинні бути захищені системою контролю доступу. Системи контролю доступу повинні ідентифікувати кожного користувача за ідентифікатором та запобігати доступу неавторизованих користувачів до інформаційних ресурсів установи. Системи контролю доступу включають як внутрішній захист (паролі, шифрування даних, таблиці контролю доступу, налаштування інтерфейсу користувача тощо), так і зовнішній захист (захист портів, брандмауери, аутентифікація на основі хоста тощо).
5. Цілісність даних пацієнтів. Заклади охорони здоров'я повинні впроваджувати та підтримувати організаційні та технічні заходи для запобігання несанкціонованим змінам або знищенню медичної документації та іншої конфіденційної інформації про пацієнта. Заклади охорони здоров'я також повинні підтримувати впровадження автоматизованих систем і програмного забезпечення для автоматичної перевірки людських помилок під час обробки даних пацієнтів. У таких закладах має бути резервна копія даних пацієнтів.
6. Доступність медичної інформації. У разі надзвичайної ситуації медичні працівники мають доступ до захищеної електронної медичної інформації. Рішення екстреного доступу використовуються лише тоді, коли звичайних процесів недостатньо для надання швидкої медичної допомоги. Спеціаліст з інформаційної безпеки розробляє, документує, впроваджує та тестує процедури екстреного доступу в разі надзвичайної ситуації. Доступ до секретних облікових даних автентифікації, таких як логіни та паролі для використання попередньо створених екстрених облікових записів, відбувається через такі засоби масової інформації, як друковані сторінки, картки, смарт-картки та жетони, залежно від методу автентифікації системи. Носії, що містять конфіденційну інформацію для автентифікації, поміщають у запечатаний конверт і зберігають. З метою забезпечення принципу «чотирьох очей» та неспростовності справи під час отримання конференції інформації необхідно пред'явити посвідчення особи отримувача конфіденційної інформації та зазначити про отримання конфіденційної інформації в протоколі реєстрації.
7. Додатково закладам охорони здоров'я необхідно подбати про: антивірусний захист (антивірусне програмне забезпечення встановлено на всіх бізнес-пристроях і серверах в організації та регулярно оновлюється; воно повинно мати підтримку розробників, можливість надсилати підозрілі файли відповідним експертам для аналізу та можливості евристичного аналізу); програмне забезпечення (на внутрішніх комп'ютерах і в мережах закладу можна використовувати лише затверджене програмне забезпечення; встановлення програмного забезпечення має здійснюватися лише авторизованим персоналом (адміністраторами); все програмне забезпечення має бути перевірено та схвалено керівником об'єкта або спеціалістом з інформаційної безпеки перед встановленням; усі файли та програми, передані в електронному вигляді з іншого місця на комп'ютер або мережу, повинні бути перевірені на наявність вірусів одразу після отримання) [9].

Висновки. Таким чином, проведені дослідження дозволяють зауважити, що розвиток надійного кіберзахисту в Україні потребує особливої уваги до сфери охорони здоров'я. Перш за все, важлива безпека особистої інформації кожного пацієнта. Кібербезпека особливо важлива в охороні здоров'я для захисту

конфіденційної медичної інформації, зокрема результатів аналізів, діагнозів і лікування. Якщо ці дані потраплять до рук зловмисника, це може поставити пацієнтів під загрозу та перешкодити їм отримати своєчасну та належну медичну допомогу. Щоб запобігти цим кіберзагрозам, необхідно впровадити такі заходи кібербезпеки, як шифрування даних, двофакторна автентифікація та антивірусний захист мереж і систем зберігання даних, а також забезпечити належний кіберзахист інформаційних систем та реєстрів сфери охорони здоров'я.

Список використаних джерел:

1. Трофименко О., Дубовий Я., Логінова Н., Прокоп Ю., Задерейко О. Питання кібербезпеки медичних комп'ютерних систем. *Захист інформації*. 2021. №23(1). С. 30–39.
2. Волинець І. Кіберзлочинність у сфері охорони здоров'я: реальність, що потребує захисту. *Теорія і практика інтелектуальної власності*. 2019. №3. С. 113–122.
3. Стрєлкіна А.А., Узун Д.Д. Забезпечення кібербезпеки медичних систем: виклики і рішення в контексті Інтернету речей. *Радіоелектронні і комп'ютерні системи*. 2017. №1. С. 44–50.
4. Коваль Б., Коваль Л., Пойда С. Навчання майбутніх лікарів основам медіаграмотності та кібербезпеки. *Перспективи та інновації науки*. 2023. №8(26). С. 171–183.
5. Про схвалення Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України; Концепція від 28.12.2020 №1671-р. URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text (дата звернення: 04.09.2023).
6. Угода про позику (Проєкт «Зміцнення системи охорони здоров'я та збереження життя» (Heal Ukraine)) між Україною та Міжнародним банком реконструкції та розвитку: Україна, МБРР; Угода, Міжнародний документ, Опис від 22.12.2022. URL: https://zakon.rada.gov.ua/laws/show/996_002-22#Text (дата звернення: 04.09.2023).
7. Про утворення Робочої групи з питань розробки та реалізації Концепції стратегічних напрямів розвитку кібербезпеки у сфері електронної охорони здоров'я: МОЗ України; Наказ, Склад колегіального органу, Положення від 15.06.2022 № 1034. URL: https://zakon.rada.gov.ua/rada/show/v1034282-22#Text (дата звернення: 04.09.2023).
8. Про затвердження Протоколу кризових комунікацій під час реагування на кібератаки та кіберінциденти: Наказ МОЗ України від 06.12.2023 № 2076. URL: https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid-06122023--2076-pro-zatverdzhennja-protokolu-krizovih-komunikacij-pid-chas-reaguvannja-na-kiberataki-ta-kiberincidenti (дата звернення: 04.09.2023).
9. Розроблено рекомендації щодо кіберзахисту закладів охорони здоров'я. Міністерство охорони здоров'я України. 2023. URL: https://moz.gov.ua/article/news/rozrobleno-rekomendacii-schodo-kiberzahistu-zakladiv-ohoroni-zdorov%e2%80%99ja (дата звернення: 04.09.2023).

