Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:616-082

Наумович
Антон Игоревич

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМЕ ЗДРАВООХРАНЕНИЯ

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-40 80 01 Компьютерная инженерия. Хранение и обработка данных

Научный руководитель
Насуро Екатерина Валериевна
кандидат технических наук,
доцент кафедры ЭВМ, БГУИР

Минск 2021

КРАТКОЕ ВВЕДЕНИЕ

Работа с медицинскими персональными данными отличается рядом особенностей. Учреждения здравоохранения обязаны хранить данные о состоянии здоровья каждого пациента в виде медкарты, и разглашать их запрещено при любых условиях. Эти сведения объединяются под широко известным термином «врачебная тайна». Сохранность врачебной тайны регулируется Ст. 46 Закона РБ О здравоохранении 2435-XII от 18.06.1993 г.

Необходимый уровень защиты персональных данных важно обеспечивать на каждом этапе их обработки, что оказывается непростой задачей в процессе сбора и записи сведений, их систематизации и хранения в базе, уточнения деталей и, наконец, уничтожения информации, потерявшей актуальность.

С ростом уровня цифровизации риски возникновения утечек персональных данных увеличиваются. Например, в медучреждениях, где уже установлены медицинские информационные системы, данные могут пропадать из-за технических сбоев. Также нельзя забывать о еще одной распространенной проблеме – человеческом факторе. Иногда сотрудники, которые отвечают за безопасность данных в информационных системах, не обладают нужными компетенциями или демонстрируют безответственное отношение к вопросу.

Последствия таких утечек могут оказаться очень серьезными для клиники и ответственных за инцидент сотрудников. Нарушения безопасности могут привести к административной, гражданско-правовой, дисциплинарной или даже уголовной ответственности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью исследования является обеспечение безопасности персональных данных в системе здравоохранения за счет разработки методического аппарата защиты информации в медицинской информационной системе «Лекарь». Для достижения данной цели необходимо решить следующие задачи:

1) провести анализ угроз информационной безопасности в системе здравоохранения;

2) провести анализ состояния и возможностей медицинской информационной системы «Лекарь»;

3) разработать модель системы защиты информации медицинской информационной системы «Лекарь»;

4) Исследовать и обобщить недостатки разработанной модели защиты

Объектом исследования является медицинская информационная система «Лекарь».

Предметом исследования является защита информации в медицинской информационной системе «Лекарь».

Актуальность исследования заключается в том, что, несмотря на значительное число публикаций, имеющих несомненное теоретическое и практическое значение, вопросы, связанные с распределением сил и средств при защите персональных данных в системе здравоохранения в целом и в медицинской информационной системе «Лекарь» в частности, в условиях высокой динамики возникновения информационных угроз не рассматриваются. Так же, целый ряд направлений в области защиты информации хозяйствующих субъектов остался недостаточно разработанным, к их числу можно отнести: отсутствие методик информационного описания ряда внешних угроз, учитывающих динамику развития недружественных действий непосредственно, как процесса; отсутствие научно обоснованных подходов к отражению массированных информационных угроз различной природы и другие.

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя Е. В. Насуро, заключается в формулировке целей и задач исследований.

Структура и объем диссертации

Диссертация состоит из введения, обзора литературы, трех глав, заключения, списка использованных источников, списка публикаций автора и приложений. В первой главе представлен анализ предметной области, выявлены

исторические особенности развития объекта исследования, выявлены недостатки и преимущества технологий блокчейн и смарт-контрактов в решении поставленной задачи. Вторая глава посвящена анализу сферы здравоохранения на предмет недостатков, процессов, требующих автоматизации путем внедрения информационных систем. Третья глава содержит этапы проектирования архитектуры системы, отдельных ее модулей и общего результата. В четвертой главе представлены результаты исследования, полученные преимущества и недостатки разработанной системы, ее перспективы

Общий объем работы составляет 79 страниц, из которых основного текста – 62 страницы, 8 рисунков на 4 страницы, 2 таблицы на 1 страницу, библиографический список из 34 наименований на 3 страницы и приложения на 9 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во введении представлено краткое описание актуальности темы работы. Также обозначены причины для выполнения данной диссертационной работы.

В первой главе введены основные понятия информационной безопасности и рассмотрены основные угрозы информационной безопасности. Также проведен анализ технологий аутентификаций в системах. Рассмотрены методы защиты данных от несанкционированного доступа, технологии и методы повышения уровня достоверности данных. Исходя из проведенного обзора литературы было принято решение что наилучшая система безопасности комбинирует различные методы защиты информации.

Во второй главе был проведен обзор существующей медицинской информационной системы «Лекарь», были описаны механизмы защиты существующей системы, а также выявлены недостатки. Также был обнаружен факт того, что в системе присутствуют небезопасные способы защиты информации, а также недоработки, которые привели к утечкам конфиденциальной информации. Для решения существующих проблем были описаны концепции доработки модели защиты информации рассматриваемой медицинской информационной системы.

