МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему«Защита данных предприятия с использованием технологии blockchain»

Исполнитель Немчинова Софья Игоревна
(фамилия, имя, отчество)

Руководитель Грызунов Виталий Владимирович
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой

(подпись)

Завгородний Владимир Николаевич
(фамилия, имя, отчество)

«___»_____20___г.

Санкт-Петербург

2019

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ _____Завгородний В.Н.

(подпись) (фамилия, имя, отчество)

« _ »_____ 2019 года

Задание

на выпускную квалификационную работу

студентке Немчиновой Софье Игоревне

(фамилия, имя, отчество)

1. Тема Защита данных предприятия с использованием технологии blockchain _____

закреплена приказом ректора Университета от «___» _____2019 года, № ____

2. Срок сдачи законченной работы «___» _____2019 года

3. Исходные данные к выпускной квалификационной работе:

«Нормативно-правовые акты обеспечения информационной безопасности»»_____

«Стандарты в области здравоохранения»

«Методология оценки рисков предприятия»

4. Перечень вопросов, подлежащих разработке (краткое содержание работы (проекта):

- Введение. Актуальность темы, цели и задачи выпускной квалификационной работы.

- Глава 1. Основы электронного документооборота ____

(наименование главы)

Анализ существующих систем электронного документооборота, выявление угроз, сравнение технологий защиты данных.

(содержание главы и её разделов, параграфов)

- Глава 2.Анализ и расчет рисков и угроз в медицинской информационной системе.

Анализируются риски и угрозы которые наиболее часто происходят на предприятии, эффективность применения СЗИ с общим риском МИС

(содержание главы и её разделов, параграфов)

- Глава 3. Проектирование работы блокчейн с электронной медицинской картой

(наименование главы)

- Глава 4.Разработка предложений по совершенствованию системы

работающей на платформе блокчейн.

(наименование главы)

- Заключение. Выводы по работе в целом. Оценка степени решения поставленных задач.

5. Перечень материалов, представляемых к защите:

- Пояснительная записка.

5. Дата выдачи задания: «_____»_____ 2018 года

Руководитель выпускной квалификационной работы

к.т.н, доцент Грызунов Виталий Владимирович _____ _____

(должность, ученая степень, ученое звание, фамилия, имя, отчество)

(подпись)

Задание приняла к исполнению «___»_____2018 года

Студентка Немчинова Софья Игоревна ИБ-С13-1 _____ _

(фамилия, имя, отчество, учебная группа)

(подпись)

РЕФЕРАТ

Дипломная работа: 60с., 2 рис., 2 табл., 1 приложение, 12 источников литературы.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА, ТЕХНОЛОГИЯ БЛОКЧЕЙН, АНАЛИЗ РИСКОВ, ПРОЕКТИРОВАНИЕ РАБОТЫ БЛОКЧЕЙН.

Объект исследования: медицинская электронная карта больного

Предмет исследования: целостность сохранения архивных данных в системе

Цель работы: является разработка защищенной системы обработки и хранения данных, на примере работы медицинской информационной системы.

В дипломной работе проводится анализ существующих систем электронного документооборота, рассчитываются угрозы и риски информационной безопасности в медицинской информационной системе.

Проектируется работа с данными в системе с технологией блокчейн.

Рассматриваются реальные случаи нарушения целостности данных в медицинской информационной системе при хранении электронной медицинской карты.

Спроектированное в данной работе программное обеспечение позволит не допустить нарушения целостности информации, создаст закрытую децентрализованную базу данных. Которая позволит всем участникам системы отслеживать вносимые изменения и происходящие назначения.

Оглавление

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронный документооборот – Документооборот с использованием автоматизированной информационной системы (системы электронного документооборота).

Электронный документ – документ, информация которого представлена в электронной форме.

Электронная цифровая подпись – информация в электронной форме, присоединенная к электронному документу или иным образом связанная с ним и позволяющая идентифицировать лицо, подписавшее электронный документ [1].

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

[Федеральный Закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ, статья 3, пункт 1)]

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

СЭД — Система автоматизации документооборота

МИС — Медицинская информационная система

АРМ — Автоматизированное рабочее место

ЛПУ — Лечебно-профилактическое учреждение

ПДн — Персональные данные

ЭЦП — Электронная цифровая подпись

ИСПдн — Информационная система персональных данных

ИПБ — Источник бесперебойного питания

СВТ — Средства вычислительной техники

ИБ — Информационная безопасность

ПО — Программное обеспечение

БД — База данных

СУБД —Система управления базами данных

ВВЕДЕНИЕ

Со стремительным ростом информатизации в мире, всё больше внедряются компьютерные технологии, объем цифровой информации постоянно увеличивается, предъявляя свои требования. В таких условиях возникла необходимость создавать и внедрять на предприятиях комплексные решения для обработки документации и автоматизации управленческого процесса.

Благодаря электронным документам теперь очень удобно получать и оплачивать счета. Даже оформлять паспорта можно на специальном государственном сайте, не прибегая к бумажным анкетам.

В медицинской сфере появились электронные медицинские карты и больничные листы, и это всё содержит личную уникальную информацию.

Получив к такой информации доступ, мошенник сможет узнать о человеке абсолютно всё, а недобросовестный работник удалить или передать данные третьему лицу или исказить информацию на благо себе.

Поэтому одним из ключевых моментов при ведении любых бизнес-процессов с автоматизированным документооборотом стала защита информации на всех этапах ее обработки. Обеспечение целостности данных, защита от несанкционированного доступа, защита данных на процедурном, нормативном и технологическом уровнях.

Использование системы электронного документооборота предполагает хранение целой базы данных, в которой будет находиться вся важная информация для организации, утечка которой может привести к угрозе деятельности предприятия.

Целью данной дипломной работы является разработка защищенной системы обработки и хранения данных, на примере работы медицинской информационной системы. Объектом исследования является электронная медицинская карта, которая содержит личные данные пациентов и врачебную тайну, подлежащая защите согласно существующему законодательству.

1. ОСНОВЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1.1 Внедрение электронного документооборота

Вся деятельность на предприятиях за последнее время стала обрабатываться в электронной форме с применением компьютерных технологий. Ведение электронного документооборота сокращает время обмена и рассмотрения документов. В большинстве случаев компании экономят на почтовых услугах и курьерах, закупках бумаги и обслуживанию печатной техники.

Перед тем как решиться на автоматизацию документооборота каждое предприятие должно определиться, как будет производиться обмен информацией, какие корректировки и правила нужно будет внести в управленческую политику, кто будет ответственным лицом за передачу цифровой документации между контрагентами. После принятия решения об использовании СЭД всегда необходимо рассмотреть законодательные и нормативно-правовые акты, которые могут потребовать от компании соблюдения новых законов и правил в работе.

В России в 2000х годах был принят целый ряд законов, одобряющий использование данных систем, на коммерческих предприятиях и в государственных учреждениях.

Одни из главных нормативно-правовых актов:

- Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ

- Федеральный закон «Об архивном деле в РФ» от 22.10.2004 № 125-ФЗ.

- Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

- Приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении порядка проведения классификации ИН персональных данных»

- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, N 48, ст. 6001).

- Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Исходя из данной нормативной документации, возникает порядок обработки и хранения данных, и обеспечение достаточного уровня защиты информации.

Использование СЭД на предприятиях накладывает обязательства по усилению безопасности автоматизированной

системы, в которой обрабатывается, хранится и пересылается информация.

Из чего следует, что система электронного документооборота должна: иметь функции разграничения доступа по уровням, уметь идентифицировать сотрудника, журналировать информацию о работе с документом и это самый простой набор требований.

1.2 Рассмотрение актуальных автоматизированных систем

В настоящее время, выбор автоматизированных систем документооборота очень велик, для деятельности компании разрабатываются различные функции. Они могут разделяться на группы по своим функциям:

Электронный архив - это система структурированного хранения электронных документов. В этой группе, основной упор может делаться, например, на улучшение средств полнотекстового поиска (нечеткий поиск, смысловой поиск и т.д.) или эффективную организацию хранения. Основные функции архива — оцифровка бумажных документов, управление web-контентом, поточный ввод и быстрый поиск. Благодаря внедрению архива можно сократить время доступа к информации, снизить риски порчи или потери важных документов, повысить уровни информационной безопасности. Электронные архивы обычно существуют в составе СЭД и отдельно используются достаточно редко.

Workflow-системы - обеспечивают автоматизацию не отдельных функций, а бизнес-процессов компании. Система

Workflow четко определяет процесс: что, кто, когда и как делает, откуда получает и куда отправляет. Сотрудник не сможет неправильно заполнить документ, пропустить какие-то сроки, в системе предусмотрены напоминания, а также уведомления руководителя о том, что на конкретном этапе у конкретного пользователя процесс обработки документа нарушен. Workflow-системы в основном устанавливают в компаниях с высокой степенью формализации бизнес-процессов, документооборот в которых при простой структуре имеет массовый характер. Недостатком таких систем является сложность и длительность внедрения. Кроме того, они не могут заменить электронный архив, поскольку хранят не все документы, а только используемые в процессе работы [2].

Для каждой организации СЭД подбирается и конструируется исходя из специфики работы предприятия. Это может быть как объединение функций представленных двух систем, так и разработка совершенно новых. Поскольку будет рассматриваться работа медицинской информационной системы важно понять процессы, происходящие при ее функционировании.

1.3 Описание работы МИС и обрабатываемых персональных данных

Для функционирования медицинской информационной системы важно соблюдать три главных аспекта информационной безопасности – целостность, конфиденциальность, доступность. Для медицинских организаций, поскольку лечебные и вспомогательные процессы

связаны с обработкой информации о пациентах, которая хранится на традиционных носителях («бумажные» документы) или в цифровом виде, защита информации является важным и обязательным требованием. При этом в МИС, как правило, не обрабатывается информация, связанная с государственной тайной или формированием законодательных актов на государственном или муниципальном уровнях, т.е. МИС относится к типу «Иные информационные системы» [3].

В соответствии с классификацией (приказом N 55/86/20 от 13 февраля 2008 года ФСТЭК России, ФСБ России и Мининформсвязи России) МИС обрабатывает данные первой категории (Ф.И.О., телефон, номер паспорта, год рождения и др.), а так же сведения о состоянии здоровья по большому количеству пациентов.

Основные модули, присущие большинству МИС:

ЭЛЕКТРОННАЯ МЕДИЦИНСКАЯ КАРТА

В зависимости от профиля медучреждения (амбулатория или стационар) может быть использована амбулаторная карта или история болезни пациентов электронном виде. Экспорт ЭМК во внешний формат.

СТАТИСТИКА

Автоматизация медицинской статистики и других форм отчетности. Оперативный доступ к отчетам разного вида: управленческим, финансовым, медицинской статистики, материального учета. Исполнимость отчетов любой сложности.

РАСПИСАНИЕ

Поддержка расписания приема врачей, диагностических кабинетов, мест групповых занятий.

КЛИНИЧЕСКАЯ ЛАБОРАТОРИЯ

Лабораторный модуль для организации бизнес-процесса лаборатории и работа по направлениям. Содержатся лабораторные профили с возможностью ручного ввода или автоматизированного импорта результатов исследований от анализаторов. Забор биоматериала. Контроль качества.

УЧЕТ УСЛУГ

Учет медицинских услуг и взаиморасчеты с разными контрагентами медицинских учреждений – страховыми компаниями, предприятиями и пациентами.

КАССА

Объединение системы с фискальным регистратором для реализации рабочего места кассира. Синхронизация с бухгалтерской системой, возможность экспорта документов и проводок в бухгалтерскую программу предприятия.

