УДК *614.2:004.056.53*
DOI *10.31673/2786-7412.2026.025816*

Артем ЛЯШУК
аспірант кафедри публічного управління, адміністрування та соціальної роботи
Національного університету охорони здоров'я України імені П.Л. Шупика
ORCID ID: 0000-0002-4206-3929

Artem LIASHUK
Graduate student of the Department of Public Management,
Administration and Social Work, Shupyk National Healthcare University of Ukraine
ORCID ID: 0000-0002-4206-3929

ГЛОБАЛЬНІ ТЕНДЕНЦІЇ КІБЕРЗАГРОЗ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

GLOBAL TRENDS IN CYBER THREATS IN THE HEALTHCARE SECTOR

Анотація. *У статті розкрито особливості сучасних кіберзагроз у сфері охорони здоров'я в умовах активної цифрової трансформації галузі та зростання обсягів обробки чутливих даних. Встановлено, що інтеграція інформаційно-комунікаційних технологій у медичні процеси сприяє розширенню спектра вразливостей і формуванню нових векторів атак. З'ясовано, що кіберзагрози трансформуються з поодиноких інцидентів у комплексні складні явища, які охоплюють технічні та поведінкові аспекти безпеки. Наголошено, що посилення цифровізації медичних систем супроводжується зростанням залежності від стабільності інформаційної інфраструктури. Підкреслено, що геополітичні чинники, вразливості ланцюгів постачання та використання сторонніх сервісів ускладнюють забезпечення кіберстійкості галузі. Констатовано стійку тенденцію до зростання кількості кіберінцидентів у сфері охорони здоров'я, що підтверджується статистичними даними.*

Визначено, що збільшення обсягів витоків даних обумовлено високою цінністю медичної інформації та тривалістю її нелегального використання. Зауважено, що кіберзловмисники щоразу активніше орієнтуються на систематичний збір і монетизацію персоналізованих медичних даних. Обґрунтовано, що фінансові наслідки кібератак мають тенденцію до зростання, що проявляється у підвищенні вартості відновлення інформаційних систем після інцидентів.

Встановлено, що атаки програм-вимагачів залишаються домінуючим видом кіберзагроз у медичній сфері. Підтверджено, що ускладнення цифрових платформ сприяє поширенню багаторівневих атак, включаючи експлуатацію вразливостей вебзастосунків і міжсистемних комунікацій. З'ясовано, що поширення хмарних технологій та IoT-рішень формує додаткові ризики перехоплення та компрометації даних. Наголошено, що недостатній рівень фінансування кіберзахисту підвищує ймовірність реалізації загроз. Підкреслено, що ефективність протидії кіберзагрозам визначається рівнем інтеграції технічних і організаційних механізмів безпеки. Констатовано, що застосування криптографічних алгоритмів, зокрема AES-256, забезпечує високий рівень захисту

медичних даних. Визначено, що впровадження методів машинного навчання та штучного інтелекту підвищує ефективність виявлення кіберінцидентів.

Обґрунтовано доцільність формування комплексної стратегії кіберзахисту, яка передбачає міжінституційну взаємодію та підвищення обізнаності персоналу. Узагальнено, що забезпечення кібербезпеки у сфері охорони здоров'я потребує системного підходу, орієнтованого на підвищення стійкості інформаційних систем і безперервності надання медичних послуг.

Ключові слова: *кіберзагрози, кібербезпека, охорона здоров'я, медичні інформаційні системи, захист даних, витоки даних, програми-вимагачі, цифровізація, штучний інтелект, кіберстійкість.*

Abstract. *The article examines the features of contemporary cyber threats in the healthcare sector in the context of active digital transformation and the increasing volume of sensitive data processing. It is established that the integration of information and communication technologies into medical processes contributes to the expansion of vulnerabilities and the emergence of new attack vectors. Cyber threats are shown to be evolving from isolated incidents into complex, multifaceted phenomena encompassing both technical and behavioral aspects of security.*

It is emphasized that the intensification of healthcare digitalization is accompanied by growing dependence on the stability of information infrastructure. Geopolitical factors, supply chain vulnerabilities, and the use of third-party services are identified as factors complicating the achievement of cyber resilience in the sector. A steady increase in the number of cyber incidents in healthcare is confirmed by statistical data.

