лодіють можливістю реєструвати і обробляти інформацію про виконувані операції. SQL Server починаючи з версії з 2008 має можливість визначати специфікацію аудиту [1] на рівні сервера або бази даних. Однак дані системного аудиту не враховують вимоги бізнес-моделі інформаційної системи. Виникає необхідність настройки процесу реєстрації з урахуванням специфіки предметної області. Крім того, найважливішим завданням захисту БД є забезпечення цілісності даних. В сучасних складних ІС більшість таблиць повинні бути захищені від небажаних операцій змін (вставок, оновлень і вилучень). Дані аудиту можуть використовуватися для скасування таких небажаних дій. В цьому випадку, інформації в системних журналах недостатньо. У даній статті розглядається підхід до вирішення завдання аудиту змін в таблицях БД з метою запобігання небажаних змін даних. Такий підхід реалізований у вигляді методики створення об'єктів бази даних, за допомогою яких здійснюється реєстрація дій користувачів і скасування небажаних змін. Для вирішення завдання реєстрації всіх дій користувача пропонується використовувати окрему схему БД для аудиту, спеціальну таблицю аудиту і тригери інформаційних таблиць БД. Для скасування небажаних змін запропоновані SQL-процедури. Для кожного етапу методики наведена програмна реалізація, що дозволяє використовувати її як частину автоматизованої захисту БД.

Ключові слова: база даних, захист даних, реєстрація і аудит, відміна небажаних змін в базі даних.

AUDIT OF CHANGES TO SQL SERVER-DATABASE TABLES

The registration and audit subsystemis an inalienable component of information systems. All modern DBMS have the ability to register and process information about performedoperations. SQL Server since version 2008 has the ability to define an audit specification [1] at the server or database level. However, the data from the system audit does not consider the requirements of theinformation system's business model. It becomes necessary to customize the registration process considering the specifics of the subject area. In addition, the most important task of database protection is to ensure data integrity. In modern complex IS a number of tables must be protected from unwanted change operations (inserts, updates and deletions). Audit data can be used to cancel such unwanted actions. In this case, there is not enough information in the system logs. This article discusses an approach to solving the audit of changes to DB tables problem in order to prevent unwanted data changes. This approach is implemented in the form of a methodology of creating database objects with the help of which user actions are registered and unwanted changes can be canceled. To solve the problem of user actions registration it is proposed to use a separate database schema for audit, a special audit table and triggers of the DB information tables.SQL procedures are proposed for unwanted changes cancellation. The software implementation that makes it possible to use it as part of automated DB protection is given for each stage of methodology.

Key words: database, data protection, registration and audit, cancelation of unwanted changes in the database.

Коломиец Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: box144.85@gmail.com.
ORCID ID 0000-0001-8460-3041.

Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».

Kolomytsev Myhailo, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: nos.sv.ol@gmail.com.
ORCID ID 0000-0002-0016-9346.

Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».

Nosok Svitlana, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

DOI: 10.18372/2410-7840.23.15153
УДК 004.056.5:61:621.397

АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕДИЧНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Олена Трофименко, Ярослав Дубовой, Наталія Логінова, Юлія Прокоп, Олександр Задерейко

За умов суворого карантину через пандемію COVID-19, завдяки можливостям сучасних інформаційно-телекомунікаційних систем, значна частина медичних послуг трансформувала у цифрове середовище в режим онлайн. Позитивний ефект цього полягає насамперед у знищенні цифрового розриву та реалізації прав громадян на рівноправне отримання медичної допомоги в електронному форматі. Проте цей процес зумовив потенційні небезпеки витоків

конфіденційної інформації з подачі кіберзлочинців. Наразі питання кібербезпеки медичних комп'ютерних систем є вельми актуальними та потребують комплексного і виваженого підходу до вирішення. Важливою складовою при цьому є нормативно-правовий захист конфіденційної інформації, що циркулює в медичних комп'ютерних системах. Аналіз цифрових технологій та комп'ютерних систем з надання медичних онлайн послуг показав, що гостро постають питання анонімізації медичних даних пацієнтів, захисту медичних пристроїв, долучених до мережі Інтернет, від витоку конфіденційної медичної інформації. Тому при розробленні відповідного програмного забезпечення мають бути дотримані суворі правила щодо забезпечення конфіденційності даних, які обробляються в медичних інформаційних системах. Питання захищеності інфраструктури збору, зберігання і передачі медичних даних насамперед полягає в обмеженні доступу та створенні надійної електронної бази медичної інформації. З'ясовано певні проблеми безпеки хмарних середовищ, які використовують як платформи для зберігання даних при наданні послуг у галузі охорони здоров'я, щодо їх вразливості до можливих кібератак. Для підвищення довіри і забезпечення надійного захисту конфіденційної медичної інформації, яка обробляється у таких сервісах, варто враховувати всі програмні, апаратні та організаційні аспекти. Аналіз питань кібербезпеки медичних комп'ютерних систем дозволив виявити низку проблем захисту даних, важливість багатофакторної автентифікації користувачів, контролю доступу, застосування ефективних криптографічних схем шифрування для ефективного захисту інформаційних ресурсів екосистем охорони здоров'я в інтернеті та визначити напрями подальших досліджень з надання якісних захищених медичних онлайн послуг.

