МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2025.155.102

УЯЗВИМОСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Научная статья

Горбунов Н.А.[1, *]
[1] ORCID : 0009-0004-2973-9594;
[1] Университет ИТМО, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (gorb-2157[at]mail.ru)

Аннотация

В статье рассмотрены различные способы классификации уязвимостей безопасности информации (УБИ) и предложена классификация УБИ для медицинских информационных систем (МИС). В ходе исследования был выявлен единый признак классификации УБИ для МИС, этим признаком стали этапы создания программного обеспечения (ПО) для МИС. Такой признак позволил выделить ранее не классифицируемые УБИ, а именно УБИ протокола Fast Healthcare Interoperability Resources (FHIR). Материалом исследования послужил анализ уязвимостей следующих МИС: «Ариадна», «Медиалог», «Реновацио Софт», «Меганом-Дата», «Симплекс», «MedIdea» за 2020–2024 гг. В процессе работы были выявлены наиболее характерные для МИС УБИ. Результатом исследования стало создание классификации УБИ для МИС. Актуальность данного исследования обусловлена спецификой разработки ПО для МИС, а также необходимостью безопасной интеграции МИС друг с другом и другими информационными системами. Результаты исследования использовались для создания моделей угроз МИС.

Ключевые слова: медицинские информационные системы, уязвимости безопасности информации.

INFORMATION SECURITY VULNERABILITIES OF MEDICAL INFORMATION SYSTEMS

Research article

Gorbunov N.[1, *]
[1] ORCID : 0009-0004-2973-9594;
[1] ITMO University, Saint-Petersburg, Russian Federation

* Corresponding author (gorb-2157[at]mail.ru)

Abstract

The article examines various ways of classifying information security vulnerabilities (ISVs) and proposes a classification of ISVs for medical information systems (MIS). In the course of the study, a single feature of classifying vulnerabilities for MIS was identified, this trait was the stages of creating software for MIS. This allowed to identify previously unclassified ISVs, namely ISVs of Fast Healthcare Interoperability Resources (FHIR) protocol. The material of the study was the vulnerability analysis of the following MIS: ‘Ariadna’, “Medialog”, “Renovatio Soft”, “Meganom-Data”, “Simplex”, “MedIdea” for 2020–2024. In the process, the most characteristic ISVs for MIS were identified. The result of the study was the creation of a classification of ISVs for MIS. The relevance of this research is due to the specificity of software development for MIS, as well as the necessity of secure integration of MIS with each other and other information systems. The results of the research were used to create threat models for MIS.

Keywords: medical information systems, information security vulnerabilities.

Введение

МИС становятся неотъемлемой частью коммерческих и государственных медицинских учреждений. Сведения, обрабатываемые МИС, нуждаются в постоянной защите, так как они представляют ценность для злоумышленника. Поиск УБИ в программном обеспечении МИС безусловно является обязательным, ввиду того, что наличие УБИ может привести к нарушению конфиденциальности, доступности и целостности защищаемой информации [1]. Более того, из всего многообразия УБИ наиболее распространёнными для МИС являются следующие УБИ: недостаточная аутентификация и авторизация, социальная инженерия, неверная конфигурация систем, недостаточный мониторинг и аудит, уязвимости в сторонних приложениях.

К статистическим данные о кибератаках на МИС в России относится то, что чаще всего хакеры атаковали клиники, пытаясь обойти средства защиты. Далее были отмечены сетевые атаки и попытки внедрения в МО вредоносного ПО. К утечке конфиденциальной информации привел большой процент результативных атак.

Тренды цифровизации здравоохранения — это увеличение объёмов обрабатываемой в МИС информации, рост киберугроз и применение новых методов для выявления УБИ.

Международные требования GDPR и HIPAA применяются для обеспечения безопасности данных, но имеют некоторые различия. HIPAA используется для защиты данных МИС в США, GDPR описывает спектр персональных данных, включающий не только медицинские сведения.