References

1. Trofymenko, O. & Dubovyi, Ya. &Lohinova, N. & Prokop, Yu. & Zadereiko, O. (2021). Pytannia kiberbezpeky medychnykh kompiuternykh system [Issues of cyber security of medical computer systems]. *Zakhyst informatsii – Protection of information*, *23(1),* 30-39 [in Ukrainian].
2. Volynets, I. (2019). Kiberzlochynnist u sferi okhorony zdorovia: realnist, shcho potrebuie zakhystu [Cybercrime in the sphere of health care: a reality that needs protection]. *Teoriia i praktyka intelektualnoi vlasnosti – Theory and practice of intellectual property, 3*, 113-122 [in Ukrainian].
3. Strielkina, A.A. & Uzun, D.D. (2017). Zabezpechennia kiberbezpeky medychnykh system: vyklyky i rishennia v konteksti Internetu rechei [Ensuring cybersecurity of medical systems: challenges and solutions in the context of the Internet of Things]. *Radioelektronni i kompiuterni systemy Radioelectronic and computer systems, 1*, 44-50 [in Ukrainian].
4. Koval, B. & Koval, L. & Poida, S. (2023). Navchannia maibutnikh likariv osnovam mediahramotnosti ta kiberbezpeky [Teaching future doctors the basics of media literacy and cyber security]. *Perspektyvy ta innovatsii nauky – Perspectives and innovations of science, 8(26*), 171-183 [in Ukrainian].

5. Pro skhvalennia Kontseptsii rozvytku elektronnoi okhorony zdorovia: Rozporiadzhennia Kabinetu Ministriv Ukrainy [On the approval of the Concept of the development of electronic health care: Decree of the Cabinet of Ministers of Ukraine]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text [in Ukrainian].
6. Uhoda pro pozyku (Proekt «Zmitsnennia systemy okhorony zdorovia ta zberezhennia zhyttia» (Heal Ukraine)) mizh Ukrainoiu ta Mizhnarodnym bankom rekonstruktsii ta rozvytku: Ukraina, MBRR; Uhoda, Mizhnarodnyi dokument, Opys vid 22.12.2022 [Loan Agreement (Project "Strengthening the Health Care and Life Saving System" (Heal Ukraine)) between Ukraine and the International Bank for Reconstruction and Development: Ukraine, IBRD; Agreement, International document, Description dated 12.22.2022]. *zakon.rada.gov.ua.* https://zakon.rada.gov.ua/laws/show/996_002-22#Text [in Ukrainian].
7. Pro utvorennia Robochoi hrupy z pytan rozrobky ta realizatsii Kontseptsii stratehichnykh napriamiv rozvytku kiberbezpeky u sferi elektronnoi okhorony zdorovia: MOZ Ukrainy; Nakaz, Sklad kolehialnoho orhanu, Polozhennia vid 15.06.2022 № 1034 [On the formation of the Working Group on the development and implementation of the Concept of strategic directions for the development of cyber security in the field of electronic health care: Ministry of Health of Ukraine; Order, Composition of the collegial body, Regulation dated 15.06.2022 № 1034]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/rada/show/v1034282-22#Text [in Ukrainian].
8. Pro zatverdzhennia Protokolu kryzovykh komunikatsii pid chas reahuvannia na kiberataky ta kiberintsydenty: Nakaz MOZ Ukrainy vid 06.12.2023 № 2076 [On the approval of the Crisis Communications Protocol when responding to cyber attacks and cyber incidents: Order of the Ministry of Health of Ukraine dated 06.12.2023 № 2076]. *moz.gov.ua.* Retrieved from https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid-06122023--2076-pro-zatverdzhennja-protokolu-krizovih-komunikacij-pid-chas-reaguvannja-na-kiberataki-ta-kiberincidenti [in Ukrainian].
9. Rozrobleno rekomendatsii shchodo kiberzakhystu zakladiv okhorony zdorovia. Ministerstvo okhorony zdorovia Ukrainy [Recommendations for cyber protection of health care facilities have been developed. Ministry of Health of Ukraine]. *moz.gov.ua.* Retrieved from https://moz.gov.ua/article/news/rozrobleno-rekomendacii-schodo-kiberzahistu-zakladiv-ohoroni-zdorov%e2%80%99ja [in Ukrainian].

Подано до редакції 27.11.2023 р.
Прийнято до друку 22.12.2023 р.