Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2023. № 4.

DOI: http://doi.org/10.32702/2307-2156.2023.4.10

УДК 004.05+61

Т. В. Підлісна,

к. держ. упр., доцент,

доцент кафедри публічного управління та адміністрування,

Хмельницький університет управління та права імені Леоніда Юзькова

ORCID ID: https://orcid.org/0000-0002-7492-923X

ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: ПРОБЛЕМИ В УМОВАХ ВІЙСЬКОВИХ КОНФЛІКТІВ

T. Pidlisna,

PhD in Public Administration, Associate Professor, Associate Professor of the Department of Public Administration and Management, Leonid Yuzkov Khmelnytskyi University of Management and Law

INFORMATION SECURITY IN HEALTHCARE: PROBLEMS IN THE CONDITIONS OF MILITARY CONFLICTS

Інформаційна безпека у сфері охорони здоров'я є важливою в будь-який час, але заходи з її підтримки є особливо актуальними в умовах військових *конфліктів, за яких зростають ризики порушення цілісності даних, що пов'язані з медичною інформацією, тобто їх повною або частковою втратою, пошкодженням або зміною внаслідок технічних помилок або зловмисних дій. Звернено увагу на те, що, якщо чутлива інформація стане доступною для непов'язаних з цим осіб або сторонніх організацій, це може призвести до серйозних наслідків для пацієнтів, таких як витік особистих даних, шантаж,*

дискримінація або навіть ставлення до них з певними упередженнями. Відповідно до вищенаведеного, метою статті є визначення базових проблем інформаційної безпеки у сфері охорони здоров'я, які виникають в умовах військових конфліктів. Звернено увагу на той факт, що умови воєнного стану та військових конфліктів не тільки підвищують цінність медичної інформації, але й послабляють захищеність інформаційних систем медичної інформації. За результатами дослідження констатовано, що проблеми інформаційної безпеки в сфері охорони здоров'я формуються за наступними зонами: формування передумов для несанкціонованого доступу до медичної інформації або пошкодження цієї системи внаслідок успішних кібератак; втрати або тимчасового блокування доступу до даних внаслідок відключення інформаційних систем медичної інформації від електромережі або інтернету (що стосується медичної інформації, яка зберігається в електронному вигляді); обмеження доступу до медичної допомоги; невідновлювальна втрата медичної інформації; обмеження зберігання медичної інформації. Звернено увагу на той факт, що зони проблем інформаційної безпеки у сфері охорони здоров'я досить типові для більшості інформаційних систем через те, що інформація про пацієнтів є цінним ресурсом. В інформаційних системах охорони здоров'я зазвичай є складні функціональні інтегровані з іншими системами, що робить їх більш вразливими до кібератак. Відтак, в умовах воєнних дій проблеми інформаційної безпеки у сфері охорони здоров'я можуть бути ще більш підсилені.

Information security in healthcare is important at all times, but measures to support it are particularly relevant in times of war, during which the risk of data integrity violations related to medical information, such as complete or partial loss, damage, or alteration, due to technical errors or malicious actions, can lead to a decrease in the effectiveness and timeliness of medical assistance. Additionally, if sensitive information becomes available to unrelated parties or third-party organizations, it can have serious consequences for patients, such as personal data leaks, blackmail, discrimination, or even biased treatment. Accordingly, the purpose of this article is to identify basic information security problems in the healthcare sector that arise in times of war and military conflicts. The author emphasizes the fact that conditions of war and military conflicts not only increase the value of medical information but also weaken the protection of medical information systems. Based on the research results, it was found that information security issues in the

healthcare sector are formed in the following areas: creating prerequisites for unauthorized access to medical information or damaging the system due to successful cyberattacks; loss or temporary blocking of access to data due to disconnection of healthcare information systems from the power grid or the internet (which only applies to medical information stored in electronic form); restriction of access to medical care; irretrievable loss of medical information; and limitation of medical information storage. The author draws attention to the fact that the areas of information security problems in healthcare are quite typical for most information systems, due to the fact that patient information is a valuable resource, healthcare information systems are usually complex, functional, and integrated with other systems, making them more vulnerable to cyberattacks. Therefore, in conditions of military action, information security issues in healthcare may be even more intensified. The prospects for further research in this direction lie in the use of the obtained data to develop more effective methods for protecting information systems in the healthcare sector in conditions of wartime and military conflicts.