АПТЕКА

Поддержка складов медикаментов и расходных материалов. Ведется персонализированный учет расхода при оказании медицинских услуг.

КОЕЧНЫЙ ФОНД

Для больниц и госпиталей в МИС предусмотрен модуль планирования и учета палатного и коечного фонда. Различные схемы бронирования палат.

ПЛАНЫ ЛЕЧЕНИЯ

План лечения – механизм поддержки стандартов лечения в единстве и взаимодействии с другими модулями МИС и удобный способ, упрощающий

работу врача.

СТАНДАРТЫ ЛЕЧЕНИЯ

Использование государственных стандартов лечения с помощью общего механизма работы с планами лечения и справочника шаблонов.

РЕПЛИКАЦИЯ

МИС обеспечивает возможность обмена электронными медицинскими картами между разными учреждениями, синхронизации справочников и объединение финансовой информации.

ОБРАБОТКА ИЗОБРАЖЕНИЙ

Получение и хранение медицинских изображений в современных условиях обеспечивают, как правило, специализированные комплексы оборудования и программных средств.

МОДУЛЬ СОПРЯЖЕНИЯ

Обеспечивает подключение медицинского оборудования и организацию импорта данных из внешних источников с помощью оригинальных технологий обмена информацией.

СТАНДАРТ HL7

Использование международного стандарта HL7 в МИС создает дополнительные возможности синхронизации с медицинским оборудованием и внешними приложениями.

СИСТЕМНОЕ ЯДРО

Обеспечение безопасности и конфиденциальности данных является одним из главных требований к современной МИС. Обеспечивает доступ к базе данных и реализует систему безопасности в работе с данными. Включает в себя модуль статистики [4].

На рисунке 1 представлена схема работы МИС ЛПУ с основными модулями программного обеспечения и внешними источниками.

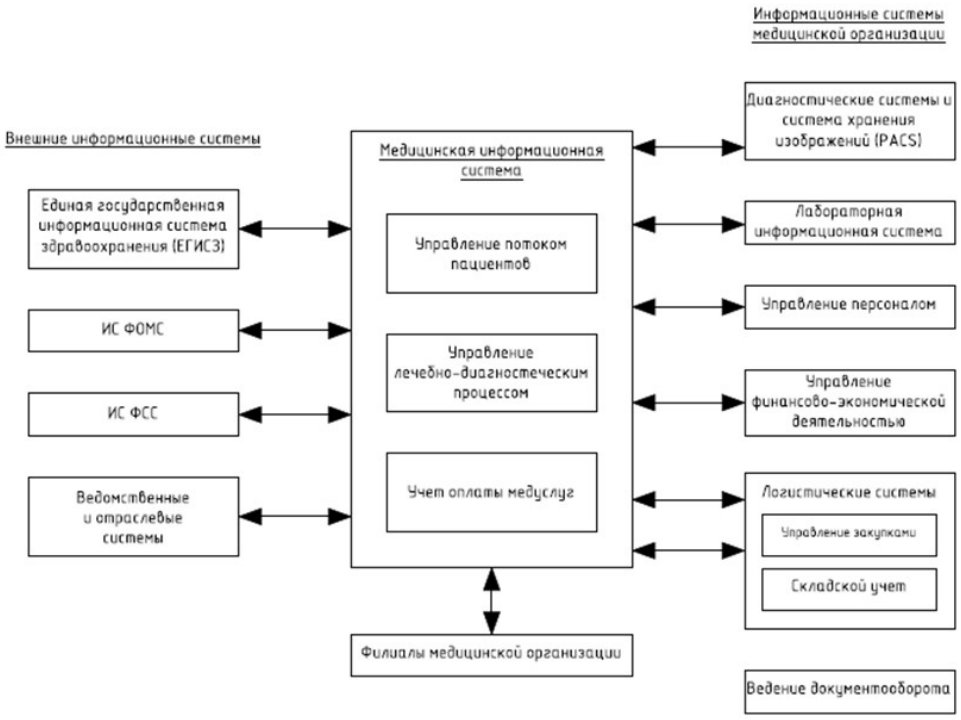


Рисунок 1 – Схема работы МИС

Обработка персональных данных:

Обработка персональных данных проводится на специализированном АРМ, только сотрудником, имеющим права на обработку персональных данных пациентов и работников ЛПУ. Данный перечень сотрудников определяется приказом Главного врача или Генерального директора, в зависимости от структуры медицинского учреждения. Смотреть Приложение 1.

1.4 Классификация информационной системы

Для определения уровня защиты информации необходимо провести классификацию информационной системы по обработке персональных данных. В процессе анализа рассматривается среднестатистическое лечебное учреждение, в котором обрабатываются данные менее 1000 субъектов являющимися сотрудниками и более 150 тысяч субъектов являющимися пациентами учреждения.

Таблица 1 Классификация информационной системы

Кол-во субъектов ПДн в системе Категория ПДн обрабатываемых в электронном виде	Более 100 тысяч субъектов	От 1 тысячи до 100 тысяч субъектов	До 1 тысячи субъектов
касающиеся национальной и расовой принадлежности, религиозных либо философских убеждений, здоровья и интимной жизни	класс 1 (К1)	класс 1 (К1)	класс 1 (К1)
позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию	класс 1 (К1)	класс 2 (К2)	класс 3 (К3)
позволяющие идентифицировать субъекта ПДн	класс 2 (К2)	класс 3 (К3)	класс 3 (К3)
обезличенные или общедоступные ПДн	класс 4 (К4)	класс 4 (К4)	класс 4 (К4)

Таким образом, информационная система данной организации относится к *классу 1 (К1)* - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них,

может привести к значительным негативным последствиям для субъектов персональных данных.

1.5 Модель нарушителя

Внутренние нарушители – сотрудники ЛПУ, с предоставленными им правами и полномочиями на деятельность в МИС, а также лица, обслуживающие аппаратно–программные комплексы МИС или допущенные к ним, в здания и помещения, где функционирует МИС ЛПУ. Внешние нарушители –– это сотрудники ЛПУ, которым не предоставлены права по доступу к ресурсам, в здания и помещения, где функционирует МИС ЛПУ, а также субъекты, не являющиеся сотрудниками ЛПУ, но осуществляющие попытки несанкционированного доступа к указанным ресурсам.

1.5.1 Внутренние нарушители

Внутренние нарушители ИБ МИС ЛПУ В рамках построения ИБ МИС ЛПУ возможны действия внутреннего нарушителя, принадлежащего к любой из следующих четырех категорий лиц:

а)пользователи МИС ЛПУ — медицинский персонал, осуществляющий доступ к информационным и вычислительным ресурсам МИС ЛПУ в рамках выполнения своих должностных обязанностей;

б)технический персонал МИС ЛПУ (системные администраторы, администраторы БД, администраторы СУБД, администраторы прикладных программных комплексов,

специалист по ИБ, операторы, программисты и инженеры сопровождения) –– сотрудники ЛПУ, задачей которых является организация эксплуатации, обслуживание ПО и технических средств МИС ЛПУ;

в)посетители ЛПУ –– лица, персональные данные которых обрабатываются МИС ЛПУ, и которым разрешен доступ на объекты и в помещения, где функционирует МИС ЛПУ, в установленном порядке;

г)обслуживающий персонал и охрана объектов и помещений, в которых размещаются технические средства МИС ЛПУ.

Принимаются следующие предположения об уровне знаний и возможностях внутреннего нарушителя ИБ:

- нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС ЛПУ, технико-программного обеспечения в целом;

- нарушитель знает структуру, функции и механизм действия средств защиты, их место в системе ИБ МИС ЛПУ;

- нарушитель правильно представляет функциональные особенности работы МИС ЛПУ, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;

- нарушитель может использовать непреднамеренные действия других пользователей МИС ЛПУ (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).

При этом нарушитель может использовать:

- штатные технические средства, входящие в состав МИС ЛПУ (при получении к ним доступа);

- штатные носители информации и технические средства, которые разрешается легально проносить через посты охраны ЛПУ;

- компактные носители информации и технические средства (например, сотовый телефон, беспроводные средства передачи информации и т.п.), непосредственно не относящиеся к СВТ.

1.5.2 Внешние нарушители ИБ МИС ЛПУ

В рамках построения ИБ МИС ЛПУ возможны действия внешнего нарушителя, принадлежащего к любой из следующих трех категорий лиц:

а)лица, разрабатывающие и предоставляющие ПО для МИС ЛПУ, — сотрудники фирм–разработчиков и фирм–поставщиков ПО;

б)лица, разрабатывающие и предоставляющие технические средства для МИС ЛПУ –– сотрудники фирм–разработчиков и фирм-поставщиков технических средств и оборудования;

в)посторонние –– лица, не относящиеся ко всем вышеперечисленным категориям.

Принимаются следующие предположения об уровне знаний и возможностях внешнего нарушителя ИБ:

- нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС, технико-программного обеспечения в целом;

- нарушитель знает структуру, функции и механизм действия средств защиты, их место в системе ИБ МИС ЛПУ;

- нарушитель правильно представляет функциональные особенности работы МИС ЛПУ, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;

- нарушитель может использовать непреднамеренные действия пользователей МИС ЛПУ (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).

При этом нарушитель может использовать штатные технические средства, входящие в состав МИС ЛПУ (при получении к ним доступа), средства сетевой атаки (при попытках доступа к данным при их передаче по сетям), а также компактные носители информации и технические средства (например, сотовый телефон, беспроводные средства передачи информации и т.п.), непосредственно не относящиеся к СВТ [5].

1.6 Системы защиты, используемые в МИС

Системы предотвращения утечек информации dlp

Под DLP-системами принято понимать программные продукты, защищающие организации от утечек конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных.

Подобного рода системы создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемой информацией должен быть не только интернет-трафик, но и ряд других информационных потоков: документы, которые

выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтере, отправляемые на мобильные носители через Bluetooth и т.д.

Поскольку DLP-система должна препятствовать утечкам конфиденциальной информации, то она в обязательном порядке имеет встроенные механизмы определения степени конфиденциальности документа, обнаруженного в перехваченном трафике. Как правило, наиболее распространены два способа: путём анализа специальных маркеров документа и путём анализа содержимого документа. В настоящее время более распространен второй вариант, поскольку он устойчив перед модификациями, вносимыми в документ перед его отправкой, а также позволяет легко расширять число конфиденциальных документов, с которыми может работать система [6].

Недостатки системы: недостатком лингвистических технологий для контроля всего спектра корпоративной конфиденциальной информации является то, что не вся конфиденциальная информация находится в виде связных текстов. Хотя в базах данных информация и хранится в текстовом виде, и нет никаких проблем извлечь текст из СУБД, полученная информация чаще всего содержит имена собственные — ФИО, адреса, названия компаний, а также цифровую информацию — номера счетов, кредитных карт, их баланс и прочее. Обработка подобных данных с помощью лингвистики много пользы не принесет.

IDS/IPS - системы обнаружения и предотвращения вторжений и хакерских атак

Основное предназначение подобных систем — выявление фактов неавторизованного доступа в корпоративную сеть и

принятие соответствующих мер противодействия: информирование ИБ-специалистов о факте вторжения, обрыв соединения и перенастройка межсетевого экрана для блокирования дальнейших действий злоумышленника, т. е. защита от хакерских атак и вредоносных программ.

Технологии IPS используют методы, основанные на сигнатурах — шаблонах, с которыми связывают соответствующие инциденты. В качестве сигнатур могут выступать соединения, входящие электронные письма, логи операционной системы и т.п. Такой способ детекции крайне эффективен при работе с известными угрозами, но очень слаб при атаках, не имеющих сигнатур.