Ключові слова: *кібербезпека, телемедицина, кібератака, конфіденційна інформація, персональні дані, медичні онлайн послуги.*

ВСТУП

Цифрова трансформація сфери охорони здоров'я за умов пандемії COVID-19 дозволила надавати медичні послуги дистанційно та передавати медичні дані між пацієнтами та постачальниками медичних послуг засобами мережі Інтернет. При цьому в комп'ютерних системах формуються і циркулюють величезні обсяги конфіденційних даних про пацієнтів, медпрацівників, сферу діяльності як таку. Це утворює вразливе середовище щодо кібератак, які можуть стосуватися несанкціонованого доступу, можливих витоків, викрадення або взагалі втрати особистих даних. При цьому не виключені ситуації заволодіння кіберзловмисниками дистанційним контролем над комп'ютерними системами, їх пошкодження або недоступності, що може спричинити серйозні наслідки.

Нині по всьому світу фіксують значне збільшення кількості кібератак на критичну інформаційну інфраструктуру, до якої належать й організації та установи медичного сектору. Відомі численні випадки атак вірусів-здирників (RoT – Ransomware of Things) на інформаційні системи установ у сфері охорони здоров'я. Потрапивши на комп'ютер-«жертву» такі віруси шифрують інформацію на ньому, тим самим виводять з ладу базову інфраструктуру, а зловмисники отримують доступ до керування пристроями в системі й вимагають викуп для відновлення її функціонування. Так, у вересні 2020 року в США внаслідок кібератаки вірусу-здирника на загальнонаціональну мережу лікарень Universal Health Services її інформаційна система відмовила, що спричинило широкомасштабні відключення, затримки лабораторних результатів, а пацієнтів перенаправляли в інші лікарні для надання медичної допомоги, адже втрата доступу до даних пацієнтів є найбільшою загрозою безпеці пацієнтів. Наприкінці грудня 2020 на британську мережу косметологічних клінік Transform Hospital Group була здійснена кібератака вірусу-здирника, внаслідок якої хакери викрали дані на 900 Гб із загрозою опублікувати фотографії пацієнтів до і після операції. Цього ж року були зафіксовані кібератаки програм-здирників на сервери лікарні Дюссельдорфського університету в Німеччині, університетської лікарні в Нью-Джерсі (США), дитячої лікарні Бостона, установи з досліджень вакцин та багато інших [1]. Лікарняні заклади повідомляють про спрямований потік фішинг-листів, завантажених шкідливим програмним забезпеченням та посиланнями, замаскованими під обіцянки про продаж захисних масок і кисневих концентраторів. А це лише один з можливих векторів кібератак, які несуть неминучу загрозу і потенційно великі ризики для постачальників медичних послуг та їх пацієнтів. Медичні установи самі по собі не в змозі впоратися з еволюцією кібератак.

Саме тому кібербезпеку у галузі охорони здоров'я слід розглядати як складову державної

політики, напрямами якої є контроль поточного стану інформаційних систем критичної інфраструктури, підвищення обізнаності та кіберграмотності працівників, підготовка кваліфікованих фахівців з кібербезпеки та залучення успішного світового досвіду у цій сфері.

Так, за прикладом Таїланду варто запроваджувати пільгове оподаткування для підприємств, які інвестують у свою кібербезпеку, тим самим стимулювати їх зацікавленість у формуванні високого статусу кіберзахищеності своєї інфраструктури. Адже національна безпека країни залежить як від бізнесу, так і від окремих громадян, невіддільною складовою сучасного життя яких є різноманітні інформаційні ресурси.

Саме тому ефективний захист відповідних систем від кібератак, високий рівень безпеки та здатності своєчасно виявляти і ліквідувати такі кіберзагрози є ключовим питанням, яке потребує термінового вирішення.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Специфічні аспекти інформаційної безпеки та загроз конфіденційності даних пацієнтів медичних підприємств досліджували різні науковці.

Так, у статті [2] розглянуто проблеми конфіденційності, пов'язані з безпекою та цілісністю медичної інформації, що стосується саме геномних даних про пацієнтів. Специфіку реалізації лабораторної безпеки з точки зору безпеки генетичної інформаційної системи збору біологічних матеріалів та їх зберігання досліджено у роботі [3]. Проте питання кібербезпеки в галузі захисту інформаційних ресурсів медичних підприємств не вичерпується лише конфіденційністю генетичної інформації людей.

Переваги технології IoT з метою покращення якості медичних послуг розглядаються у дослідженнях [4, 5]. Елементи політики безпеки в телемедицині проаналізовано в статті [6]. Стрімкий розвиток біометричних технологій моніторингу (BioMeTs) під час світової пандемії коронавірусу COVID-19 з метою дистанційного моніторингу і збору даних життєво важливих показників пацієнтів відзначається у роботі [7].

