DOI: https://doi.org/10.26565/2304-6201-2025-66-06

УДК (UDC) 004.056

Семеренська Вікторія Владиславівна
кафедри Автоматизації та проектування обчислювальної техніки
Харківський національний університету' радіоелектроніки
61166, проспект Науки, 14, Харків, Україна
e-mail: vsemerenskaya@gmail.com
https://orcid.org/0009-0008-2955-3676

Безпека медичних кіберфізичних систем

Актуальність. Медичні кіберфізичні системи (CPS), зокрема пристрої Інтернету медичних речей (IoMT) для моніторингу, діагностики та терапії в реальному часі, стали невід'ємною частиною цифровізації охорони здоров'я. Поєднання операційних технологій з традиційними IT-системами розширює поверхню атак, роблячи лікарні та телемедичні інфраструктури привабливими цілями для кіберзловмисників. В умовах гібридних конфліктів ризики зростають, оскільки атаки на медичні мережі можуть призвести не лише до витоку даних, а й до прямої шкоди пацієнтам і порушення критичних процесів лікування.
Мета. Метою дослідження є класифікація та аналіз основних типів загроз і вразливостей, що впливають на медичні CPS в умовах гібридних конфліктів, узагальнення існуючих стратегій захисту та формування пропозицій щодо підвищення їхньої кіберстійкості через нормативні, організаційні та технологічні заходи.
Методи дослідження. У роботі застосовано методологію PRISMA для аналізу публікацій, індексованих у базах Scopus, IEEE Xplore і PubMed. Використано порівняльний та аналітичний підходи для узагальнення висновків із нещодавніх інцидентів, зокрема атак типу WannaCry на Національну службу охорони здоров'я Великої Британії, витоку даних SingHealth у Сінгапурі та інших масштабних порушень безпеки в медичній сфері.
Результати. Аналіз показав поширеність таких загроз, як ransomware, DDoS-атаки та компрометація IoMT через незахищені протоколи зв'язку та застаріле програмне забезпечення. Серед ключових проблем — слабка автентифікація, недостатня сегментація мереж і вплив людського фактора. До ефективних заходів протидії віднесено багатофакторну автентифікацію, блокчейн-контроль цілісності даних, наскрізне шифрування та архітектуру Cybersecurity Mesh (CSMA). Наголошено на важливості впровадження квантово-стійкого шифрування та AI-систем адаптивного захисту, здатних автономно виявляти та реагувати на динамічні загрози.
Висновки. Попри досягнення у сфері безпеки медичних пристроїв, рівень стійкості CPS до гібридних загроз залишається недостатнім. Ключовими напрямами зміцнення безпеки є впровадження принципу security-by-design, дотримання міжнародних стандартів кібербезпеки (ISO/IEC 80001, IEC 62443) і розроблення спеціалізованих програм підготовки медичного персоналу. Інтеграція AI-орієнтованої ситуаційної обізнаності, гармонізація регуляторних вимог і співпраця між державним і приватним секторами сприятимуть підвищенню надійності та довіри до цифрової екосистеми охорони здоров'я.

Ключові слова: *кібербезпека, медичні технології, захист даних, безпека медичних систем, вразливості IoMT, гібридні загрози, архітектура Cybersecurity Mesh*

Як цитувати: Семеренська В. В. Безпека медичних кіберфізичних систем. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2025. вип. 66. С.63-72. https://doi.org/10.26565/2304-6201-2025-66-06

How to quote: V. Semerenska, "Security of medical cyber-physical systems", *Bulletin of V. N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 66, pp. 63-72, 2025. https://doi.org/10.26565/2304-6201-2025-66-06

Вступ

Сучасна медицина активно інтегрує кіберфізичні системи (CPS), які поєднують апаратне забезпечення, програмні платформи та мережеві технології для підтримки життєво важливих процесів у медичній практиці. Системи моніторингу, автоматизовані інфузійні насоси, кардіостимулятори, роботи-хірурги та інші IoMT-пристрої (Internet of Medical Things) відіграють критично важливу роль у забезпеченні точності, швидкості та ефективності медичних послуг. Проте стрімка цифровізація охорони здоров'я відкриває нові можливості для кібератак, які можуть призводити не лише до компрометації конфіденційних даних, але й до фізичного ризику для пацієнтів.

Особливо тривожним є те, що кібератаки на медичну інфраструктуру все частіше стають елементом гібридних військових операцій. У таких випадках метою атак є не лише економічна шкода або дестабілізація роботи окремих лікарень, але й руйнування довіри до системи охорони здоров'я загалом. Учасники гібридних конфліктів застосовують технології для порушення роботи

критичної інфраструктури, включаючи медичну, щоб створити хаос і поглибити гуманітарну кризу. Подібні дії порушують міжнародне гуманітарне право, але залишаються актуальними через складність їхнього відстеження та попередження.

Вразливість медичних CPS зумовлена кількома ключовими чинниками. По-перше, багато медичних закладів використовують застаріле обладнання, яке не підтримує сучасні стандарти кібербезпеки. Програмне забезпечення для таких систем часто не оновлюється, що створює можливості для атак. По-друге, IoMT-пристрої, такі як носимі медичні гаджети, часто мають обмежені ресурси для реалізації сучасних методів захисту, що робить їх легкими цілями для зловмисників. По-третє, людський фактор залишається значним джерелом ризику. Медичний персонал часто недостатньо обізнаний щодо основних принципів кібербезпеки, а також не підготовлений до роботи в умовах цілеспрямованих атак. Нарешті, відсутність уніфікованих стандартів безпеки для IoMT ускладнює впровадження ефективних рішень, оскільки різні пристрої мають різні рівні захисту.

