МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ПОДГОТОВКИ ПЕДАГОГОВ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ И
ПРЕДМЕТНЫХ МЕТОДИК

Анализ защищенности информационных систем персональных данных в образовательной организации

Выпускная квалификационная работа по направлению

44.04.04 Профессиональное обучение (по отраслям)

Направленность программы магистратуры

«Управление информационной безопасностью в профессиональном образовании»

Форма обучения очная

Проверка на объем заимствований:
59 % авторского текста

Работа рекомендована к защите
«13» 05 2023 г.
Зав. кафедрой АТИТиМОТД
_____ Руднев В.В.

Выполнил:
студент группы ОФ-209-210-2-1
Янтимиров Олег Альфредович

Научный руководитель:
доктор педагогических наук,
профессор
Уварина Наталья Викторовна

Челябинск
2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Современное высшее образование трудно представить без использования информационных средств, коммуникативных технологий и дистанционных образовательных технологий. В тоже время виртуальная и информационная вузовская среда представляет собой потенциальную угрозу для ее субъектов, в частности для раскрытия их персональных данных и манипуляции ими третьими лицами [1]. Поэтому проблема организации системы защиты персональных данных в образовательных организациях высшего образования столь актуальна на данный момент.

Защита персональных данных является актуальной темой во многих областях, включая образование. Образовательные организации хранят большое количество информации о своих учащихся и сотрудниках, включая персональные данные, такие как имена, адреса, номера телефонов, электронные адреса и т.д. Кроме того, заполнение бумажных форм, отчетов и других документов также может содержать чувствительные данные, такие как данные о здоровье, финансовые данные и другие личные сведения.

Нарушение безопасности персональных данных может привести к серьезным последствиям, таким как кража личной информации, злоупотребление личными данными и финансовыми ресурсами, фальшивые операции и другие виды мошенничества, которые могут нанести значительный ущерб репутации и доверию к образовательной организации.

С учетом значимости защиты персональных данных, необходимо проводить регулярный анализ защищенности информационных систем персональных данных (ИСПД) в образовательной организации и принимать все меры для минимизации рисков. Такой анализ поможет выявить потенциальные угрозы безопасности данных, определить уязвимости и слабости в системах защиты, а также разработать и реализовать

соответствующие меры защиты, чтобы свести к минимуму возможность нарушения безопасности данных.

В итоге, проведение анализа защищенности ИСПД в образовательной организации становится не только необходимым, но и важным шагом для обеспечения защиты персональных данных и поддержания высокого уровня доверия со стороны студентов, их родителей и персонала образовательной организации.

Ключевыми факторами, обуславливающими проблему информационной безопасности персональных данных обрабатываемых в вузе, выступают:

− постоянно возрастающий объем обрабатываемых в вузе персональных данных, добавлением пользователей, пользующихся удаленным доступом;

− возрастающими темпами цифровизации образовательных ресурсов, усложняющейся структурой информационных систем в вузе;

− обновление состава внешних и внутренних угроз для безопасности персональных данных, повышение востребованности сетевого доступа к цифровым ресурсам университета.

К основным угрозам безопасности персональных данных возможно отнести следующие:

− получение доступа третьими лицами к информационным сервисам вуза;

− перехват третьими лицами аутентифицирующей информации;

− получение доступа во внутренние информационные подсистемы;

− кражи заинтересованными лицами личных персональных данных сотрудников вуза и студентов.

На современном этапе развития общества и цифровых технологий, становится очевидным тот факт, что вузам все сложнее обеспечивать соответствие законодательству по обеспечению персональных данных всех

субъектов образовательного процесса. Рекомендации Рособразования, имеющиеся ИТ-продукты направленные на разрешение изучаемой проблемы, обеспечивают вузам возможность ее решить, при этом не тратить лишние средства и не прибегать к сложным решениям [43; 29].

Особенность защиты персональных данных в вузе обусловлена различными аспектами деятельности в нем. Сюда можно отнести технические, кадровые, организационные и финансовые аспекты. Также эффективная защита персональных данных всех субъектов образовательного процесса вуза требует комплексного и ответственного подхода со стороны IT-отдела: необходима актуализация моделей угроз для безопасности персональных данных различных классов (на основе максимальной типизации документов и требований); необходимо повышение уровня знаний сотрудников вуза в вопросах обработки персональных данных, а также повышения культуры информационной безопасности обучающихся и их родителей [29].

Таким образом, можно сделать вывод, что тема исследования «Разработка рекомендаций по организации системы защиты персональных данных в образовательной организации высшего образования» является актуальной, а полученные результаты имеют важное практическое значение.

Это определяет актуальность создания системы защиты информации на объекте, ориентированной на угрозы безопасности, представленные в документах ФСТЭК и ФСБ России.

Целью исследования является разработка рекомендаций по организации системы защиты персональных данных в образовательной организации с учетом комплексной оценки уровня защищенности и требований нормативно-правовой базы Российской Федерации.

Объектом исследования является организация системы защиты персональных данных в образовательной организации.

Предметом исследования является защита персональных данных

Для достижения поставленной цели были сформулированы следующие задачи:

1. Рассмотреть понятие и значение защищенности информационных систем персональных данных в образовательной организации.
2. Изучить нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.
3. Определить этапы организации защищенности информационных систем персональных данных в образовательной организации.
4. Провести оценку информационной безопасности персональных данных в ФГБОУ ВО «Южно-уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.
5. Разработать рекомендации по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.
6. Оценить эффективность рекомендаций по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.

