ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

контроль сетевого взаимодействия (например, с помощью eBPF или iptables) и чёткое понимание цели их использования.

Заключение

В ходе настоящего исследования продемонстрирована высокая эффективность использования honeypot-систем как инструмента проактивной защиты информационных систем. На основе экспериментальных данных показано, что даже с минимальными затратами можно получить ценную информацию о текущих атаках, применяемых инструментах и поведении злоумышленников. Это делает honeypot-системы важным элементом современной архитектуры кибербезопасности, наряду с SIEM, NIDS и системами анализа поведения.
Результаты работы могут быть полезны специалистам по информационной безопасности при проектировании систем обнаружения атак, формировании стратегии киберразведки и разработке обучающих платформ для подготовки кадров SOC-центров.

Список использованных источников

1. Spitzner L. Honeypots: Tracking Hackers. Addison-Wesley, 2002.

2. Provos N., Holz T. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley, 2007.

3. Mokube I., Adams M. Honeypots: Concepts, Approaches, and Challenges // Proceedings of the 45th ACM Southeast Conference. ACM, 2007.

4. Танкелевич В. Системы-ловушки (Honeypots) как инструмент повышения уровня защищенности информационных систем // Информационная безопасность, №1, 2019.

5. Cowrie Honeypot Project. URL: https://github.com/cowrie/cowrie

6. Dionaea Honeypot. URL: https://github.com/DinoTools/dionaea

УДК 004.056:614.2

АНАЛИЗ РИСКАМИ БЕЗОПАСНОСТИ ДАННЫХ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Нуриева Дана Робертовна
nurievadana5@gmail.com
Исайнова Алия Насиповна
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Аннотация

Предмет. В последние годы цифровизация здравоохранения значительно ускорила процессы обработки и хранения медицинских данных. Медицинские учреждения все чаще используют электронные информационные системы, облачные платформы и технологии дистанционного медицинского обслуживания. Однако вместе с этим значительно возросли и риски утечек, несанкционированного доступа и кибератак на базы данных пациентов.

Медицинская информация является крайне чувствительной, поскольку содержит персональные данные, историю болезней, результаты анализов и другие сведения, которые могут использоваться злоумышленниками в преступных целях, включая мошенничество, шантаж и незаконную продажу данных. Казахстан, активно развивающий сферу цифровой медицины, столкнулся с необходимостью усиления мер по обеспечению кибербезопасности в медицинских учреждениях. Государственная система «Дамумед», предназначенная для автоматизации медицинских процессов, подвергалась критике за уязвимости, что подчеркивает необходимость совершенствования системы защиты данных.

Актуальность исследования обусловлена потребностью в системном анализе существующих угроз, выявлении слабых мест в системе безопасности медицинских учреждений и разработке эффективных подходов к управлению рисками. Это особенно важно в контексте развития законодательных и нормативных требований в Казахстане и приведения системы защиты данных в соответствие с международными стандартами.

Цели. Комплексным авторским исследованием являются системы управления рисками информационной безопасности в медицинских учреждениях Казахстана.

Предмет исследования. Механизмы выявления, анализа и минимизации угроз, направленных на компрометацию медицинских данных, а также способы адаптации международных стандартов к казахстанским условиям.

Методология. Исследование основано на сочетании нескольких методологических подходов:

- Онтологический анализ позволяет определить и систематизировать ключевые понятия, связанные с информационной безопасностью медицинских данных, а также разработать структуру классификации угроз и уязвимостей;
- Сравнительный анализ применяется для сопоставления казахстанской системы «Дамумед» с зарубежными медицинскими информационными системами, выявления различий в подходах к обеспечению безопасности данных;
- Системный анализ используется для изучения структуры угроз, взаимосвязи факторов риска и последствий их реализации;
- Аналитический обзор литературы позволяет выявить основные тенденции в развитии информационной безопасности медицинских учреждений и интеграции нормативных стандартов;
- Методы количественной оценки рисков применяются для расчета потенциальных угроз и вероятности их реализации.

Научная новизна заключается в комплексном изучении проблематики кибербезопасности медицинских учреждений Казахстана, адаптации международных стандартов к отечественным условиям и разработке модели управления рисками, ориентированной на национальную систему здравоохранения.

Результаты.