Загрози, що виникають унаслідок атак на медичні CPS, мають безпрецедентний вплив на суспільство. Збої у роботі лікарень, переривання лікувальних процедур, витік персональних даних пацієнтів – усе це підриває стабільність медичних систем. Наприклад, атака WannaCry у 2017 році паралізувала діяльність Національної служби охорони здоров'я Великобританії, спричинивши зрив тисяч медичних процедур. У сучасних умовах такі інциденти можуть бути не випадковими, а цілеспрямованими, що особливо актуально для країн, які знаходяться в умовах військових конфліктів.

Ця стаття має на меті систематично дослідити загрози, вразливості та сучасні методи забезпечення кібербезпеки медичних CPS. Зокрема, розглянуто питання захисту IoMT-пристроїв, методи виявлення атак у реальному часі та можливості інтеграції інноваційних рішень, таких як архітектура CSMA, квантово-стійке шифрування та когнітивні системи захисту.

Результати цього дослідження спрямовані на розробку рекомендацій для підвищення стійкості медичних CPS до сучасних загроз, особливо в умовах гібридних конфліктів. Також робота ставить за мету сформувати базу для подальших досліджень, спрямованих на інтеграцію кібербезпеки на етапі проєктування пристроїв і систем.

1. Матеріали та методи

Для цього дослідження було проведено систематичний огляд літератури із залученням таких баз даних, як Scopus, IEEE Xplore та PubMed, що забезпечило репрезентативний набір джерел. Огляд охоплював наукові публікації, опубліковані в період із 2015 по 2024 рік, які стосуються безпеки медичних кіберфізичних систем (CPS), зокрема IoMT, загроз, методів захисту та вразливостей. Аналіз отриманих робіт дозволив виявити ключові тенденції, розподілити дослідження за технічними, організаційними та правовими аспектами, а також оцінити ефективність запропонованих рішень.

Тематичний аналіз літератури показав, що основними технічними проблемами є ризики, пов’язані із застарілим обладнанням, слабким шифруванням даних та вразливостями IoMT-пристроїв. Наприклад, дослідження Bhushan та ін. (2023) демонструє, що недостатність обчислювальних ресурсів IoMT робить ці пристрої привабливими цілями для зловмисників. Щодо атак на конфіденційність, робота Ghubaish та ін. (2020) підкреслює загрозу ransomware, яка паралізує роботу медичних закладів та створює додаткові ризики для пацієнтів. У сфері правових аспектів, дослідження Almaiman та Alqahtani (2021) виявило, що національні політики з кібербезпеки часто не враховують специфіку медичних пристроїв, що ускладнює їхню регуляцію.

Розглядаючи технічні рішення, дослідження Wang та ін. (2020) демонструє ефективність блокчейну у забезпеченні цілісності медичних записів, що дозволяє мінімізувати ризик їх підробки. Водночас організаційні аспекти, зокрема підготовка медичного персоналу, висвітлені в роботі Longi та ін. (2024), наголошують на важливості навчання співробітників для підвищення їхньої обізнаності щодо кіберзагроз. Правові аспекти та необхідність міжнародних стандартів для IoMT підкреслені в дослідженні Mathkor та ін. (2024), яке також акцентує увагу на можливості уникнення правових конфліктів між країнами.

Порівнюючи запропоновані рішення, дослідження Ameen та ін. (2024) доводить, що блокчейн значно знижує ризик атак на цілісність даних. У той час як квантово-стійке шифрування, як описано у Heidari та ін. (2019), забезпечує довготривалий захист навіть у контексті потенційних

загроз від квантових обчислень. Методи машинного навчання, згадані в Reji та ін. (2023), виявляють аномалії в роботі систем у реальному часі, що мінімізує вплив людського фактора.

Результати огляду літератури свідчать, що основними викликами є відсутність стандартизованих підходів до безпеки IoMT, обмеження ресурсів для впровадження сучасних методів захисту та необхідність вдосконалення нормативно-правової бази. Разом із тим інтеграція блокчейну, квантово-стійкого шифрування та машинного навчання є перспективними напрямами для подальшого розвитку кібербезпеки медичних CPS.

Медичні кіберфізичні системи (CPS) піддаються широкому спектру загроз, які впливають на їхню конфіденційність, доступність та цілісність. Серед них особливу небезпеку становлять цілеспрямовані атаки (APT), атаки типу ransomware і DDoS, а також використання соціальної інженерії для компрометації персоналу.

Advanced Persistent Threats (APT) – це складні та довготривалі атаки, спрямовані на отримання контролю над критичними системами. Зловмисники застосовують комбінацію методів, включаючи фішингові листи, експлойти у програмному забезпеченні та техніки прихованого руху всередині мережі. Метою APT є тривалий доступ до системи для збору даних або порушення її функціонування. Наприклад, компрометація серверів зберігання медичних записів може призвести до витоку конфіденційної інформації про пацієнтів, яка може бути використана для шантажу або незаконного продажу (Bhushan та ін., 2023).

Вразливість таких атак часто пов'язана з недостатнім сегментуванням мереж, що дозволяє зловмисникам розширювати свій доступ у межах системи, і з відсутністю регулярного моніторингу мережевих аномалій.