Гипотеза исследования состоит в предположении о том, что повышение эффективности системы защиты персональных данных возможно на основе оценки уязвимостей существующих средств защиты и обеспечения их оптимального обновления с учетом максимального соответствия организационно-распорядительной документации и техническим требованиям.

Для решения поставленных задач были использованы следующие методы исследования: изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод как анализ документации образовательной организации; анализ и сопоставление

имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты персональных данных; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авдеев М.Ю., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Кузнецова Т.В., Лушников А., Медведева Т.М., Савельев А.И., Серков П.П., Ситникова Е.Г., Сенаторова Н.В., Терещенко Л.К.

Практическая значимость работы заключается в разработке рекомендаций по организации системы защиты персональных данных в образовательной организации, разработанной на основе анализа частной модели угроз ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации, которая может быть применено в других образовательных организациях.

База исследования: ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

ГЛАВА 1. ПОНЯТИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ЗАЩИТА В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Понятие и значение защищенности информационных систем персональных данных в образовательной организации

Персональные данные – любая информация, которая может быть использована для идентификации определенного человека или контактирования с ним, такая информация может включать имя, адрес электронной почты, фото, адрес проживания, номер телефона, номер социального страхования, информацию о здоровье и финансовые данные. Обработка персональных данных должна проводиться в соответствии с законодательством о защите данных и правилами конфиденциальности для обеспечения безопасности и неприкосновенности частной жизни.

Персональные данные – это любая информация, относящаяся к определенному физическому лицу, которая может быть использована для его идентификации. К таким данным могут относиться: ФИО, адрес проживания, номера телефона, электронная почта, паспортные данные, фотографии, медицинская информация и т.д.

Федеральный закон «О персональных данных» регулирует сбор, хранение, использование и распространение персональных данных. Закон определяет требования к организациям, обрабатывающим такие данные, и устанавливает права граждан на защиту их персональных данных.

Согласно закону, сбор персональных данных возможен только с согласия владельца данных, кроме случаев, когда сбор данных является обязательным по закону. Организации, отвечающие за персональные данные, обязаны предоставить их безопасность и конфиденциальность. О любой утечке персональных данных нужно сразу же сообщить владельцу данных.

Граждане имеют право на пользование и полноценный доступ к своим персональным данным. Они также могут запретить использование своих

данных в рекламных целях и требовать компенсации за ущерб, причиненный использованием их данных без согласия.

В целом, ФЗ «О персональных данных» обеспечивает защиту прав граждан на конфиденциальность и безопасность их персональных данных и устанавливает жесткие требования к организациям, обрабатывающим такие данные. [2].

Защита персональных данных - это меры, направленные на обеспечение сохранности, конфиденциальности и доступности информации о пользователе, а также на предотвращение неправомерного доступа к ней и ее использования без согласия ее владельца.

К таким мерам относятся:

– сбор и хранение только необходимых данных;

– защита информации от несанкционированного доступа;

– шифрование передачи данных;

– контроль доступа к информации;

– регулярное обновление антивирусных программ и программных обновлений;

– обучение сотрудников безопасным методам работы с информацией.

Каждая компания, которая собирает, хранит и обрабатывает персональные данные клиентов, обязана соблюдать основные правила и требования по защите своих данных.

Основные принципы защиты персональных данных:

– прозрачность. Клиенты должны быть проинформированы о том, какие данные собираются, для каких целей их собирают, кто будет управлять ими и как они будут храниться и использоваться;

– согласие. Без согласия клиентов организация не может собирать какие-либо персональные данные;

– обработка данных. Обработка персональных данных для достижения каких-либо целей, для которых они были собраны, могут быть использованы только в тех объемах, которые необходимы для достижения этих целей;

– безопасность. Организация должна принимать меры для защиты персональных данных от несанкционированного доступа, утери или кражи;

– право на доступ. Граждане имеют право на пользование и полноценный доступ к своим персональным данным. Имеется множество технических средств для защиты персональных данных. Некоторые из них приведены ниже:

– антивирусное программное обеспечение – защищает от вирусов и малвари;

– средства шифрования – защищают данные путем кодирования их при передаче;

– фаерволы – обеспечивают контроль доступа к сетевым ресурсам, блокируют нежелательные подключения к сети;

– системы обнаружения и предотвращения вторжений (IDS / IPS) – определяют и пресекают попытки несанкционированного доступа к данным;

– устройства для хранения данных с защитой паролем – защищают информацию от несанкционированного использования;

– блокировщики слежки – защищают приватность, предотвращают слежку за пользователем;

– устройства биометрической аутентификации – использование уникальных физических характеристик пользователя для аутентификации;

– средства приватности в браузере – защищают пользовательские данные при использовании веб-браузера. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Безопасность персональных данных заключается в сохранении конфиденциальности информации, касающейся личности человека. Это

включает в себя сбор, хранение, использование и передачу персональных данных только с согласия субъекта, а также защиту информации от несанкционированного доступа. Для обеспечения безопасности персональных данных используются различные технологии, политики и процедуры в соответствии с законодательством страны [4].