Специалисты по информационной безопасности рассматривают разные способы классификации УБИ, помогающие реализовать процессы выявления и митигации рисков. К наиболее распространенным классификациям можно отнести по типу уязвимости, то есть УБИ программного обеспечения. Например, нарушение конфигурации или версионности, а также ошибки программного кода. Рассуждая о классификации УБИ аппаратного обеспечения, важно

подчеркнуть недостатки в функционале и производстве оборудования. Если рассмотреть УБИ процессов, то это некомпетентность обслуживающего персонала и недостатки управления доступом. Определяя классификацию по степени воздействия, выделяют низкий, средний и высокий уровни, для которых характерны незначительное, умеренное и серьёзное воздействие соответственно. УБИ по способам эксплуатации делятся на требующие аутентификации, для которых доступ возможен только для авторизованных пользователей, а также не требующие аутентификации, для которых достаточно общедоступных ресурсов. Для классификации УБИ по времени обнаружения характерны известные, которые уже задокументированы и для них существуют возможные меры по устранению, и новые УБИ, которые ещё не внесены банк данных регулятора. В вопросах классификации УБИ по источнику уязвимости выделяют внутренние, которые ставятся следствием ошибок или недостатков внутри организации, и внешние, которые происходят из-за атак со сторонних злоумышленников [2].

К общепризнанной классификации по сфере воздействия относят УБИ, соответствующие триаде информационной безопасности: конфиденциальности, целостности и доступности. Где для УБИ, затрагивающих конфиденциальность, характерны утечки сведений или данных, для УБИ, затрагивающих целостность, характерна модификация информации, и для УБИ, касающиеся доступности, характерны DDoS-атаки.

Приведённые выше типы классификации УБИ помогают идентифицировать риски, связанные с УБИ, и реализовать адекватные меры по их минимизации и предотвращению. Данные классификации помогают организациям лучше понять риски, связанные с уязвимостями, и разработать соответствующие меры по их устранению и предотвращению.

В данной работе мы предлагаем адаптированную для МИС классификацию УБИ.

Новизна заключается в выделении единых признаков для всех УБИ, характерных для МИС и классификация УБИ на основе этих признаков.

Актуальность исследования заключается необходимости создания единой классификации УБИ для МИС для дальнейшего использования при разработке специального программного обеспечения для обнаружения УБИ в МИС.

Метод

Классификация занимает особое место в теории познания. Объекты упорядочиваются через их объединения в классы по определенным признакам (свойствам, характеристикам), которые позволяют установить их сходство или различие. В основе методологии классификации лежит трехуровневая иерархия научного знания, включающая философский, системологический (общенаучный) и специально-научный уровни. Основная цель любой классификации «состоит в том, чтобы свернуть всю доступную нам информацию о рассматриваемых сложных объектах, процессах или явлениях произвольной природы в компактную, но емкую и удобную для познания форму, идентифицирующую и отображающую сущность этих объектов» [3].

Для классификации были выбраны только те УБИ, которые наиболее характерны для МИС [4]. УБИ отбирались на основе анализа уязвимостей следующих МИС: «Ариадна», «Медиалог», «Реновацио Софт», «Меганом-Дата», «Симплекс», «MedIdea» и других, интегрированных с компанией «Нетрика Медицина» с 2020 по 2024 год. Данные МИС наиболее распространены среди медицинских учреждений в Санкт-Петербурге и Ленинградской области. Количество пользователей этих МИС насчитывает порядка пяти миллионов человек. Все эти МИС имеют сходный функционал и интегрируются с единой государственной информационной системой здравоохранения при помощи протокола FHIR. В таблице 1 представлены наиболее часто встречающиеся в МИС УБИ. Представлена вероятность обнаружения УБИ в исследуемых МИС, которая была выявлена опытным путём.