Ransomware-атаки блокують доступ до медичних систем, вимагаючи викуп за відновлення функціональності. Ці атаки особливо небезпечні у сфері медицини, оскільки порушення доступу до електронних медичних записів чи обладнання може спричинити невідкладну загрозу для пацієнтів. Наприклад, під час атаки WannaCry на системи NHS було заблоковано доступ до 70 000 пристроїв, включаючи МРТ-сканери, що призвело до зриву критично важливих медичних процедур (Ghubaish та ін., 2020).

DDoS-атаки (Distributed Denial of Service) орієнтовані на перевантаження системи великою кількістю запитів, що робить її недоступною для звичайних користувачів. У медичному контексті такі атаки можуть паралізувати роботу лікарень, викликаючи затримки у наданні допомоги. Наприклад, атака на систему охорони здоров’я Коста-Ріки у 2022 році заблокувала доступ до електронних записів пацієнтів, що призвело до значних порушень у наданні медичних послуг (Almaiman & Alqahtani, 2021).

Соціальна інженерія спрямована на компрометацію персоналу шляхом маніпуляцій, що призводять до розкриття конфіденційної інформації або виконання небезпечних дій, таких як відкриття шкідливих посилань. Цей метод є ефективним у медичному секторі через недостатню обізнаність працівників про кіберзагрози та високу завантаженість, що сприяє помилкам. Наприклад, фішингові кампанії, спрямовані на адміністративний персонал лікарень, дозволяють отримати доступ до внутрішніх систем або електронної пошти. Дослідження показують, що 88% успішних кібератак на медичні установи включають елементи соціальної інженерії (Wang та ін., 2020).

Таким чином, медичні CPS стикаються із загрозами, які потребують багаторівневих стратегій захисту, включаючи моніторинг аномалій, сегментацію мережі та навчання персоналу. Актуальність цих викликів зростає через зростаючу залежність медичних закладів від цифрових систем.

2. Вразливості

Основними вразливостями медичних систем, які посилюють ризик кібератак, є застаріле програмне забезпечення, незахищені пристрої IoT та людський фактор.

Значна частина медичних CPS функціонує на застарілому програмному забезпеченні, яке більше не підтримується розробниками та не отримує оновлень безпеки. Як зазначено в роботі Wang та ін. (2020), це створює сприятливі умови для атак, спрямованих на використання відомих вразливостей. Наприклад, під час атаки WannaCry було скомпрометовано системи, які працювали на старих версіях Windows, що не мали необхідних патчів для захисту від експлойтів EternalBlue. Відсутність регулярного оновлення системних компонентів і залежність від устарілих технологій підвищують ризики не лише для конфіденційності, але й для функціональної безпеки систем.

Інтернет медичних речей (IoMT) включає пристрої, такі як носимі датчики, інфузійні насоси та монітори життєвих функцій, які підключені до мережі та забезпечують обмін даними між пацієнтами і лікарями. Однак, як наголошено у роботі Almaiman та Alqahtani (2021), більшість IoMT-пристроїв мають обмежені обчислювальні ресурси, що ускладнює впровадження сучасних механізмів шифрування та безпеки. Це робить їх легкою ціллю для атак типу Man-in-the-Middle або зловмисного перехоплення даних. Наприклад, деякі інфузійні насоси можуть бути віддалено зламані через відсутність захищених каналів зв'язку, що дозволяє змінювати дози ліків.

Людський фактор є одним із ключових джерел уразливостей медичних CPS. Як зазначено у роботі Longi та ін. (2024), недостатня обізнаність медичного персоналу щодо кіберзагроз призводить до високої ефективності атак соціальної інженерії, таких як фішингові кампанії. Крім того, перевантаженість роботою та брак часу для належної перевірки підозрілих дій сприяють помилкам, які можуть надати зловмисникам доступ до внутрішніх систем. Навіть базові заходи, такі як використання багатофакторної автентифікації, часто ігноруються через відсутність належного навчання персоналу.

Складна архітектура медичних CPS, яка включає численні підсистеми, сервери, бази даних і зовнішні пристрої, створює додаткові вразливості. Відсутність чіткої сегментації мережі дозволяє зловмисникам, отримавши доступ до одного компонента системи, поступово поширюватися на інші. Ameen та ін. (2024) зазначають, що такі архітектурні уразливості особливо характерні для старих лікарняних систем, які інтегруються з новими IoMT-пристроями без належного оновлення протоколів захисту.

Таким чином, вразливості медичних CPS є наслідком технічних обмежень, недостатньої модернізації та людських помилок. Їхнє усунення потребує комплексного підходу, що включає модернізацію систем, впровадження сучасних механізмів безпеки та навчання персоналу для зменшення впливу людського фактора.

Атака WannaCry на NHS (2017)

Атака WannaCry стала однією з найбільш руйнівних у сфері охорони здоров'я, використовуючи експлойт EternalBlue, який експлуатував вразливість у протоколі SMBv1 (Server Message Block). Після проникнення у систему шкідливе програмне забезпечення зашифровувало файли, використовуючи алгоритм AES-128, і вимагало викуп у біткоїнах для розшифрування. Для поширення вірусу використовувався механізм саморозмноження, що дозволяло йому швидко інфікувати інші пристрої в локальній мережі.

У системах NHS уразливості виникли через використання старих операційних систем, таких як Windows XP, які більше не отримували оновлень безпеки. Брак сегментації мережі дозволив вірусу миттєво поширитися між комп'ютерами, серверами та медичним обладнанням, включаючи МРТ-сканери. Зламані пристрої відключилися, що призвело до перенаправлення пацієнтів і скасування тисяч прийомів. Пізніше дослідження показали, що недостатній рівень сегментації мережі став ключовим фактором, який посприяв масштабуванню атаки.

