ПОТЕНЦИАЛЬНЫЕ КАНАЛЫ УТЕЧКИ МЕДИЦИНСКИХ ДАННЫХ И ПРИЧИНЫ ИХ ВОЗНИКНОВЕНИЯ

Осипова Ксения Сергеевна
Аналитик по информационной безопасности ООО «Иннова»

Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, Доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Аннотация: *В статье описана информация о возможных каналах утечки при использовании стандарта FHIR, в медицинской информационной системе и уязвимостях веб-приложениях. Так как потенциальные каналы утечки медицинских данных прямо зависят от конфигурации медицинской информационной системы и типа обмена медицинскими данными между организациями, то в статье рассматриваются общие случаи по каждому направлению потенциальных каналов утечки информации. Также описаны возможные причины возникновения, на которые стоит обратить внимание при аудите системы безопасности, чтобы обнаружить потенциальные каналы утечки медицинских данных.*

Ключевые слова: *медицинская информационная система, медицинские данные, каналы утечки информации, стандарт FHIR, уязвимости веб-приложений.*

Abstract: *This article describes information about possible leakage channels when using the FHIR standard, in the medical information system, and vulnerabilities in web applications. Since potential channels of medical data leakage directly depend on the configuration of the medical information system and the type of medical data exchange between organizations, the article considers General cases for each direction of potential channels of information leakage. It also describes possible causes that should be considered when auditing the security system in order to detect potential channels of medical data leakage.*

Keywords: *medical information system, medical data, information leakage channels, FHIR standard, web application vulnerabilities.*

Введение. В последнее время большим спросом пользуется перенос бумажного документооборота в электронный вид. Эта тенденция проявляется и в сфере медицины. Использование электронного медицинского документооборота значительно упрощает работу сотрудников медицинских организаций. Кроме того, появляются новые возможности: использование интегрированной электронной медицинской карты пациента (взаимодействие медицинских организаций между собой при наблюдении и лечении одного и того же пациента), а также связь медицинской информационной системы и лабораторной информационной системой (автоматизация процесса получения результатов необходимых анализов). В медицинской карте пациента содержатся его персональные данные, состояние здоровья, результаты исследований и прочее — все это является конфиденциальной информацией, доступ посторонних лиц к которой должен быть исключен. Но не все разработчики МИС учитывают каналы утечки информации, что повышает риски несанкционированного доступа к конфиденциальной медицинской информации.

Потенциальные каналы утечки при обмене данными по стандарту FHIR.

Большая часть медицинских информационных систем использует протокол передачи данных FHIR[1]. Он не является протоколом безопасности и не определяет никаких функций, связанных с безопасностью. Однако FHIR определяет протоколы обмена и модули системы, которые необходимо использовать с различными протоколами безопасности.

Безопасность в FHIR должна быть сосредоточена на ряде средств защиты информации и условий, необходимых для обеспечения того, чтобы данные можно было открывать, получать к ним доступ или изменять только в соответствии с правилами доступа и

политиками. Внедрение должно использовать существующие стандарты безопасности и обеспечивать защиту от: несанкционированного доступа; утечки информации при возникновении ошибок; внедрения вредоносного кода; аномальных схем доступа.

Для API RESTful применяются правила безопасности HTTP. Сервер должен требовать аутентификацию клиента, используя требование для клиентских сертификатов.

Необходимо учитывать, что при возврате ответов неавторизованным клиентам заголовки веб-сервера по протоколу гипертекстовой передачи (HTTP) и сообщения об ошибках API, а также сами ошибки не должны раскрывают подробную информацию о базовом веб-сервере, так как этим может воспользоваться злоумышленник.

Использование дополнительных методов безопасности для API, поможет идентифицировать, откуда поступают ответы системы доменных имен (DNS), и убедиться, что они действительны. Например, использование расширений безопасности системы доменных имен, набора расширений, которые добавляют дополнительную безопасность к протоколу DNS, следовательно, может обеспечить безопасность доменов, связанных с конечными точками API, которые передают информацию о работоспособности или информацию, необходимую для доступа к API.