В третьей главе было выполнено высокоуровневое проектирование системы. После этого были спроектированы компоненты системы, и

разработаны подходы для обеспечения наивысшей степени сохранности персональных данных.

В 4 главе был проведен анализ системы на соответствия требованиям технических нормативно-правовых актов Республики Беларусь. По результатам анализа были сделаны выводы о том, что система полностью соответствует требованиям, а в разрезе некоторых подходов предлагает наисовременнейшие решения в хранении, распределении и сохранности конфиденциальных данных. Однако в ходе оценки затрат на внедрение данных подходов в реальные системы, был выявлен тот факт, что такой подход к реализации систем безопасности едва-ли является бюджетным решением, и требует значительного количества средств на внедрение. Учитывая репутационные риски, данный подход к реализации безопасности персональных данных в учреждениях здравоохранения является оправданным.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

С ростом уровня цифровизации риски возникновения утечек персональных данных увеличиваются. Например, в медучреждениях, где уже установлены медицинские информационные системы, данные могут пропадать из-за технических сбоев. Также нельзя забывать о еще одной распространенной проблеме – человеческом факторе. Иногда сотрудники, которые отвечают за безопасность данных в информационных системах, не обладают нужными компетенциями или демонстрируют безответственное отношение к вопросу.

Последствия таких утечек могут оказаться очень серьезными для клиники и ответственных за инцидент сотрудников. Нарушения безопасности могут привести к административной, гражданско-правовой, дисциплинарной или даже уголовной ответственности.

Диссертационное исследование было направлено на повышение уровня информационной безопасности персональных данных в системе здравоохранения. В ходе работы были получены следующие результаты:

- проведен анализ угроз информационной безопасности в медицинских информационных системах;

- проведен анализ состояния и возможностей системы медицинской информационной системы «Лекарь»;
- разработана архитектура и компоненты системы защиты информации медицинской информационной системы «Лекарь»;
- исследованы и обобщены недостатки разработанной модели защиты информации, ее особенности;
- проанализированы выгоды, которые могут быть получены от внедрения.

Для оценки надежности спроектированной системы защиты информации была произведена оценка условий по защите информации, установленных действующим законодательством и обеспечение возможности разграничения и контроля доступа к системе в целом, отдельным ее функциям, реестрам документов, отдельным документам и частям документов на ролевой основе, в том числе для групп пользователей.

Медицинская информационная система поддерживает ряд функций защиты информации от несанкционированного доступа:

- аутентификация и авторизация пользователя по логину и паролю условно-постоянного действия;
- управление списками контроля доступа для всех основных объектов медицинской информационной системы, включая базы данных, отдельные записи в БД, объекты интерфейса и т.д.;
- изменение прав управления доступом пользователей к ресурсам медицинской информационной системы «Лекарь»;
- регистрация действий пользователей по доступу к информационным ресурсам и использованию функций медицинской информационной системы, любых изменений и запросов к данным, включая их содержание, а также регистрация изменений прав управления доступом;
- регистрация неудачных попыток доступа и изменения системных объектов с сохранением даты и времени, регистрационного имени пользователя системы и типа события в журнале и возможность его анализа;

– обеспечение доступа к данным системы только зарегистрированным авторизованным пользователям, подписавшим специальное соглашение о неразглашении конфиденциальной информации и врачебной тайны.

В рамках проекта внедрения медицинской информационной системы «Лекарь» со стороны информационной системы реализованы инфраструктурные сервисы безопасности, обеспечивающие базовый уровень информационной безопасности для медицинской информационной системы, которые обеспечивают:

– идентификацию и авторизацию пользователей;
– управление событиями информационной безопасности;
– инвентаризацию и мониторинг состояния информационной безопасности;
– контроль действий администраторов систем;
– систему антивирусной защиты;
– систему сетевой безопасности, включающую в себя средства межсетевого экранирования, IDS/IPS, сегментирование сетевой инфраструктуры и инфраструктуры систем хранения, VPN.

Предложенная система обеспечения безопасности персональных данных позволяет значительно повысить уровень надежности медицинских информационных систем и предоставляет возможности для многоступенчатой защиты данных.

Рекомендации по практическому использованию результатов

1. Полученные результаты исследования надежности существующей системы и требований к информационной безопасности медицинских данных в целом формируют достаточную теоретическую базу для разработки высококлассной системы защиты информации. Кроме того, они могут быть использованы для дальнейшего исследования и развития представленной системы.

2. Разработанная архитектура системы защиты информации и подходы к обеспечению конфиденциальности личных данных могут применяться не только

в сфере здравоохранения, но и в любой другой области, требующей повышенного внимания к надежной защите данных. На основе разработанной архитектуры возможно создание системы любой сложности и масштаба.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1) Наумович А.И., Шелягович А.С., «Защита информации в компьютерных сетях методом DECEPTION», технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно – технической конференции, Минск, 5 июня 2018 г. – Минск, С. 69.

2) Наумович А.И., Насуро Е.В., «Трехуровневая система обнаружения вторжений для промышленных систем управления», Международный научный журнал «Молодой ученый» №21(363), май 2021г.; ISSN 2072-0297.3