Тут обговорюються сильні сторони та обмеження використання технологій BioMeTs та IoT у дистанційній допомозі пацієнтам, проте не розглядаються ризики порушення конфіденційності медичних даних. Вивченню проблем захисту та управління приватним життям медичних служб присвячено дослідження [8]. Методи розробки моделей загроз, які найчастіше спрямовані на інформаційну систему в цілому, розглядають у роботі [9]. Можливі ризики витоків важливої і критичної інформації і подальших збитків при використанні підприємствами програмного забезпечення з відкритим вихідним кодом досліджено в статтях [10, 11], але при цьому не враховується специфіка захисту інформаційних ресурсів медичних підприємств.

Мета статті полягає в узагальненні питань захисту медичних інформаційних комп'ютерних систем від кібератак, включаючи дослідження нормативно-правових аспектів захисту медичних персональних даних, специфіки захисту медичних персональних даних за умов пандемії COVID-2019 та захищеності інформаційної інфраструктури медичного сектору.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Останнім часом парадигма інтернету речей (IoT) охоплює все більше сфер життєдіяльності. Різноманітні цифрові пристрої, об'єднані в мережі та підключені до інтернету, формують сфери надання сучасних високоефективних дистанційних послуг, доступних у будь-який час і в будь-якому місці. У галузі охорони здоров'я ці пристрої можуть варіюватися від інноваційних вимірювачів активності (наприклад, крокомірів) та приладів моніторингу артеріального тиску і серцевого ритму до сучасних пристроїв, здатних контролювати спеціалізовані імплантати (наприклад, підшкірні монітори глюкози, кардіостимулятори або вдосконалені слухові апарати). Такі можливості дозволяють суттєво покращити якість медичної допомоги при одночасному зменшенні витрат [4]. Так, стає можливим дистанційний скринінг у режимі реального часу фізіологічних параметрів пацієнтів для раннього виявлення клінічного погіршення стану, що покращує процес прийняття рішень щодо діагнозу і призна-

чення лікування.

Однак покращення якості персоналізованих онлайн медичних послуг нерозривно пов'язане із забезпеченням захищеності відповідного програмного та апаратного забезпечення від витоків персональної інформації медичного характеру. Позаяк електронні медичні послуги формують великі масиви різнорідних медичних даних про пацієнтів та лікарів, життєво важливо щоб ця приватна інформація була надійно захищеною і недоступною для сторонніх осіб.

Нормативно-правові аспекти захисту медичних персональних даних. Дані про стан здоров'я належать до специфічної категорії персональних даних і потребують ступеня захисту вищого, ніж інші категорії персональних даних.

Саме тому дані про стан здоров'я потребують окремого правового регулювання, яке б впорядковувало їх збір та використання. У різних країнах розроблено та запроваджено відповідну нормативно-правову базу з питань забезпечення захисту приватного життя [12]. Наприклад, у США діє Закон HIPAA (Health Insurance Portability and Accountability Act) [13] про мобільність та підзвітність медичного страхування, який допомагає зберігати конфіденційну інформацію про здоров'я громадян штатів. В Євросоюзі Загальний регламент захисту даних (General Data Protection Regulation, GDPR) накладає на громадян серйозну відповідальність за недотримання правил конфіденційності приватного життя на різних рівнях, передусім це стосується медичних та страхових організацій, позаяк порушення даних у галузі охорони здоров'я не лише може спричинити значні негативні особисті та соціальні наслідки для пацієнтів та їхніх сімей.

Так, у GDPR в переліку даних, що належать до персональних даних користувачів, серед інших віднесено [14]:

– генетичні дані – персональні дані, що стосуються успадкованих або придбаних генетичних ознак фізичної особи, які надають унікальну інформацію про фізіологію або здоров'я зазначеної фізичної особи і які витікають, зокрема, з аналізу біологічного зразка відповідної фізичної особи;

– біометричні дані – персональні дані після спеціального технічного опрацювання, що стосуються фізичних, фізіологічних або поведінкових ознак фізичної особи, які дозволяють провести або підтвердити унікальну ідентифікацію зазначеної фізичної особи, наприклад, зображення людського обличчя або дактилоскопічні дані;

– дані про здоров'я – персональні дані, пов'язані з фізичним або психічним здоров'ям фізичної особи, в тому числі з наданням послуг з догляду за здоров'ям, які надають інформацію про стан його здоров'я.

GDPR жорстко регламентує прозорість для користувача того, як збираються й обробляються дані про нього [14]:

– персональні дані повинні оброблятися законно, справедливо і прозоро, з обов'язковою декларацією інформації про цілі, методи та обсяги їх оброблення в максимально доступній та зрозумілій формі;

– персональні дані повинні збиратися і використовуватися виключно в заявлених цілях інтернет-ресурсом;

– персональні дані повинні збиратися в обсягах, що не перевищують необхідний обсяг для заявлених цілей оброблення;

– персональні дані, які є неточними, мають бути виправлені на першу вимогу користувача;

– збереження персональних даних, які однозначно ідентифікують користувача, мають зберігатися протягом терміну, що не перевищує термін заявленої мети оброблення;

– персональні дані повинні бути захищені від несанкціонованого і незаконного оброблення, пошкодження та знищення.