Таблица 1 - Уязвимости безопасности информации в медицинских информационных системах

DOI: https://doi.org/10.60797/IRJ.2025.155.102.1

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
1	BDU:2025-01829	Библиотеки SPID.AspNetCore .Authentication программной платформы ASP.NET Core, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации	Связана с недостатками процедуры аутентификации МИС	1,1
2	BDU:2025-01818	Функции set_lang_Country	Эксплуатация уязвимости	3,4

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
		Code() сценария login.cgi микропрограммного обеспечения маршрутизаторов Wavlink AC3000 (WL-WN533A8), позволяющая нарушителю выполнить межсайтовые сценарные атаки и получить несанкционированный доступ к защищаемой информации	может позволить нарушителю, действующему удаленно, выполнить межсайтовые сценарные атаки и получить несанкционированный доступ к защищаемой информации, обрабатываемой МИС, путем отправки специально сформированных HTTP-запросов	
3	BDU:2025-01813	Компонента vsock ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	Связана с ошибками управления ресурсами МИС. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании МИС	4,5
4	BDU:2025-01808	Компонента net ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	Связана с ошибками управления ресурсами МИС. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании МИС	2,2
5	BDU:2025-01803	Функции run_job() ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	Связана с ошибками управления ресурсами МИС. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании МИС	2,1
6	BDU:2025-01789	Системы сбора и анализа событий IBM QRadar SIEM	Связанная с передачей критичной информации открытым текстом, позволяющая нарушителю	1,9

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
			реализовать атаку типа «человек посередине» в МИС	
7	BDU:2025-01777	Драйвера модуля Google Virtual Ethernet Module (gve) (drivers/net/ethernet/google/gve/gve_tx.c) ядра	Связана с разыменованием указателей в результате отсутствия проверки деления на ноль. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании МИС	3,2
8	BDU:2025-01763	Компонента KVM ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	Связана с разыменованием указателя NULL. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании МИС	2,2
9	BDU:2025-01762	Программного средства для обновления драйверов Intel Driver & Support Assistant (DSA)	Связана с недостаточной проверкой подлинности данных. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии МИС	3,1
10	BDU:2025-01741	Браузера Microsoft Edge	Связана с переадресацией URL на ненадежный сайт при загрузке страницы входа. Эксплуатация уязвимости может позволить нарушителю обойти существующие ограничения безопасности МИС	1,9

Признаком для классификации послужили этапы создания самих МИС от разработки на уровне алгоритмов до интеграции МИС с другими программными продуктами.

Существующие классификации уязвимостей, описанные в национальном стандарте Российской Федерации «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (ГОСТ Р 56546-2015), на сегодняшний день не включают в себя уязвимости интеграционных протоколов. По данному стандарту устанавливается классификация уязвимостей информационных систем по области происхождения уязвимостей, типах недостатков ИС и местах их возникновения (проявления). Для МИС вопрос безопасной интеграции с другими системами остро стоит. Разработчики МИС часто не обращают внимание на безопасность интеграции, оценивая лишь риски уязвимостей ПО и алгоритмов. Задача же специалистов по информационной безопасности обнаружить новые места появления уязвимостей и указать на них. Таким образом, по сравнению с вышеперечисленными и описанными классификациями, выработанная в данном исследовании классификация имеет преимущество, которое позволяет выйти за рамки непосредственно ПО и посмотреть в сторону интеграции одного ПО с другим. Эта интеграция часто остается без внимания с точки зрения безопасности и использование данной классификации при разработке модели угроз позволит избежать проблем в будущем.

Результаты и обсуждение

Таким образом, было выделено три метрики:

- метрика «А» — УБИ алгоритмов МИС;
- метрика «Б» — УБИ программного обеспечения МИС;
- метрика «В» — УБИ протокола FHIR.

Прежде чем начать процесс реализации программного обеспечения МИС, то есть создания исполняемого файла, необходимо тщательно продумать функциональную составляющую. Она закладывается в МИС при составлении уникального алгоритма реализации, который не зависит от конечной формы представления, а именно языка программирования [5]. Описывая главные характеристики для метрики «А», важно упомянуть корректность, скорость и уникальность реализации, задающие главные направления векторов процесса программирования [6].

В таблице 2 представлены основные УБИ алгоритмов МИС.