Персональные данные могут стать целью хакеров, мошенников и других злоумышленников, которые могут использовать их в различных незаконных целях. Например:

– кража идентификационных данных для мошенничества и кражи денег;

– доступ к медицинской и финансовой информации для мошеннической деятельности;

– кража личных данных для шантажа и угроз;

– использование информации о личных интересах, предпочтениях и поведении для персонализированных атак;

– незаконное использование персональных данных для спама, рекламы и маркетинговых активностей;

– сбор и продажа персональных данных третьим лицам без согласия владельца.

Утечка персональных данных может привести к серьезным негативным последствиям, включая финансовые потери, угрозы безопасности и нарушение частной жизни. Поэтому необходимо обеспечивать максимальную защиту персональных данных и принимать меры по их безопасному хранению и использованию.

Ошибки в программном обеспечении могут привести к утечке персональных данных. Некоторые из основных причин, по которым это может произойти, включают в себя:

– неправильная настройка системы безопасности, которая может позволить злоумышленникам получить доступ к персональным данным;

– уязвимости в программном обеспечении, которые могут быть использованы для взлома системы;

– неправильная обработка или хранение персональных данных, такая как хранение их в незашифрованном виде или на не защищенных серверах.

В любом из этих случаев ошибки в программном обеспечении могут привести к утечке критически важных данных, таких как имена, пароли, адреса электронной почты, номера кредитных карт и другие персональные данные. Эти ошибки могут оказать негативное воздействие на репутацию компании, а также создать серьезные проблемы для пользователей, которые могут стать жертвами мошенничества.

1.2 Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации

Государство, с помощью законодательных и нормативных правовых актов, несет защиту персональных данных. которые определяют порядок сбора, использования, хранения, передачи и защиты персональных данных.

Основным законодательным актом в этой области является Федеральный закон «О персональных данных» от 27 июля 2006 года №152-ФЗ, который определяет правила обработки персональных данных как физических, так и юридических лиц [1].

В соответствии с этим законом, субъекты персональных данных имеют право на защиту своих персональных данных от незаконной обработки, а операторы имеют обязанность обеспечить безопасность персональных данных, соблюдая установленные правила и требования.

Федеральное агентство по защите персональных данных обеспечивает государственный контроль и выполняет требование по защите информации и персональных данных.

В целом, данные регулирование защиты персональных данных в России является довольно важным, сложным и требовательным направлением в правах граждан страны.

Итак, основными нормативно-правовыми актами, стандартами защиты персональных данных являются:

1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Конвенция Совета Европы от 28 января 1981 года № 108 «О защите персональных данных».

3. ГОСТ Р ИСО/МЭК 27001-2013 «Информационная технология. Методы обеспечения информационной безопасности. Системы управления информационной безопасностью. Требования».

4. ГОСТ Р ИСО/МЭК 27799-2012 «Информационная технология. Методы обеспечения информационной безопасности. Руководство по риск-анализу в области информационной безопасности».

5. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении Правил обработки персональных данных».

6. Рекомендации различных организаций, таких как Институт информационной безопасности ISO, The International Association of Privacy Professionals (IAPP) и др.

Приказом Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных.

Данное положение устанавливает методы и способы защиты информации в информационных системах, содержащих персональные данные. Оно охватывает процедуры обеспечения конфиденциальности, доступности, целостности и достоверности персональных данных, а также меры по предотвращению несанкционированного доступа к данным.

К основным мерам защиты информации относятся следующие стандарты и методы:

– системы управления доступом: для ограничения доступа к персональным данным должны использоваться системы управления доступом, которые позволяют контролировать доступ к данным, определять права пользователя и аудиторскую отчетность;

– криптографические методы: для защиты персональных данных, которые передаются по сети, необходимо использовать криптографические методы, такие как шифрование и дешифрование данных, хэширование и цифровые подписи;

– физический контроль: для защиты персональных данных должен применяться физический контроль, который включает системы контроля доступа к помещениям, меры по уничтожению бумажных копий персональных данных и т.д.;

– программные средства: для защиты персональных данных должны применяться программные средства защиты, такие как антивирусные программы, программы мониторинга, системы обнаружения вторжений и т.д.;

– обучение: для гарантии безопасности персональных данных в информационных системах персонала организации необходимо обучать основам информационной безопасности и требованиям к защите персональных данных.

Данные меры защиты информации должны соответствовать современным требованиям к безопасности персональных данных и регулярно обновляться в соответствии с новыми угрозами и опасностями, которые могут возникнуть.

Необходимо выделить требования, которые данные акты предъявляют к организациям. Условно их можно разделить на административные и технические. К административным относятся требования организационного

характера, создание внутренних нормативных и правовых актов. К техническим требованиям относят внедрение программных и аппаратных средств защиты, а также средства контроля и ограничения доступа. В приложение А представим требования законодательства Российской Федерации в области персональных данных, предъявляемые организациям.