***Ключові слова**: технічні помилки; зловмисні дії; медична інформація; дані про пацієнтів; інформаційні системи медичної інформації.*

***Keywords:** technical errors, malicious actions, medical information, patient data, healthcare information systems.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Інформаційна безпека у сфері охорони здоров’я є важливою в будь-який час, але заходи з її підтримки є набувають особливої значущості в умовах військових конфліктів, за яких зростають ризики порушення цілісності даних, що пов’язані з медичною інформацією (зокрема, такі, що містять комплексні дані про пацієнтів, про стан їх здоров’я, діагнози, результати тестів та інші чутливі дані), тобто їх повною або частковою втратою, пошкодженням або зміною, внаслідок технічних помилок або зловмисних дій. Якщо чутлива інформація стане доступною для непов'язаних з цим осіб або сторонніх організацій, це може призвести до серйозних наслідків для пацієнтів, таких як: витік особистих даних; шантаж; дискримінація або навіть ставлення до них з певними упередженнями. Відтак пріоритетними є не лише заходи, спрямовані на забезпечення конфіденційності,

цілісності та доступності медичної інформації у медичному забезпеченні військ, але і в у медичному забезпеченні населення (адже під час конфлікту доступ до медичної допомоги може бути обмежений або навіть неможливий в районах де йдуть активні військові дії). Надзвичайна ситуація завжди стає каталізатором зростання числа травм та захворювань, що потребують негайного лікування.

Аналіз останніх досліджень і публікацій. Серед досліджень і публікацій в яких започатковано визначення базових проблем інформаційної безпеки у сфері охорони здоров'я можна виділити розробки Ясінської Я. О. Куперштейна Л. М. [5] (якими досліджено етапи побудови політики інформаційної безпеки медичних закладів, проаналізовано кожен етап та визначено проблеми такої безпеки із врахуванням вітчизняних реалій) та Дюжева Д.В. [1] (яким конкретизовано актуальні питання забезпечення медичних прав людини в умовах конфлікту на сході України). Саме на ці праці спирається автор для виділення не вирішених раніше частин загальної проблеми визначення базових проблем інформаційної безпеки у сфері охорони здоров'я, які виникають в умовах військових конфліктів, котрим присвячується означена стаття.

Формулювання цілей статті (постановка завдання). Відповідно до вищенаведеного, метою статті є визначення базових проблем інформаційної безпеки у сфері охорони здоров'я, які виникають в умовах військових конфліктів.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Сфера охорони здоров'я - це галузь діяльності, пов'язана зі збереженням та покращенням здоров'я людей, яка охоплює медичні послуги, дослідження та розробку нових методів лікування та профілактики захворювань, а також дії, спрямовані на збереження здорового способу життя та запобігання захворюванням. В окресленій сфері циркулює не лише інформація щодо стану здоров'я людини, але інша інформація, яка стосується збереження або відновлення здоров'я, а саме та, що мітиться в [2; 5]: медичних записах, у звітах про стан здоров'я; призначеннях та у змісті

лікарських рецептів; інших даних, які збираються та зберігаються в процесі медичного обслуговування пацієнта.

Отже, наведена інформація узагальнює дані про стан здоров'я людини, які потенційно можуть бути використані зловмисниками для шахрайства, зокрема, для відкриття нових кредитних рахунків або отримання кредитів на ім'я пацієнтів, а також для перепродажу інформації компаніям страхування, рекламодавцям та іншим сторонам, для шантажу та інших злочинів. Враховуючи цінність медичних даних, вони є об’єктом особливого інтересу для зловмисників та сторонніх організацій, які зацікавлені у відстеженні або отриманні доступу до таких даних. Чисельні випадки викрадання медичної інформації, що мали місце в різних країнах, підтверджують цю проблему.

Наприклад, у 2015 р. в США було викрадено медичну інформацію близько 80 млн. пацієнтів з компанії Anthem Inc. Ця крадіжка призвела до витоку особистої інформації про пацієнтів, включаючи їх ім'я, адресу, дату народження, СНІЛС та медичну інформацію [4]. В 2017 р. в Великобританії було викрадено медичну інформацію близько 150 тис. пацієнтів з компанії Bupa (яка надає послуги зі страхування та медичного обслуговування). У результаті цієї крадіжки, зловмисники отримали доступ до імені, дати народження, адреси та іншої особистої інформації про пацієнтів [4]. У 2018 р. в Сінгапурі було викрадено медичну інформацію більше 1,5 млн. пацієнтів з Національного університетського госпіталю (який надає різноманітні медичні послуги та є академічним центром зі спеціалізацією на медичних дослідженнях і освіті). У результаті цієї крадіжки зловмисники отримали доступ до особистої інформації про пацієнтів, включаючи їх ім'я, адресу, дату народження та медичну інформацію [4]. Ці приклади демонструють, що медична інформація є дуже цінною, підкреслюють важливість її захисту та необхідність зміцнення безпеки в галузі охорони здоров'я.