Крім того, вимоги GDPR встановлюють жорстку процедуру щодо форми отримання згоди користувача на оброблення його персональних даних у формі затвердження або у формі передбачених дій користувача на інтернет-сервісах. Також цим Законом передбачено, що згода користувача на оброблення персональних даних втрачає силу в разі, якщо не було надано можливості вибору або була відсутня можливість

відкликання згоди без нанесення будь-якої шкоди для користувача.

В Україні в цілях забезпечення захисту персональних даних, до яких стосуються і дані про стан здоров'я, біометричні або генетичні дані, діє Закони України «Основи законодавства України про охорону здоров'я» [15] та «Про захист персональних даних». Саме вони регулюють питання забезпечення захисту персональних даних у сфері охорони здоров'я, функціонування медичних інформаційних комп'ютерних систем, державних фінансових гарантій медичного обслуговування населення тощо.

Так, у ст. 7 Закону України «Про захист персональних даних» зазначено про заборону обробки персональних даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Проте, це не стосується обробки персональних даних коли вона «необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я» [16].

Приміром, під час пандемії COVID-19 у світі виникла нагальна потреба у зборі та зберіганні значної кількості інформації про стан здоров'я населення. Роботодавці почали слідкувати за захворюваністю на COVID-19 серед працівників, державні органи – збирати дані про переміщення осіб і дотримання режиму ізоляції, а люди все частіше почали звертатися у заклади охорони здоров'я для проходження тестування на COVID-19 чи наявність антитіл [17]. Інформацію про охорону здоров'я стали часто використовувати для посилань, які можуть бути використані для ідентифікації пацієнта. Забезпечення конфіденційності інформації, що ідентифікує особу, має взяти на себе та суворо контролювати на законодавчому рівні держава. При цьому слід зважати на швидкий прогрес інформаційно-комунікаційних технологій, що може випереджати та не відповідати нормам галузевих і нормативних вимог з питань конфіденційності та проблем, пов'язаних з охороною здоров'я, а тому і потребу коригування нормативно-правової бази.

Захист медичних персональних даних за умов COVID-2019. Світова пандемія COVID-19 стрімко змінила кількість пацієнтів, які отримують онлайн медичну допомогу. Телемедицина та онлайн-скринінг стали більш поширеними, а вимірювання показників (температури, частоти серцевих скорочень, кров'яного тиску, насичення киснем та частоти дихання), проведені вдома у пацієнта за допомогою біометричних технологій моніторингу, надають зручні можливості для збору даних життєво важливих ознак.

При цьому суттєво знижуються ризики поширення захворювання, завдяки соціальному дистанціюванню. Тому можна стверджувати, що нині телемедицина допомагає уповільнити поширення захворюваності коронавірусом. Всесвітня організація охорони здоров'я (ВООЗ), Центри контролю за захворюваннями США та Європи визнали, що цифрові технології та системи моніторингу можуть відігравати важливу роль у підтримці здоров'я населення.

Дослідження [18] показали, що впровадження телемедичних послуг значно зменшує навантаження на лікарні під час пандемії, оскільки дистанційні медичні послуги мінімізують потребу в догляді за пацієнтами.

Вочевидь, і після пандемії більшість користувачів віддаватимуть перевагу отриманню онлайн медичної допомоги з дому для дистанційної профілактики, діагностики, порад та навіть лікування, як альтернативній моделі надання клінічних послуг. Цифрові екосистеми охорони здоров'я еволюціонували на вершині хмарних платформ, технологій IoT, мобільних обчислень, штучного інтелекту (AI) та машинного навчання (ML) для медичної аналітики. Хоча такі екосистеми формують майбутнє загальнодоступної та інтелектуальної охорони здоров'я, конфіденційність пацієнтів, лікарів, медсестер та постачальників медичних послуг сьогодні викликає велике занепокоєння, як ніколи раніше. Анонімізація геномних даних, захист медичних пристроїв, долучених до мережі Інтернет, від витоку конфіденційних даних про стан здоров'я

пацієнтів потребують ретельного контролю щодо дотримання конфіденційності у цьому питанні.

Підходи до протоколювання та функціоналу мобільних програмних платформ з надання медичних онлайн послуг відрізняються в різних країнах з урахуванням специфіки потреб і менталітету держав. Нині попит на якісні програмні застосунки такого призначення лише зростає. Пропорційно попиту на ринку IT-послуг з'являється широкий спектр спеціалізованих програмних застосунків з цікавими винахідницькими рішеннями і новими можливостями у галузі охорони здоров'я. Деякі з них обмежуються збором статистики спостережень (демографічних показників, симптомів хвороби, контактних даних) пацієнтів і передачею її медичним працівникам у відповідних географічних районах з метою виявлення, звітування, активного моніторингу і швидкого втручання у випадках зараження COVID-19. Інші мають ще й функціонал відстеження, визначення та контролю відстані між користувачами за допомогою Bluetooth з метою обмеження поширення захворюваності. Дистанційне відстеження, з одного боку, допомагає захистити близьких від несвідомого зараження, оскільки автоматично виявляє і збирає дані про можливі контакти з інфікованою людиною та останні поїздки.