К основным требованиям по безопасности персональных данных можно отнести:

– конфиденциальность: необходимо обеспечить конфиденциальность информации, чтобы предотвратить несанкционированный доступ к данным;

– целостность: информация должна быть защищена от изменений и вмешательства несанкционированных лиц;

– доступность: необходимо обеспечить доступность информации только тем, кто имеет право ее просматривать;

– авторизация: доступ к информации должен быть предоставлен только с авторизацией;

– аутентификация: система должна проверять подлинность пользователей и предоставлять доступ только тем, кто имеет право на этом;

– шифрование: информация должна быть зашифрована, чтобы предотвратить ее взлом и использование несанкционированными лицами;

– безопасность сети: сеть должна быть защищена от атак внешних лиц, в том числе и вредоносного ПО;

– управление доступом: Пользователям должен быть предоставлен доступ только к необходимой информации в соответствии с их полномочиями;

– аудит: необходимо следить за действиями пользователей и системными событиями для обеспечения безопасности системы;

– физическая безопасность: Данные должны быть защищены от утери или кражи, например, размещая их в безопасном месте и/или используя сейфы или шифрование на дисках.

Составив таблицу с требованиями, можно легко отследить какие из них выполняются в организации, а какие еще необходимо выполнить. Большинство требований, указанных в данной таблице остаются очень общими. Что приводит к вольной трактовке и страдает качество их выполнения внутри организации.

1.3 Этапы организации защищенности информационных систем персональных данных в образовательной организации

Информационная система персональных данных (ИСПДн) – это специальный комплекс средств и технологий, предназначенный для сбора, обработки, хранения и использования персональных данных субъектов, которые находятся в отношениях с организацией.

В образовательной организации ИСПДн используется для хранения информации о студентах, преподавателях и других работниках учебного заведения. Эта система позволяет обрабатывать информацию, как о студентах, так и о персонале учебного заведения.

Использование ИСПДн позволяет администрации учебного заведения обеспечить безопасность и конфиденциальность персональных данных, а также повысить эффективность управления процессом обучения и управления своей организацией в целом.

Система включает в себя базу данных персональных данных, защиту от несанкционированного доступа и средства обеспечения конфиденциальности. Она также обеспечивает возможность доступа к информации только авторизованным пользователям, и позволяет автоматически обновлять информацию, связанную с учебным процессом.

ИСПДн является неотъемлемой частью работы современной образовательной организации, которая не только обеспечивает безопасность

и конфиденциальность персональных данных, но и облегчает управление учебным процессом и повышает его эффективность.

Угрозы безопасности персональных данных (УБПДн) могут включать в себя различные типы атак и угроз:

– кибератаки. Они могут принимать форму вирусов, червей, троянов и других вредоносных программ, которые могут произвести кражу, уничтожение или изменение ПДн;

– физические угрозы. Они могут включать в себя угрозы, связанные с доступом к ПДн, нарушением их целостности или уничтожением. К таким угрозам могут относиться взломы, кражи, пожары, наводнения, землетрясения и т.д.;

– социальные угрозы. Они могут происходить в результате атак со стороны человеческого фактора, таких как фишинг (мошенничество), скамы, фишинговые атаки, социальная инженерия, кража идентификаторов и так далее;

– угрозы, связанные с недостаточной защитой ПДн. Они могут включать в себя угрозы, связанные с недостаточной защитой в ИТ-инфраструктуре, слабые пароли, незашифрованные данные, уязвимости в программах и технологиях, недостаточная защита PDA сетей и т.д.;

– угрозы, связанные с нарушением законодательства в области защиты персональных данных. Если организации не будут соблюдают нормы законодательства в области защиты персональных данных, то все нарушения в области защиты будут выявлены;

– если система управления персональными данными не работает должным образом, оборудование выходит из строя, то угрозы будут связаны с техническими отказами.

Все эти угрозы могут оказаться опасными для безопасности персональных данных и могут привести к значительным материальным и

нематериальным убыткам, таким как утечки данных, штрафы, утрата репутации и т.д.

База данных содержит информацию о различных образовательных учреждениях, таких как школы, колледжи, университеты и т.д.

Структура:

– название учреждения;

– адрес;

– телефон;

– E-mail;

– веб-сайт;

– вид образовательной организации (школа, колледж, университет и т.д.);

– количество студентов;

– список предоставляемых образовательных программ;

– информация о факультетах/отделениях/кафедрах;

– дополнительная информация (например, кружки, секции и т.д.).

База данных может быть использована для поиска нужной образовательной организации, сравнения ее параметров с другими и выбора наиболее подходящей. Также база данных может быть полезна для организации мероприятий и проектов в сфере образования.

За обработку информацию, в которую включены ПДн, выделяют несколько подразделений в образовательной организации:

– административное подразделение, в которое входят сотрудники, обрабатывающие ПДн учащихся и персонала. Это может включать в себя отдел кадров, финансовый отдел, отдел образовательных программ и другие подразделения, которые имеют доступ к ПДн;

– образовательное подразделение, в которое входят учителя, профессора и другие преподаватели, которые используют ПДн учащихся для оценки успеваемости, проведения занятий и контроля знаний. Кроме того, в

этом подразделении могут находиться специалисты по информационным технологиям, которые обрабатывают ПДн в рамках использования электронных образовательных ресурсов и онлайн-курсов.

Защита персональных данных в образовательной организации обычно организуется следующим образом:

1. Подготовка правил обработки персональных данных - образовательная организация должна разработать внутренние правила и политику обработки персональных данных, которые будут утверждены руководством организации и согласованы с регуляторами (например, Генеральным инспектором по защите персональных данных).

2. Обучение персонала - все сотрудники образовательной организации, которые работают с персональными данными, должны быть обучены правилам обработки данных и о том, как защищать их. Также может потребоваться обучение учащихся и их родителей.