Еще один метод обнаружения несанкционированного доступа, называемый HIPS, заключается в статистическом сравнении уровня активности происходящих событий с нормальным, значения которого были получены во время так называемого «обучающего периода». Данный способ может дополнять сигнатурную фильтрацию и блокировать хакерские атаки, которые смогли ее обойти.

Резюмируя функции и принципы работы IDS и IPS систем предотвращения вторжений, можно сказать, что они решают две крупные задачи:

-анализ компонентов информационных сетей;

-адекватное реагирование на результаты данного анализа [7].

Недостатки системы: для эффективной работы системы нужна грамотная точная настройка, если использовать стандартные установки, система не сможет в полной мере обеспечить высокий уровень защиты.

Электронная цифровая подпись

ЭЦП представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (т. е. обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, сохраняющая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Наиболее защищенной считается квалифицированная электронная подпись, она изготавливается при помощи методов ФСБ. Такой квалификационный сертификат имеет ключ проверки, выпускаемый аккредитованным центром.

Недостатки: Цифровая подпись не всегда привязана жестко к автору, а может быть привязана к предприятию, отделу, компьютеру или логину пользователя, которые являются разделяемыми ресурсами. Конечно, доступ во внутреннюю сеть предоставляется только правомерным пользователям после соответствующей авторизации, а все действия протоколируются, но помешать авторизованному

пользователю выполнить разрешенные ему операции в сети невозможно. Если ключ ЭЦП — один на отдел, то практически любой его сотрудник может изменить документ, подменить его или уничтожить. Внутренний злоумышленник способен нарушить как целостность документа, так и его авторство [8].

1.7 Подсистемы защиты, используемые в МИС

Типовая медицинская информационная система, предназначенная для поддержки технологических процессов работы ЛПУ, уже содержит в себе встроенные подсистемы защиты данных. Чаще всего это бывает:

Подсистема журналирования. Функция предназначена для отражения в журналах системы информации об учетных и системных событиях. Для каждой подсистемы должен быть заведен собственный журнал. Записи должны вестись в хронологическом порядке. Для каждого события должен быть указан пользователь.

Требование к реализации: функция журналирования должна обеспечить сбор и хранение полных и непротиворечивых данных о событиях.

Занесение информации происходит в рамках одной транзакции с регистрацией факта учетного или системного событий. При возникновении программной или аппаратной ошибки действия по изменения данных в рамках транзакции отменяются, и данные в базе данных должны быть приведены в предшествующее состояние. Информация должна быть разделена по типам и отображаться в хронологическом порядке. Доступ к функционалу должен быть доступен только

пользователям с ролью администратор. Изменения информации при просмотре не допускаются.

Недостаток подсистемы: при нарушении параметров информационной безопасности, их практически невозможно расследовать в соответствии со стандартами ИБ, так как не хватает конкретизации некоторых событий при журналировании.

Резервное копирование. Во избежание потери данных и в целях защиты инвестиций в структуру базы данных следует регулярно делать резервные копии. Имея резервную копию, можно будет легко восстановить всю базу данных или ее отдельные объекты.

Если число записей в базе данных постоянно растет, имеет также смысл архивировать старые данные.

Для автоматизации создания резервных копий файлов баз данных рекомендуется использовать ПО, выполняющее автоматическое резервное копирование файловой системы, например, программу резервного копирования файлового сервера.

Резервное копирование позволяет защитить базу данных от системных сбоев и от ошибок.

Однако если для удаления записей или изменения данных был использован запрос на изменение, такие изменения нельзя отменить с помощью команды «отменить». Например, если выполнен запрос на обновление, старые значения, обновленные в результате запроса, не могут быть восстановлены командой «отменить».

Поскольку база данных активная и постоянно изменяется, то ее резервное копирование стоит выполнять по расписанию.

Недостатки: возможно несколько ошибок при использовании резервного копирования, которые приведут к потери данных, например:

- Хранение резервного копирования и базы данных на одном и том же физическом устройстве;

- Отсутствие проверки успешного окончания резервного копирования;

- Подмена резервной копии репликацией.

Рассмотрев системы защиты, применяющиеся в работе МИС можно с уверенностью сказать, что ни одна из них не обеспечит целостность данных на высоком уровне, а к архивной цепочке документа даже и не предъявляются требования по защите целостности, но ведь документ мог быть изменен в любой момент от его создания. Важно увидеть и знать, кто вносил изменения, и действительно ли это подлинный документ, все рассмотренные актуальные технологии не имеют такой функции. Но в настоящие дни стремительно развивается технология блокчейн, известная по криптовалюте, как раз-таки она способна рассказать всю историю документа, транзакции или ценных бумаг.

1.8 Технология блокчейн

В современном мире перспективность развития данной технологии очевидна, зарекомендовав себя в финансовом секторе, она уже нашла применение в политике, экономике, социальной сфере и многих других.

Блокчейн — это распределённая база данных, которая хранится на сотнях и тысячах компьютерах по всему миру. Она объединяет в себе множество блоков, каждый из которых

представляет собой определённый тип информации об операциях, совершённых участниками сети. Передаваемая по сети блокчейна информация хэшируется, то есть для каждого сообщения создается уникальный цифровой “отпечаток пальца” – хэш. Проверив, что сообщение соответствует своему хэшу, можно убедиться, что в ходе передачи оно не было изменено. Также, отпадает необходимость, в централизованном регулирующем органе.

В традиционной реализации, все совершенные транзакции прописываются в публичный реестр, и становятся доступным для уполномоченных участников. Другим, немаловажным свойством подобных систем, является децентрализванность, что влечет за собой отсутствия единой точки отказа. Таким образом, достигается целостность хранимых и обрабатываемых в блокчейн данных.

Принципы работы

Блокчейн, это распределённая база данных, представляющая собой структуру для хранения транзакций, например, для Биткойна или других криптовалют.

Совокупность транзакций, объединенных в блоки, а в дальнейшем и объединение этих блоков – называется блокчейн. Принцип формирования блока прост: это каждый вновь созданный блок, который хранит группу накопившихся и упорядоченных транзакций за все время, а также заголовок блока.

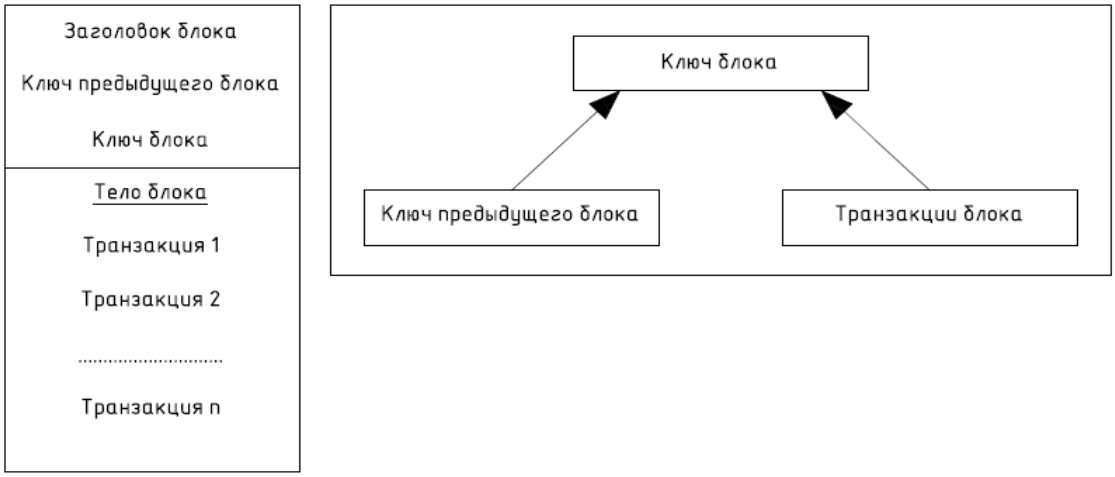


Рисунок 2 - Схема блока

Блок всегда содержит:

а)Адрес - публичный ключ, генерируемый ассиметричным алгоритмом шифрования (например, RSA), на основе придуманного пользователем приватного ключа;

б)Дата и время – тот момент, когда был создан блок (у транзакции тоже есть дата и время создания);

в)Хэш (связующий) – вычисляется с помощью SHA512 от адреса предыдущего блока и суммы хэшей всех транзакций текущего блока. Связующий хэш назван так, потому что при его вычислении требуется адрес предыдущего блока;

г)Информация — сообщение, сумма денег, документы, история болезней, программный код (умные контракты) и т.д. Чтобы информацию внутри транзакций нельзя было подделать, каждая транзакция внутри блока подписывается электронной цифровой подписью (ЭЦП).

Когда блок сформирован, он проверяется всеми участниками сети и, если все согласны, он прицепляется к

цепочке блоков, как только это происходит внести изменения в него невозможно, а база автоматически обновится на всех подключенных к сети компьютерах.

Применение технологии блокчейн в медицинской информационной системе поможет обеспечить сохранности полной истории болезни всех пациентов.

Возможность доступа к данным уполномоченных лиц, в любой точке мира. Снижение страхового мошенничества благодаря контролю врачебных записей и записей о здоровье пациента. Проверка происхождения лекарств, снижение уровня незаконного производства наркотиков.

1.9 Обоснование применения технологии блокчейн

Проведя анализ МИС можно прийти к выводу, что для защиты информации потребуются дополнительные разработки и программное обеспечение, которое будет сохранять данные в целостности, что поведет за собой увеличение работ по разработке МИС, а соответственно увеличение затрат.

Применение технологии блокчейн будет более рациональным, так как он позволит работать с данными в режиме реального времени, и упростит все вспомогательных операций или сведет к минимуму. В сетях блокчейн всегда есть возможность прямого общения между узлами, а высокая степень безопасности самой системы и сложные механизмы идентификации и аутентификации, избавляют участников системы от необходимости производить дополнительные действия для повышения доверия между ними.

1.10 Нормативно-правовые акты

Разработка системы защиты для ИСПДн в медицинской организации осуществляется в соответствии с требованиями законодательства РФ в области защиты Пдн. Для определения требований к системе защиты ИСПдн медицинской организации используются следующие документы:

- Федеральный закон Российской Федерации от 27.07.2006 N 152-ФЗ "О персональных данных";
- Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
- Федеральный закон от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации";
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 27.07.2010 N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" (ред. от 13.07.2015);
- Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
- Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании";
- "Стратегия развития информационного общества в Российской Федерации" (утв. Президентом Российской Федерации 07.02.2008 N Пр-212);
- "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ;

- "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ.

- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

- Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375).

1.11 Проблемы выполнения нормативно-правовых требований при разработке МИС

Закон «О персональных данных» несет позитивные требования по обеспечению безопасности персональных данных граждан, и направлен на выполнение их конституционных прав, однако нормативные документы раскрывающие требования данного закона ведут серьезному увеличению затрат как со стороны разработчиков информационных систем, так и стороны потенциальных пользователей этих систем. А, следовательно, создают дополнительные препятствия при использовании информационных технологий и повышении эффективности труда с их применением. К проблемам исполнения закона, а так же факторам, которые влияют на увеличение стоимости разработки можно отнести:

- ограничение доступа к нормативно-правовым документам;

- необоснованно жесткие требования к уровню защищенности информационных систем;

- длительность и высокая стоимость сертификации информационных систем;

- существенные затраты на аттестацию рабочих мест пользователей со стороны заказчика МИС.

1.11.1 Ограничение доступа к нормативно-правовым документам

С началом работ по выполнению требований законодательства сталкиваешься с ограничением доступа к нормативно-правовым документам. Так часть документов регламентирующих работу с персональными данными имеют гриф «Для служебного пользования». А именно так: ознакомиться с данными документами можно лишь в специализированной организации.