Domain Name System Security Extensions обеспечивает полномочия источника, целостность данных и аутентифицированный отказ в существовании. С этим расширением безопасности протокол DNS гораздо менее подвержен определенным типам атак. Но при внедрении дополнительной безопасности могут возникнуть сложности с поддержанием общей системы. Важно уметь балансировать доступные ресурсы сервера и ресурсы, потраченные на безопасность, чтобы не возникало конфликтных ситуаций и общая работа медицинской информационной системы не подвергалась риску.

Для защищенной передачи медицинских данных по международному стандарту FHIR перед любой командой / ответом HTTP устанавливается соединение по протоколу TLS. Безопасность канала связи должна управляться с учетом возможных рисков (например, не должна производится запись параметров GET в незащищенный журнал аудита).

Потенциальные каналы утечки при использовании аутентификации OAuth и SMART on FHIR

Сервер может выбрать аутентификацию клиентской системы или аутентификацию отдельного пользователя различными способами. Рекомендуется использовать OAuth для аутентификации и / или авторизации клиента и пользователя [3].

В настоящее время активно используется набор открытых спецификаций для интеграции приложений с электронными медицинскими записями, порталами, информационными службами здравоохранения и другими ИТ-системами здравоохранения - Smart-On-FHIR.

Среда запуска приложений SMART позволяет подключать сторонние приложения к данным электронной медицинской карты, что позволяет запускать приложения изнутри или снаружи пользовательского интерфейса системы электронной медицинской карты. Инфраструктура поддерживает приложения для использования врачами, пациентами и другими лицами через портал для пациентов, а также любую систему FHIR, где пользователь может дать разрешения на запуск приложения и отметить какие именно права доступа он дает конкретному приложению. Это обеспечивает надежный и безопасный протокол авторизации для различных архитектур приложений, включая приложения, работающие на устройстве конечного пользователя, например, браузер, а также приложения, работающие на защищенном сервере.

Этот профиль защиты предназначен для разработчиков приложений, которым необходим доступ к ресурсам FHIR путем запроса маркеров доступа с серверов авторизации, совместимых с OAuth 2.0. Серверы авторизации OAuth 2.0 настроены на посредничество в доступе на основе набора правил, настроенных для обеспечения соблюдения политики, которые могут включать в себя запрос авторизации конечного пользователя. Профиль определяет метод, с помощью которого приложение запрашивает авторизацию для доступа к ресурсу FHIR, а затем использует эту авторизацию для получения ресурса. Синхронизация контекста пациента не рассматривается. Другими словами, если данные пациента изменяются во время сеанса, приложение, по сути, не будет обновляться. Другие механизмы безопасности, такие как аутентификация конечного пользователя, время ожидания сеанса, выходят за рамки этого профиля, что может привести к наличию уязвимостей в системе. Об этих нюансах необходимо заранее обдумать и обеспечить должную защиту от несанкционированного доступа и возможных утечках информации. Возможно стоит прибегнуть к дополнительной системе защиты или программным путем доработать дыры в системе безопасности.

Приложение отвечает за защиту от возможных неправильных действий или вредоносных значений, передаваемых в URL-адрес перенаправления (например, значения, введенные с помощью исполняемого кода, такого как SQL, что позволяет предотвратить угрозы SQL-инъекции), а также за защиту кодов авторизации, токенов доступа и токенов обновлений от несанкционированного доступа и использования.

Разработчик приложения должен знать о потенциальных угрозах, таких как вредоносные приложения, работающие на той же платформе, поддельные серверы авторизации и поддельные серверы ресурсов, и применять контрмеры для защиты как самого приложения, так и любой важной информации, которую оно может содержать.

Потенциальные каналы утечки данных авторизации и контроля доступа

Основа, на которой построена любая система безопасности — это правильная идентификация. Аутентификация, контроль доступа, цифровые подписи

и т. д., полагаются сопоставление между соответствующими системами безопасности, описывающими какие-то правила и проверяемыми ресурсами. В FHIR нет встроенной системы безопасности, на которую можно основываться при проверке ресурсов или реализации безопасности.