Враховуючи специфічний характер медичної інформації, яка зберігається в базах даних сфери охорони здоров’я, інформаційна безпека інтерпретована автором як категорія, що охоплює заходи та процедури, спрямовані на

забезпечення захисту конфіденційності, цілісності та доступності будь-якої інформації, щодо здоров'я людини та її медичного обслуговування [5].

Констатуємо, що інформаційна безпека у сфері охорони здоров’я особлива актуальна для країн, які перебувають у стані військових конфліктів, адже в таких країнах можливі не тільки крадіжки, тимчасові блокування доступу до медичної інформації, але і її повна втрата. Це підтверджують чисельні приклади. Зокрема, найбільш ілюстративним прикладом є Сирія, де військовий конфлікт розпочався 15 березня 2011 р. з демонстрацій, які були частиною Арабської весни. Після цього конфлікт переріс у повстання та громадянську війну у яку втрутилися треті країни, серед яких РФ. Потрапивши до зони бойових дій велика кількість медичних закладів Сирії була зруйнована, медичний персонал був примусово виселений або заарештований [4]. У таких умовах інформаційна безпека у сфері охорони здоров’я країни стала особливо складною. Часто медична інформація ставала об’єктом викрадення або втрати. Багато пацієнтів було змушено переїжджати до інших регіонів країни або за її межі, втрачаючи доступ до своїх медичних записів. Іншим інформативним прикладом є Ізраїль. Зазначимо, що це країна, яка перебуває у стані війни з сусідніми країнами протягом багатьох років, тому вже мала проблему порушення безпеки медичних даних. Одним з прикладів втрати медичних даних було те, що сталося внаслідок війни Ізраїлю з Ліваном у 2006 р. Під час цього конфлікту були пошкоджені медичні заклади в містах Нацерет-Іліт та Хайфа та дата центри, в яких зберігалися медичні дані. Ці медичні заклади втратили доступ до електронної медичної інформації та до паперових медичних карток, що своєю чергою призвело до значного ускладнення процесу надання медичної допомоги. Зокрема, одним з медичних центрів, що був бомбардований та зазнав значних пошкоджень в цей час - найбільший та найважливіший медичний заклад Rambam (який надає медичні послуги населенню північної частини країни) [4]. Інший приклад втрати медичних даних відбувся у 2014 р., коли війна між Ізраїлем та ХАМАСом призвела до руйнування ряду медичних шпиталів в місті Єрусалим, а також їх дата центру [4]. Це спричинило втрату великої кількості медичних даних, що призвело до

серйозних проблем у наданні медичної допомоги та відновленні медичного обліку.

Наразі інформаційна безпека у сфері охорони здоров’я особливо актуальна і для України, оскільки 24 лютого 2022 р. Російські регулярні війська атакували кордони України в областях, які межують з РФ, Білоруссю та в околицях терористичних угрупувань Придністров'я, ОРДЛО. У відповідь в Україні запровадили воєнний стан по всій підконтрольній Україні території. В таких умовах наша країна зберегла інформаційну безпеку у сфері охорони здоров’я, адже до цього це питання вже загострила війна на сході України, розпочата російськими загонами, які вторглися у квітні 2014 року на території української частини Донбасу (після захоплення Російською Федерацією Криму). При цьому актуалізація питання захисту медичних даних хоча і зумовлена факторами, що докорінно відрізняються від інших країн, що у той чи інший час перебували або перебувають у зоні конфлікту, однак в усіх випадках умови військових конфліктів створюють типові проблеми у сфері, що і досліджується автором.

Умови військових конфліктів не тільки підвищують цінність медичної інформації, але й послабляють захищеність інформаційних систем медичної інформації. Проблематика інформаційної безпеки у сфері охорони здоров’я формується за наступними зонами: формування передумов для несанкціонованого доступу до медичної інформації; втрата або тимчасове блокування доступу до даних; формування передумов для обмеження доступу до медичної допомоги; формування передумов для невідновлювальної втрати медичної інформації; формування передумов для обмеження зберігання медичної інформації. Узагальнення окреслених проблем інформаційної безпеки у сфері охорони здоров’я може сприяти системному погляду на них в умовах військових конфліктів, що рекомендується реалізовувати за даними рис. 1.