Таблица 2 - Уязвимости метрики «А»

DOI: https://doi.org/10.60797/IRJ.2025.155.102.2

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
1	BDU:2025-00322	Программной платформы на базе git для совместной работы над кодом GitLab EE/ CE	Связана с лгоритмической сложностью программного обеспечения, используемого при разработке МИС. Позволяет нарушителю вызвать отказ в обслуживании	0,1
2	BDU:2024-10981	Программной платформы на базе git для совместной работы над кодом GitLab	Связана с неэффективной алгоритмической сложностью программной платформы, используемой при разработке МИС. Позволяет нарушителю, действующему удаленно, вызвать отказ в обслуживании	0,4
3	BDU:2024-08707	Программной платформы Microsoft .NET и редактора исходного кода Visual Studio	Связана с алгоритмической сложностью программного обеспечения, используемого	0,2

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
			при разработке МИС. Позволяет нарушителю вызвать отказ в обслуживании	
4	BDU:2024-06372	Средства управления трафиком и балансировки нагрузки Ivanti Virtual Traffic Manager	Связана с некорректной реализацией алгоритма аутентификации средства управления трафиком. Характерна при интеграции МИС	0,3
5	BDU:2024-05577	Корпоративной версии платформы GitHub Enterprise Server	Связана с неправильной реализацией алгоритма аутентификации, позволяющая нарушителю получить полный доступ к системе с привилегиями администратора. Характерна для программного обеспечения, используемого при разработке МИС	0,1
6	BDU:2023-07965	Реализации алгоритма Hash-based Message Authentication Code операционных систем Windows	Связана с недостатками разграничения доступа при формировании ключа. Позволить нарушителю обойти ограничения безопасности и повысить свои привилегии при работе в МИС	0,1
7	BDU:2023-01027	Микропрограммного обеспечения маршрутизаторов TP-Link	Связана с использованием устаревшего криптографического алгоритма MD5. Характерна при интеграции МИС	0,9
8	BDU:2022-05599	Интерпретатора языка программирования Python	Связана с ошибками при преобразовании численных и	0,4

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
			строковых типов данных, позволяющая нарушителю вызвать отказ в обслуживании из-за алгоритмической сложности. Характерна языка программирования, используемого при разработке МИС	
9	BDU:2021-05707	Алгоритма программного обеспечения Cisco	Связана с недостаточной проверкой вводимых данных, позволяющая нарушителю вызвать отказ в обслуживании. Характерна при интеграции МИС	0,2
10	BDU:2021-03177	Реализации алгоритмов WEP, WPA, WPA2 и WPA3 ядра операционной системы Linux	Позволяет нарушителю оказать воздействие на целостность защищаемой информации при работе в МИС	0,1

Каждое программное обеспечение МИС проходит этап разработки, который начинается с формирования общих идей о будущих выполняемых задачах, затем идёт алгоритмическая составляющая и завершается написанием кода для создания исполняемого файла [7]. Недоработки программного обеспечения МИС, включая уязвимости, могут появляться на любом этапе этого цикла, изменяясь и интегрируясь в программное обеспечение в ходе его разработки. Таким образом, ошибки, связанные с основами работы продукта, будут трудно выявляемыми в представлении его в виде машинного кода, так как они основаны на абстрактных концепциях и универсальны по сравнению с процессом написания кода на языках программирования.

Наиболее ярким примером уязвимости алгоритма, характерной для МИС, является BDU:2023-01027, относящаяся к микропрограммному обеспечению маршрутизаторов TP-Link. Эксплуатация данной УБИ возможна, так как в функционале сетевого оборудования применяется устаревший криптографического алгоритма MD5, который может позволить злоумышленнику получить несанкционированный доступ к защищаемой информации или инициировать инцидент информационной безопасности, связанный с отказом в обслуживании субъекту МИС, имеющему право доступа. Максимальный процент обнаружения данной УБИ из представленных в таблице 2 свидетельствует о значительной частоте выявления.

Практические рекомендации по устранению уязвимостей Метрики «А» (алгоритмов) медицинских информационных систем — это защита специализированного медицинского оборудования. В частности, системы лучевой диагностики и терапии требуют особых мер безопасности, так как напрямую влияют на постановку диагноза и ход лечения пациентов. Рекомендуется внедрить многофакторную аутентификацию для доступа к такому оборудованию и обеспечить шифрование передаваемых данных.

Главной характеристикой для метрики «Б» является зависимость значения неопределённости реализации программного обеспечения от фактического рабочего времени тестировщиков, программистов и аналитиков.