Таблица 1

Классификация ключевых понятий кибербезопасности медицинских данных

Термин	Определение	Применение в кибербезопасности медицины
Доступность	Гарантия того, что данные доступны уполномоченным лицам в нужный момент	Обеспечение работы медицинских информационных систем в экстренных ситуациях
Целостность	Защита информации от несанкционированных изменений и подделок	Предотвращение модификации медицинских записей, защита от атак на базы данных
Киберугрозы	Потенциальные атаки на информационные системы, направленные на кражу, модификацию или уничтожение данных	Фишинг, ransomware, DDoS-атаки, уязвимости в ПО
Уязвимости	Слабые места в системе, которые могут быть использованы злоумышленниками	Ошибки в коде, устаревшие системы, недостаточная подготовка персонала

Управление рисками	Анализ угроз, оценка вероятности атак, разработка мер реагирования	Внедрение стандартов безопасности (ISO 27001, NIST), мониторинг кибератак
Источник: [1 - 4]		

Как показано в Таблице 1, ключевые понятия кибербезопасности медицинских данных включают конфиденциальность, доступность и целостность (CIA-триада), а также управление рисками и киберугрозы. Однако, в отличие от международных стандартов, в казахстанских исследованиях большее внимание уделяется техническим аспектам защиты, а не адаптивности системы к возможным атакам и стратегиям восстановления данных. Это указывает на необходимость дальнейшей интеграции международных стандартов, таких как NIST Cybersecurity Framework и ISO 27001, в национальную практику кибербезопасности, что позволит обеспечить не только защиту, но и устойчивость медицинских информационных систем к современным угрозам.

Как следует из данных Таблицы 2, элементы зарубежных стандартов реализуются преимущественно в государственных учреждениях, тогда как частный сектор зачастую остаётся вне рамок строгого регулирования. Для формирования полноценной системы информационной безопасности в здравоохранении требуется усиление институциональных механизмов, развитие программ подготовки специалистов, гармонизация законодательства с глобальными нормами и создание национальных механизмов сертификации, что обеспечит устойчивость и доверие к цифровым медицинским сервисам.[5-6]

Таблица 2

Сравнительная характеристика международных стандартов кибербезопасности в медицине.

Стандарт	Основные положения	Применение в здравоохранении	Адаптация в Казахстане
ISO/IEC 27001	Комплексная система управления информационной безопасностью (ISMS), включает идентификацию рисков, контроль доступа, меры по защите данных, шифрование и аудит безопасности	Используется для защиты электронных медицинских карт, систем хранения данных пациентов, а также контроля над доступом к медицинской информации	Внедряется в крупных медицинских учреждениях, однако сертификация сложна и требует значительных финансовых затрат для частных клиник
HIPAA	Обеспечение конфиденциальности пациентов, строгий контроль доступа, требования к шифрованию данных, обязательные меры по аудиту и мониторингу	Применяется операторами медицинской информации, больницами, страховыми компаниями и провайдерами электронных медицинских записей в США	Частично адаптирован в Казахстане – используется шифрование данных и многофакторная аутентификация, но на законодательном уровне нет четких требований к соблюдению HIPAA
NIST Cybersecurity Framework	Комплексный подход к управлению киберрисками, включает выявление угроз, защиту данных, мониторинг атак, реагирование и восстановление системы	Используется для защиты медицинских систем, раннего обнаружения атак, разработки планов реагирования на инциденты	Отдельные принципы применяются в государственных клиниках, особенно в сфере мониторинга угроз и реагирования на инциденты

Архитектура системы «Дамумед» построена по клиент-серверной модели, что обеспечивает гибкость, масштабируемость и отказоустойчивость платформы. Центральной частью системы является серверная инфраструктура, включающая в себя централизованную базу данных, серверы приложений, модули безопасности и распределенные точки доступа.

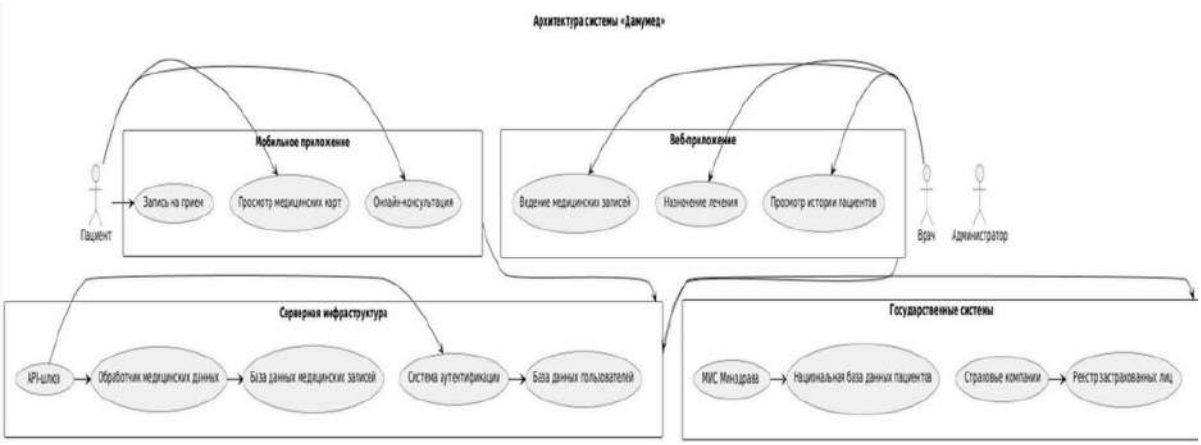

Рисунок 1 Схема архитектуры системы «Дамумед».