Це означає, що для вирішення цих проблем потрібно не просто реагувати на окремі інциденти, а досліджувати їх системно, з урахуванням усіх можливих чинників, які можуть вплинути на безпеку медичної інформації. Відмітимо, що такий погляд дозволяє не лише виявляти кореневі причини проблем

інформаційної безпеки, але й розробляти схеми їх вирішення, забезпечуючи високий рівень захисту медичної інформації в умовах воєнних дій. Цей процес включає наступні етапи: 1) аналіз ризиків та вразливостей інформаційної системи закладів охорони здоров'я в умовах воєнного стану; 2) розробка та впровадження заходів щодо мінімізації ризиків та вразливостей; 3) поточний контроль та моніторинг інформаційної системи закладів охорони здоров'я з метою виявлення аномальних дій та несанкціонованого доступу до медичної інформації.

Рис. 1. Системний погляд на проблематику інформаційної безпеки в сфері охорони здоров'я в умовах військових конфліктів

Джерело: сформовано автором на основі [5; 3; 1]

Так, серед ризиків та вразливостей інформаційної безпеки закладів охорони здоров'я - можливість несанкціонованого доступу до медичної інформації або пошкодження цієї системи внаслідок успішних хакерських атак. Зокрема, за даними компанії Kaspersky (Kaspersky Security Bulletin: Тенденції кібербезпеки України за 2020 рік"), Національної поліції Україні та

PricewaterhouseCoopers [4] з 2014 по 2015 рр. (на які припав початок війни на сході України) та з 2022 по 2023 рр. (на які припав відкритий воєнний напад Росії на Україну) спостерігався значний приріст кількості хакерських атак на заклади охорони здоров'я (при чому як в районах бойових дій, так і поза ними), що здійснювалися з метою зламу захисту, незаконного доступу до конфіденційної інформації, викрадення даних. Один з найбільш відомих випадків такої атаки стався у 2017 р., коли вірус-шифрувальник Petya пошкодив інформаційні системи цілого ряду медичних закладів (серед яких, Київський міський клінічний онкологічний центр; Харківська міська лікарня № 17; Тернопільська обласна лікарня; Львівська міська дитяча клінічна лікарня № 1; Київська міська дитяча клінічна лікарня № 1; Львівська міська клінічна лікарня № 8; Київська міська клінічна лікарня № 9; Херсонська міська клінічна лікарня [4]). Petya заблокував доступ до медичних даних, що зумовило порушення роботи закладів (які працювали на скороченому режимі або повністю зупинили свою діяльність). Також, у 2017 р. була зареєстрована кібератака на Центральну клінічну лікарню МВС України у Києві, під час якої викрадено медичні дані пацієнтів [4]. Інший випадок стався у грудні 2019 р. та пов'язаний з хакерською атакою на міську лікарню № 1 у м. Чернівці, в результаті якої було викрадено медичні дані більш як 23 тисяч пацієнтів (їх особисті дані, результати лабораторних досліджень, діагнози, іншу конфіденційну медичну інформацію) [4]. Також, як приклад, можна навести випадок 2020 р., коли хакери вимагали викуп від лікарень в Україні в обмін на повернення доступу до заблокованих медичних даних [4]. Це стало загрозою для безпеки пацієнтів, оскільки в заблокованих даних могли міститися відомості про стан здоров’я пацієнтів, їх лікування та інші конфіденційні дані. Фактично саме окреслені атаки на інформаційні системи медичних закладів в Україні спричинили певні їх трансформації які дозволили захистити медичні дані після 24 лютого 2021 р. Ці трансформації були спрямовані на дії, що окреслені на рис. 2.