Поэтому важно делать дополнительный свод правил для реализации безопасности, например, организация не должна передавать данные другой организации, если нет достаточных гарантий того, что другая сторона уполномочена их получать. Это верно, как при передаче с одной стороны, так и при передаче, с другой стороны. Каждый должен убедиться, что есть должное разрешение на передачу.

Существуют две классических модели контроля доступа: управление доступом на основе ролей (RBAC) и управление доступом на основе атрибутов (ABAC). Давайте рассмотрим оба случая.

В первой модели разрешения — это операции над объектом, к которому пользователь хочет получить доступ. Роль состоит из нескольких разрешений, объединенных по необходимости (например, права доступа необходимые для выполнения служебных обязанностей). По роли можно выделить функции пользователя. Если у роли пользователя есть соответствующие разрешения для доступа к объекту, то этому пользователю предоставляется доступ к объекту. В стандарте FHIR можно реализовать управление доступом на ролевой основе.

В управлении доступом на основе атрибутов пользователь запрашивает выполнение операций над объектами. На основе набора политик контроля доступа пользователь может получить или не получить доступ к ресурсу. В стандарте FHIR можно реализовать управление доступом на основе атрибутов ресурсов. Эти атрибуты включают теги безопасности, условия среды и т.д.

Чтобы решить давать ли доступ или не давать, обычно следует проанализовать информацию о клиенте (его роль, уровень доступа, к какому ресурсу обращается, т.е. является ли он конфиденциальным/чувствительным) и пациенте (отношение пациента к пользователю, наличие согласия пациента на обработку его персональных данных).

В законодательстве Российской Федерации для медицинских информационных систем определены требования по управлению доступом на ролевой основе. Поэтому управление доступом на основе атрибутов не рассматривается в данном выпускной квалификационной работе.

Потенциальные каналы утечки информации в модуле авторизации в медицинской информационной системе.

Для идентификации и аутентификации в медицинской информационной системе необходимо ввести логин и пароль. Логин и пароль можно получить, зарегистрировавшись самостоятельно или от системного администратора, если в МИС не предусмотрена самостоятельная регистрация. Помимо регистрации, во втором случае сразу будет назначена роль и определены права доступа, соответствующие назначенной роли. В зависимости от медицинской информационной системы роли могут различаться, но в общем случае можно выделить несколько ролей[5]. Они представлены в таблице 1. Основными при этом будут являться три: администратор, пациент и врач.

Для защиты входа в систему необходимо принять парольную политику, которая будет определять длину и состав пароля, а также количество попыток, после которых блокируется аккаунт, способ и время разблокировки.

Разблокировка может осуществляться автоматически после прохождения определённого времени, не слишком ограничивающего права пользователя, но и не позволяющее злоумышленники путем бутфорса взломать аккаунт.

Также разблокировать может системный администратор вручную. Для этого должна быть возможность

Таблица 1. Описание стандартных ролей в медицинской информационной системе.

Название роли	Возможности	Примечание
Пациент	Просмотр расписания работы врача, запись на прием, просмотр своей электронной карты пациента.	Имеет минимальные привилегии в системе.
Регистратор	Просмотр расписания работы врача, запись на прием, редактирование записей к врачу, работа приёмного отделения, работа с кассой, просмотр чеков.	
Врач	Просмотр календаря, просмотр и редактирование пациентов, просмотр и редактирование электронной медицинской карты пациента, настройки врача (протоколы приема, результаты исследований и анализов).	
Руководитель	Возможность управление пользователями и ролями пользователей.	Имеет возможности врача, при занимаемой должности главного врача или начмеда.
Администратор	Повышенные привилегии, доступ ко всем модулям медицинской информационной системы, возможность создания роли, добавление/удаление прав доступа.	Не может просматривать кабинет врача.

обращения в техподдержку для связи и описание причины.