В таблице 3 представлены основные УБИ программного обеспечения МИС.

Таблица 3 - Уязвимости метрики «Б»

DOI: https://doi.org/10.60797/IRJ.2025.155.102.3

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
1	BDU:2024-11096	Программной платформы для медицинской визуализации и обработки изображений syngo.plaza	Связана с непринятием мер по защите структуры запроса SQL, позволяющая нарушителю выполнить произвольный SQL-код при работе в МИС	0,2
2	BDU:2024-02084	Функции sopen_FAMOS_read библиотеки обработки медицинских сигналов libbiosig	Позволяет нарушителю выполнить произвольный код с помощью специально созданного файла при работе в МИС	0,7
3	BDU:2023-07369	Веб-сервера средства оптимизации процессов управления медицинским обслуживанием Mirth Connect	Позволяет нарушителю выполнить произвольный код с помощью специально созданного файла при работе в МИС	0,1
4	BDU:2023-05988	Программного обеспечения для управления медицинской организацией OpenEMR	Связана с недостатками контроля доступа, позволяющая нарушителю просматривать, создавать и редактировать защищаемую информацию при работе в МИС	1,1
5	BDU:2023-04945	Файла /patient/appointment.php. системы управления малыми медицинскими учреждениями SourceCodester Free Hospital Management System for Small Practices	Позволяет нарушителю получить выполнять произвольные SQL-запросы к базе данных при работе в МИС	0,3
6	BDU:2023-05980	Программного обеспечения для	Связана с ошибками	0,1

№	Номер уязвимости в банке ФСТЭК	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
		управления медицинской организацией OpenEMR	авторизации, позволяющая нарушителю осуществить HTML-инъекцию при работе в МИС	
7	BDU:2022-03259	Функции func2.php веб-приложения для управления медицинским учреждением PHPGurukul Hospital Management System	Позволяет нарушителю раскрыть защищаемую информацию при работе в МИС	0,3
8	BDU:2022-00334	Функции make_task программного обеспечения для управления медицинской организацией OpenEMR	Позволяет нарушителю проводить атаки основанные на SQL-инъекии при работе в МИС	0,2
9	BDU:2021-01651	Медицинского диагностическог о оборудования GE Healthcare	Связана с отсутствием защиты служебных данных, позволяющая нарушителю получить несанкционирова нный доступ к защищаемой информации или повысить свои привилегии при работе в МИС	0,5
10	BDU:2021-03268	Компонента portal/patient/_ma chine_config.php программного обеспечения для управления медицинской организацией OpenEMR	Позволяет нарушителю получить несанкционирова нный доступ к защищаемой информации при работе в МИС	0,4

Наиболее ярким примером уязвимости программного обеспечения, характерной для МИС, является BDU:2023-05980, относящаяся к программному обеспечению для управления медицинской организацией OpenEMR. Эксплуатация данной УБИ возможна, так как в функционале инструмента для управления цифровыми медицинскими записями возможно осуществить удалённому нарушителю HTML-инъекцию в процессе некорректной проверки данных, которые вводит пользователь при авторизации. Подобные действия злоумышленника могут привести модификации структуры данных пользователя МИС. Максимальный процент обнаружения данной УБИ из представленных в таблице 3 свидетельствует о значительной частоте выявления.

Практические рекомендации по устранению уязвимостей Метрики «Б» (программного обеспечения) медицинских информационных систем — это регулярное обновление операционных систем, антивирусных баз и сигнатур, системного и прикладного ПО. Причиной многих атак становятся именно уязвимости устаревших решений.

Протокол FHIR используется для стандартизированного взаимодействия в части интеграции МИС [8]. Данный протокол — это открытый стандарт, который обеспечивает внешним программным приложениям возможность быстро находить и получать доступ к клинической информации из электронной медицинской карты, используя удобные для разработчиков методы, основанные на современных структурных стандартах [9]. Для того чтобы внешние программные приложения из состава МИС могли получить доступ к информации через протокол FHIR, им нужно активно отслеживать поток сообщений, которые описывают клинические события. Лишь после получения таких сообщений внешнее программное обеспечение сможет собирать и обрабатывать данные. Разработчикам программного обеспечения для МИС с новым функционалом доступны различные бесплатные и общедоступные ресурсы структуры FHIR.