Зокрема, серед дій, які забезпечили мінімізацію передумов для несанкціонованого доступу до медичної інформації в Україні, були [4]: регулярні оновлення антивірусного та іншого програмного забезпечення

інформаційних систем медичних закладів; створення резервних копій медичних даних на зовнішні носії (такі як жорсткі диски, флеш-карти, або віртуальні диски); забезпечення їх захищеного зберігання; впровадження систем шифрування даних інформаційних систем медичних закладів (у різних медичних закладах можуть використовуватися різні системи шифрування даних, наприклад, AES (Advanced Encryption Standard), DES (Data Encryption Standard), або RSA (Rivest–Shamir–Adleman). Втім, для подальшого захисту від несанкціонованого доступу до медичної інформації в Україні в нових умовах, коли триває масштабна агресія Росії проти України, можна рекомендувати: впровадити обов'язкові аудити безпеки мереж та систем; використовувати захист від зламу та інших загроз; регулярно проводити навчання медичного та технічного персоналу медичних закладів з питань кібербезпеки.

Рис. 2. Дії, які забезпечили мінімізацію ризиків несанкціонованого доступу до медичної інформації в умовах військових конфліктів

Джерело: сформовано автором на основі [5; 4]

Серед ризиків інформаційної безпеки закладів охорони здоров’я – втрата або тимчасове блокування доступу до даних, внаслідок відключення інформаційних систем медичної інформації від електромережі або інтернету (стосується медичної інформації, яка зберігається в електронному вигляді). Зокрема, ця проблема стала очевидною коли масовані ракетні удари РФ по енергетичних об’єктах завершувалися блекаутами (чисельні ТЕС та ГЕС були пошкоджені й перестали видавати електроенергію), за яких був неможливий доступ до важливої медичної інформації. Як виявилося, для забезпечення інформаційної безпеки у сфері охорони здоров’я в умовах військових конфліктів необхідно реалізувати дії, що окреслені на рис. 3.

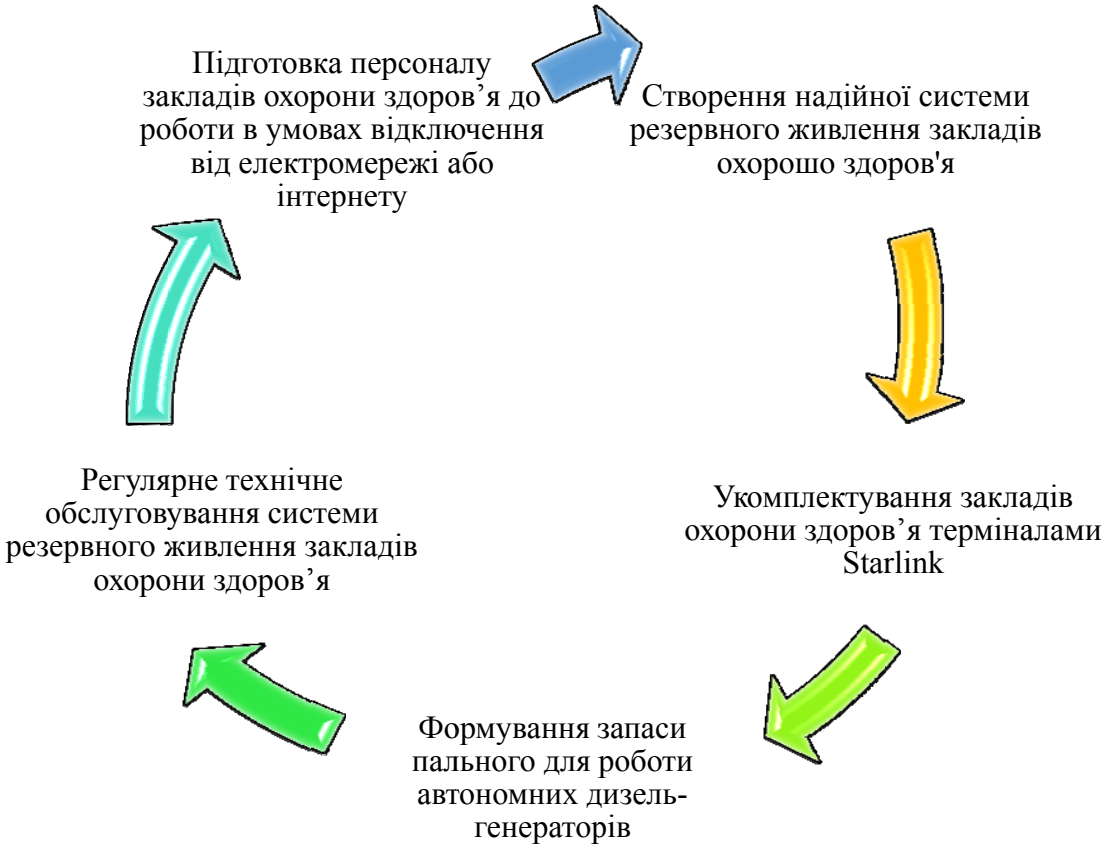

Рис. 3. Дії які забезпечують мінімізацію ризиків втрати або тимчасового блокування доступу до медичних даних в умовах військових конфліктів

Джерело: сформовано автором на основі [5; 4].