3. Регистрация базы данных - все базы данных, которые содержат персональные данные, должны быть зарегистрированы в должном органе по защите персональных данных.

4. Разграничение доступа к данным - доступ к персональным данным должен быть предоставлен только сотрудникам, которые нуждаются в них для выполнения своих профессиональных обязанностей. Важно обеспечить различные уровни доступа для разных категорий пользователей.

5. Шифрование персональных данных - данные должны быть зашифрованы перед передачей через сети или хранением на цифровых носителях. Шифрование должно соответствовать современным стандартам и не противоречить законодательству.

6. Аудит безопасности - образовательные организации должны периодически проводить аудиты безопасности, чтобы определить риски и возможные слабые места в системе защиты персональных данных.

7. Реагирование на инциденты безопасности – в случае нарушения безопасности данных, образовательная организация должна немедленно принимать меры для устранения проблемы и уведомлять пострадавших пользователей и уполномоченный орган по защите персональных данных.

В общем, организация защиты персональных данных является обязательной для образовательных учреждений и налаживается в соответствии с законом.

Для создания и использования баз данных (БД) образовательного учреждения используются различные типы программных продуктов. Каждый из них имеет свои особенности, свои слабые и сильные стороны.

1. Системы управления базами данных (СУБД). Это программное обеспечение, которое позволяет создавать, обновлять и управлять базами данных. Они обладают высокой скоростью работы, масштабируемостью и возможностью установки дополнительных модулей и расширений. Однако у СУБД высокая стоимость и сложность в настройке и поддержке.

2. Графические интерфейсы для баз данных. Эти программы предоставляют удобный интерфейс для создания и управления базами данных без необходимости знания языков программирования. Они позволяют создавать отчеты, анализировать данные и экспортировать данные в различных форматах. Однако, у них есть недостатки, такие как низкая скорость работы и невозможность внедрения дополнительных функций.

3. Базы данных веб-приложений. Они представляют из себя программные платформы для создания веб-приложений с БД. Такие базы данных могут использоваться для хранения любой информации об учреждении (информация о студентах, преподавателях и т.д.). Однако, у данных программ есть ограничения в возможностях настройки и требуют определенных знаний веб-разработки.

4. Эксель и Google Таблицы. Эти программы позволяют хранить и обрабатывать данные в таблицах. Они просты в использовании и могут

использоваться для небольших баз данных. Однако у них низкая масштабируемость и они не обладают всеми возможностями СУБД.

В целом, выбор типа программного обеспечения для создания и использования баз данных образовательного учреждения зависит от его потребностей и бюджета. Каждый тип программ имеет свои достоинства и недостатки, которые необходимо учитывать при выборе.

Базы данных образовательного учреждения создаются и используются несколькими типами программ: Office Access 2003, либо Microsoft Office Access 2007 (данные хранятся в формате mdb, реже accdb); Office Excel 2003, либо Microsoft Office Excel 2007 (данные хранятся в формате xls).

Каждый из этих типов программ позволяет создавать и управлять базами данных, но каждый из них имеет свои специфические особенности. Office Access и Excel более просты в использовании и позволяют создать базы данных, которые могут управляться в рамках одного компьютера или локальной сети. Однако они могут иметь ограничения по количеству данных и скорости работы.

SQL Server и MySQL предназначены для работы с большими объемами данных и поддерживают многопользовательский доступ. Они имеют более сложную структуру и требуют определенных знаний для управления ими. Однако они позволяют создавать базы данных, которые могут использоваться не только в рамках одной сети, но и через Интернет.

Выбор программного обеспечения для создания базы данных зависит от требований к ее функциональности и доступности, а также от уровня знаний.

Штатная служба образовательного учреждения для защиты персональных данных - это команда специалистов, назначенных для обеспечения безопасности и конфиденциальности персональных данных студентов, учителей и других сотрудников учреждения. Она включает в себя ответственных лиц, занимающихся оценкой угроз, контролем за

соблюдением законодательства в области персональных данных, разработкой политики безопасности и подготовкой сотрудников к работе с конфиденциальной информацией.

Функции штатной службы образовательного учреждения для защиты персональных данных могут включать в себя:

– информирование сотрудников и студентов об угрозах безопасности персональных данных и необходимых мерах для их защиты;

– разработка и внедрение политики безопасности, устанавливающей требования к обработке персональных данных;

– контроль за соблюдением требований законодательства в области защиты персональных данных;

– аудит системы обработки и хранения персональных данных для выявления уязвимостей и угроз безопасности;

– оценка рисков нарушения конфиденциальности и разработка планов действий в случае возникновения угроз;

– подготовка сотрудников и студентов к работе с персональными данными, проведение обучающих мероприятий, контроль за соблюдением правил работы с конфиденциальной информацией.

Штатная служба образовательного учреждения для защиты персональных данных является необходимым элементом системы безопасности и конфиденциальности информации, обрабатываемой учреждением. В ее задачи входит обеспечение защиты всех данных о студентах, сотрудниках, учителях и административных работниках от недобросовестного использования.