Наиболее очевидные уязвимости протокола FHIR связаны, в большей мере, с его качественной реализацией, а не со структурой самого стандарта.

В исследуемых МИС за период с 2020 по 2024 гг. были выявлены только четыре УБИ. Однако, мы считаем необходимым добавить эту метрику в нашу классификацию, т.к. протокол FHIR в его русской адаптации FHIR RU-core используется в России недавно с 2014 года и прогнозируется рост использования этого протокола для интеграции МИС.

Практические рекомендации по устранению уязвимостей Метрики «В» (протокола FHIR) медицинских информационных систем — это регулярный аудит безопасности**.** Медицинским организациям необходимо проводить оценку защищённости информационных систем не реже одного раза в квартал. Это позволит своевременно выявлять и устранять потенциальные уязвимости в системах передачи и обработки данных пациентов.

В таблице 4 представлены УБИ протокола FHIR.

Таблица 4 - Уязвимости метрики «В»

DOI: https://doi.org/10.60797/IRJ.2025.155.102.4

№	Номер уязвимости в банке NIST	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
1	CVE-2023-28465	Функция распаковки пакетов в библиотеках HL7 (Health Level 7) FHIR Core до версии 5.6.106	Позволяет злоумышленникам при работе в МИС копировать произвольные файлы в определённые каталоги с помощью обхода каталогов, если разрешённое имя каталога является подстрокой имени каталога, выбранного злоумышленником	1,2
2	CVE-2023-24057	Основных библиотеки Health Level 7 FHIR до версии 5.6.92	Позволяют злоумышленникам при работе в МИС извлекать файлы в произвольные каталоги с помощью обхода каталогов из созданного ZIP- или TGZ-архива (для предварительно упакованного	4,5

№	Номер уязвимости в банке NIST	УБИ	Краткое описание УБИ (почему именно для МИС характерно)	Вероятность обнаружения (%)
			кэша терминов, пакета NPM или архива для сравнения)	
3	CVE-2024-50589	API (Application Programming Interface) - интерфейс FHIR	Злоумышленник, не прошедший аутентификацию, но имеющий доступ к локальной сети медицинского учреждения, может получить доступ к конфиденциальным электронным медицинским картам при работе в МИС	5,1
4	CVE-2022-39230	Реализации интерфейса авторизации из интерфейса FHIR Works. Версии 3.1.1 и 3.1.2	Позволяет раскрыть конфиденциальной информации неавторизованному субъекту при работе в МИС	2,1

Примером использования разработанной методики определения УБИ стали исходные данные моделей угроз информационной безопасности МИС компании «Нетрика Медицина»: «N3. Здравоохранение», «Портал пациента», «Управление потоками пациентов», «Интегрированная электронная медицинская карта» и «Система управления доступом» [11]. Были проанализированы перечни устранённых актуальных УБИ, которые были выявлены смешанным способом идентификации.

Метрика «А» относится к источнику негативных УБИ, внедренных злоумышленником с целью изменить логику работы программного обеспечения в свою пользу. Для того чтобы подтвердить данные УБИ, необходимо привлекать ряд экспертов, имеющих опыт работы как на этапах проектирования МИС, так и на этапах процесса функционирования после ввода в эксплуатацию.

Метрика «Б» относится к источнику случайных УБИ, возникающих из-за ошибок, допущенных программистом, а также не выявленных при тестировании. Основные постулаты написания программного кода представлены в стандартах языка и имеют четкую формализацию, что даёт возможность экспертам выявлять УБИ сканерами, которые точечно проверяют соблюдение правил.

Метрика «В» включает в себя перечни УБИ как самой структуры протокола FHIR, так и УБИ сторонних сервисов, сопутствующих цифровизации здравоохранения. Стандарт FHIR является международным и рекомендован для интеграционных процессов различных МИС, соответственно структура стандарта является защищенной. Но параметры метрики «В» нельзя рассматривать в отрыве от таких аспектов МИС как агрегаторы данных, мобильные приложения, стек сетевых технологий, атака «человек посередине» [10], типов доступа, аутентификаций, идентификаций многого и другое.