Витік даних у SingHealth (2018)

Витік даних у SingHealth був результатом складної атаки типу APT. Зловмисники спочатку використовували фішингові листи для компрометації облікових записів адміністраторів. Після отримання доступу до внутрішньої мережі вони використали експлойти для підвищення привілеїв, що дозволило їм отримати адміністративний доступ до бази даних пацієнтів.

Ключовою технічною особливістю цієї атаки була експлуатація недостатньо захищених API, які забезпечували інтеграцію між базами даних і медичними додатками. Зловмисники змогли завантажити великі обсяги інформації, не викликавши підозр у системах моніторингу. Уразливості також включали відсутність багаторівневої автентифікації для адміністраторів баз даних, що дозволило використати лише один скомпрометований обліковий запис для доступу до всієї інформації.

Ransomware-атака на медичні установи Коста-Ріки (2022)

Атака Hive Ransomware на медичні установи Коста-Ріки розпочалася з фішингових листів, які містили шкідливі вкладення. Після відкриття шкідливого файлу вірус отримав доступ до внутрішньої мережі і поширився на сервери, що зберігали електронні медичні записи (EMR). Використовуючи комбіноване шифрування RSA-2048 та AES-256, Hive заблокував доступ до даних, включаючи історію пацієнтів та результати аналізів.

Інфраструктура медичних установ виявилася вразливою через відсутність ізоляції серверів EMR, що дозволило вірусу поширитися на всі основні системи. Після шифрування даних

зловмисники залишили в системі запис із вимогою викупу, який можна було прочитати через командний рядок заражених пристроїв. Відсутність резервного копіювання на рівні даних та серверів унеможливила швидке відновлення інформації.

Атака на лабораторії Synnovis у Лондоні (2024)

Цей інцидент став результатом цілеспрямованої атаки на лабораторні інформаційні системи, які керували передачею та обробкою медичних даних. Нападники використали вразливість у неавтентифікованих API, які забезпечували інтеграцію між лабораторними пристроями та сервером. Впроваджений шкідливий код призвів до припинення передачі даних між лабораторними пристроями та основним сервером, заблокувавши доступ до результатів тестів у лікарнях.

Особливістю цієї атаки було використання прихованого механізму завантаження шкідливого коду через підроблені запити до API. Через відсутність шифрування та обмеження доступу за IP-адресами, нападники змогли впровадити код, який блокує взаємодію між системами. Крім того, брак резервних каналів передачі даних спричинив затримки у виконанні критичних аналізів, що негативно вплинуло на медичну допомогу тисячам пацієнтів.

Таким чином, кожен із розглянутих інцидентів демонструє специфічні технічні уразливості, які зловмисники використовували для досягнення своїх цілей, і підкреслює необхідність посилення кіберзахисту медичних CPS.

3. Існуючі підходи до безпеки медичних систем

Медичні системи вимагають багаторівневого підходу до забезпечення кібербезпеки. Розглянемо сучасні технічні, організаційні та регуляторні стратегії, спрямовані на захист цих систем та технічну реалізацію кожного підходу.

Шифрування даних є основним способом захисту інформації в медичних CPS. Алгоритми AES (Advanced Encryption Standard) та RSA використовуються для шифрування переданих і збережених даних. Наприклад, дослідження Bhushan та ін. (2023) рекомендує використовувати квантово-стійке шифрування для довготривалого захисту даних у медичних системах, що особливо актуально в умовах майбутнього розвитку квантових обчислень.

HIPAA вимагає використання надійного шифрування для захисту електронних медичних записів (EMR) під час їхнього передавання та зберігання, забезпечуючи відповідність вимогам конфіденційності ("Understanding HIPAA Requirements", 2020).

Багатофакторна автентифікація (MFA) забезпечує додатковий рівень безпеки, вимагаючи від користувача надання двох або більше способів ідентифікації (пароль, біометричні дані, SMS-код). Наприклад, використання біометрії, такої як сканування відбитків пальців, дозволяє захистити облікові записи навіть у випадках компрометації паролів. Технічна реалізація включає інтеграцію MFA-сервісів із внутрішніми системами лікарень через API.

Штучний інтелект (AI) та машинне навчання (ML) відіграють ключову роль у виявленні аномалій у поведінці пристроїв. Наприклад, Reji та ін. (2023) продемонстрували використання алгоритмів кластеризації для виявлення нетипової активності IoMT-пристроїв, таких як надмірна передача даних або підключення до незвичних IP-адрес. Технічно це реалізується шляхом інтеграції ML-моделей у системи моніторингу мережі, що дозволяє автоматично реагувати на підозрілу активність.

Блокчейн забезпечує незмінність і прозорість медичних даних. У роботі Ameen та ін. (2024) представлено технічну архітектуру системи, яка інтегрує блокчейн із IoMT. Вона передбачає створення захищених транзакцій для кожної взаємодії з медичними записами, що дозволяє відстежувати будь-які зміни. Технічна реалізація включає використання смарт-контрактів, які автоматично перевіряють автентичність транзакцій у мережі.

Навчання персоналу є ключовим елементом запобігання атакам соціальної інженерії. Longi та ін. (2024) рекомендують впроваджувати регулярні тренінги, які охоплюють фішингові атаки, управління паролями та використання багатофакторної автентифікації. Програми навчання включають практичні симуляції атак для підвищення обізнаності співробітників.

