ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ HL7-СООБЩЕНИЙ: АНАЛИТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ

Фомин Д.А., магистрант гр. 467241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. тех. наук, доцент

Аннотация. В статье представлен аналитический обзор проблем обеспечения информационной безопасности при обмене медицинскими данными в стандарте HL7. Рассмотрены уязвимости протоколов HL7, связанные с отсутствием шифрования, аутентификации и контроля целостности. Проанализированы существующие подходы к защите: ручная проверка, брандмауэры, сегментация сети и VPN, а также современные научно-технические решения на основе шифрования и технологий распределенных реестров. Обоснована необходимость разработки специализированного программного модуля.

Ключевые слова: HL7; защита медицинских данных; информационная безопасность; шифрование; Twofish; Electronic Health Records; уязвимости; анализ угроз; межсетевые экраны.

Стандарт HL7 (Health Level 7) является доминирующим протоколом для обмена электронными медицинскими записями (EHR) в информационных системах здравоохранения. Однако, как отмечается в современных исследованиях, его широкое распространение сопряжено с серьезными проблемами безопасности. Таким образом для выявления основных угроз и обоснования подхода к разработке программного модуля защиты HL7-сообщений необходимо провести аналитический обзор литературных источников и существующих решений.

Критический анализ литературы показывает, что стандарт HL7 был разработан без учета современных требований безопасности. В работе [1] подчеркивается необходимость внедрения эффективных схем шифрования и иерархического контроля доступа. Однако, как показывают источники, фундаментальные проблемы протокола заключаются в отсутствии нативной поддержки шифрования (данные передаются в открытом виде), слабой или отсутствующей аутентификации (злоумышленник может подключиться к порту TCP 2575) и отсутствии встроенных механизмов проверки целостности сообщений, что делает возможным атаки «человек посередине» с подменой клинических данных, таких как диагнозы или дозировки лекарств.

В исследовании [2] подчёркивается, что технологии защиты медицинских данных должны обеспечивать три основных требования: конфиденциальность (доступ к данным только авторизованных лиц), целостность (защита от несанкционированного изменения) и доступность (обеспечение доступа к данным при лечении пациентов). HL7 в чистом виде не удовлетворяет ни одному из этих требований, что делает необходимым применение дополнительных средств защиты.

Современные исследования подтверждают актуальность этих угроз. В обзоре [3] отмечается, что методы машинного обучения, внедряемые в медицину, сами становятся мишенью для атак, что требует разработки устойчивых и безопасных конвейеров обработки данных, включая этап очистки и валидации входных HL7-сообщений. Кроме того, как указано в отчете CVE-2024-52807, даже современные инструменты для работы с HL7 FHIR подвержены классическим уязвимостям, таким как внедрение XML External Entity (XXE), что может привести к раскрытию данных сервера. Это доказывает, что проблема защиты актуальна для всех поколений стандарта.

В исследовании Хасельхорста [4] представлен детальный анализ методов защиты HL7-интерфейсов, который включает как традиционные, так и специализированные подходы.

Ручная проверка (manual validation) является простейшим методом, позволяющим сверять количество сообщений на отправляющей и принимающей сторонах. Однако, как справедливо отмечается, этот метод не масштабируется и не обеспечивает проверки содержания сообщений.

Хостовые межсетевые экраны (host-based firewalls) могут ограничить круг систем, имеющих доступ к HL7-порту, и предотвратить DoS-атаки путём исчерпания максимального количества соединений. Тем не менее, они не защищают данные от перехвата и не препятствуют ARP-spoofing-атакам.

Сегментация сети (network segmentation) ограничивает видимость HL7-интерфейсов с менее защищённых сегментов сети, что является важной мерой defence-in-depth. Однако интерфейсный движок по своей природе должен взаимодействовать с системами из разных сетей, а сами данные по-прежнему передаются в открытом виде.

VPN и SSH-туннелирование обеспечивают шифрование передаваемых данных. Особый интерес представляет SSH-туннелирование, которое требует минимальных изменений в существующей HL7-инфраструктуре и может быть реализовано с помощью встроенных средств операционных систем. При этом HL7-данные остаются зашифрованными даже при успешной ARP-spoofing-атаке.

Технологии распределённых реестров (blockchain) рассматриваются в систематическом обзоре [5] как средство обеспечения неизменяемости и аудируемости транзакций с медицинскими данными. Однако авторы отмечают такие ограничения, как высокая вычислительная сложность и задержки, что затрудняет применение в реальном времени.

Проведённый аналитический обзор литературных источников подтверждает, что проблема защиты HL7-сообщений остаётся актуальной и нерешённой. Существующие подходы – от нормативного регулирования (HIPAA) до технологий blockchain и машинного обучения – имеют свои достоинства, но не предоставляют готового, производительного и совместимого решения для HL7-инфраструктур. Обоснована необходимость разработки специализированного программного модуля, который станет предметом дальнейших исследований.

Список использованных источников:

1. Вора Дж., Италия П., Танвар С., Тьяги С., Кумар Н., Обайда М.С., Сяо К.Ф. Обеспечение конфиденциальности и безопасности электронных медицинских карт. В сборнике: Труды Международной конференции по компьютерным, информационным и телекоммуникационным системам (CITS). – Кольмар, Франция, – 2018 г. – С. 1-5.

2. Мбониханкуйе С., Нкунзимана А., Ндагиджимана А. Технология безопасности медицинских данных: соответствие требованиям HIPAA. Беспроводная связь и мобильные вычисления. – 2019. – С. 1-7.

3. Кайюм А., Кадир Дж., Билал М., Аль-Фукаха А. Безопасное и устойчивое машинное обучение для здравоохранения: обзор. IEEE Reviews in Biomedical Engineering. 2020. – Т. 14. – С. 156-180.

4. Даллас Хазелхорст, Взлом интерфейсов данных HL7 в медицинских средах: атака и защита – ахиллесова пята здравоохранения [Электронный ресурс]. – Режим доступа: https://linuxincluded.com/hl7-medical-attacking-defending/: 24.02.2025.

5. Агбо К.С., Махмуд Х., Эклунд Дж.М. Технология блокчейн в здравоохранении: систематический обзор. Healthcare. 2019. Т. 7. № 2. – 56 с.