Ограничения предложенного метода классификации УБИ связаны с банками уязвимостей ФСТЭК и NIST, где требуется проводить переоценку рисков, ведение отчетности, инвентаризацию активов и выстраивание процессов системы менеджмента информационной безопасности.

Аудит безопасности МИС с применением классификации УБИ на практике сводится к систематическому анализу МИС с целью выявления УБИ, входящие в метрики «А», «Б» и «В».

Направлением будущих исследований является разработка методов и алгоритмов выявления УБИ в МИС, где используются иные протоколы линейки стандарт HL7 (Health Level Seven International), к которому относится протокол FHIR.

Заключение

В статье предложена новая классификация УБИ для МИС. В данную классификацию вошли три метрики А, Б и В. Основой классификации послужил принцип разработки МИС. Метрика А отражает УБИ на уровне алгоритмов МИС, метрика Б относится к программному коду, а метрика В фиксирует угрозы интеграции МИС, связанные с протоколом

FHIR. В результате исследования выделены основные УБИ, которые встречались в МИС, разработанных компанией «Нетрика Медицина» за 2020-2024 гг. Предложенная классификация УБИ в МИС была опробована при разработке модели угроз информационной безопасности «N3. Здравоохранение», «Портал пациента», «Управление потоками пациентов», «Интегрированная электронная медицинская карта» и «Система управления доступом». Были получены следующие результаты: помимо учтённых в банке данных уязвимостей ФСТЭК для МИС актуальны УБИ, связанные с протоколом FHIR, которых нет в банке данных регулятора. В связи с этим при разработке новых МИС для определения перечня актуальных УБИ необходимо использовать классифицировать с помощью метода, описанного в настоящей статье.

Конфликт интересов

Не указан.

Рецензия

Мангушева А.Р., Казанский национальный исследовательский технологический университет, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2025.155.102.5

Conflict of Interest

None declared.

Review

Mangusheva A.R., Kazan National Research Technological University, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2025.155.102.5

Список литературы / References

1. ГОСТ Р 58142-2018 Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей : утв. Приказом Федерального агентства по техническому регулированию и метрологии от 24 мая 2018 г. № 273-ст. — Введ. 2018-05-24. — М. : Стандартинформ, 2018.

2. Grabovschi C. Mapping the concept of vulnerability related to health care disparities: a scoping review / C. Grabovschi, C. Loignon, M. Fortin // BMC Health Services Research. — 2013. — Vol. 13. — Art. 94. DOI: 10.1186/1472-6963-13-94.

3. Омельченко В.В. Общая теория классификации. Ч. 2: Теоретико-множественные основания / В.В. Омельченко. — Москва : Либроком, 2010. — 296 с.

4. Mejía-Granda C.M. Security vulnerabilities in healthcare: an analysis of medical devices and software / C.M. Mejía-Granda, J.L. Fernández-Alemán, J.M. Carrillo-de-Gea [et al.] // Medical & Biological Engineering & Computing. — 2024. — Vol. 62, № 1. — P. 257–273. DOI: 10.1007/s11517-023-02912-0.

5. Iannone E. The secret life of software vulnerabilities: a large-scale empirical study / E. Iannone, R. Guadagni, F. Ferrucci [et al.] // IEEE Transactions on Software Engineering. — 2022. DOI: 10.1109/TSE.2022.3140868.

6. Kassab M. Software development for medical devices: State of practice / M. Kassab, J.F. DeFranco, P.A. Laplante // 2017 IEEE 28th Annual Software Technology Conference (STC). — 2017. DOI: 10.1109/STC.2017.8234459.

7. Loftus T.J. Ideal algorithms in healthcare: Explainable, dynamic, precise, autonomous, fair, and reproducible / T.J. Loftus, P.J. Tighe, T. Ozrazgat-Baslanti [et al.] // PLOS Digital Health. — 2022. — Vol. 1, № 1. — Art. e0000006. DOI: 10.1371/journal.pdig.0000006.