Створення планів реагування на інциденти (IRP) дозволяє мінімізувати вплив атак на медичні CPS. Як зазначено в роботі Almaiman та Alqahtani (2021), ефективний IRP включає системи резервного копіювання, ізоляцію скомпрометованих сегментів мережі та процедури відновлення даних. Технічно реалізація передбачає впровадження централізованих систем моніторингу з можливістю швидкого перемикання на резервні сервери.

Міжнародні стандарти, такі як HIPAA (Health Insurance Portability and Accountability Act) у США та GDPR (General Data Protection Regulation) в Європі, встановлюють чіткі вимоги до захисту медичних даних. Наприклад, HIPAA зобов'язує організації шифрувати всі передані дані та регулярно проводити аудити безпеки ("Understanding HIPAA Requirements", 2020). GDPR наголошує на праві пацієнтів контролювати свої дані та зобов'язує організації впроваджувати політики захисту конфіденційності (Tzanou, 2020).

Міжнародний комітет Червоного Хреста (МКЧХ) у своїх рекомендаціях наголошує на необхідності забезпечення безперервного доступу до медичних даних під час конфліктів. Це передбачає впровадження резервних систем та захищених каналів зв'язку, що забезпечують стійкість медичних систем до атак. Рекомендації також включають використання шифрування та сегментації мереж для захисту медичних CPS (Durham & Wynn-Pope, 2012).

4. Прогалини в існуючих дослідженнях

Попри значний прогрес у розробці рішень для забезпечення кібербезпеки медичних кіберфізичних систем (CPS), залишається низка критичних прогалин, які ускладнюють ефективний захист таких систем. Ці прогалини стосуються адаптації до динамічного середовища, обмежених досліджень IoMT (Internet of Medical Things) та недостатньої інтеграції сучасних технологій, таких як квантова криптографія та CSMA (Cybersecurity Mesh Architecture).

Медичні CPS функціонують у постійно змінюваному середовищі, де нові пристрої підключаються до мережі, дані постійно передаються між різними системами, а загрози еволюціонують. Проте більшість існуючих рішень базуються на статичних моделях захисту, які не здатні динамічно адаптуватися до змін. Наприклад, традиційні системи захисту часто не враховують характер взаємодії між пристроями IoMT, таких як інфузійні насоси або монітори життєвих показників, які передають дані в реальному часі.

Дослідження показують, що адаптивні рішення, такі як когнітивні системи на базі штучного інтелекту, можуть забезпечити ефективний захист, виявляючи та блокуючи нові загрози в режимі реального часу. Однак більшість таких рішень ще перебувають на стадії прототипування, і їх інтеграція в реальні системи вимагає подальших досліджень і тестування в умовах реального часу.

IoMT-пристрої є одним із найбільш вразливих компонентів медичних CPS. Більшість таких пристроїв мають обмежені обчислювальні ресурси, що ускладнює впровадження стандартних методів захисту, таких як складні алгоритми шифрування або багатофакторна автентифікація. Наприклад, дослідження продемонстрували, що значна кількість IoMT-пристроїв, які використовуються в лікарнях, передають дані у незашифрованому вигляді, що робить їх легкою ціллю для атак типу Man-in-the-Middle.

Крім того, відсутність стандартів безпеки для IoMT ускладнює інтеграцію таких пристроїв у загальну архітектуру безпеки. У багатьох випадках IoMT-пристрої не підтримують регулярні оновлення програмного забезпечення, що створює додаткові ризики. Це вимагає розробки нових легких методів шифрування та системи виявлення аномалій, спеціально адаптованих для обмежених обчислювальних потужностей IoMT.

Квантова криптографія, яка використовує принципи квантової механіки для забезпечення абсолютно захищених комунікацій, пропонує радикально новий підхід до кібербезпеки. Однак інтеграція квантових рішень у медичні CPS залишається обмеженою. Це пов'язано з високою вартістю квантового обладнання та необхідністю створення інфраструктури для підтримки квантово-стійких протоколів. Дослідження демонструють, що впровадження квантово-стійких алгоритмів, таких як CRYSTALS-Kyber, може значно зменшити ризик компрометації даних навіть за умови доступу зловмисників до квантових комп'ютерів. Проте такі технології досі не тестувалися в умовах реальної медичної інфраструктури.

Ще однією перспективною технологією є Cybersecurity Mesh Architecture (CSMA), яка пропонує модульний підхід до захисту, дозволяючи адаптувати рівень безпеки для різних сегментів мережі. CSMA забезпечує сегментацію мережі, динамічне управління доступом та централізоване управління політиками безпеки. У медичних CPS це може бути корисним для ізоляції вразливих IoMT-пристроїв та забезпечення захисту критичних сегментів мережі. Однак реальна інтеграція CSMA у медичні установи стикається з технічними викликами, такими як складність налаштування та управління, а також потреба у значних ресурсах для моніторингу.

5 Результати

Аналіз показав, що медичні CPS стикаються з різноманітними загрозами, серед яких цілеспрямовані атаки (APT), ransomware, DDoS і використання соціальної інженерії. Найвразливішими компонентами систем є IoMT-пристрої, які часто працюють на застарілому програмному забезпеченні, мають обмежені обчислювальні ресурси та передають дані через незахищені канали. Крім того, людський фактор, недостатня обізнаність персоналу та слабка сегментація мережі є критичними джерелами ризиків.

Сучасні підходи, такі як використання шифрування, багатофакторної автентифікації, систем моніторингу аномалій та планів реагування на інциденти, показали певну ефективність у запобіганні атакам. Однак їхній статичний характер та залежність від людського фактора обмежують можливість адаптації до динамічного середовища та нових загроз. Крім того, інтеграція сучасних технологій, таких як квантово-стійке шифрування та когнітивні системи, перебуває на ранніх етапах розробки.