It is determined that the growth in data breaches is driven by the high value of medical information and the prolonged period of its illegal use. It is noted that cybercriminals are increasingly focusing on the systematic collection and monetization of personalized medical data. The financial impact of cyberattacks is shown to be rising, particularly due to the increasing cost of restoring information systems after incidents.

Ransomware attacks remain the dominant type of cyber threat in the healthcare sector. The growing complexity of digital platforms contributes to the proliferation of multi-layered attacks, including the exploitation of vulnerabilities in web applications and inter-system communications. The spread of cloud technologies and IoT solutions creates additional risks of data interception and compromise.

It is highlighted that insufficient funding for cybersecurity increases the likelihood of threat realization. The effectiveness of countering cyber threats is determined by the level of integration of technical and organizational security mechanisms. The use of cryptographic algorithms, particularly AES-256, ensures a high level of protection of medical data. The implementation of machine learning and artificial intelligence methods enhances the effectiveness of cyber incident detection.

The study substantiates the need for a comprehensive cybersecurity strategy that includes inter-institutional cooperation and increased staff awareness. It is concluded that ensuring cybersecurity in the healthcare sector requires a systemic approach aimed at enhancing the resilience of information systems and ensuring the continuity of healthcare services.

Keywords: *cyber threats, cybersecurity, healthcare, medical information systems, data protection, data breaches, ransomware, digitalization, artificial intelligence, cyber resilience.*

Постановка проблеми. Цифрова трансформація системи охорони здоров'я зумовлює глибинні зміни в організації надання медичних послуг і управлінні інформаційними ресурсами. Інтеграція цифрових технологій, своєю чергою, підвищує залежність галузі від стабільного функціонування інформаційних систем. Відтак зростання інтенсивності кіберзагроз свідчить про наявність недосконалостей у механізмах державного регулювання у цій сфері. Відповідно виникає необхідність переосмислення механізмів до організації кіберзахисту, що стає об'єктивною вимогою розвитку галузі. Тому формування цілісної державної політики кібербезпеки у сфері охорони здоров'я постає пріоритетним напрямом реагування на сучасні виклики.

Аналіз останніх досліджень і публікацій. Науковий доробок сучасних дослідників у сфері кібербезпеки охорони здоров'я засвідчує комплексний характер кіберзагроз, їх динамічну еволюцію та необхідність поєднання організаційно-управлінських і технологічних механізмів для забезпечення захисту медичних систем і даних. Передусім Е. А. Аль-Карні у своєму дослідженні [1] узагальнює сучасні кіберзагрози у сфері охорони здоров'я та обґрунтовує необхідність комплексних стратегій їх мінімізації, акцентуючи увагу на зростанні масштабів атак і критичності захисту медичних даних. **С**. Лі, К. Сурінені та Н. Прабхакаран здійснюють наративний огляд кібератак на лікарняні системи та демонструють еволюцію їх форм і наслідків для функціонування медичних установ [2]. П. Евох та Т. Вартіайнен зосереджують увагу на вразливостях систем охорони здоров'я, обґрунтовуючи соціотехнічний характер кіберризиків і необхідність інтегрованих заходів для їх подолання [3]. М. Кларк та К. Мартін переходять до управлінського виміру проблеми, підкреслюючи важливість проактивного та колаборативного підходів до управління кіберризиками в медичних організаціях [4]. А. Кавіта, Б. С. Рао, Н. Ахтар, С. М. Рафі, П. Сінгх, С. Дас та Г. Манікандан пропонують прикладні технічні рішення, зокрема алгоритмічні інструменти для захисту даних у системах охорони здоров'я нового покоління на основі IoT-технологій [5].

Метою статті є аналіз кіберзагроз у сфері охорони здоров'я та обґрунтування способів до формування ефективної системи кіберзахисту з метою забезпечення безпеки даних і стійкості медичних інформаційних систем.