8. Thun S. The Use of FHIR in Digital Health — a Review of the Scientific Literature / S. Thun // German Medical Data Sciences: Shaping Change — Creative Solutions for Innovative Medicine. — 2019. — Vol. 267. DOI: 10.3233/SHTI190805.

9. Mandel J.C. SMART on FHIR: a standards-based, interoperable apps platform for electronic health records / J.C. Mandel, D.A. Kreda, K.D. Mandl [et al.] // Journal of the American Medical Informatics Association. — 2016. — Vol. 23, № 5. — P. 899–908. DOI: 10.1093/jamia/ocv189.

10. Gangan S. A Review of Man-in-the-Middle Attacks / S. Gangan // arXiv. — 2015. — Art. abs/1504.02115.

Список литературы на английском языке / References in English

1. GOST R 58142-2018 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Detalizatsiya analiza uyazvimostey programmnogo obespecheniya v sootvetstvii s GOST R ISO/MEK 15408 i GOST R ISO/MEK 18045. Chast 1. Ispolzovanie dostupnykh istochnikov dlya identifikatsii potentsialnykh uyazvimostey [Information Technology. Security Assurance Methods and Tools. Software Vulnerability Analysis Elaboration in Accordance with GOST R ISO/IEC 15408 and GOST R ISO/IEC 18045. Part 1: Use of Available Sources for Potential Vulnerability Identification] : approved by Order No. 273-st of the Federal Agency for Technical Regulation and Metrology, May 24, 2018. — Eff. 2018-05-24. — Moscow : Standartinform, 2018. [in Russian]

2. Grabovschi C. Mapping the concept of vulnerability related to health care disparities: a scoping review / C. Grabovschi, C. Loignon, M. Fortin // BMC Health Services Research. — 2013. — Vol. 13. — Art. 94. DOI: 10.1186/1472-6963-13-94.

3. Omelchenko V.V. Obshchaya teoriya klassifikatsii. Ch. 2: Teoretiko-mnozhestvennye osnovaniya [General Classification Theory. Part 2: Set-Theoretic Foundations]. — Moscow : Librokom, 2010. — 296 p. [in Russian]

4. Mejía-Granda C.M. Security vulnerabilities in healthcare: an analysis of medical devices and software / C.M. Mejía-Granda, J.L. Fernández-Alemán, J.M. Carrillo-de-Gea [et al.] // Medical & Biological Engineering & Computing. — 2024. — Vol. 62, № 1. — P. 257–273. DOI: 10.1007/s11517-023-02912-0.

5. Iannone E. The secret life of software vulnerabilities: a large-scale empirical study / E. Iannone, R. Guadagni, F. Ferrucci [et al.] // IEEE Transactions on Software Engineering. — 2022. DOI: 10.1109/TSE.2022.3140868.

6. Kassab M. Software development for medical devices: State of practice / M. Kassab, J.F. DeFranco, P.A. Laplante // 2017 IEEE 28th Annual Software Technology Conference (STC). — 2017. DOI: 10.1109/STC.2017.8234459.

7. Loftus T.J. Ideal algorithms in healthcare: Explainable, dynamic, precise, autonomous, fair, and reproducible / T.J. Loftus, P.J. Tighe, T. Ozrazgat-Baslanti [et al.] // PLOS Digital Health. — 2022. — Vol. 1, № 1. — Art. e0000006. DOI: 10.1371/journal.pdig.0000006.

8. Thun S. The Use of FHIR in Digital Health — a Review of the Scientific Literature / S. Thun // German Medical Data Sciences: Shaping Change — Creative Solutions for Innovative Medicine. — 2019. — Vol. 267. DOI: 10.3233/SHTI190805.

9. Mandel J.C. SMART on FHIR: a standards-based, interoperable apps platform for electronic health records / J.C. Mandel, D.A. Kreda, K.D. Mandl [et al.] // Journal of the American Medical Informatics Association. — 2016. — Vol. 23, № 5. — P. 899–908. DOI: 10.1093/jamia/ocv189.

10. Gangan S. A Review of Man-in-the-Middle Attacks / S. Gangan // arXiv. — 2015. — Art. abs/1504.02115.