Особое внимание надо уделить на механизмы защиты при восстановлении аккаунта. Стоит ввести систему проверки личности: секретный вопрос, привязка аккаунта к почте и т.п. При входе в систему должна соблюдаться сетевая безопасность, на автоматизированном рабочем месте должно стоять антивирусное программное обеспечение.

Потенциальные каналы утечки при контроле доступа в REST API

При разработке системы защиты для авторизации и доступа к информации необходимо учитывать все возможные методы доступа, создания или запроса информации. Их можно описать как следующие:

- Основные методы CRUD по ресурсам. Система безопасности должна анализировать возможности клиента на чтение, создание, удаление или модификацию ресурсов.
- Поиск информации не должен раскрывать связанные ресурсы.
- Параметры поиска _include и _revinclude позволяют клиенту запрашивать связанные ресурсы.
- Метки безопасности ресурсов.
- Некоторые ресурсы могут быть использованы для вложения других ресурсов. Система безопасности должна учитывать, открывает ли доступ ко всему ресурсу, также доступ к использованным внутри ресурсам, или для каждого ресурса нужен свой доступ.
- Определение операций, которые могут поддерживаться сервером. Система безопасности должна оценивать, может ли клиент вызывать эти операции и какую информацию следует возвращать из них.
- Система безопасности должна учитывать протокол «Break the Glass protocol» (в чрезвычайной ситуации, врач может запросить экстренный несанкционированный доступ к записи пациента для лечения, обычно такие случаи могут происходить при нахождении пациента в бессознательном состоянии.).

Должен анализироваться ответ веб-сервера при выводе наличия ошибки «Отказано в доступе». Слишком большое количество информации может раскрыть конфиденциальные детали, которыми может воспользоваться злоумышленник. Ошибка «Отказано в доступе» может быть вызвана отсутствием обязательной аутентификацией, т.е. пользователь не авторизован для доступа к конечной точке или пользователь не авторизован для доступа к конкретным данным, а также по другим причинам политики.

Чтобы сбалансировать соответствующую защиту, результат должен контролироваться политикой и данным контекстом. Типичные методы обработки ошибок[2]:

- Без результатов - это не выявит, какой-либо информации ни о пациентах, ни о данных, которые могут быть раскрыты.
- Ошибка 404 «Not Found» - подобен запросу к несуществующему ресурсу, поэтому тоже может защитить от утечки информации. Тем не менее, он подтверждает, что аутентификация пользователя подтверждена.
- Ошибка 403 «Forbidden» - сбой авторизации. Этот ответ следует использовать только тогда, когда клиент и / или пользователь достаточно хорошо известны, чтобы получить эту информацию. Таким образом, этот метод наиболее часто используется, когда пользователь может знать, что ему запрещен доступ. Но нельзя гарантировать, что такой ответ защищает от действий пользователя, которые могут изменить что-то, чтобы стать авторизованным.
- Ошибка 401 «Unauthorized» - предпринята попытка аутентификации пользователя, и она не была принята.

Стоит обратить внимание, что если сервер разрешает метод PUT в новое местоположение, то возврат 404 Not Found невозможен. Это означает, что клиенты могут использовать это для проверки того, существует ли контент, к которому у них нет доступа, что является незначительной информацией, но потенциально утечкой информации, которой может воспользоваться злоумышленник в корыстных целях, для взлома системы.

Список угроз медицинской информационной системы:

- Для формирования списка угроз для медицинской информационной системы был использован Банк данных угроз безопасности информации федеральной службы по техническому и экспортному контролю России [4]. В данном банке содержится перечень потенциальных угроз информационной безопасности и описание этих угроз, а также информация о источниках угроз и каким свойствам информационной безопасности может быть нанесен ущерб. После анализа особенностей медицинской информационной системы, ее различных конфигураций, можно выделить следующие актуальные угрозы:
- Угроза несанкционированного восстановления удалённой защищаемой информации.
- Угроза неправомерного ознакомления с защищаемой информацией.
- Угроза несанкционированного доступа к аутентификационной информации.
- Угроза несанкционированного изменения аутентификационной информации.
- Угроза несанкционированного копирования защищаемой информации.
- Угроза несанкционированного удаления защищаемой информации.
- Угроза несанкционированного создания учётной записи пользователя.
- Угроза несанкционированной модификации защищаемой информации.