Виклад основного матеріалу. Зростання кількості кіберзагроз, спрямованих на лікарняні установи протягом останніх років, свідчить про наявність тривалої вразливості у функціонуванні сучасних систем охорони здоров'я, що, своє чергою, акцентує увагу на необхідності впровадження ефективніших та випереджувальних механізмів захисту. Відповідно з урахуванням поступового ускладнення характеру кіберзагроз, важливим напрямом розвитку стає модернізація технічних інструментів захисту, а також формування організаційної культури кібербезпеки, яка передбачає підвищення рівня обізнаності та готовності персоналу до реагування на інциденти [2].

В умовах цифровізації медичної сфери спостерігається розширення спектра потенційних кіберризиків, що обумовлюється інтеграцією інформаційно-комунікаційних технологій у клінічні та управлінські процеси. Тому інтенсивне впровадження телемедичних сервісів і підключених медичних пристроїв формує нові вектори атак, які поєднують технічні та поведінкові аспекти вразливостей. Наведене, своєю чергою, призводить до трансформації кіберзагроз із поодиноких

інцидентів у комплексні складні явища, що охоплюють інфраструктурні та людські чинники безпеки.

Посилення кіберзагроз у глобальній системі охорони здоров'я упродовж 2025 року відбувалося паралельно з розширенням цифрової трансформації клінічних, адміністративних та технологічних процесів, що суттєво ускладнило забезпечення кіберстійкості. При цьому активне використання телемедичних платформ, взаємопов'язаних медичних пристроїв і цифрових сервісів сприяло розширенню площини потенційних атак для медичних організацій, виробників обладнання та постачальників технологій. Геополітична нестабільність, ризики фізичної безпеки та вразливості ланцюгів постачання додатково ускладнювали діяльність управлінців у сфері охорони здоров'я, відповідальних за забезпечення безперервності надання послуг і безпеки пацієнтів. Також зауважимо, що програми-вимагачі, складні методи соціальної інженерії та компрометація третіх сторін залишалися пріоритетними загрозами, що відповідно актуалізує необхідність розроблення узгоджених стратегій захисту, підвищення рівня стійкості систем і посилення міжінституційної взаємодії в межах сектору охорони здоров'я [6].

Тому простежується тенденція до конвергенції кіберзагроз із ширшими безпековими викликами, що охоплюють цифровий та фізичний простір функціонування медичних систем. Відповідно формується нова парадигма безпеки, у якій кіберзахист розглядається як складова загальної стратегії стійкості галузі.

За даними Statista [7], упродовж періоду з листопада 2023 року по жовтень 2024 року у сфері охорони здоров'я було зафіксовано 1542 кіберінциденти, що супроводжувалися підтвердженою втратою даних. Водночас, відповідно до узагальнених статистичних спостережень за попередній часовий інтервал, а саме з листопада 2022 року по жовтень 2023 року, кількість подібних випадків становила 1378 атак [8], що, таким чином, відображає тенденцію до зростання інтенсивності кіберзагроз у зазначеній галузі.

Узагальнюючи наведені показники, доцільно відзначити, що динаміка кіберінцидентів у медичному секторі формується під впливом цифровізації медичних сервісів та зростання обсягів обробки чутливих даних. У цьому контексті простежується посилення зацікавленості зловмисників до інформаційних систем охорони здоров'я, оскільки вони містять значні масиви персоналізованої інформації, яка має високу комерційну цінність. Відтак зростання кількості атак відображає системні зміни у глобальному кіберпросторі.

Порушення безпеки даних у сфері охорони здоров'я демонструють тривалу та масштабну ескалацію. Так, у період з 2009 по 2025 рік було зафіксовано 7357 випадків витоку даних, що охоплювали щонайменше 500 осіб кожен, які були офіційно зареєстровані в OCR (Office for Civil Rights). Унаслідок цих інцидентів відбулося розголошення або несанкціоноване поширення захищеної медичної інформації щодо 935521931 особи, що еквівалентно більш ніж подвійному перевищенню чисельності населення Сполучених Штатів Америки [9].

Аналіз часових змін дозволяє встановити, що у 2018 році частота таких інцидентів становила приблизно один випадок на добу, натомість у 2023-2024 роках цей показник зріс більш ніж удвічі, перевищивши два випадки щоденно. Зокрема, у 2024 році середня кількість постраждалих осіб досягала 792226 на добу, що значною мірою було зумовлено масштабним витоком даних у системі Change

Healthcare, який охопив 192,7 мільйона осіб. Разом із тим, у 2025 році спостерігається певне зниження масштабів ураження, оскільки середньодобова кількість постраждалих зменшилася до 168647 осіб, що відповідає рівням 202102022 років [9].