Полное функционирование комплексной системы защиты информации в образовательном учреждении предполагает следующие организационные и организационно-технические мероприятия:

– разработка политики информационной безопасности, которая определяет стратегическую и целевую защиту информации. Создают меры

по обеспечению безопасности и распределяют ответственность за информационную безопасность между всеми сотрудниками.Создают технические меры для обеспечения безопасности информации;

– организация службы информационной безопасности, которая отвечает за реализацию информационной безопасности, направляет деятельность сотрудников в области безопасности, организует внутренние аудиты и следит за программным и аппаратным обеспечением;

– разработка процедур доступа к информации, которые определяют кто и каким образом может иметь доступ к информации, какая информация является конфиденциальной и как ее необходимо хранить;

– установка средств аутентификации пользователей, которые обеспечивают идентификацию и аутентификацию пользователей перед предоставлением им доступа к информации;

– разработка и внедрение системы резервного копирования и архивирования информации, которые обеспечивают сохранность информации в случае ее случайного удаления или повреждения;

– установка антивирусного программного обеспечения, которое обеспечивает защиту от вредоносных программ;

– разработка и внедрение системы защиты от вторжений, которая обнаруживает и предотвращает попытки несанкционированного доступа к информации;

– проведение регулярных обучающих программ для сотрудников, направленных на повышение их осведомленности в области информационной безопасности, а также проведение периодических проверок и аудитов по предотвращению утечек информации.

Важно отметить, что создание и поддержание функционирования комплексной системы защиты информации в образовательном учреждении требует не только внедрения технических мер защиты, но и организационных

мер, отраженных, прежде всего, в политике и процедурах информационной безопасности.

Для полной и эффективной работы комплексной системы компьютерной безопасности, должным образом разрабатывают следующие группы важных документов:

1. Политика безопасности информации – документ, со всеми составляющими, обеспечивает безопасности информации в организации.

2. Положение о комплексной системе компьютерной безопасности - документ, определяющий структуру и функции системы компьютерной безопасности, порядок ее создания, управления и контроля.

3. Инструкции по использованию ИТ-ресурсов - документы, содержащие правила использования компьютерных средств, программного обеспечения и сетевых ресурсов, а также ограничения и ответственность за их нарушение.

4. Положение о службе информационной безопасности - документ, определяющий структуру, функции и компетенцию сотрудников службы информационной безопасности организации.

5. Положение о защите персональных данных - документ, определяющий порядок сбора, хранения, обработки и защиты персональных данных в организации, а также права и обязанности субъектов персональных данных.

6. Указания по защите информации от несанкционированного доступа - документ, содержащий рекомендации и инструкции по защите информации от кибератак, в том числе от вирусов, хакеров и иных угроз.

7. Регламент по обеспечению бесперебойной работы систем и сетей - документ, определяющий правила и процедуры по обеспечению непрерывной работы компьютерной инфраструктуры, включая создание резервных копий данных и устранение сбоев.

8. Положение о прохождении аттестации уровня компетентности сотрудников по вопросам информационной безопасности - документ, определяющий порядок и условия проведения аттестации персонала по вопросам информационной безопасности.

План защиты информации в АС должен содержать следующие сведения:

описание сбора и использования персональных данных - в плане должна быть предоставлена ясная информация о том, какие персональные данные собираются, для каких целей они будут использоваться и как долго они будут храниться.

процедуры контроля и доступа - необходимо определить, кто имеет доступ к персональной информации и как этот доступ будет контролироваться.

Обучение и обучение персонала - необходимо определить процедуры, регулирующие обучение и обучение персонала по вопросам безопасности персональной информации.

Регулярные проверки безопасности - рекомендуется в плане включать процедуры для регулярного тестирования системы на наличие уязвимостей и проверки ее соответствия соответствующим нормам и стандартам в области защиты данных.

Меры безопасности при обработке персональных данных работников - необходимо определить процедуры, регулирующие обработку персональных данных работников (например, процедуры оценки производительности и защиты от дискриминации).

Меры безопасности при передаче данных - необходимо определить процедуры для обеспечения безопасной передачи персональных данных к другим структурам и организациям.

Обработка персональных данных наталкивает на создание определенного режима работы, который обеспечит безопасность

информации и защиту прав субъектов персональных данных. Данный режим должен быть описан в документах по защите персональных данных, а также включать в себя следующие меры:

– ограниченный доступ к персональным данным сотрудникам, которые имеют соответствующие права и разрешения;

– шифрование и защиту данных при передаче и хранении;

– регулярную проверку на наличие угроз безопасности данных;

– обучение сотрудников правилам обработки персональных данных и предотвращение утечек информации;

– соблюдение требований законодательства России, в том числе требований Федерального закона «О персональных данных»;

– составление списка лиц, имеющих доступ к персональным данным, и контроль за их действиями;

– проведение аудита системы защиты персональных данных.

Создание специального режима обработки персональных данных позволяет минимизировать риски нарушения прав субъектов персональных данных, а также может обеспечить защиту конфиденциальной информации. Данное действие является важным условием для доверия клиентов и партнеров и поддержания репутации организации.

Определение сроков обработки ПДн зависит от целей обработки и категории субъектов ПДн, а также от применяемых средств обработки. В общем случае сроки обработки должны быть обоснованы и согласованы с субъектом ПДн.

Например, обработка ПДн с целью заключения или исполнения договора может осуществляться в течение срока действия договора. Обработка ПДн на основе согласия субъекта может осуществляться до отзыва согласия. Обработка ПДн для целей налогового учета может осуществляться в течение законодательно установленного срока хранения учетной документации.