1.11.2 Необоснованно жесткие требования к разработчикам информационных систем

В настоящее время законодательство в области защиты систем персональных данных является очень жестким. Однако многие требования остаются необоснованными и ведут к серьезным финансовым затратам. Вызывают вопрос многие подходы, которые были использованы при разработке требований к обеспечению сохранности персональных данных при обработке в информационных системах. Создается

впечатление, что к требованиям по обеспечению сохранности персональных данных применяются точно такие же подходы как при обеспечении безопасности государственной тайны. Хотя очевидно, что они не могут применяться в связи с:

- Отсутствием системы защиты данных вне информационных систем;

- Широким кругом лиц и областью использования персональных данных, а следовательно более значительными общими экономическими затратами на их защиту;

- Иным объемом и характером ущерба, который может быть нанесен в связи с утечкой или разглашением персональных данных.

Многие требования носят формальный характер и не могут быть реализованы на практике.

Так положением «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» предусмотрено:

а)Использование системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии;

б)Использование программных средства удовлетворяющих устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации;

в)Что средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия;

г) Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств;

д)Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

ж) Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий

Так в соответствии с классификацией наша система соответствует 1 классу защищенности от несанкционированного доступа.

Требования рассмотрены в Руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя

Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992.

За годы разработки, в соответствии с требованиями заказчиков в МИС была реализована ролевая модель управления, которая позволяет проводить разграничение доступа пользователей, как к отдельным функциям системы, так и к отдельным объектам используемых системой.

Администраторы системы имеют возможность гибко изменять права пользователей на доступ к модулям системы, отдельным функциям системы, разграничивать права на просмотр, изменение, удаление определенных типов данных системы, а так же доступ к конкретным наборам данных.

Однако в случае применения нормативных документов этого недостаточно. Поскольку в России существует очень мало сертифицированных ФСТЭК операционных систем, которые имели бы высокую функциональность и расширяемость, возможность синхронизации с другими приложениями, то большинство программ пишутся на иностранном дистрибутиве. Это приводит к тому, что необходимо внедрять дополнительные меры защиты.

Очевидно, что 1 компания не может одинаково успешно заниматься разработкой сертифицированных средств защиты и медицинских информационных, а, следовательно:

- либо разработчик МИС должен продавать конечное решение совместно со сторонними средствами защиты увеличивая стоимость системы;

- либо заказчик должен отдельно приобретать дополнительные сертифицированные средства защиты от НСД, что так же в конечном итоге удорожает стоимость автоматизации ЛПУ.

Отдельно встает вопрос защиты информации от побочных электромагнитных излучений и физическая охрана помещений. Это так же дополнительные затраты.

Представим электромагнитный томограф, рядом с которым стоит генератор шума для подавления излучения монитора и специальный аппаратный комплекс технической разведки, который стоит за окном и пытается его перехватить.

Или пациента, которого нельзя оставить одного в палате, т.к. там установлен ПК, подключенный в информационной системе. Т.к. пациент потенциально может установить закладку в ПК.

Однако при этом, ни учет медицинских карт, их выдача и ознакомление, транспортировка по ЛПУ производится без охраны. Любой сотрудник регистратуры может свободно ознакомиться с содержанием медицинской карты больного. В системе используется 2 типа разграничения доступа к данным уровне:

- Самой МИС;
- СУБД [9].

1.12 Определение уровня защищенности системы

В ЛПУ МИС обрабатывает данные которые подразделяются на:

- ПДн сотрудников;
- ПДн пациентов;

На основании постановления правительства №1119 «Об Утверждении

требований к защите персональных данных при их обработке в информационных системах персональных данных» было установлено, что

угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных". Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается наличием следующего условия:

Для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора [10].

Таким образом, при построении МИС необходимо будет учитывать наивысший уровень защищенности.

1.13 Классификация факторов, воздействующих на безопасность защищаемой информации

1.13.1 Факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения подразделяют на классы:

- объективные;
- субъективные.

1.13.2 По отношению к ОИ факторы, воздействующие на безопасность защищаемой информации, подразделяют на внутренние и внешние.

1.13.3 Факторы, воздействующие на безопасность защищаемой информации, в соответствии с признаками классификации подразделяют на:

- подклассы;
- группы;
- подгруппы;
- виды;
- подвиды.

1.13.4 Перечень основных подклассов (групп, подгрупп и т.д.) факторов, воздействующих на безопасность защищаемой информации (объективных и субъективных), в соответствии с их классификацией, приведенной в 1.14 [11].

1.14 Угрозы ИБ МИС

Модель угроз в медицинской организации представлена в таблице 2.

Таблица 2 Угрозы в МИС

Угроза	Вероятность реализации	Уровень опасности	Актуальность	Принятые защитные меры
Воздействие на физическом уровне				
Кража носителя информации	Низкая	Низкий	Неактуальна	Контроль доступа в рабочую зону
Уничтожение аппаратуры БД	Низкая	Низкий	Неактуальна	Доступ в рабочую зону БД имеет только администратор и обслуживающий техник
Воздействие на сетевом уровне				
Блокирование доступа к серверу	Низкая	Низкий	Неактуально	Создание закрытой сети
Воздействие на уровне операционной системы				
Уничтожение/ нарушение ПО	Средняя	Средний	Актуально	Настройка разграничения доступа к системным параметрам ПО
Заражение вирусом	Средняя	Средний	Актуально	Настройка средств защиты, установка антивируса
Воздействие на уровне управления БД				

Продолжение Таблица 2

Получение административных паролей	Низкая	Низкий	Неактуально	Пароли не хранятся на носителях
Несанкционированные действия администратора БД	Низкая	Низкий	Неактуально	При работе с БД проводится обязательная идентификация/ аутентификация, журналирование работ
Воздействия на уровне технологического процесса				
Ввод фиктивной информации	Высокая	Высокий	Актуально	Журналирование работы и внесения данных операторами
Разглашение конфиденциальной информации	Высокая	Высокий	Актуально	Ответственность за разглашение информации ограниченного доступа
Воздействия на уровне пользователей				
Непреднамеренноеуничтожение, изменение информации ограниченного доступа	Средняя	Средняя	Актуально	Оповещение администратора о действиях пользователя, возможность восстановления
Непреднамеренное отключение технических средств	Низкая	Низкий	Неактуально	Использование ИПБ

2. АНАЛИЗ И РАСЧЕТ РИСКОВ

В соответствии с данными, полученными во время проведения анализа организации, было определено что, необходимо обеспечить защиту информации, содержащую сведения о персональные данных сотрудников и пациентов. Для создания комплексной системы защиты информации ограниченного доступа необходимо изучить нормативно-правовую базу по защите персональных данных, определить требования и меры, установленные законодательством РФ по защите персональных данных.

Также, чтобы осуществить выбор средств защиты информации, необходимо классифицировать защищаемую информацию и определить тип угроз, актуальный для медицинской организации.

2.1 Анализ риска

2.1.1 Идентификация риска

2.1.1.1 Введение в идентификацию риска

Цель идентификации риска - определить, что могло бы произойти при нанесении возможного ущерба, и получить представление о том, как, где и почему мог иметь место этот ущерб. Этапы, описанные ниже, должны объединять входные данные для деятельности, по количественной оценке, риска.

2.1.1.2 Определение активов

Входные данные. Сфера действия и границы проведения оценки риска, перечень, включающий владельцев, местоположение, функцию и т.д.

Действие. Должны быть определены активы, входящие в установленную сферу действия [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 1)].

Руководство по реализации. Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите. При определении активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств.

Определение активов следует проводить с соответствующей степенью детализации, обеспечивающей информацию, достаточную для оценки риска. Степень детализации, используемая при определении активов, влияет на общий объем информации, собранной во время оценки риска. Эта информация может быть более детализирована при последующих итерациях оценки риска.

Для установления учетности и ответственности в отношении каждого актива должен быть определен владелец. Владелец актива может не обладать правами собственности на актив, но он несет ответственность за его получение, разработку, поддержку, использование и безопасность. Чаще всего владелец актива является наиболее подходящим лицом, способным определить реальную ценность актива для организации.

Границей анализа является периметр активов организации, управляемый в рамках процесса менеджмента риска ИБ.

Выходные данные. Перечень активов, подлежащих менеджменту риска, и перечень бизнес-процессов, связанных с активами, а также их значимость.

2.1.1.3 Определение угроз

Входные данные. Информация об угрозах, полученная в результате анализа инцидента от владельцев активов, пользователей, а также из других источников, включая списки внешних угроз.

Действие. Угрозы и их источники должны быть определены [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 2)].

Руководство по реализации. Угроза может причинить ущерб активам организации, таким как информация, процессы и системы. Угрозы могут возникать в результате природных явлений или действий людей, они могут быть случайными или умышленными. Должны быть установлены и случайные, и преднамеренные источники угроз. Угрозы могут проистекать как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться в общем и по виду (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные угрозы, не будет упущена, но объем требуемой работы, несмотря на это, сокращается.

Некоторые угрозы могут влиять более чем на один актив. В таких случаях они могут быть причиной различных влияний в зависимости от того, на какие активы оказывается воздействие.

Входные данные для определения и количественной оценки вероятности возникновения угроз могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в области ИБ, экспертов в области физической безопасности, специалистов юридического отдела и других структур, а также от юридических организаций, метеорологических служб, страховых компаний, национальных правительственных учреждений. При анализе угроз должны учитываться аспекты среды и культуры.

Опыт, извлеченный из инцидентов, и предыдущие оценки угроз должны быть учтены в текущей оценке. При необходимости для заполнения перечня общих угроз может быть целесообразным справиться в других реестрах угроз (возможно, специфичных для конкретной организации или бизнеса). Списки угроз и их статистику можно получить от промышленных предприятий, федерального правительства, юридических организаций, страховых компаний и т.д.

Используя списки угроз или результаты предыдущих оценок угроз, не следует забывать о том, что происходит постоянная смена значимых угроз, особенно, если изменяются бизнес-среда или информационные системы.

Выходные данные. Перечень угроз с определением их вида и источника.

2.1.1.4 Определение существующих мер и средств контроля и управления

Входные данные. Документация по мерам и средствам контроля и управления, планы по реализации обработки риска.

Действие. Должны быть определены существующие и планируемые меры и средства контроля и управления.

Руководство по реализации. Во избежание лишней работы или расходов, например, при дублировании мер и средств контроля и управления, необходимо определить существующие меры и средства контроля и управления. Кроме того, при определении существующих мер и средств контроля и управления следует провести проверку, чтобы убедиться в правильности функционирования мер и средств контроля и управления - обращение к существующим отчетам по аудиту СМИБ должны сокращать время, затрачиваемое на решение этой задачи. Ненадлежащее функционирование мер и средств контроля и управления может стать причиной уязвимости. Следует уделить внимание ситуации, когда выбранные меры и средства контроля и управления (или стратегия) не выполняют своих функций, и для эффективного и своевременного реагирования на идентифицированные риски требуются дополнительные меры и средства контроля и управления. В СМИБ, в соответствии с ИСО/МЭК 27001, это поддерживается измерением эффективности мер и средств контроля и управления. Один из способов количественной оценки действия мер и средств контроля и управления - выявить, как оно снижает вероятность возникновения угрозы, затрудняет использование уязвимости и возможности влияния инцидента. Проверки, проводимые руководством, и отчеты по аудиту также обеспечивают информацию об эффективности существующих мер и средств контроля и управления.

Меры и средства контроля и управления, которые планируется реализовать в соответствии с планами реализации обработки риска, должны быть определены тем же самым способом, который уже был реализован.