У сфері охорони здоров'я спостерігається значно вищий рівень витоків даних порівняно з іншими галузями, що пояснюється підвищеною цінністю медичної інформації на нелегальних ринках. Це зумовлено тим, що процес виявлення шахрайських дій у медичному секторі є тривалішим, унаслідок чого викрадені дані можуть використовуватися протягом довшого періоду, тоді як, наприклад, компрометація платіжних карток оперативно ідентифікується та блокується. Тому підвищена тривалість експлуатації викрадених медичних даних формує додаткову мотивацію для кіберзловмисників.

Розгортання цифрових медичних екосистем супроводжується зростанням привабливості галузі як цілі для атак, оскільки інформаційні ресурси стають стратегічним активом. Відповідно простежується зміщення акцентів із одиничних інцидентів до систематичного збору медичних даних, що формує стійкі нелегальні ринки їх обігу. Представлена трансформація зумовлює необхідність переосмислення способів до кібербезпеки, адже захист має охоплювати технічні аспекти та економічні механізми протидії незаконному використанню інформації.

Ключове значення у протидії кіберзагрозам належить інвестиціям у розвиток безпекової інфраструктури медичних організацій, оскільки фінансове забезпечення заходів кіберзахисту визначає рівень їх ефективності. Безумовно недостатнє фінансування створює сприятливі умови для експлуатації наявних вразливостей, що, у підсумку, посилює ризики реалізації кіберзагроз та ускладнює забезпечення належного рівня захисту інформаційних ресурсів [3].

Нині у сфері охорони здоров'я ідентифікується широкий спектр кіберзагроз, серед яких вагоме місце посідають атаки на вебзастосунки, що спрямовані на використання вразливостей програмного коду на стороні клієнта, а також на стороні сервера. Зокрема, такі втручання забезпечують несанкціонований доступ до баз даних із персональною та фінансовою інформацією, а також створюють можливості для проникнення у внутрішню інфраструктуру організацій і порушення функціонування систем. Найбільш поширеними формами залишаються SQL-ін'єкції, міжсайтовий скриптинг, віддалене виконання коду, обхід автентифікації та розкриття конфіденційних відомостей, що формує комплексний характер загроз [10].

Також відбувається ускладнення структури цифрових медичних платформ, унаслідок чого зростає кількість точок потенційного втручання. Відповідно кіберзловмисники щоразу активніше орієнтуються на багаторівневі атаки, які поєднують технічні та поведінкові механізми впливу. Суттєвою загрозою для медичних установ є також програми-вимагачі, які блокують доступ до інформаційних систем до моменту сплати викупу. Тому поширення цього типу шкідливого програмного забезпечення у галузі охорони здоров'я стає визначальним, оскільки значна частка організацій уже зазнала відповідних атак. Унаслідок цього зловмисники використовують високу цінність і чутливість медичних даних як інструмент тиску, що значно підвищує ефективність вимагання.

Окрему категорію становлять атаки типу «людина посередині», які реалізуються шляхом перехоплення комунікацій між учасниками інформаційного обміну. Відтак зловмисники інтегруються у процес передачі даних з метою

отримання конфіденційної інформації, використовуючи, зокрема, незахищені мережі або вразливості у взаємодії медичних пристроїв. Тому розширення застосування хмарних та IoT-рішень у медичній сфері створює додаткові передумови для реалізації таких атак [10].

Порушення безпеки даних у медичній галузі характеризуються підвищеним рівнем критичності, адже оброблювана інформація безпосередньо стосується стану здоров'я пацієнтів. Зростання використання сторонніх постачальників послуг призводить до збільшення частки зовнішніх інцидентів, серед яких переважають витоки, пов'язані з третіми сторонами. Відповідно необхідність інтегрованого підходу до кіберзахисту стає визначальною умовою забезпечення інформаційної безпеки [10].