Проте, з іншого боку, програма такого роду реалізує масовий нагляд, збір та використання особистих даних про всі пересування клієнта, його діагностичні анкети, підключення до індивідуальної електронної медичної картки, телесеанси між пацієнтами та медпрацівниками.

Ці персональні дані за згодою користувача можуть використовуватись службами охорони здоров'я задля моніторингу і контролю стану захворюваності у регіоні. Дані моніторингу пацієнтів у режимі реального часу, які ведуть з метою віддаленого скринінгу, мають бути надійно захищеними і недоступними для сторонніх. При розробленні відповідного програмного забезпечення мають бути дотримані суворі нормативні правила щодо забезпечення конфіденційності даних для унеможливлення можливих порушень особистої безпеки та особистих свобод.

З іншого боку через зацікавленість у доступі до подібного роду персональних даних іноді замовниками такого програмного забезпечення виступають спецслужби або злочинні компанії. Тому важливо вести просвітницьку діяльність у суспільстві та контролювати уповноваженими офіційними органами вихід на ринок відповідного програмного забезпечення для запобігання зловживанням. Попри різні технологічні методи ризик зловживань повністю усунути не можна. Дилему між особистими свободами та здоров'ям населення слід розглядати по-філософськи і вирішувати їх дуже обережно та за згодою суспільства. Цифрові технології при цьому мають засоби для забезпечення найбільш "безболісних" технологічних рішень.

Питання захищеності інфраструктури збору, зберігання і передачі медичних даних. Керування доступом до медичних даних, які передаються між пацієнтами та постачальниками медичних послуг, полягає в обмеженні доступу на основі обліку персональних характеристик всіх уповноважених осіб. Концепція надійної електронної бази медичної інформації є центральною при оцінюванні ступеня гарантованості надійності системи. Механізм протоколювання є важливим засобом забезпечення безпеки [6]. Постачальники медичних послуг можуть не мати попереднього досвіду використання дистанційної допомоги пацієнтам, а отже, можуть бути незнайомі з протоколами збору даних та контекстом зібраних значень. Для прийняття зважених рішень щодо догляду за пацієнтами на основі біометричних даних, зібраних віддалено, важливо розуміти технічні рішення, вбудовані у вироби, протоколи збору даних, формфактори (фізичний розмір і форма), міркування щодо якості даних та наявність інформації про перевірку. Ведення протоколів медичної інформації повинно доповнюватись аудитом, тобто аналізом реєстрації медичної інформації.

Також є певні проблеми безпеки з можливими вразливостями до атак хмарних середовищ, які пропонують нині послуги у галузі здоров'я, через різні типи інсайдерських загроз (адміністраторів хмарних провайдерів, менеджерів хмарних стеків та адміністраторів рішень) і складністю керуван-

ням ідентифікацією та контролем доступу у багатокористувацькому режимі з єдиним вікном доступу (з одного робочого комп'ютера різних працівників медичних лабораторій, підприємств тощо, де автоматично зберігаються логіни та паролі). Навіть коли хмарні платформи відповідають усім нормативним вимогам щодо безпеки та конфіденційності даних, вони обробляють дані, які насправді не є анонімними, а тому залишаються чутливими до ідентифікації. Через це хмарні технології не підходять для сфер, де потрібно зберігати і пересилати дані, що становлять таємницю. Хмарне середовище саме по собі є достатньо надійною системою, однак при проникненні до нього зловмисник отримує доступ до величезного сховища даних. Провайдери хмарних сервісів постійно працюють над покращенням надійності і захищеності: нарощують резервні потужності заради забезпечення надійності при стрибку навантаження у разі DDOS атак, дублюють канали зв'язку для можливості перемикання на них, посилюють управління ідентифікацією та контроль доступу до своїх ресурсів для зниження ризиків підбору та зламу паролів. Проте провайдери SaaS-сервісу не можуть контролювати коректність організації доступу на стороні користувача, а при наданні PaaS-сервісу вони не можуть гарантувати, що клієнти розроблятимуть своє програмне забезпечення відповідно до встановленої політики безпеки на наданій платформі. Крім того, при стрімкому припливі користувачів хмарних сервісів зростає кількість помилок і витоків інформації з подібних ресурсів. Тому для підвищення довіри до хмарних послуг і забезпечення надійного захисту важливих даних користувача у таких сервісах до формування високого рівня кіберзахищеності інфраструктури треба підходити з великою уважністю та враховувати усі програмні, апаратні та організаційні аспекти. Безпека медичних інформаційних комп'ютерних систем передбачає визначення способу захисту даних, процесів та систем охорони здоров'я від можливих кібератак. Відсутність шифрування або застосування поширених схем шифрування, зневажання питанням керування ключами дозволили зловмисникам отримати доступ до мільйонів записів даних [8]. Якщо не вживати відповідних криптографічних засобів та заходів безпеки щодо перевірки цілісності, це може призвести до витоків конфіденційної інформації. Розуміння проблем захисту даних, багатофакторна автентифікація користувачів, контроль доступу, застосування ефективних криптографічних схем шифрування є складовими для ефективного захисту інформаційних ресурсів екосистем охорони здоров'я в інтернеті.