Существующие или планируемые меры и средства контроля и управления могут быть отнесены к разряду неэффективных, недостаточных или необоснованных. Если их посчитали необоснованными или недостаточными, меру и средство контроля и управления необходимо подвергнуть проверке, чтобы определить, подлежат ли они удалению, замене более подходящими, или стоит оставить их, например, из соображений стоимости.

Для определения существующих или планируемых мер и средств контроля и управления могут быть полезны следующие мероприятия:

- просмотр документов, содержащих информацию о средствах контроля (например, планы обработки рисков), если процессы менеджмента ИБ документированы должным образом, то информация о всех существующих или планируемых мерах и средствах контроля и управления, а также о состоянии их реализации должна быть доступна;

- проверка, проводимая совместно с сотрудниками, отвечающими за ИБ (например, сотрудником, занимающимся обеспечением ИБ, сотрудником, отвечающим за безопасность информационной системы, комендантом здания или руководителем работ) и пользователями, касающаяся того, какие меры и средства контроля и управления действительно реализованы для рассматриваемого информационного процесса или информационной системы;

- обход здания с целью осмотра физических средств контроля, сравнение существующих средств контроля с перечнем тех, которые должны быть реализованы, и проверка существующих средств контроля на предмет правильной и эффективной работы;

- рассмотрение результатов внутренних аудитов.

Выходные данные. Перечень всех существующих и планируемых мер и средств контроля и управления, их нахождение и состояние использования.

2.1.1.5 Выявление уязвимостей

Входные данные. Перечни известных угроз, перечни активов и существующих мер и средств контроля и управления.

Действие. Необходимо выявить уязвимости, которые могут быть использованы угрозами для нанесения ущерба активам или организации [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 3)].

Руководство по реализации. Уязвимости могут быть выявлены в следующих областях:

- организация работ;
- процессы и процедуры;
- установившийся порядок управления;
- персонал;
- физическая среда;
- конфигурация информационной системы;
- аппаратные средства, программное обеспечение и аппаратура связи;
- зависимость от внешних сторон.

Наличие уязвимости само по себе не наносит ущерба, поскольку необходимо наличие угрозы, которая сможет воспользоваться ею. Для уязвимости, которой не соответствует определенная угроза, может не потребоваться внедрение средства контроля и управления, но она должна осознаваться и подвергаться мониторингу на предмет изменений. Следует отметить, что неверно реализованное, неправильно функционирующее или неправильно используемое средство контроля и управления само может стать уязвимостью. Меры и средства контроля и управления могут быть эффективными или неэффективными в зависимости от среды, в которой они функционируют. С другой стороны, угроза, которой не соответствует определенная уязвимость, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при приобретении или создании актива. Необходимо учитывать уязвимости, возникающие из разных источников, например, те, которые являются внешними или внутренними по отношению к активу.

Выходные данные. Перечень уязвимостей, связанных с активами, угрозами и мерами, и средствами контроля и управления; перечень уязвимостей, не связанных с выявленной угрозой, подлежащей рассмотрению.

2.1.1.6 Определение последствий

Входные данные. Перечень активов, бизнес-процессов, угроз и уязвимостей, где это уместно, связанных с активами, и их значимость.

Действие. Должны быть определены последствия для активов, вызванные потерей конфиденциальности, целостности и доступности [см. ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 4)].

Руководство по реализации. Последствием может быть снижение эффективности, неблагоприятные операционные условия, потеря бизнеса, ущерб, нанесенный репутации, и т.д.

Эта деятельность определяет ущерб или последствия для организации, которые могут быть обусловлены сценарием инцидента. Сценарий инцидента - это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте ИБ (см. ИСО/МЭК 27002, раздел 13). Влияние сценариев инцидентов обусловливается критериями влияния, определяемыми в течение деятельности по установлению контекста. Влияние может затрагивать один или несколько активов, а также часть актива. Поэтому активам может назначаться ценность, обусловленная как их финансовой стоимостью, так и последствиями для бизнеса в случае их порчи или компрометации. Последствия могут быть временными или постоянными, как это бывает в случае разрушения активов.

Организации должны определять операционные последствия сценариев инцидентов на основе (но не ограничиваясь):

- времени на расследование и восстановление;
- потерь (рабочего) времени;
- упущенной возможности;

- охраны труда и безопасности;
- финансовых затрат на приобретение специфических навыков, необходимых для устранения неисправности;
- репутации и иного "неосязаемого капитала".

Выходные данные. Перечень сценариев инцидентов с их последствиями, связанными с активами и бизнес-процессами [12].

2.2 Связь эффективности применения СЗИ с общим риском МИС

Количественная оценка использует шкалу с числовыми значениями (а не описательные шкалы, используемые в качественной оценке) и последствий, и вероятности, применяя данные из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев количественная оценка использует фактические данные за прошлый период, обеспечивая преимущество в том, что она может быть напрямую связана с целями информационной безопасности и проблемами организации. Недостатки количественного подхода могут иметь место тогда, когда фактические проверяемые данные недоступны, поэтому создаётся иллюзия ценности и точности оценки риска.

Из формулы выразим уменьшение ALE:

Возврат инвестиций (ROI) = (Уменьшение ALE – Стоимость защитных мер) / Стоимость защитных мер

При ROI = 0.9

*Уменьшение среднегодовых потерь = Годовые потери (ALE) * (1-Вероятность использования угрозы).*

*Величина риска = Вероятность использования угрозы * Размер ущерба*

1. Проблема. Возможность несанкционированного доступа к медицинской информации.

1.1 Уязвимость. Слабый механизм аутентификации администратора БД.

1.2 Уязвимость. Возможность подмены медицинских записей в карте.

1.3 Уязвимость. Возможность уничтожения информации, находящейся в медицинской карте

1.4 Уязвимость. Нет системы журналирования архива с историей изменения и удаления данных персоналом.

Уязвимость 1.1 может быть устранена с применением смарт-карты для входа в БД. Стоимость считывателя и карт составит 12000 рублей.

Уменьшение ALE=12000*(0,9+1)=22800

Годовые потери (ALE)=22800/(1-0,136) =26388

Уязвимости 1.2 ,1.3 и 1.4 можно устранить тем, что будет разработана МИС на платформе блокчейн. Стоимость по разработке такой системы составит 600 000 рублей.

Уменьшение ALE=600 000*(0,9+1)=1 140 000

Годовые потери (ALE)= 1 140 000 /(1-(0.084+0.168+0.044))=1 619 318

2. Проблема. Прекращение работы программы.

2.1 Уязвимость. Отключение электропитания.

2.2 Уязвимость. Отключение от сети Internet.

Уязвимость 2.1 можно устранить автоматическим вводом резерва (АВР) и обеспечением ЭВМ ИБП. Стоимость АВР

200 000 рублей и обеспечение 120 работающих постоянно ЭВМ ИБП 420 000 рублей. Стоимость одного ИБП составляет 3500 рублей.

Уменьшение ALE=620 000*(0,9+1)=1 178 000

Годовые потери (ALE)= 1 178 000 /(1- 0.312)=1 712 209

Уязвимость 2.2 можно устранить, проведя резервную интернет линию.

Стоимость работ составит 40 000 рублей.

Уменьшение ALE=40 000*(0,9+1)=76 000

Годовые потери (ALE)= 76 000/(1-0.028)=78 189

Вероятность использования угрозы:

1) P=0.136

2) P=0.084

3) P=0.168

4) P=0.044

5) P=0.312

6) P=0.028

Измерение уровня риска:

1) Величина риска = 0,136*26388 = 3588

2) Величина риска = (0.084+0.168+0.044)*1 619 318= 479 318

3) Величина риска = 0,312*1 712 209 = 534 209

4) Величина риска = 0,028*78 189 = 2189

Системы, основанные блокчейн, кардинальным образом отличаются от систем, работающих с реляционными базами данных. Блокчейн использует децентрализованный подход, в то время как с базой данных пользователи имеют ограниченный доступ, и администратор или злоумышленник, может изменять данные в любое время. Оценив риски и рассчитав уязвимости можно с уверенностью сказать, что целью информационной

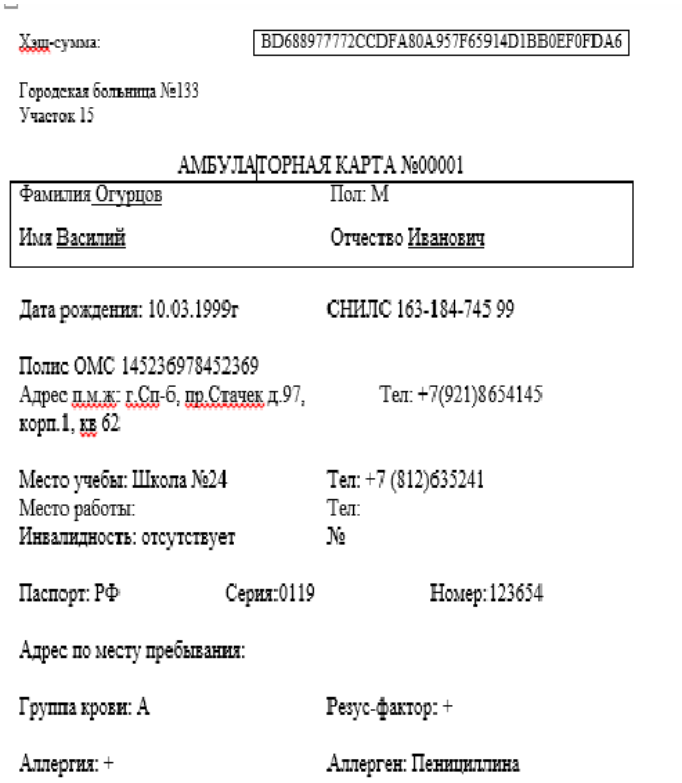
системы на основе блокчейн, является обеспечение безопасного хранения архива данных. Благодаря криптографии все подписи могут быть защищены, в то время как блокчейн может выполнять проверку и ведение журнала реестра. Для хранения документов используется общедоступное хранилище. Сами файлы зашифрованы криптографическими методом, но доступ к файлам предоставляется всем сотрудникам, однако, без ключа шифрования этот файл представляет собой простой набор байтов.

3. ПРОЕКТИРОВАНИЕ РАБОТЫ БЛОКЧЕЙН С МЕДИЦИНСКОЙ ЭЛЕКТРОННОЙ КАРТОЙ

Для того чтобы понять, как работает платформа блокчейн в сфере использования документов и создания архивной цепочки, необходимо вручную воссоздать процесс построения цепочки данных. В качестве примера будет использоваться медицинская карта пациента ЛПУ, при создании МИС с применением технологии блокчейн для российского рынка с учетом законодательства в сфере здравоохранения. Будет рассмотрено предотвращение самой частой угрозы, порча или подмена документации внутренним нарушителем.

3.1 Развертывание цепочки данных

Для развертки данной цепочки вручную создается медицинская карта больного в Microsoft Word.