Таблица 3

Основные угрозы безопасности в системе «Дамумед» и методы защиты

Тип угрозы	Описание	Методы защиты
Фишинговые атаки	Злоумышленники рассылают поддельные письма или создают фальшивые сайты, чтобы украсть учетные данные пользователей	Обучение персонала, двухфакторная аутентификация (2FA), фильтрация подозрительных e-mail
Программы-вымогатели (ransomware)	Шифрование данных с требованием выкупа за их восстановление	Регулярное резервное копирование, антивирусный контроль, защита доступа к серверу
Уязвимости в мобильном приложении	Недостаточная защита API-интерфейсов может привести к утечке данных через мобильное соединение	Использование шифрования TLS 1.3, проверка безопасности API, аудит кода
DDoS-атаки	Массовые запросы перегружают серверы, делая систему недоступной	Защита от перегрузок, автоматическое масштабирование, фильтрация трафика
Инсайдерские угрозы	Сотрудники или медицинский персонал могут умышленно передавать конфиденциальные данные	Контроль доступа, ведение логов активности пользователей, мониторинг подозрительных действий
Примечание: Составлено автором в результате исследования.		

Как показано в Таблице 3, для повышения уровня безопасности «Дамумед» необходимо развивать защитные механизмы мобильного приложения, усиливать мониторинг активности пользователей, внедрять дополнительные алгоритмы шифрования и повышать уровень цифровой грамотности медицинского персонала. Дальнейшая модернизация системы и адаптация международных стандартов кибербезопасности позволят существенно снизить риски несанкционированного доступа и обеспечить надежную защиту медицинских данных пациентов.

Таблица 4

Основные функциональные различия «Дамумед» и зарубежных систем

Система	ЭМК	Телемедицина	Интеграция с госструктурами	Мобильные приложения	Аналитика и прогнозирование
Дамумед (Казахстан)	Поддержка ЭМК, интеграция с гос. структурами	Ограниченный функционал	Подключение к нац. базам	Есть мобильное приложение	Ограниченный функционал
EPIC (США)	Полнофункциональные ЭМК	Развитая телемедицина	Ограничено	Поддержка мобильных устройств	ИИ-аналитика
Cerner (США)	Гибкая настройка ЭМК	Встроенные телемедицинские сервисы	Ограничено	Поддержка приложений	Прогнозирование на основе данных
Allscripts (США, ЕС)	Ориентация на частные клиники	Поддержка удаленных консультаций	Ограничено	Упор на мобильные сервисы	Анализ медицинских данных
NHS Digital (Великобр.)	Государственная база ЭМК	Полная интеграция с NHS	Полная интеграция	Интеграция с NHS-приложениями	Использование AI-решений
Meditech (США, Канада)	Простая интеграция с другими системами	Базовая телемедицина	Нет	Базовая поддержка	Базовый анализ

Анализ сравнительных характеристик показывает, что система «Дамумед» по ряду ключевых направлений — в частности, в области телемедицины, интеллектуального анализа данных и внедрения прогностических инструментов — отстает от признанных международных решений, таких как EPIC, Cerner или NHS Digital. Зарубежные платформы активно применяют искусственный интеллект, машинное обучение и предиктивную аналитику для раннего выявления заболеваний, персонализированного лечения и повышения эффективности управленческих решений. В то же время функционал «Дамумед» в этих аспектах пока ограничен и требует дальнейшего развития. Это ограничивает потенциал системы в части интеграции с современными сервисами цифрового здравоохранения и сдерживает ее адаптацию к быстро меняющимся условиям медицинской практики в эпоху глобальной цифровизации.[10]

Совершенствование кибербезопасности медицинских информационных систем требует интеграции организационных, технических и правовых решений. Ключевыми направлениями являются: Внедрение политик информационной безопасности и обучение персонала; Использование современных технологий: шифрование (AES-256, RSA), многофакторная аутентификация (MFA), SIEM-системы; Адаптация международных стандартов (GDPR, HIPAA, ISO/IEC 27001) в казахстанскую практику.