ВИСНОВКИ

Вивчення питань захисту медичних інформаційних комп'ютерних систем від кібератак дозволило виявити ключові проблеми та напрямки подальших досліджень у галузі кібербезпеки сфери телемедицини.

Дослідження нормативно-правових аспектів захисту медичних персональних даних виявило потребу окремого правового регулювання, яке б впорядковувало їх збір та використання при наданні онлайн медичних послуг.

Проаналізовано нормативно-правову базу різних країн з питань забезпечення захисту конфіденційної інформації про здоров'я громадян. Дослідження специфіки захисту медичних персональних даних за умов пандемії COVID-19 довело важливу роль телемедичних послуг для підтримки здоров'я людей. Зазначено про високу ймовірність подальшого поширення онлайн медичних послуг і після завершення пандемії. За таких умов питання важливості захисту інформаційної інфраструктури медичного сектору від витоків конфіденційних даних про стан здоров'я пацієнтів потребують ретельного контролю з боку держави. Аналіз безпеки інформаційних систем збору, зберігання і передачі даних екосистем охорони здоров'я дозволив виявити проблеми з можливими вразливостями до атак хмарних середовищ.

Важливими засобами забезпечення безпеки дистанційної допомоги пацієнтам є надійна електронна база медичних даних, механізми протоколювання, керування доступом до медичних даних, які передаються між пацієнтами та постачальниками медичних послуг. До забезпечення надійного захисту обчислювальних систем охорони здоров'я треба підходити з великою уважністю та враховуючи програмні, апаратні та ор-

ганізаційні аспекти. Спектр проблем щодо захисту інформаційних систем охорони потребують детального подальшого дослідження та запровадження новітніх засобів з надання якісних захищених медичних онлайн послуг.

ЛІТЕРАТУРА

[1] *Misery of Ransomware Hits Hospitals the Hardest*. [Електронний ресурс] – Режим доступу до ресурсу: https://threatpost.com/ransomware-hits-hospitals-hardest/162096/.

[2] Luh F., Yen Y. Cybersecurity in Science and Medicine: Threats and Challenges. *Trends in biotechnology*. 2020. № 38(8). pp. 825-828.

[3] Schumacher G., Sawaya St., Nelson D., Hansen A. Genetic Information Insecurity as State of the Art. *Frontiers in Bioengineering and Biotechnology*. 2020. Vol. 8. pp. 1-9.

[4] Dridi A., Sassi S., Faiz S. A Smart IoT Platform for Personalized Healthcare Monitoring Using Semantic Technologies. *IEEE International Conference on Tools with Artificial Intelligence*. 2017. pp. 1198-1203.

[5] Yehia L., Khedr A., Darwish A. Hybrid Security Techniques for Internet of Things Healthcare Applications. *Advances in Internet of Things*. 2015. №5. pp. 21-25.

[6] Шупяцький І. М. Комплексна система захисту інформації медичної – надійний алгоритм надання якісної медичної допомоги в закладах охорони здоров'я. *Актуальні проблеми клінічної та профілактичної медицини*. 2013. Т. 1. № 2. С. 20-24.

[7] Manta C., Jain S., Coravos A., Mendelsohn D., Izmailova E. An Evaluation of Biometric Monitoring Technologies for Vital Signs in the Era of COVID-19. *Clinical and Translational Science,* 2020. № 13. pp. 1-35.

[8] Iyengar A., Kundu A., Pallis G. Healthcare Informatics and Privacy. *IEEE Internet Computing*. 2018. Т. 22. № 2. pp. 29-31.

[9] Silic M., Back A. The Influence of Risk Factors in Decision-Making Process for Open Source Software Adoption. *International Journal of Information Technology & Decision Making*. 2016. № 15, 2016. – 30 p.

[10] Гапон А.О., Федорченко В.М., Поляков А.О. Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного коду. *Захист інформації та кібернетична безпека*. 2020. Вип. 1(160). С. 128-135.

[11] Zadereyko O., Trofymenko O., Loginova N. Algorithm of user's personal data protection against data leaks in Windows 10 OS. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*. Lublin University of Technology. 2019. Vol. 9. No 1, pp. 41-44.

[12] Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21. № 3. Київ: Національний авіаційний університет. С. 150–157.