Хэш-сумма: BD688977772CCDFA80A957F65914D1BB0EF0FDA6

Городская больница №133
Участок 15

АМБУЛАТОРНАЯ КАРТА №00001

Фамилия Огурцов Пол: М

Имя Василий Отчество Иванович

Дата рождения: 10.03.1999г СНИЛС 163-184-745 99

Полис ОМС 145236978452369
Адрес п.м.ж: г.Сп-б, пр.Стачек д.97, Тел: +7(921)8654145
корп.1, кв 62

Место учебы: Школа №24 Тел: +7 (812)635241
Место работы: Тел:
Инвалидность: отсутствует №

Паспорт: РФ Серия:0119 Номер:123654

Адрес по месту пребывания:

Группа крови: А Резус-фактор: +

Аллергия: + Аллерген: Пенициллина

Рисунок 3 - Созданная карта

Если рассматривать работу программы, то карте присвоится автоматически хэш-сумма, хэш-сумма уникальный номер (отпечаток), который и начинает архивную цепочку ведения карты пациента. В данном случае с использование дополнительной программы вручную присваивается уникальный слепок для документа. В дальнейшем каждому последующему файлу будет присваиваться номер предыдущего и, если будет сделана копия или подменен файл, он выбьется из цепочки данных, что тут же поможет обнаружить подлог или внесение изменений в файл. Так же каждый врач после внесения записей и сохранения файла должен его подписать цифровой подписью. Для этого можно используется программа CryptoPro. Поскольку данная программа лицензионная и необходимо ее приобретать, то в работе используется учебная версия КриптоАрм, с возможностью подписи файлов. В

работающей программе на практике после заполнения записей и сохранении документа, это бы происходило автоматически.

3.2 Создание истории болезни

На момент прикрепления и последующего обращения пациента в ЛПУ формируется история болезни, каждая запись в профиле медицинской карты создает слепок в памяти системы, закрепляя за каждым файлом хэш-функцию.

При первом обращении такой номер создается случайным образом.

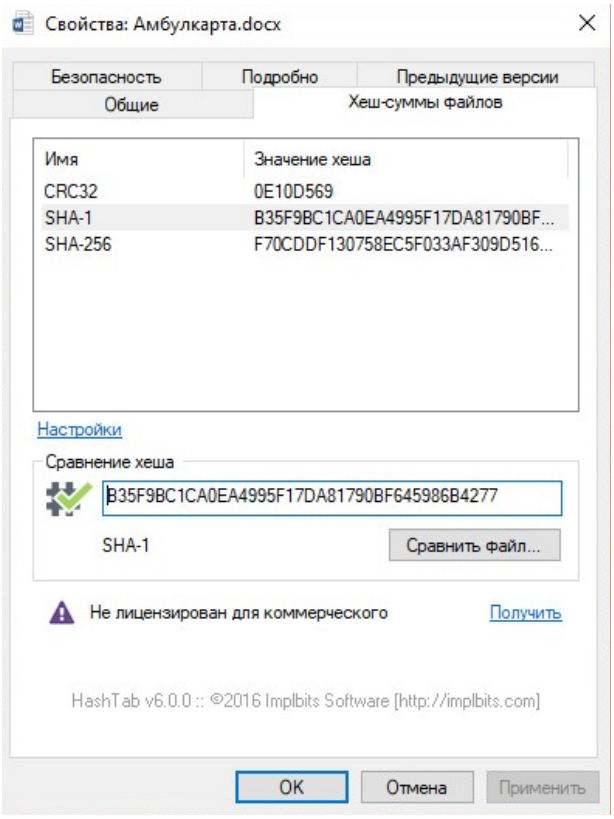


Рисунок 4 - Хэш-сумма первого документа в истории болезни

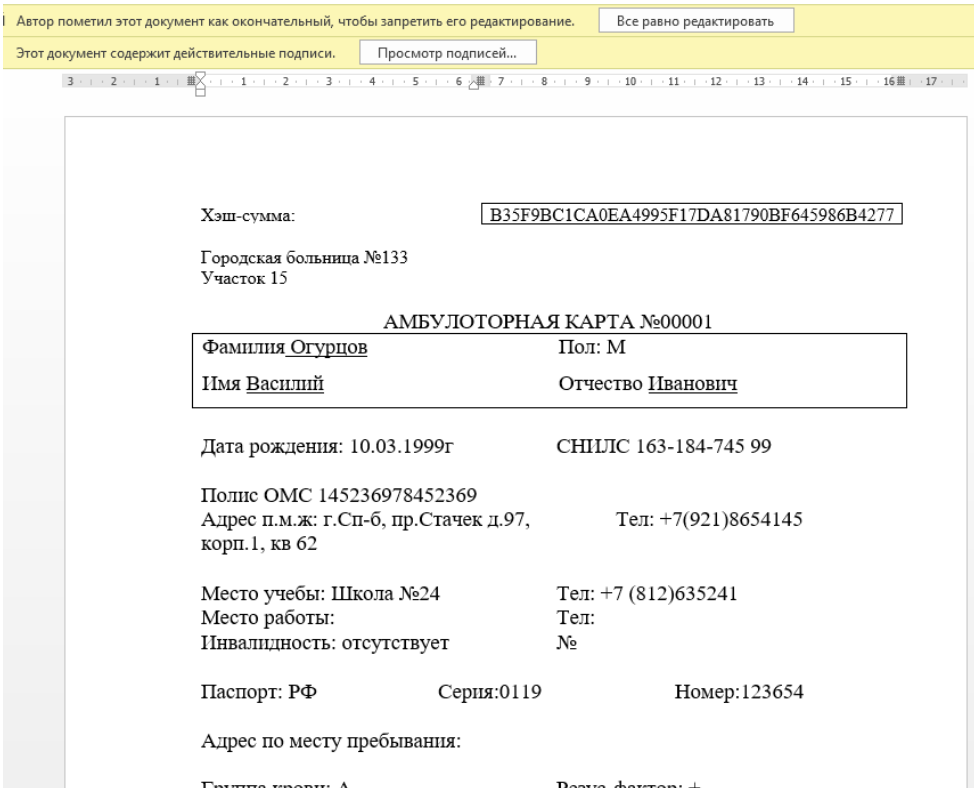


Рисунок 5 - Хэш-сумма 1го документа присвоена продолжению болезни (2ой файл в истории)

Программа проверила и сравнила хэши созданной в начале карты и нового документа которому был поставлен отпечаток, далее при сохранении у второго файла в истории появляется собственная хэш-сумма. Которая будет отпечатком последующей истории.

Так создается цепочка где каждый номер следует друг за другом и ставит отпечаток предыдущего на последующий.

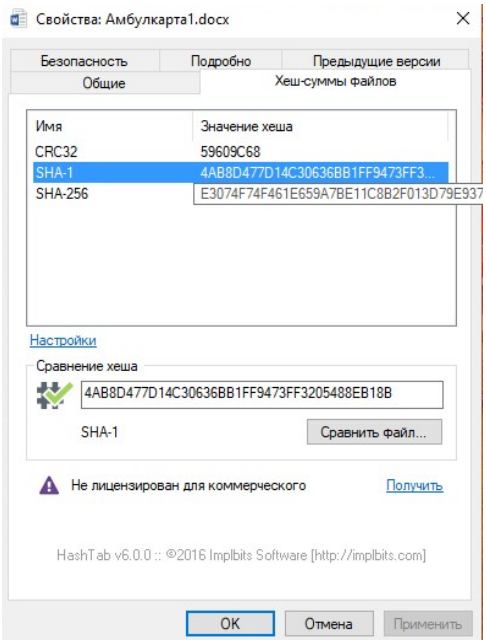


Рисунок 6 - Хэш-сумма второго документа

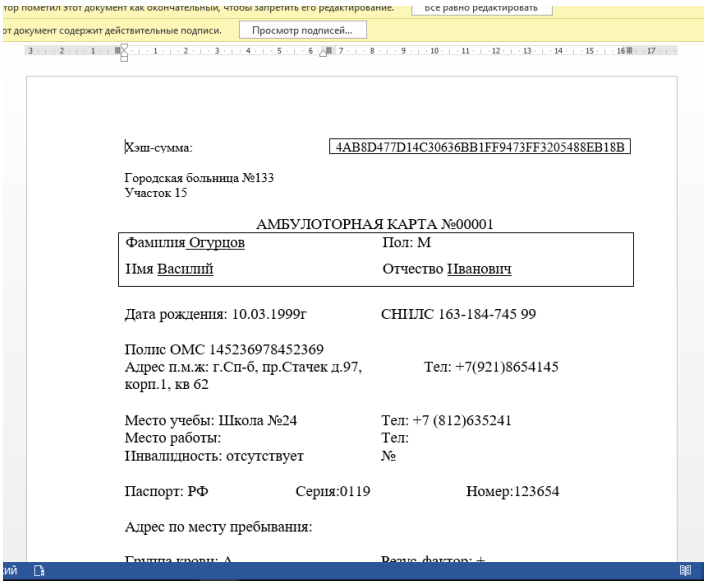


Рисунок 7 - Отпечаток на третьем созданном документе с хэш-суммой второго документа

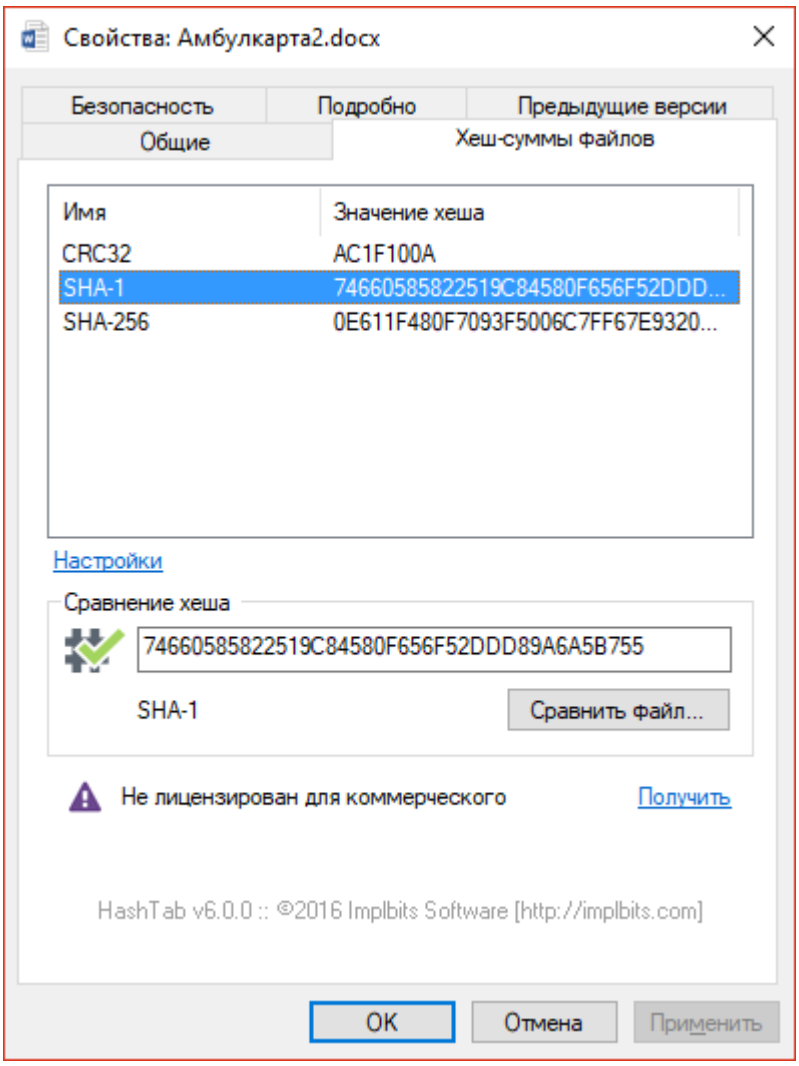


Рисунок 8 - Хэш-сумма 3 документа

Данная цепочка обращений и ведения пациента может быть достаточно длинной. Далее рассматривается реальный случай, когда наступит угроза целостности данных от внутреннего злоумышленника.

Случай: пациента обращается вновь, в медкарте у него указанно, что имеется аллерген и какой именно. Врачу автоматически при назначении лекарств выходит предупреждение, что на данный препарат выявлена аллергия. Врач не обращая внимания на уведомление или из корыстных целей игнорирует.