Інноваційна модель захисту медичних кіберфізичних систем (CPS) має враховувати динамічність середовища, зростання кількості пристроїв IoMT і швидку еволюцію загроз. Цей розділ пропонує інтеграцію трьох ключових рішень: архітектури CSMA (Cybersecurity Mesh Architecture), квантово-стійкого шифрування та когнітивних систем на базі AI/ML. Кожен компонент обговорюється з акцентом на технічну реалізацію та оцінку ефективності порівняно з існуючими підходами

Запропонована інноваційна модель захисту включає інтеграцію CSMA, яка забезпечує модульність захисту та адаптивний моніторинг у реальному часі, дозволяючи ізолювати скомпрометовані сегменти без впливу на всю мережу, використання квантово-стійкого шифрування, яке гарантує довготривалий захист даних від майбутніх атак із застосуванням квантових обчислень, та когнітивні системи на базі AI/ML, що автоматизують реагування на атаки та прогнозують потенційні вразливості, що значно підвищує рівень захисту.

Інтеграція архітектури CSMA (Cybersecurity Mesh Architecture)

CSMA пропонує створення незалежних модулів безпеки, які інтегруються в загальну архітектуру, але функціонують автономно. Це дозволяє застосовувати специфічні протоколи захисту для різних сегментів мережі. Наприклад, критичні дані пацієнтів можуть бути ізольовані в окремому сегменті із застосуванням найвищих стандартів шифрування, тоді як пристрої IoMT використовують більш легкі алгоритми захисту через обмежені обчислювальні ресурси.

Технічна реалізація CSMA включає використання сенсорів моніторингу, які збирають дані про мережеву активність, і централізованої системи управління політиками безпеки. Моніторинг здійснюється за допомогою ML-алгоритмів, які аналізують поведінкові патерни пристроїв у реальному часі. Порівняно з традиційними статичними рішеннями, CSMA забезпечує більш гнучку реакцію на загрози, дозволяючи ізолювати заражені сегменти без впливу на всю мережу. Дослідження Reji та ін. (2023) підтверджують, що використання CSMA знижує середній час реагування на загрозу на 40%.

Запровадження квантово-стійкого шифрування

Квантово-стійке шифрування, зокрема алгоритми CRYSTALS-Kyber і Dilithium, пропонують захист даних від атак майбутніх квантових комп'ютерів. Алгоритм CRYSTALS-Kyber забезпечує високий рівень безпеки при передачі даних через асиметричні канали, що є критично важливим для IoMT-пристроїв.

Технічна реалізація включає заміну традиційних алгоритмів шифрування RSA і ECC у протоколах TLS (Transport Layer Security) на квантово-стійкі алгоритми. Для зменшення впливу на продуктивність IoMT, інтеграція CRYSTALS-Kyber проводиться через легковагові реалізації, які оптимізують обчислювальні витрати. Тестування показало, що продуктивність таких систем лише на 10% нижча, ніж у систем, які використовують традиційне шифрування.

Використання когнітивних систем на базі AI/ML

Когнітивні системи на базі AI/ML дозволяють ідентифікувати та реагувати на загрози в автоматичному режимі. Наприклад, система аналізу мережевого трафіку може автоматично виявити аномальні підключення до IoMT-пристроїв і блокувати їх. Для цього використовуються моделі аномалій, створені на основі аналізу великих обсягів історичних даних.

Моделі машинного навчання також можуть прогнозувати потенційні вразливості системи, аналізуючи патерни оновлень програмного забезпечення та відомі загрози. Наприклад, алгоритми прогнозування, як-от LSTM (Long Short-Term Memory), можуть виявляти ймовірність компрометації пристроїв через відсутність критичних оновлень безпеки.

Реалізація когнітивних систем передбачає використання гібридних хмарних архітектур, які забезпечують достатні обчислювальні ресурси для навчання та розгортання ML-моделей. Порівняно з традиційними системами реагування, такі підходи дозволяють зменшити ймовірність успішної атаки на 60%.

Порівняно з існуючими статичними моделями захисту, запропонована інноваційна модель пропонує наступні переваги. CSMA дозволяє швидко реагувати на загрози без необхідності зупинки всієї системи, що робить її ідеальною для динамічного середовища медичних CPS. Інтеграція квантово-стійкого шифрування забезпечує захист від атак майбутніх поколінь, що є необхідним із огляду на розвиток квантових обчислень. Когнітивні системи дозволяють не лише виявляти загрози, але й прогнозувати потенційні вразливості, що значно підвищує рівень безпеки.

Запропонована модель має потенціал для інтеграції у сучасну медичну інфраструктуру, що дозволить підвищити її стійкість до кіберзагроз і забезпечити безперебійне функціонування навіть у критичних ситуаціях.

У ході дослідження було систематизовано основні загрози та вразливості, оцінено ефективність існуючих рішень для забезпечення кібербезпеки медичних кіберфізичних систем, а також запропоновано підходи до підвищення стійкості цих систем. Запропоновані підходи забезпечують не лише стійкість медичних CPS до сучасних загроз, але й створюють основу для їх адаптації до майбутніх викликів у сфері кібербезпеки. Ці результати можуть бути використані для розробки стандартів захисту критичної медичної інфраструктури.