Зокрема, серед таких дій: створення надійної системи резервного живлення, яка забезпечать неперервну роботу інформаційної системи медичної

інформації (може містити генератори електроструму, акумуляторні батареї, інвертори, автоматичні перемикачі, системи стабілізації напруги та інші елементи); укомплектування закладів охорони здоров’я терміналами Starlink (щоб вони могли працювати й з електронною системою охорони здоров’я та мали доступ до Інтернету); формування запасів пального для роботи автономних дизель-генераторів, які можуть бути використані у випадку відключення електропостачання; регулярне технічне обслуговування системи резервного живлення закладів охорони здоров’я; підготовка персоналу закладів охорони здоров’я до роботи в умовах відключення від електромережі або інтернету.

Відтак, щоб уникнути втрати або тимчасового блокування доступу до даних в таких умовах кожен вітчизняний медичний заклад був змушений перелаштувати свою інформаційну систему та бути готовим до роботи в умовах повного блекауту, шляхом забезпеченості альтернативними джерелами живлення. Наразі понад 3 тис. генераторів уже працюють у закладах, і Міністерство охорони здоров'я України продовжує закупівлі й постачання додаткових генераторів у лікарні [4]. Крім того, Українським медичним закладам та установам у сфері охорони здоров’я було передано 590 станцій супутникового інтернету StarLink американської компанії SpaceX, завдяки яким вони мають безперебійний доступ до супутникового інтернету [4]. Також в українських закладах охорони здоров’я сформовано 5-добовий запас пального для роботи автономних дизель-генераторів [4].

Серед ризиків та вразливостей інформаційної безпеки закладів охорони здоров’я - обмеження доступу до медичної допомоги. Умови воєнного стану можуть призвести до обмеження доступу до медичної допомоги через ускладнений обмін медичною інформацією між лікарями, що перебувають у зоні бойових дій (які надають допомогу на передовій лінії) та за її межами. На прикладі України та інших країн, що перебували або перебувають у зоні конфлікту, очевидно, що повноцінний доступ до медичних даних з зони бойових дій неможливий через ризик витоку конфіденційних даних для

прискореної ідентифікації пацієнта, які є особливо цінними для іншої сторони конфлікту [4].

Відтак, наприклад, вітчизняні лікарі на місці мають лише обмежений доступ до інформації про пацієнта, що затримує надання необхідної медичної допомоги та впливає на її ефективність. Для полегшення процесу доступу до медичних записів та інших даних про пацієнтів можна використовувати спеціальні рішення, такі як чіп з зашифрованими медичними даними для пацієнтів та використання децентралізованих мереж для зберігання медичної інформації. Цей чіп містить інформацію про стан здоров'я пацієнта, його медичну історію, результати діагностичних тестів та інші дані, які можуть бути корисними для лікарів. За допомогою спеціального зчитувача, який може бути підключений до смартфона або комп'ютера лікаря, цю інформацію можна швидко та безпечно передавати з одного пристрою на інший з використанням децентралізованих мереж. Ідея з використанням чіпів для зберігання медичної інформації для пацієнтів в умовах війни є досить новою, але вже є приклади її застосування в Ізраїлі, де триває збройний конфлікт [4]. Зокрема, у 2014 році в цій країні запроваджена національна ініціатива з використання електронних медичних записів, яка передбачала створення електронного медичного досьє громадянина на захищеному чіпі, що розміщувався на браслеті. Така ініціатива може бути адаптована для доступу до медичних записів та інших даних про пацієнтів в зонах бойових дій Україні.

Серед інших ризиків та вразливостей інформаційної безпеки закладів охорони здоров'я можна відмітити руйнування медичних установ та пов'язану з цим невідновлювальну втрату медичної інформації пацієнтів (яка може спричинити важкі наслідки для здоров'я пацієнтів та ускладнити процес надання медичної допомоги). Наприклад, після повномасштабного вторгнення Росії в Україну медична інфраструктура України суттєво постраждала. Зокрема 1218 закладів охорони здоров'я зазнали пошкодження, при цьому 540 лікарень – зруйновані частково, а 173 – повністю із втратою медичної інформації, яку неможливо відновити [4]. Найбільших

руйнувань через активні бойові дії зазнали медичні заклади Харківської області, у Донецьку, Луганську, Миколаєві та Херсоні [4].