Впоследствии пациент попадает в реанимацию и, выясняя сложившуюся ситуацию, все приводит к тому, что врач сделал неправильное назначение. Чтобы не остаться виновным врач решает произвести подлог данных в медкарте пациента. Создает точную копию приема с заменой лечащего препарата, удаляя предыдущую запись.

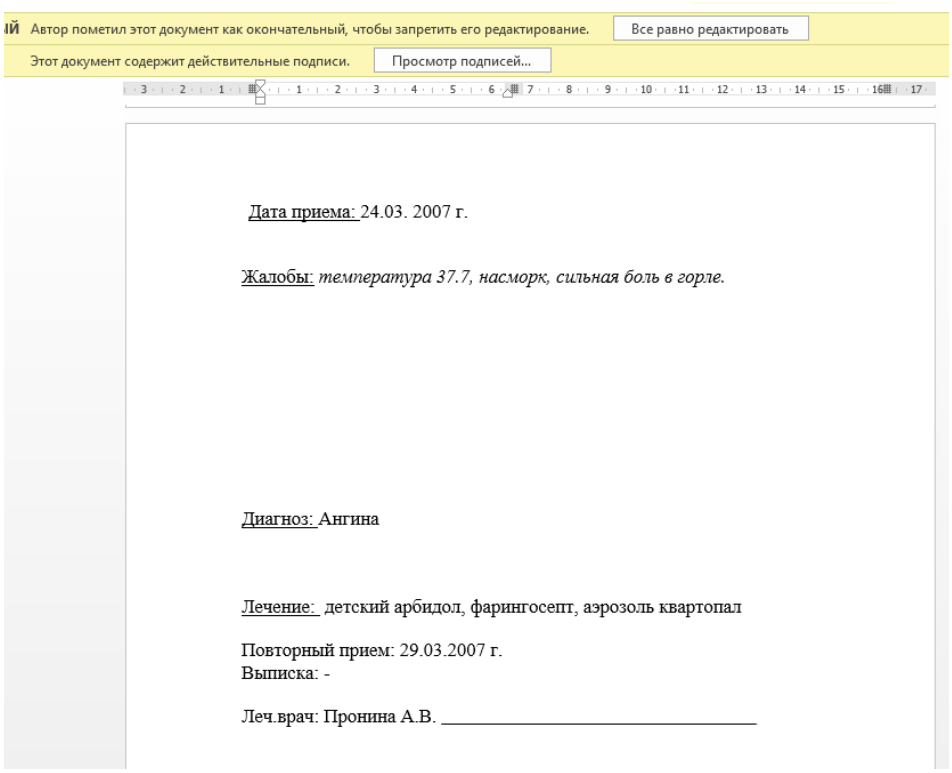


Рисунок 9 - Подлинная история болезни

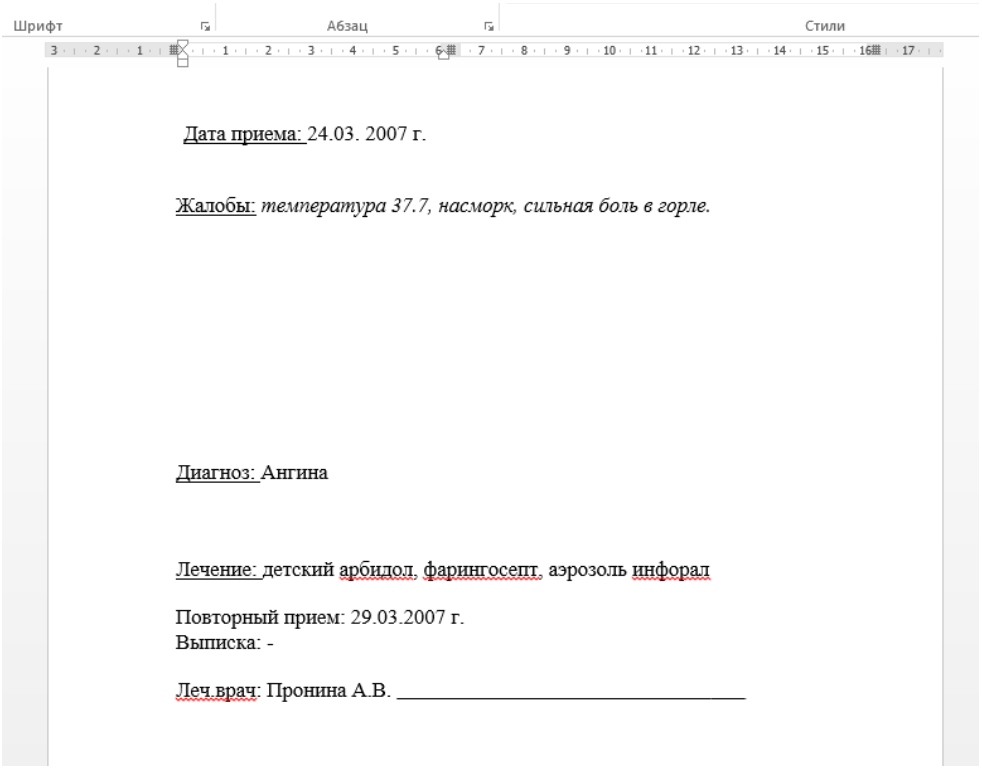


Рисунок 10 - Подделанный документ

Данный документ был подделан врачом, где меняется название препарата на тот, что не вызвал бы аллергию. В документе уже нет нужного отпечатка из архивной цепочки и так же нет автоматической цифровой подписи врача. Проводя проверку данных, выясняется, что произошел подлог информации, платформа блокчейн позволит найти удаленный файл и произвести сверку хэш-суммы, чтобы выяснить какой файл подлинный.

Проводя проверку, обнаруживается последний документ перед изменениями и сравнивая хэш-сумму с отпечатком на последующем файле, обнаруживаются первоначальные данные.

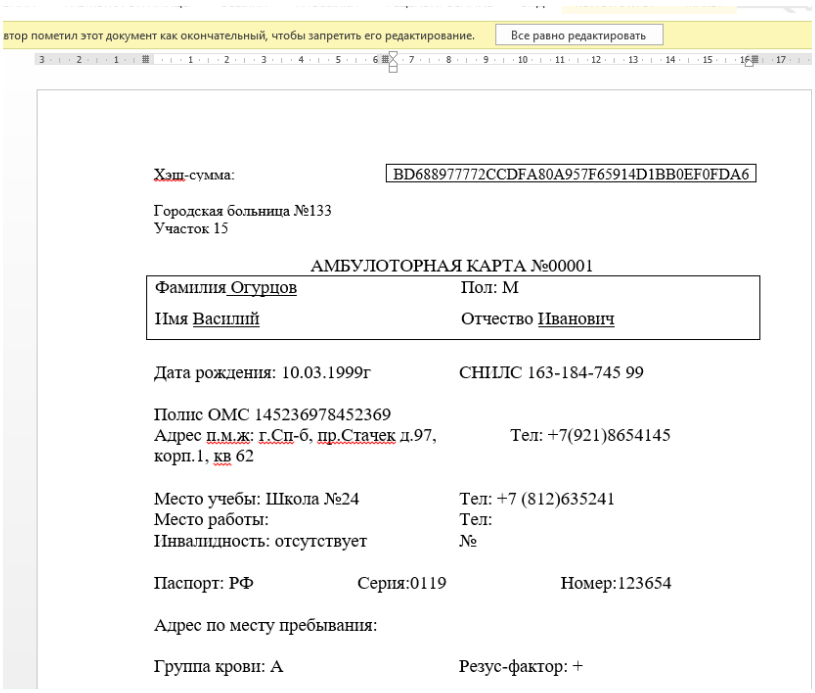


Рисунок 11 - Хэш-сумма на подделанном документе

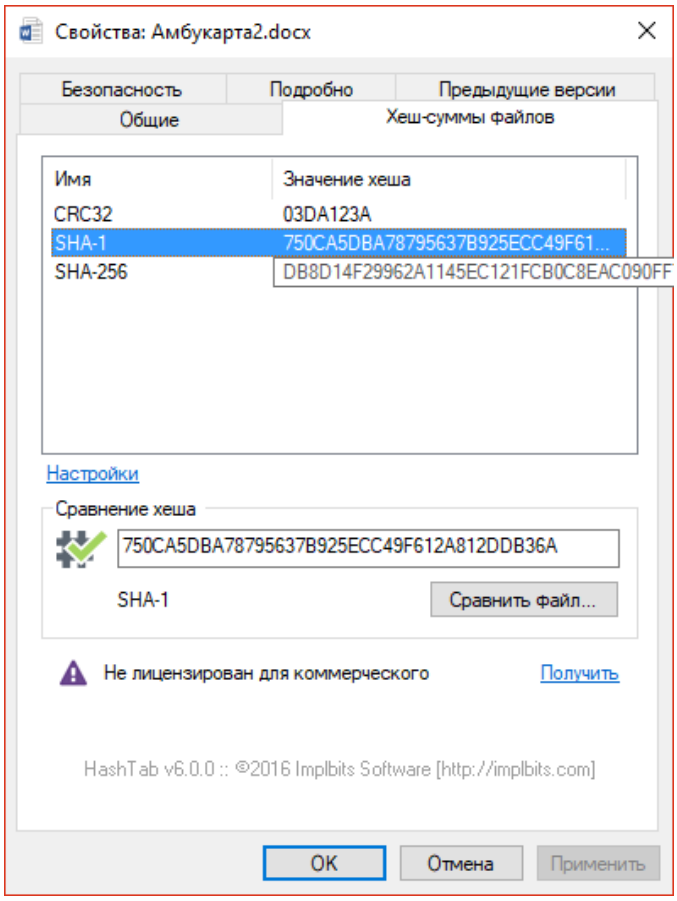


Рисунок 12 - Хэш-сумма подделанного документа

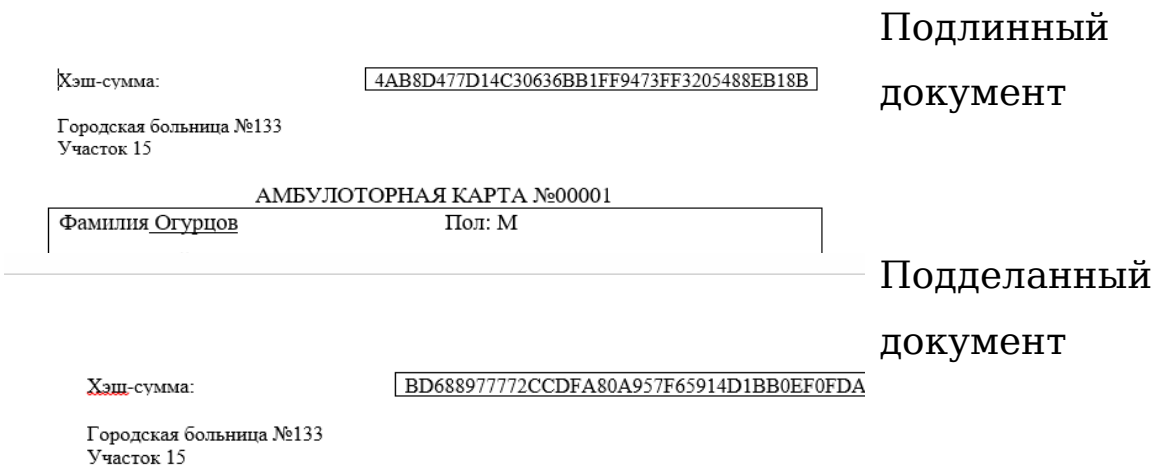


Рисунок 13 - Сравнение хэш-функций файлов

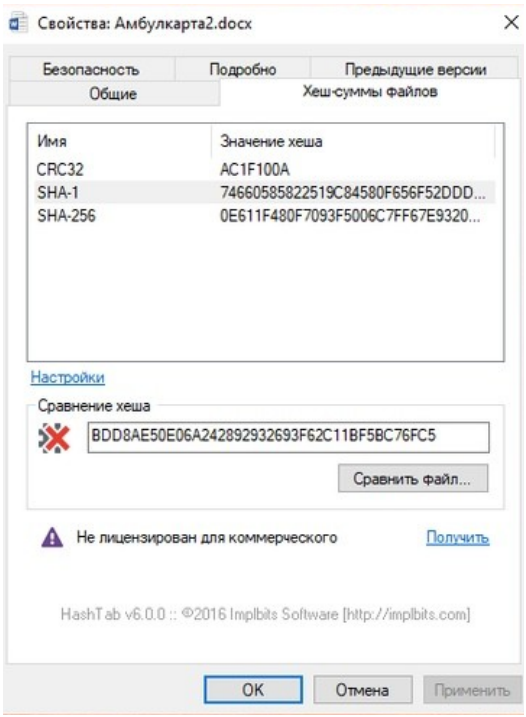


Рисунок 14 - Сравнение хэш-суммы

Таким образом, платформа блокчейн помогла избежать последующих модификаций. После того как данные были опубликованы в ней, используя надежную технику простановки времени и сложной ссылки на предыдущий блок уже

невозможно что-либо откатить назад и внести изменения в запись.