Согласно требованиям Закона "О персональных данных", сроки обработки ПДн не должны превышать целей обработки. Также организация, осуществляющая обработку ПДн, должна обеспечить сохранность и конфиденциальность этих данных в соответствии с требованиями законодательства.

Определение сроков обработки ПДн крайне важно потому, что Федеральный закон определяет, что «в случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки».

Выводы по первой главе

По итогам первой главы магистерской диссертации главы можно сделать следующие выводы.

1. Раскрыто понятие персональных данных и значение их защиты в образовательной организации высшего образования.

Персональные данные – это информация, связанная с конкретным человеком, такая как ФИО, дата рождения, адрес проживания, номер телефона, паспортные данные и т.д. Они могут также включать в себя информацию о медицинских проблемах, учебном процессе, результаты тестов, оценках и др.

Защита персональных данных в образовательной организации высшего образования является основной и важной задачей. Это важно для защиты личной жизни и конфиденциальности студентов и сотрудников образовательной организации. Защищая персональные данные, учреждение высшего образования также гарантирует соблюдение законодательства о защите персональных данных (ОЗПД), которое обязывает организации обрабатывать персональные данные только в рамках установленных законом целей и требований.

Защита персональных данных также обеспечивает безопасность предоставления информации о студентах и сотрудниках. Кроме того, защита персональных данных гарантирует, что никакие конфиденциальные данные не будут использованы в несанкционированных целях, таких как мошенничество или кража личности. Руководство образовательной организации должно принимать меры для обеспечения безопасности и конфиденциальности данных студентов и сотрудников.

2. Проанализировано нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.

Защита персональных данных в Российской Федерации регулируется несколькими законодательными актами:

– Конституция Российской Федерации: статья 24 обеспечивает право на тайну обмена сообщениями, переписки, связи, телефонных переговоров, почтовых, телеграфных и иных сообщений;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: этот закон определяет правовые основы обработки персональных данных и устанавливает требования к технической защите информации;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: закон определяет правила использования информационных технологий при обработке персональных данных и установлен порядок обработки информации ограниченного доступа;

– Гражданский кодекс Российской Федерации: кодекс определяет правила отношений субъектов при обработке персональных данных и защиту прав потребителей;

– Административный регламент по обеспечению доступа к информации, которое имеется на официальных сайтах органов государственной власти (Федеральной закон от 27 июля 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»).

3. Описаны этапы организации защиты персональных данных в образовательной организации.

Формирование команды по защите персональных данных. Назначение ответственных сотрудников, обучение команды требованиям закона о персональных данных.

Категории персональных данных определяются и обрабатываются в образовательной организации. В соответствии с категориями персональных данных будут определены меры по их защите.

Оценка рисков, связанных с обработкой персональных данных. Необходимо определить угрозы, возможные последствия нарушения

законодательства о персональных данных, а также вероятность их реализации.

Разработка политики обработки персональных данных. Документ должен включать в себя информацию о целях обработки персональных данных, категориях обрабатываемых данных, порядок доступа к ним, меры по защите данных и пр.

Обеспечение защиты персональных данных. В соответствии с политикой обработки персональных данных необходимо реализовать технические и организационные меры по защите данных, такие как организация доступа к базам данных, шифрование информации, контроль доступа и т.д.

Обеспечение безопасности персональных данных. Необходимо обеспечить безопасность хранения и передачи персональных данных, производить резервное копирование данных, защиту от несанкционированного доступа и т.д.

Регулярные проверочные работы, в связи с соответствием защиты персональных данных установленным требованиям. Необходимо проверять правильность обработки и хранения персональных данных, а также выявлять оценку эффективности мер по защите данных.

В целом защита персональных данных представляет собой сложный технологический процесс, который включает в себя множество технических, организационных и правовых мероприятий. Этот процесс начинается с оценки угроз безопасности персональных данных, которая позволяет определить требуемый уровень защиты. Затем необходимо выбрать соответствующие меры защиты, такие как криптографические методы шифрования, механизмы аутентификации и контроля доступа, а также процедуры обработки и хранения данных.

Разработка правил и процедур для сбора, использование и раскрытие персональных данных, а также реализацию механизмов контроля и ревизии.

Также необходимо обеспечивать обучение персонала и проводить аудит системы защиты персональных данных с целью определения и устранения уязвимостей.

ГЛАВА 2. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ ФГБОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1 Оценка информационной безопасности персональных данных в ФГБОУ ВО «Южно-уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации

Базой исследования является ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации, располагающийся по адресу: г. Челябинск, ул. Воровского, 64.

Ректор – заслуженный деятель науки РФ, д-р мед. наук, профессор Волчегорский Илья Анатольевич.

Южно-Уральский государственный медицинский университет (ЮУрГМУ) – это высшее учебное заведение в Челябинске, созданное в 1930 году. Университет находится под управлением Министерства здравоохранения Российской Федерации.

ЮУрГМУ предлагает образовательные программы на 8 факультетах: факультет медицины, факультет стоматологии, факультет фармации, факультет педиатрии, факультет медицинской биологии, факультет переподготовки и повышения квалификации, факультет дополнительного образования, факультет медицинской психологии.

Университет имеет развитую научную исследовательскую базу, включающую 6 научно-исследовательских институтов и 26 научных

лабораторий. Также ЮУрГМУ является соучредителем научных центров Российской академии медицинских наук.