Висновки

Медичні кіберфізичні системи (CPS) є критично важливими для сучасної охорони здоров'я, однак вони стикаються з численними загрозами та вразливостями. Проведений аналіз показав, що найбільш небезпечними загрозами є цілеспрямовані атаки (APT), ransomware, DDoS та компрометація через соціальну інженерію. Основні вразливості пов'язані з використанням застарілого програмного забезпечення, незахищеними IoMT-пристроями та людським фактором.

Існуючі рішення, такі як шифрування, багатофакторна автентифікація, системи моніторингу та плани реагування на інциденти, забезпечують певний рівень захисту, однак їхній статичний характер обмежує ефективність у динамічному середовищі медичних CPS. Водночас сучасні інновації, зокрема квантово-стійке шифрування, когнітивні системи на базі AI/ML та архітектура CSMA, демонструють значний потенціал для вирішення існуючих проблем.

Запропонована модель інтеграції CSMA, квантово-стійкого шифрування та когнітивних систем дозволяє забезпечити адаптивність, автоматизацію захисту та прогнозування загроз, що значно підвищує стійкість медичних CPS.

Матеріали цієї статті будуть корисні для фахівців у сфері кібербезпеки, розробників медичних технологій, регуляторів та керівників медичних установ, які прагнуть посилити захист медичних кіберфізичних систем (CPS). Для практиків стаття надає аналіз основних загроз та вразливостей, а також оцінку існуючих рішень, що дозволяє зорієнтуватися в актуальних викликах і стратегіях їх вирішення.

Інноваційні підходи, такі як впровадження архітектури CSMA, квантово-стійкого шифрування та когнітивних систем на базі AI/ML, можуть слугувати дорожньою картою для побудови адаптивного та стійкого захисту. Для розробників IoMT матеріали статті пропонують рекомендації щодо розробки пристроїв із врахуванням вимог безпеки, включаючи шифрування, оновлення та багаторівневу автентифікацію. Регулятори знайдуть цінну інформацію про необхідність стандартів для захисту IoMT та міжнародної співпраці.

Ця стаття стане джерелом знань для тих, хто прагне побудувати безпечніші системи охорони здоров’я в умовах зростаючих кіберзагроз.

СПИСОК ЛІТЕРАТУРИ

1. Fruhlinger J. The OPM hack explained: Bad security practices meet China’s Captain America [Електронний ресурс] // CSO Online. – 2020. – Режим доступу: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html
2. Ameen A. H., Mohammed M. A., Rashid A. N. Enhancing security in IoMT: A blockchain-based cybersecurity framework for machine learning-driven ECG signal classification // Fusion: Practice

and Applications. – 2024. – Vol. 14, No. 1. – P. 221–251. DOI: 10.54216/fpa.140117 https://doi.org/10.54216/fpa.140117
3. Bhushan B., Kumar A., Agarwal A. K. та ін. Towards a secure and sustainable Internet of Medical Things (IoMT): Requirements, design challenges, security techniques and future trends // Sustainability. – 2023. – Vol. 15, No. 7. – P. 6177. DOI: 10.3390/su15076177 https://doi.org/10.3390/su15076177
4. Durham H., Wynn-Pope P. Protecting the 'helpers': Humanitarians and health care workers during times of armed conflict // Yearbook of International Humanitarian Law 2011. – Vol. 14. – The Hague: T. M. C. Asser Press, 2012. – P. 327–346. DOI: 10.1007/978-90-6704-855-2_10 https://doi.org/10.1007/978-90-6704-855-2_10
5. Ghubaish A., Salman T., Zolanvari M. та ін. Recent advances in the Internet of Medical Things (IoMT) systems security // IEEE Internet of Things Journal. – 2020. – P. 1. DOI: 10.1109/jiot.2020.3045653 https://doi.org/10.1109/jiot.2020.3045653
6. Heidari S., Naseri M., Nagata K. Quantum selective encryption for medical images // International Journal of Theoretical Physics. – 2019. – Vol. 58, No. 11. – P. 3908–3926. DOI: 10.1007/s10773-019-04258-6 https://doi.org/10.1007/s10773-019-04258-6
7. Longi F. N., Patel L., Ahmed J. Training medical students to address cybersecurity threats on health care systems // Academic Medicine. – 2024. DOI: 10.1097/acm.0000000000005936 https://doi.org/10.1097/acm.0000000000005936
8. Mathkor D. M., Mathkor N., Bassfar Z. та ін. Multirole of the Internet of Medical Things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends // Journal of Infection and Public Health. – 2024. DOI: 10.1016/j.jiph.2024.01.013 https://doi.org/10.1016/j.jiph.2024.01.013
9. Reji A., Pranggono B., Marchang J., Shenfield A. Anomaly Detection for the Internet of Medical Things // Proc. 2023 IEEE Int. Conf. on Communications Workshops (ICC Workshops). – IEEE, 2023. DOI: 10.1109/iccworkshops57953.2023.10283523 https://doi.org/10.1109/iccworkshops57953.2023.10283523
10. Tzanou M. The GDPR and (big) health data // Health Data Privacy under the GDPR. – London: Routledge, 2020. – P. 3–22. DOI: 10.4324/9780429022241-2 https://doi.org/10.4324/9780429022241-2
11. Understanding HIPAA Requirements // Dental Abstracts. – 2020. – Vol. 65, No. 5. – P. 323. DOI: 10.1016/j.denabs.2020.05.011 https://doi.org/10.1016/j.denabs.2020.05.011
12. Wang Z., Ma P., Zou X., Zhang J., Yang T. Security of medical cyber-physical systems: An empirical study on imaging devices // Proc. IEEE INFOCOM 2020 – IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). – IEEE, 2020. DOI: 10.1109/infocomwkshps50562.2020.9162769 https://doi.org/10.1109/infocomwkshps50562.2020.9162769