[13] *Health insurance portability and accountability act*. URL: https://aspe.hhs.gov/report/health-insurance -portability-and-accountability-act-1996

[14] *Complete guide to GDPR compliance*. URL: https://gdpr.eu / (дата звернення: 12.02.2021).

[15] *Закон України «Основи законодавства України про охорону здоров'я»*. URL: https://zakon. rada.gov.ua/laws/show/2801-12#Text.

[16] *Закон України «Про захист персональних даних»*. URL: https://zakon.rada.gov.ua/laws /show/ 2297-17#Text (дата звернення: 12.02.2021).

[17] *HIPAA: як захищають медичні дані пацієнтів в США?* URL: https://everlegal.ua/hipaa-yak-zakhy schayut -medychni-dani-patsientiv-v-ssha.

[18] Kosmidis, D., Nestoras, K. Telehealth and telenursing in time of COVID-19. *The step of ASCLIPI*. 2020. Vol. 19, № 4. P. 256-272.

CYBERSECURITY ISSUES OF MEDICAL COMPUTER SYSTEMS

In conditions of strict quarantine due to the COVID-19 pandemic, thanks to the capabilities of modern information and telecommunications systems, a significant part of medical services has been transformed into a digital environment online. The positive effect of this lies primarily in the elimination of the digital divide and realization of citizens' rights to equal medical care in electronic format. However, this process has led to the potential danger of confidential information leaks. Nowadays, the cybersecurity issues of medical computer systems are very relevant and require a comprehensive and balanced approach to the solution. An important component is the legal protection of confidential information circulating in medical computer systems. Analysis of digital technologies and computer systems for the provision of online medical services has shown the urgency of anonymizing patients' medical data, protecting medical devices connected to the Internet from leaks of confidential medical information. Therefore, the rules for ensuring the confidentiality of data processed in medical information systems must be strictly observed when developing appropriate software. The issue of security of the infrastructure for collection, storage and transmission of medical data is primarily to limit access and create a reliable electronic database of medical information. Certain security issues have been identified for cloud platforms used to store data in the provision of health services related to their vulnerability to possible cyberattacks. To increase the credibility and ensure the reliable protection of confidential medical information processed in such services, all software, hardware and organizational aspects should be considered. Analysis of cybersecurity of medical computer systems has identified a number of data protection issues, the importance of multifactor user authentication, access control, the use of effective cryptographic encryption schemes to effectively protect health ecosystems on the Internet and identify areas for further research to provide quality secure online health services.

Keywords: cybersecurity, telemedicine, cyberattack, confidential information, personal data, online medical services.

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ МЕДИЦИНСКИХ КОМПЬЮТЕРНЫХ СИСТЕМ

В условиях строгого карантина из-за пандемии COVID-19, благодаря возможностям современных информационно-телекоммуникационных систем, значительная часть медицинских услуг трансформировалась в цифровую среду в режим онлайн. Положительный эффект этого заключается прежде всего в устранении цифрового разрыва и реализации прав граждан на равноправное получение медицинской помощи в электронном формате. Однако этот процесс обусловил потенциальную опасность утечек конфиденциальной информации с подачи киберпреступников. Сейчас вопросы кибербезопасности медицинских компьютерных систем являются весьма актуальными и требуют комплексного и взвешенного подхода к их решению. Важной составляющей при этом является нормативно-правовая защита конфиденциальной информации, циркулирующей в медицинских компьютерных системах. Анализ цифровых технологий и компьютерных систем по предоставлению медицинских онлайн услуг показал остроту вопросов анонимизации медицинских данных пациентов, защиты медицинских устройств, подключенных к сети Интернет, от утечек конфиденциальной медицинской информации. Поэтому при разработке соответствующего программного обеспечения должны строго соблюдаться правила по обеспечению конфиденциальности данных, обрабатываемых в медицинских информационных системах. Вопрос защищенности инфраструктуры сбора, хранения и передачи медицинских данных в первую очередь заключается в ограничении доступа и создании надежной электронной базы медицинской информации. Выявлены определенного рода проблемы безопасности облачных платформ, используемых для хранения данных при предоставлении услуг в сфере охраны здоровья, касающиеся их уязвимости к возможным кибератакам. Для повышения доверия и обеспечения надежной защиты конфиденциальной медицинской информации, обрабатываемой в таких сервисах, следует учитывать все программные, аппаратные и организационные аспекты. Анализ вопросов кибербезопасности медицинских компьютерных систем позволил выявить ряд проблем защиты данных, важность многофакторной аутентификации пользователей, контроля доступа, применения эффективных криптографических схем шифрования для эффективной защиты информационных ресурсов экосистем здравоохранения в интернете и определить направления дальнейших исследований по предоставлению качественных защищенных медицинских онлайн услуг.

Ключевые слова: кибербезопасность, телемедицина, кибератака, конфиденциальная информация, персональные данные, медицинские онлайн услуги.