Повна втрата медичної інформації особливо загрозлива в тих випадках, коли пацієнти потребують довготривалого лікування або спостереження, а саме для пацієнтів з онкологічними захворюваннями, з хронічними захворюваннями, які потребують постійної медичної допомоги та контролю. Ця проблема може бути знята, якщо Міністерство охорони здоров'я України запровадить обов'язкові електронні картки для пацієнтів в Електронній системі охорони здоров'я (далі - ЕСОЗ), в яких буде зібрана вся медична інформація про нього. Наразі до ініціативи долучилися лише комунальні медичні заклади (якими до ЕСОЗ вже внесені 700 млн медичних записів), однак приватні клініки також мають зобов'язані вносити дані про пацієнта в єдину базу [4]. Таким чином, вся медична інформація про пацієнта буде зберігатися в електронній медичній картці, доступ до якої буде мати як пацієнт, так і лікарі різних закладів. При цьому важливо розглянути можливість застосування новітніх технологій, таких як штучний інтелект і блокчейн, для забезпечення безпеки медичної інформації ЕСОЗ.

Іншим ризиком для інформаційної безпеки закладів охорони здоров'я є обмеження зберігання медичної інформації. Може бути важко забезпечити безпеку даних в умовах війни. Це зумовлено цілою низкою факторів, серед яких: підвищений ризик руйнування вітчизняних дата-центрів, які обслуговують заклади сфери охорони здоров'я; підвищений ризик втрати електронних баз даних та засобів зберігання інформації в результаті руйнування медичних установ, комп'ютерних систем, переривання комунікаційних ліній та інших факторів. Перехід на закордонні дата-центри може бути одним зі засобів зменшення ризиків втрати медичної інформації в умовах військових конфліктів (хоча це вимагає додаткових витрат на оренду простору на серверах, підтримку зв'язку з цими серверами та виконання інших юридичних вимог). Закордонні дата-центри можуть бути розташовані в країнах з вищим рівнем безпеки даних та більш стійкою інфраструктурою, що може допомогти забезпечити безпеку даних, що зберігаються на цих серверах.

Крім того, необхідно забезпечити наявність резервних копій інформації (які можуть забезпечити відновлення даних у разі їх втрати або пошкодження) та їх зберігання у захищених приміщеннях (а саме таких, що розташовані в бомбосховищах, підземних сховищах, тунелях та інших місцях з підвищеною стійкістю). В Україні існують компанії, які надають послуги зберігання електронної медичної інформації у вітчизняних дата центрах, але також можуть надати послуги зберігання на закордонних серверах. Наприклад, компанія "Інтернет Клініка" має партнерство з дата центрами у Німеччині та Швейцарії, та пропонує можливість зберігання даних у захищених приміщеннях з підвищеною стійкістю. Також, в Україні є компанії, які спеціалізуються на створенні резервних копій інформації для систем електронної медичної інформації з можливістю паралельного зберігання на кількох закордонних серверах, наприклад "MedHub" та "Med-IT".

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Констатовано, що умови військових конфліктів не тільки підвищують цінність медичної інформації, але й послабляють захищеність інформаційних систем медичної інформації. За результатами дослідження констатовано, що:

- Проблематика інформаційної безпеки у сфері охорони здоров’я формується за наступними зонами: формування передумов для несанкціонованого доступу до медичної інформації або пошкодження цієї системи внаслідок успішних кібератак; формування передумов для втрати або тимчасового блокування доступу до медичних даних внаслідок відключення інформаційних систем медичної інформації від електромережі або інтернету (що стосується медичної інформації, яка зберігається в електронному вигляді); формування передумов для обмеження доступу до медичної допомоги; формування передумов для невідновлювальної втрати медичної інформації; формування передумов для обмеження зберігання медичної інформації.
- Зони проблем інформаційної безпеки у сфері охорони здоров’я є досить типовими для більшості інформаційних систем через деякі загальні причини. По-перше, інформація про пацієнтів (медичні діагнози, результати

аналізів, рецепти індивідуальної медичної допомоги) є цінним ресурсом, який може бути використаний стороною конфлікту для швидкої ідентифікації особи. По-друге, інформаційні системи охорони здоров'я зазвичай є складними, функціональними й інтегрованими з іншими системами, що робить їх більш вразливими до кібератак. Відтак, в умовах військових конфліктів проблеми інформаційної безпеки у сфері охорони здоров'я можуть бути ще більш підсилені.