Зростання складності ланцюгів постачання у сфері охорони здоров'я формує додаткові ризики, пов'язані з міжорганізаційною взаємодією. Унаслідок цього кіберінциденти можуть призводити до витоку даних, а також до порушення функціонування логістичних процесів і постачання медичних ресурсів. Тому забезпечення стійкості всієї екосистеми охорони здоров'я потребує необхідного врахування взаємозалежностей між її складовими [10]. У цьому контексті кількісне відображення економічних наслідків реалізації кіберзагроз дозволяє більш ґрунтовно оцінити масштаб їх впливу на функціонування галузі.

Так, аналіз даних рисунка 1 відображає послідовне зростання вартості відновлення після атак програм-вимагачів у сфері охорони здоров'я протягом 2021-2024 років. Зокрема, у 2021 році відповідний показник становив 1,27 млн дол. США, натомість у 2022 році він зріс до 1,85 млн дол. США, що, своєю чергою, демонструє істотне підвищення фінансового навантаження на медичні організації. Наступний період характеризується подальшим збільшенням витрат до 2,2 млн дол. США у 2023 році, внаслідок чого формується стійка тенденція до зростання економічних збитків. Завершальний етап аналізованого інтервалу відображає досягнення рівня 2,57 млн дол. США у 2024 році, тому динаміка показника набуває чітко вираженого висхідного характеру.

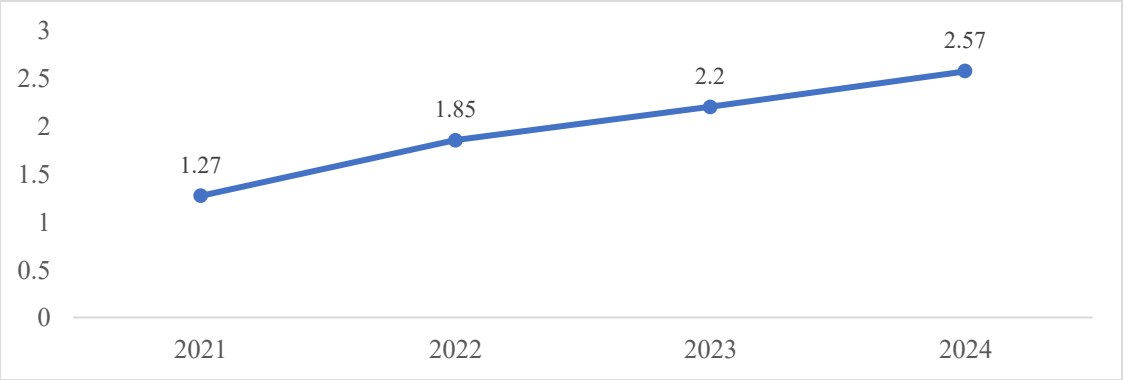

Рис. 1. Вартість відновлення після зіткнень програм-вимагачів в організаціях охорони здоров'я в усьому світі, млн. дол. США

Джерело: складно на основі [11].

Посилення фінансових наслідків кібератак у медичній галузі відображає трансформацію самих загроз, які стають більш складними та ресурсомісткими. Відповідно простежується зростання частки витрат, пов'язаних з технічним відновленням систем, а також із забезпеченням безперервності надання медичних послуг. Отримані результати дозволяють дійти висновку, що зростання вартості відновлення після атак програм-вимагачів є індикатором загального ускладнення кіберзагроз у сфері охорони здоров'я. Тому підвищення ефективності систем кіберзахисту потребує технологічного вдосконалення та стратегічного планування ресурсів, спрямованих на попередження інцидентів та зменшення їхніх наслідків.

У 2025 році програми-вимагачі зберігали статус найбільш значущої кіберзагрози для сфери охорони здоров'я, що підтверджується активною діяльністю численних угруповань, орієнтованих на медичні організації в глобальному масштабі. При цьому інтенсивність атак із боку таких груп, як Qilin, INC Ransom та SAFEPAY, суттєво зростала, унаслідок чого було зафіксовано сотні інцидентів у межах галузі. Водночас динаміка активності окремих угруповань, зокрема Qilin, продемонструвала істотне збільшення порівняно з попереднім роком, натомість нові учасники, серед яких SAFEPAY і Sinobi, також значно продемонстрували свою присутність у кіберпросторі охорони здоров'я [6].