Трофименко Олена Григорівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: egt@ukr.net.
Orcid ID: 0000-0001-7626-0886.
Трофименко Елена Григорьевна, кандидат технических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Trofymenko Olena, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

Дубовой Ярослав Володимирович, інженер комп'ютерних систем Одеського казенного експериментального протезно-ортопедичного підприємства.
E-mail: dubovoy97@gmail.com.
Orcid ID: 0000-0002-3987-9409.
Дубовой Ярослав Владимирович, инженер компьютерных систем Одесского казенного экспериментального протезно-ортопедического предприятия.
Dubovoy Yaroslav, Computer Systems Engineer of the Odessa State Experimental Prosthetic and Orthopedic Enterprise.

Логінова Наталія Іванівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: loginova@onua.edu.ua.
Orcid ID: 0000-0002-9475-6188.
Логинова Наталья Ивановна, кандидат педагогических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Loginova Nataliia, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

Прокоп Юлія Віталіївна, кандидат історичних наук, старший викладач кафедри інформаційних технологій Одеської національної академії зв'язку ім. О.С. Попова
E-mail: yulia13.prokop@gmail.com.
Orcid ID: 0000-0002-6608-3668.
Прокоп Юлия Витальевна, кандидат исторических наук, старший преподаватель кафедры информационных технологий Одесской национальной академии связи им. А.С. Попова.
Prokop Yuliya, Candidate of Historical Sciences, Senior

lecturer at the Department of Information Technology of the O.S. Popov Odessa National Academy of Telecommunications.

Задерейко Олександр Владиславович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: zadereyko@onua.edu.ua.

Orcid ID: 0000-0003-0497-9861.
Задерейко Александр Владиславович, кандидат технических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Zadereyko Olexander, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

DOI: 10.18372/2410-7840.23.15433
УДК 004.81:004.056.5

ПРИСТРІЙ ДЛЯ ПРИВЕДЕННЯ ЧИСЕЛ ЗА МОДУЛЕМ З АНАЛІЗОМ ЧОТИРЬОХ РОЗРЯДІВ ТАКОГО ЧИСЛА ЗА КРОК

Сахибай Тинимбаєв, Сергій Гнатюк, Рат Бердибаєв, Юлія Поліщук, Юлія Бурмак

Сучасна криптографія з відкритим ключем (асиметрична криптографія) дає можливість не лише шифрувати дані, але й вирішувати деякі актуальні проблеми симетричної криптографії – зокрема, проблему розподілу секретних ключів. Проте, алгоритми асиметричної криптографії є досить повільними і ресурсоємними, через що потребують новітніх підходів до підвищення швидкодії та оптимізації їх реалізації на різних платформах. Авторами у статті розглядається питання підвищення швидкодії асиметричних алгоритмів криптографії і пропонується схематичне рішення (пристрій) приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем. Відомо, що такі операції, як множення, піднесення до квадрату і приведення за модулем впливають на швидкодію апаратних пристроїв криптографії. Особливо, операція приведення за модулем є найскладнішою і громіздкою в аспекті реалізації, що потребує особливої уваги вчених і дослідників до розробки алгоритмів і апаратних рішень для цієї проблеми. Таким чином, в цій статті авторами пропонується розробка і дослідження пристрою приведення чисел за модулем з аналізом чотирьох розрядів за крок. Розроблений пристрій був верифікований шляхом перевірки створеного алгоритму опису поведінкової моделі на мові Verilog HDL за допомогою часових діаграм. Тестування показало коректність алгоритму поведінкової моделі, що підтвердило ефективність розробленого пристрою приведення чисел за модулем з аналізом чотирьох розрядів такого числа за крок, а також можливість його використання для криптографічних застосувань.
Ключові слова: *асиметрична криптграфія, арифметичні операції, приведення чисел за модулем, схематичне рішення, алгоритм, швидкодія.*

ВСТУП

Сьогодні криптографічні методи і засоби використовуються для забезпечення конфіденційності і цілісності даних у різних галузях, операційних системах і програмних застосунках [1-6]. Криптографія з відкритим ключем дає можливість не лише шифрувати дані, але й вирішувати деякі актуальні проблеми симетричної криптографії – зокрема, проблему розподілу секретних ключів. Проте, алгоритми асиметричної криптографії є досить повільними і ресурсоємними, через що потребують новітніх підходів до підвищення швидкодії та оптимізації [5-9].

АНАЛІЗ ДОСЛІДЖЕНЬ І ПОСТАНОВКА ЗАВДАННЯ

Авторами розглядається питання підвищення швидкодії асиметричних алгоритмів криптографії і пропонується схематичне рішення приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем.

Відомо, що такі операції, як множення, піднесення до квадрату і приведення за модулем впливають на швидкодію апаратних пристроїв криптографії [9-12]. Особливо, операція приведення за модулем є найскладнішою і громіздкою в аспекті реалізації, що потребує особливої уваги вчених і дослідників до розробки алгоритмів і апаратних рішень для цієї проблеми [2, 6, 8, 13-25].

З огляду на зазначене, **метою** цієї роботи є розробка і дослідження пристрою приведення