- Угроза повышения привилегий.
- Угроза использования механизмов авторизации для повышения привилегий.
- Угроза доступа к защищаемым файлам с использованием обходного пути.
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию.
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.
- Угроза обхода некорректно настроенных механизмов аутентификации.
- Угроза подделки записей журнала регистрации событий.
- Угроза хищения аутентификационной информации из временных файлов cookie.

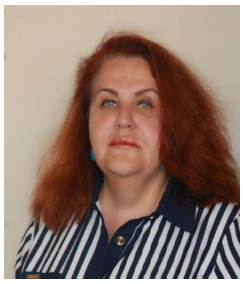
Полный перечень угроз перечислен в Банке данных угроз безопасности информации.

Вывод. Введение новых информационных технологий должно сопровождаться соответствующим развитием системы защиты информации от несанкционированного доступа. Обзор потенциальных каналов утечки информации, поможет разработчикам медицинской информационной системы учесть возможные угрозы и устранить их при планировании архитектуры МИС.

Список литературы:

1. ГОСТ Р ИСО/HL7 27932-2015 Информатизация здоровья. Стандарты обмена данными. Архитектура клинических документов HL7. Выпуск 2, Стандартинформ (Последняя редакция 2016 г.)
2. Матео Меуччи Руководство по тестированию OWASP // Цикл статей – 2015 г. – Вып.4, - 349 с.
3. Thomas Erl, Benjamin Carlyle, Cesare Pautasso, Raj Balasubramanian SOA with REST v. 5.1. — Prentice Hall, 2013. — 624 p. — ISBN 978-0-13-701251-0
4. Банк данных угроз информационной безопасности Федеральной службы по техническому и экспортному контролю // Угрозы [Электронный ресурс] Режим доступа к ресурсу: https://bdu.fstec.ru/threat, свободный. (Дата обращения 05.01.2020).
5. Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО) (утв. Министерством здравоохранения РФ 1 февраля 2016 г.)

ПРИМЕНЕНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСТИНИЧНЫХ ПРЕДПРИЯТИЙ



Авилова Наталья Леонидовна
Доктор исторических наук, заместитель заведующего кафедрой по научной работе ,профессор кафедры «Туризм и гостиничное дело» Института туризма, рекреации, реабилитации и фитнеса ФГБОУ ВО «Российский государственный университет физической культуры, спорта, молодёжи и туризма (ГЦОЛИФК)»

Аннотация: *в статье рассматриваются проблемы построения и развития эффективной системы обеспечения безопасности в сфере гостиничных услуг, применения современных средств безопасности в области оборудование систем видеонаблюдения и кибербезопасности.*

Ключевые слова: *средства безопасности, технические средства защиты, и физические средства защиты, конфиденциальная информация, кибербезопасность, системы видеонаблюдения.*

Abstract: *the article deals with the problems of construction and development of an effective security system in the field of hotel services, the use of modern security equipment in the field of video surveillance and cybersecurity.*

Keywords: *security means, technical means of protection, and physical means of protection, confidential information, cybersecurity, video surveillance systems.*

Применение современных средств безопасности, наряду с профессиональными и компетентными действиями сотрудников службы безопасности гостиниц позволяют обеспечить рост финансово-экономической результативности гостиничного предприятия и повышению удовлетворенности.

В современных условиях безопасность гостиничных предприятий, обеспечивается за счет технических и физических средств защиты, безубыточной деятельности предприятия, а также, неразглашения конфиденциальной информации предприятия и его клиентов, и сохранение имущества.

Решение этих вопросов должно происходить с позиции системного подхода, который обеспечивает выявление проблемных зон и опасных угроз в деятельности гостиницы и предлагает дальнейшие меры по их устранению

Особенно острыми вопросами совершенствования системы безопасности гостиничного предприятия на сегодняшний