Зауважимо, що забезпечення рівноваги між кібербезпекою та функціональністю медичних систем потребує комплексного та скоординованого механізму. Зокрема, у процесі розширення мережевої інфраструктури та інтеграції нових пристроїв підвищуються вимоги до узгодженості дій усіх учасників, відповідальних за підтримку безпеки. Відтак формування цілісної стратегії кіберзахисту передбачає активну участь технічного персоналу та медичних працівників у процесах управління ризиками. Відтак ефективна протидія кіберзагрозам у сфері охорони здоров'я досягається шляхом консолідації зусиль ІТ-фахівців, клініцистів і управлінського персоналу. Унаслідок цього створюються передумови для комплексного захисту даних пацієнтів і забезпечення безперервності функціонування медичних установ [4].

Ефективне підтримання процесів захисту інформації забезпечує належний рівень безпеки даних у сфері охорони здоров'я. Зокрема, алгоритм AES-256 розглядається як один із найбільш надійних засобів шифрування, оскільки характеризується високим рівнем криптографічної стійкості. Простота його впровадження та обслуговування сприяє широкому використанню у сучасних медичних інформаційних системах, унаслідок чого підвищується ефективність захисту даних. За оцінками експертів, злам цього алгоритму потребує тривалого часу, що підтверджує його доцільність для застосування у критично важливих інфраструктурах. Тривалість життєвого циклу AES перевищує можливості окремих алгоритмів, що використовуються в IoT-середовищі, отже, його інтеграція у медичні системи є виправданою [5, с. 274-275].

Зростання ролі криптографічних механізмів у медичних інформаційних системах відображає загальну тенденцію до посилення технічної складової кіберзахисту. У цьому контексті впровадження стійких алгоритмів шифрування розглядається як базовий елемент протидії несанкціонованому доступу.

З метою протидії кіберзагрозам у сфері охорони здоров'я доцільно приділяти значну увагу використанню методів машинного навчання та штучного інтелекту для виявлення й запобігання інцидентам у медичних установах [1, с. 139]. Тому інтеграція інтелектуальних технологій у системи кіберзахисту сприяє

формуванню ефективних моделей реагування на загрози. Відповідно автоматизований аналіз поведінкових аномалій дозволяє своєчасно ідентифікувати потенційні атаки та мінімізувати їх наслідки.

Висновки. Таким чином, узагальнення наведених положень дозволяє констатувати, що інтенсифікація кіберзагроз у сфері охорони здоров'я є наслідком системної цифровізації галузі та зростання обсягів обробки чутливої інформації, що, своєю чергою, обумовлює підвищення вразливості медичних інформаційних систем. Аналіз статистичних даних засвідчує стійку тенденцію до зростання кількості кіберінцидентів і масштабів витоків даних, що підтверджує посилення зацікавленості зловмисників до медичних ресурсів як стратегічно цінного активу. Ускладнення архітектури цифрових медичних екосистем, а також вплив зовнішніх чинників, зокрема геополітичної нестабільності та вразливостей ланцюгів постачання, зумовлюють необхідність формування інтегрованого механізму до кіберзахисту. Відповідно зростання економічних втрат від атак програм-вимагачів свідчить про підвищення ресурсомісткості кіберінцидентів, унаслідок чого актуалізується потреба у стратегічному плануванні фінансового забезпечення безпекових заходів. Відтак ефективна протидія сучасним кіберзагрозам передбачає поєднання технологічних рішень, зокрема використання криптографічних алгоритмів і методів штучного інтелекту, з організаційними механізмами підвищення обізнаності персоналу та міжінституційної взаємодії. Тому формування цілісної парадигми кібербезпеки, інтегрованої у загальну стратегію стійкості системи охорони здоров'я, є визначальною передумовою забезпечення безперервності надання медичних послуг і захисту даних пацієнтів.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Al-Qarni E. A. Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications*. 2023. № 14(5). P. 135–140. URL: https://pdfs.semanticscholar.org/6602/dc04b31e9e12c47c1854faa65776776989.pdf
2. Li S., Surineni K., Prabhakaran N. Cyber-attacks on hospital systems: A narrative review. *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*. 2025. № 7. P. 30–39. DOI: https://doi.org/10.1016/j.ajgoe.2025.03.002
3. Ewoh P., Vartiainen T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *Journal of Medical Internet Research*. 2024. № 26. e46904. DOI: https://doi.org/10.2196/46904
4. Clarke M., Martin K. Managing cybersecurity risk in healthcare settings. In: *Healthcare Management Forum*. 2024. Vol. 37, No. 1. P. 17–20. DOI: https://doi.org/10.1177/08404704231195804
5. Kavitha A., Rao B. S., Akthar N., Rafi S. M., Singh P., Das S., Manikandan G. A novel algorithm to secure data in next generation health care system from cyber attacks using IoT. *International Journal of Electrical and Electronics Research (IJEER)*. 2022. № 10(2). P. 270–275. DOI: https://doi.org/10.37391/IJEER.100236