В силу нерушимости и децентрализации блокчейна, если эту технологию использовать для замены системы доменных имен, то так же атаки типа «отказ в обслуживании» (DDoS-атаки) станут невозможны.

Более общее применение — это использование блокчейн в криптографии. Ведь это очень логичный способ использования данной технологии, учитывая, что она позволяет передавать информацию очень безопасным способом. Она также используется для предотвращения манипуляции с данными. Поскольку природа блоков неизменна, используя последовательное хэширование вместе с криптографией в децентрализованной структуре, станет возможно построить систему, которой будет практически невозможно манипулировать. Принципиальное отличие в технологическом подходе позволяет выйти за пределы конечных устройств, включая безопасность цифровой «личности» пользователя, передачу информации и защиту критической инфраструктуры.

3.3 Используемые программные средства при развертывании цепочки данных

Для того, чтобы можно было создавать хэш-суммы файла и проверять, понадобилась программа *Hash-Tab*. Данная программа предлагает на выбор двадцать криптографических алгоритмов, по которым будет производиться расчет хэш-суммы для файла. Можно выбрать как один алгоритм, так и несколько. В работе были использованы такие алгоритмы как:

CRC-32, SHA-1, SHA-256.

1.SHA-256

Алгоритм работает с данными, разбитыми на «куски» по 512 бит (64 байт), криптографически их смешивает и выдаёт 256-битный (32 байта) хэш. SHA-256 состоит из относительно простого раунда, повторяющегося 64 раза.

2.SHA-1

Реализует хеш-функцию, построенную на идее функции сжатия. Входами функции сжатия являются, блок сообщения длиной 512 бит и выход предыдущего блока сообщения.

3.CRC-32

Одним из основных параметров CRC является порождающий полином.

С порождающим полиномом связан другой параметр — его степень, которая определяет количество битов, используемых для вычисления значения CRC. На практике наиболее распространены 8-, 16- и 32-битовые слова, что является следствием особенностей архитектуры современной вычислительной техники.

Так же в работе использовалась программа *КриптоАрм,* предназначенная для шифрования и расшифрования данных, создания и проверки электронной цифровой подписи (ЭЦП) с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами. «КриптоАРМ», наряду со стандартными криптопровайдерами (входящими в поставку Windows), использует реализацию криптоалгоритмов сертифицированных ФСБ РФ.

4. РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ РАБОТАЮЩЕЙ НА ПЛАТФОРМЕ БЛОКЧЕЙН

4.1 Усовершенствование программного обеспечения

В основном программное обеспечение МИС разрабатывается для государственных лечебных учреждений, при разработке приложения на базе блокчейн возникнет ряд проблем с сертификацией ФСТЭК и функциональными возможностями.

Лучше всего для разработки данных систем программистам написать код самим, не прибегая к заимствованию частей. Так же при внедрении МИС на базе блокчейн будет необходимо отказаться от старых настроек и программного обеспечения, и отладить синхронизацию с другими внешними источниками.

Запустив такой проект, необходимо продумать на какой операционной системе он будет работать для того, чтобы пройти сертификацию. Прописаны ли все функции в код программы на этапе разработке, иначе в работающее приложение будет очень сложно внедрять дальнейшие наработки.

4.2 Усовершенствование аппаратного обеспечения

Технология обмена данными в системах блокчейн требует очень много объема, поэтому перед внедрением следует рассчитать, сможет ли учреждение по правилам содержать серверное оборудование.

Так же для бесперебойной работы блокчейн потребуется несколько серверов с определенными ASIC-микросхемами. Для увеличения производительности и быстроты обмена данными внутри системы.

Технология блокчейн является весьма энергозатратной из-за больших вычислительных мощностей, поэтому при подключении к городским энергосетям на случай различных не предвиденных отключений, потребуется достаточно мощный источник резервного питания.

4.3 Усовершенствование подготовки кадрового состава

Система, использующая блокчейн, является децентрализованной, но даже в такой системе необходим специалист по самоуправлению. Поскольку это медицинская информационная система, то необходим целый комитет по самоуправлению, который разработает правила обмена данными и качества предоставляемых услуг и будет следить за их исполнением.

В таком комитете обязательно должны состоять кадры с медицинским образованием, отвечающие за настройку работы в медицинской части программы. Специалист, отвечающий за логистику, необходим для настройки обмена данными между узлами программы. Технические специалисты, поддерживающие работу аппаратно-программного комплекса.

Обучить весь медицинский и операторский состав, работе с совершенно новым видом программного приложения. Составить должностную инструкцию исходя из занимаемой должности и обработки данных на АРМ.

Проводить обучающие мероприятия для персонала во избежание большого количества ошибок и некорректной работы. Отправлять персонал на специализированные курсы, которые чаще всего устраивают разработчики МИС.

Проведя анализ необходимых мероприятий перед внедрением новой технологии, можно сказать, что учреждению придется сменить привычный ход работы и освоить систему с чистого листа. Обучить персонал, внести изменения в должностных инструкциях, провести замену оборудования.

Что в свою очередь даст высокую безопасность от разных видов нарушителей и практически полную автоматизацию процесса в учреждении.

ЗАКЛЮЧЕНИЕ

Цель дипломной работы была разработка защищенной системы обработки и хранения данных, на примере работы медицинской информационной системы. В ходе работы было проведено:

1. Анализ и описание современных систем электронного документооборота.
2. Исследование и описание работы МИС.
3. Анализ работы технологии блокчейн.
4. Проведение анализа угроз и расчет рисков.
5. Проектирование системы работающей на платформе блокчейн.

Была разработана защищенная система хранения данных на примере медицинской информационной системы. Благодаря проведенным исследованиям стала понятна целесообразность применения технологии блокчейн в электронных системах документооборота.

Исходя из полученных результатов, можно сказать, что цель

дипломной работы была достигнута.

Также в процессе выполнения дипломной работы были получены

теоретические знания, при анализе нормативно-правовых актов Российской Федерации и практический опыт, при разработке системы защиты.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. ГОСТ Р 7.0.8.-2013 [Электронный ресурс] : Делопроизводство и архивное дело - Термины и определения. Режим доступа: https://ecm-journal.ru/card.aspx?ContentID=5146136 . Дата обращения: 06.01.2019.

2. Системы электронного документооборота и эффективность бизнес-процессов [Электронный ресурс] : Электронное издание – Комсомольская правда – Режим доступа: https://www.kp.ru/guide/sistemy-dokumentooborota.html Дата обращения: 06.01.2019.

3. Я. И. Гулиев, А. А. Цветков Обеспечение информационной безопасности в медицинских организациях [Электронный ресурс] : Электронный журнал — Москва, изд. Менеджер здравоохранения, 2016. – Режим доступа: http://www.interin.ru/datas/documents/viit_2016_6_5.pdf Дата обращения: 08.01.2019.

4. Модель угроз типовой медицинской информационной системы (МИС) типового лечебно профилактического учреждения (ЛПУ) организациях [Электронный ресурс] : Минздравсоцразвития России, 2009. – Режим доступа: https://static2.rosminzdrav.ru/system/attachments/attaches/000/017/251/original/Modely_ugroz_MIS_LPU_2009_all.pdf?1389769143 Дата обращения: 10.01.2019.

5. Я. И. Гулиев, И. А. Фохт, О. А. Фохт, А. Ю. Белякин ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ [Электронный ресурс]: Электронный журн. Медицинские информационные системы и информационная безопасность. Проблемы и решения — Переславль-Залесский, 2009. – Режим доступа: http://skif.pereslavl.ru/psi-info/psi/psi-publications/e-book-

2009/volume2/175-Guliev.Healthcare_Information.pdf Дата обращения: 10.01.2019.

6. Обзор DLP-систем [Электронный ресурс] : Режим доступа: https://searchinform.ru/blog/2016/02/08/obzor-dlp-sistem/ Дата обращения: 11.01.2019.

7. Information Security Technologies [Электронный ресурс] : Системы обнаружения и предотвращения вторжений (IDS/IPS) – Режим доступа: http://zaschita-it.ru/systemy-obnaruzheniya-vtorzheniy Дата обращения: 11.01.2019.

8. Юрий Мельников, Алексей Теренин, Вадим Погуляев, Статья. Недостатки ЭЦП как средства защиты электронных документов. [Электронный ресурс] : Электронный журнал – ИЗДАТЕЛЬСТВО СК ПРЕСС,2017. – Режим доступа:https://www.itweek.ru/security/article/detail.php?ID=105054 Дата обращения: 06.01.2019.

9. Автор неизв. Закон «О персональных данных» с точки зрения разработчика медицинских информационных систем. [Электронный ресурс] : Электрон. текстовые дан. –2010. – Режим доступа: http://www.armit.ru/pd/pd.pdf Дата обращения: 06.01.2019.

10. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]: КонсультантПлюс,1997—2018. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ Дата обращения: 10.01.2019.

11. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности.

Менеджмент риска информационной безопасности. 7.2 Основные критерии [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации — Санкт-Петербург,2019. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 Дата обращения: 06.01.2019.

12. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. 8 Оценка риска информационной безопасности [Электронный ресурс]: Электронный фонд правовой и нормативно-технической документации — Санкт-Петербург,2019. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 Дата обращения: 06.01.2019.

Приложение 1.

Обрабатываемые ПДн сотрудников:

1. Фамилия, имя, отчество;
2. Дата рождения;
3. Адрес регистрации;
4. Адрес фактического проживания;
5. Серия, номер паспорта, кем выдан;
6. ИНН;
7. СНИЛС;
8. Должность, период работы и данные о трудовом договоре;
9. Сведение о доходах и заработной плате;
10. Лицевые счета;
11. Справка 2-НДФЛ с предыдущего места работы;
12. Сведения о квалификации и переподготовке;
13. Номер телефона домашнего и мобильного;
14. Семейное положение.

Обрабатываемые ПДн пациентов:

1. Фамилия, имя, отчество;
2. Дата рождения;
3. Серия, номер паспорта, кем выдан;
4. СНИЛС;
5. Адрес регистрации;
6. Полис ОМС;
7. Сведения об инвалидности;
8. Информация об инфекционных заболеваниях;
9. Данные оплаты услуг;
10. История болезней и исход лечения;
11. Больничные листы;

12. Результаты лабораторных исследований;