Заключение. В процессе исследования была проведена всесторонняя оценка текущего состояния кибербезопасности в медицинских учреждениях Казахстана. Выявлены ключевые угрозы, такие как фишинговые атаки, уязвимости мобильных приложений и недостаточная защита облачных решений. Сравнительный анализ показал, что система «Дамумед» уступает зарубежным аналогам по уровню защиты данных и соответствию международным стандартам. Адаптация ISO/IEC 27001, HIPAA и GDPR в условиях Казахстана требует модернизации нормативной базы, развития ИТ-инфраструктуры и подготовки профильных специалистов. Для повышения уровня киберустойчивости предложены конкретные меры: внедрение многофакторной аутентификации, использование современных алгоритмов шифрования, развитие SIEM-систем и обучение персонала. Особое внимание уделяется перспективным технологиям — искусственному интеллекту, блокчейну и облачным платформам, способным существенно усилить защиту данных пациентов. Полученные выводы могут быть использованы для выработки государственной стратегии информационной безопасности и дальнейших научных исследований в сфере цифрового здравоохранения.

Список использованных источников

1. Nowrozy R., Ahmed K. Enhancing health information systems security: An ontology model approach // International Conference on Health Information. – 2023. – https://link.springer.com/chapter/10.1007/978-981-99-7108-4_8.

2. Mozzaquatro B.A., Agostinho C., Goncalves D., Martins J. An ontology-based cybersecurity framework for the internet of things // Sensors. – 2018. – https://www.mdpi.com/1424-8220/18/9/3053.
3. Hannou F.Z., Atigui F., Lammari N., Cherfi S.S. SafecareOnto: A cyber-physical security ontology for healthcare systems // International Conference on Advanced Information Networking and Applications. – 2021. – https://link.springer.com/chapter/10.1007/978-3-030-86475-0_3.
4. Arunprasath S., Annamalai S. Improving patient-centric data retrieval and cybersecurity in healthcare: privacy-preserving solutions for a secure future // Multimedia Tools and Applications. – 2024. – https://link.springer.com/article/10.1007/s11042-024-18253-5.
5. Harris S., Liu J., Ta V.T., Hadi H.J., Khan A., Zukaib U. Cybersecurity Standards for AI-based Healthcare Networks // ResearchGate. – 2023. – https://www.researchgate.net/publication/385622651_Cybersecurity_Standards_for_AI_based_Healthcare_Networks.
6. Singh G.P., Bharti V., Hooda M.K. A Review on NIST, ISO 27001, HIPAA and MITRE ATT&CK Cybersecurity Frameworks // Webology. – 2021. – https://www.researchgate.net/publication/371313513_A_Review_on_NIST_ISO_27001_HIPAA_and_MITRE_ATTCK_Cybersecurity_Frameworks.

УДК 004.056

КЕСКІНДЕРДЕГІ СТАТИСТИКАЛЫҚ СТЕГОАНАЛИЗ ӘДІСТЕРІ

Нұрлан Айсұлу Таңатқызы
nurlanaisulu19@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті
Ақпараттық қауіпсіздік жүйелері кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекші – Онгарбаева Айнагуль Игиликовна

Аңдатпа. Бұл мақалада кескіндердегі статистикалық стегоанализдеу әдістері қарастырылады. Сонымен қатар, қазіргі стеганализ алгоритмдері мен әдістерінің жұмыс істеу принциптері берілген. Әртүрлі стеганализ әдістерінің тиімділігіне және олардың шектеулеріне көп көңіл бөлінеді. Кескіндегі жасырын ақпаратты анықтаудағы статистикалық стегоанализдің әдістеріне төменгі биттік талдау, хи-квадрат әдісі, RS талдауы және тағы да басқа әдістер жұмыста көрсетілген.

Кілт сөздер: стеганография, стегоанализ, статистикалық стеганография, статистикалық стегоанализ, кескіндерді талдау, жасырын акпарат, пиксельдер, ақпараттық қауіпсіздік.

Кіріспе

Стеганография - бұл деректердің ішінде құпия ақпараттың болуын анықтауды мүмкін емес ететіндей оны жасыру туралы ғылым. Статистикалық стеганография мәліметтерді кескіндер, аудио файлдар және мәтіндік құжаттар сияқты деректерді өзгеріссіз цифрлық тасымалдаушыларға енгізуді білдіреді. Құпия хабарламалар саласында стеганографияның бірнеше негізгі әдістері бар. Олардың ішінде статистикалық стеганография әдіс ақпаратты енгізу процесінен кейінгі статистикалық өзгерістерді барынша көрінбейтіндей етіп жасырады.

Стеганографияның дамуымен бірге оған қарама-қарсы стегоанализ әдістері де жетілдірілуде. Оның мақсаты - цифрлық медиада жасырын ақпараттың болу фактісін анықтау. Стегоанализ жасаудың әртүрлі тәсілдер бар, ең кең таралған және тиімдісі статистикалық стеганализ болып табылады. Өйткені ол статистикалық сипаттамаларға негізделген және ең