Перспективи подальших розвідок у даному напрямі полягають у використанні отриманих даних для розробки більш ефективних методів захисту інформаційних систем в галузі охорони здоров'я в умовах військових конфліктів. Необхідно проводити детальніші дослідження, щоб визначити конкретні загрози та вразливості медичних інформаційних систем і розробити відповідні стратегії захисту.

Література

1. Дюжев Д. В. Актуальні питання забезпечення медичних прав людини в умовах конфлікту на сході України", Матеріали Всеукраїнської наукової конференції "Українство : динаміка сенсів і вимірів національного буття". Донецький юридичний інститут МВС України, м. Кривий Ріг, 08.11.2019 р., - с. 208 - 212.
2. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця: ВНТУ, 2013. 221 с.
3. Миколайчук Б. Ваші діагнози в їхніх руках: що електронні медсервіси роблять з даними і чим це загрожує, Центр демократії та верховенства права, 2022, URL.: https://cedem.org.ua/analytics/elektronni-medservisy/
4. PricewaterhouseCoopers database (2023) PwC report "Experience of information security in the healthcare sector of countries during military state and military conflicts.", URL.: https://www.pwc.com/content/pwc/userReg/login.en_gx.html?redirectUrl=gG0V-55Ilpsw21J2UMYgbIH5ktcJLK2-lwWPau2GN84=&referrer=gG0V-55Ilpsw21J2UMYgbIH5ktcJLK2lwWPau2GN84=&parentPagePath=/content/pwc/gx/en (Accessed: 01.10.2022).

5. Ясінська Я. О. Куперштейн Л. М. Розробка політики інформаційної безпеки медичного закладу, Матеріали Молодь в науці: дослідження, проблеми, перспективи, 2021, URL.: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/31280/%d0%a2%d0%b5%d0%b7%d0%b8_%d0%af%d1%81%d1%96%d0%bd%d1%81%d1%8c%d0%ba%d0%b0.pdf?sequence=1&isAllowed=y

References

1. Dyuzhev, D. V. (2019), “Current issues of ensuring human medical rights in the conditions of the conflict in eastern Ukraine", *Zbirka dopovidej na Vseukrayins’kiy naukoviy konferentsiyi* [Conference "Ukrainianism: the dynamics of meanings and dimensions of national existence"], Donetsk Law Institute of the Ministry of Internal Affairs of Ukraine, Ukraine, pp. 208 - 212.

2. Luzhetsky, V.A., Kozhukhivskyi, A.D. and Voytovych, O.P. (2013), Osnovy informatsiynoyi bezpeky [Basics of information security], VNTU, Vinnytsia, Ukraine

3. Mykolaichuk, B. (2022), “Your diagnoses are in their hands: what electronic medical services do with data and what threatens it”, Tsentr demokratiyi ta verkhovenstva prava, available at.: https://cedem.org.ua/analytics/elektronni-medservisy/ (Accessed 05 April 2023).

4. PricewaterhouseCoopers database (2023), PwC report “Experience of information security in the healthcare sector of countries during military state and military conflicts.”, available at.: https://www.pwc.com/content/pwc/userReg/login.en_gx.html?redirectUrl=gG0V-55Ilpsw21J2UMYgbIH5ktcJLK2-lwWPau2GN84=&referrer=gG0V-55Ilpsw21J2UMYgbIH5ktcJLK2lwWPau2GN84=&parentPagePath=/content/pwc/gx/en (Accessed: 01.10.2022).

5. Yasinska, Ya.O. and Kupershtein, L.M. (2021), “Development of information security policy of a medical institution”, *Zbirka dopovidej na Vseukrayins’kiy naukoviy konferentsiyi* [Conference "Youth in science: research, problems, prospects], Available at.: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/31280/%d0%a2%d0%b5%d0%b7%d0%b8_%d0%af%d1%81%d1%96%d0%bd%d1%81%d1%8c%d0%ba%d0%b0.pdf?sequence=1&isAllowed=y (Accessed 05 April 2023).

Стаття надійшла до редакції 19.04.2023 р.