6. Cyber Threats Intensify Across Global Health Sector. *Cyber Threats Intelligence*. 2023. URL: https://healthmanagement.org/c/it/News/cyber-threats-intensify-across-global-health-sector
7. Global number of data breaches with confirmed data loss from November 2023 to October 2024, by target industry. *Statista*. 2024. URL: https://www.statista.com/statistics/329608/security-incidents-confirmed-data-loss-industry-size/
8. Global number of cybercrime incidents from November 2022 to October 2023, by industry and organization size. *Statista*. 2023. URL: https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/
9. Healthcare Data Breach Statistics Updated for 2026. *HIPAA Journal*. 2026. URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/
10. Why the Healthcare Industry Is a Prime Target for Cyberattacks. *Locknet*. 2024. URL: https://locknet.com/why-the-healthcare-industry-is-a-prime-target-for-cyberattacks/
11. Cost of recovery after ransomware encounters at healthcare organizations worldwide from 2021 to 2024. *Statista*. 2024. URL: https://www.statista.com/statistics/1538141/healthcare-orgs-ransomware-recovery-cost/

REFERENCES

1. Al-Qarni, E. A. (2023). *Cybersecurity in healthcare: A review of recent attacks and mitigation strategies*. International Journal of Advanced Computer Science and Applications, 14(5), 135–140.
2. Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-attacks on hospital systems: A narrative review. *The American Journal of Geriatric Psychiatry Open Science, Education, and Practice, 7*, 30–39. https://doi.org/10.1016/j.ajgoe.2025.03.002
3. Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: A systematic review. *Journal of Medical Internet Research, 26*, e46904. https://doi.org/10.2196/46904
4. Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum, 37*(1), 17–20. https://doi.org/10.1177/08404704231195804
5. Kavitha, A., Rao, B. S., Akthar, N., Rafi, S. M., Singh, P., Das, S., & Manikandan, G. (2022). A novel algorithm to secure data in next generation health care system from cyber attacks using IoT. *International Journal of Electrical and Electronics Research, 10*(2). https://doi.org/10.37391/IJEER.100236
6. HealthManagement.org. (2023). *Cyber threats intensify across global health sector*. https://healthmanagement.org/c/it/news/cyber-threats-intensify-across-global-health-sector
7. Statista. (2024). *Global number of data breaches with confirmed data loss from November 2023 to October 2024, by target industry*. https://www.statista.com/statistics/329608/security-incidents-confirmed-data-loss-industry-size/

8. Statista. (2023). *Global number of cybercrime incidents from November 2022 to October 2023, by industry and organization size*. https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/
9. HIPAA Journal. (2026). *Healthcare data breach statistics*. https://www.hipaajournal.com/healthcare-data-breach-statistics/
10. Locknet. (2024). *Why the healthcare industry is a prime target for cyberattacks*. https://locknet.com/why-the-healthcare-industry-is-a-prime-target-for-cyberattacks/
11. Statista. (2024). *Cost of recovery after ransomware encounters at healthcare organizations worldwide from 2021 to 2024*. https://www.statista.com/statistics/1538141/healthcare-orgs-ransomware-recovery-cost/

Received (надійшла до редакції): 12.04.2026
Accepted (прийнята до друку): 11.05.2026
Published (опублікована): 12.06.2026