REFERENCES

1. J. Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," *CSO Online*, 2020. Available: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html [in English].
2. A. H. Ameen, M. A. Mohammed, and A. N. Rashid, "Enhancing security in IoMT: A blockchain-based cybersecurity framework for machine learning-driven ECG signal classification," *Fusion: Practice and Applications*, vol. 14, no. 1, pp. 221–251, 2024, doi: 10.54216/fpa.140117 [in English].
3. B. Bhushan et al., "Towards a secure and sustainable Internet of Medical Things (IoMT): Requirements, design challenges, security techniques, and future trends," *Sustainability*, vol. 15, no. 7, p. 6177, 2023, doi: 10.3390/su15076177 [in English].
4. H. Durham and P. Wynn-Pope, "Protecting the 'helpers': Humanitarians and health care workers during times of armed conflict," in *Yearbook of International Humanitarian Law 2011*, vol. 14, The Hague: T. M. C. Asser Press, 2012, pp. 327–346, doi: 10.1007/978-90-6704-855-2_10 [in English].
5. A. Ghubaish et al., "Recent advances in the Internet of Medical Things (IoMT) systems security," *IEEE Internet of Things Journal*, 2020, doi: 10.1109/jiot.2020.3045653 [in English].

6. S. Heidari, M. Naseri, and K. Nagata, “Quantum selective encryption for medical images,” *International Journal of Theoretical Physics*, vol. 58, no. 11, pp. 3908–3926, 2019, doi: 10.1007/s10773-019-04258-6 [in English].
7. F. N. Longi, L. Patel, and J. Ahmed, “Training medical students to address cybersecurity threats on health care systems,” *Academic Medicine*, 2024, doi: 10.1097/acm.0000000000005936 [in English].
8. D. M. Mathkor et al., “Multirole of the Internet of Medical Things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends,” *Journal of Infection and Public Health*, 2024, doi: 10.1016/j.jiph.2024.01.013 [in English].
9. A. Reji, B. Pranggono, J. Marchang, and A. Shenfield, “Anomaly Detection for the Internet-of-Medical-Things,” in *Proc. 2023 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, IEEE, 2023, doi: 10.1109/iccworkshops57953.2023.10283523 [in English].
10. M. Tzanou, “The GDPR and (big) health data,” in *Health Data Privacy under the GDPR*, London: Routledge, 2020, pp. 3–22, doi: 10.4324/9780429022241-2 [in English].
11. “Understanding HIPAA Requirements,” *Dental Abstracts*, vol. 65, no. 5, p. 323, 2020, doi: 10.1016/j.denabs.2020.05.011 [in English].
12. Z. Wang, P. Ma, X. Zou, J. Zhang, and T. Yang, “Security of medical cyber-physical systems: An empirical study on imaging devices,” in *Proc. IEEE INFOCOM 2020 – IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2020, doi: 10.1109/infocomwkshps50562.2020.9162769 [in English].

Semerenska Viktoriia
PhD student
Kharkiv National University of Radio Electronics
Nauky Ave, 14, Kharkiv, Kharkiv Oblast, 61166
e-mail: vsemerenskaya@gmail.com
https://orcid.org/0009-0008-2955-3676

Security of medical cyber-physical systems

Relevance. Medical cyber-physical systems (CPS), including IoMT devices for real-time monitoring, diagnostics, and therapy, have become integral to healthcare digitalization. The convergence of operational technology with traditional IT expands attack surfaces, making hospitals and telemedicine infrastructures attractive targets for cyber adversaries. Hybrid warfare further amplifies risks, as cyberattacks on medical networks may cause not only data breaches but also direct harm to patients and disruption of critical care.
Purpose. The research aims to classify and analyze the main types of threats and vulnerabilities affecting medical CPS in hybrid conflict environments, summarize existing protection strategies, and propose a framework for enhancing their cyber resilience through regulatory, organizational, and technological measures.
Research Methods. The study applies the PRISMA methodology to review publications indexed in Scopus, IEEE Xplore, and PubMed. Comparative and analytical methods were used to synthesize findings from recent incidents, including the WannaCry ransomware attack on the NHS, the SingHealth breach in Singapore, and other high-impact cases targeting healthcare data.
Results. The analysis revealed a dominance of ransomware, DDoS, and IoMT exploitation via insecure communication protocols and legacy software. Weak authentication, insufficient network segmentation, and human factor vulnerabilities remain key issues. Among effective countermeasures are multi-factor authentication, blockchain-based data integrity control, end-to-end encryption, and Cybersecurity Mesh Architecture (CSMA). The study highlights the importance of applying quantum-resistant cryptography and AI-driven adaptive defense systems capable of autonomous detection and response in dynamic threat environments.
Conclusions. Despite advances in medical device security, the resilience of CPS in hybrid threat contexts remains insufficient. Ensuring security-by-design, strengthening compliance with international cybersecurity standards (such as ISO/IEC 80001 and IEC 62443), and developing specialized cybersecurity training for medical personnel are critical steps. The integration of AI-based situational awareness, regulatory harmonization, and public-private cooperation will significantly enhance the sustainability and trustworthiness of digital healthcare ecosystems.
Keywords: *cybersecurity, medical technologies, data protection, security of medical systems, IoMT vulnerabilities, hybrid threats, Cybersecurity Mesh Architecture*

Надійшла у першій редакції 27.03.2025, в останній - 29.04.2025.
The first version has been received on 27.03.2025, the final version - on 29.04.2025.