В центре внимания ЮУрГМУ – качественное медицинское образование и подготовка квалифицированных специалистов в области здравоохранения. Студенты университета имеют возможность проходить практику в лучших клиниках и больницах города, области и страны. ЮУрГМУ – это престижное учебное заведение, где обучающиеся получают знания и навыки, необходимые для успешной профессиональной деятельности в медицинской отрасли.

Важнейшим направлением образовательной политики ЮУрГМУ является повышение качества образования, развитие научных и инновационных исследований, а также формирование профессиональной компетенции студентов для успешной адаптации на рынке труда. Кроме того, в университете активно осуществляется работа по развитию международного сотрудничества, обеспечение доступности образования и поддержка социальной мобильности студентов. Одной из ключевых идей в образовательной политике ЮУрГМУ является интеграция научных и практических знаний, а также методов обучения, чтобы обеспечить максимальную эффективность образовательного процесса.

ЮУрГМУ предлагает образовательные программы на следующих уровнях:

1. Бакалавриат – этот уровень программы предназначен для студентов, которые только начинают свой путь в образовании. Продолжительность программы обычно составляет 4 года. ЮУрГМУ предлагает бакалавриат в таких областях, как медицина, здравоохранение, стоматология, фармация и биология.

2. Магистратура – программы магистратуры для тех, кто уже получил диплом бакалавра и хочет продолжить свой профессиональный рост.

Продолжительность программы обычно составляет 2 года. В ЮУрГМУ магистратура доступна в областях медицины, фармации и здравоохранения.

3. Аспирантура – программы аспирантуры для тех, кто заинтересован в научных исследованиях и хочет стать профессиональным научным работником. Продолжительность программы обычно составляет от 3 до 4 лет.

4. Послевузовское образование – эти программы предназначены для тех, кто уже имеет высшее образование и хочет получить дополнительные навыки или знания в своей области. Программы послевузовского образования доступны в ЮУрГМУ в области медицины, здравоохранения, стоматологии и фармации.

5. Дистанционное обучение – ЮУрГМУ предлагает также возможность изучения некоторых программ в режиме онлайн. Это предоставляет студентам большую гибкость и возможность изучения материала в удобное для них время.

Кроме того, в ЮУрГУ есть программы для иностранных студентов, такие как программы подготовки бакалавров и магистров на английском языке.

Организационная структура ФГБОУ ВО ЮУГМУ Минздрава России представлена на рисунке 2.

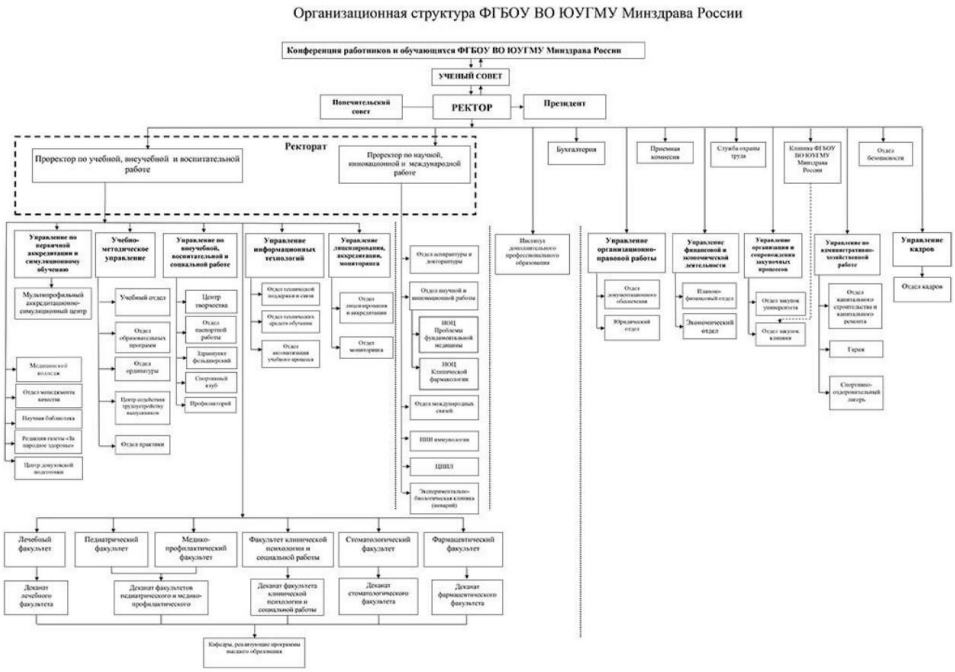

Рисунок 2 – Организационная структура [44]

ФГБОУ ВО ЮУГМУ Минздрава России занимается следующими видами деятельности:

1. Образовательная деятельность. Университет предоставляет бакалаврские, магистерские и аспирантские образовательные программы по медицине, стоматологии, фармации, педиатрии, медицинской биологии, биоинженерии и другим медицинским специальностям.

2. Научно-исследовательская деятельность. ЮУГМУ осуществляет научную работу в области медицины, биологии и экологии. В университете создан центр трансляционной медицины и фундаментальные исследования.

3. Медицинская деятельность. На базе ФГБОУ ВО ЮУГМУ работают многочисленные клиники, в том числе клиника детской онкологии, перинатальный центр, клиника стоматологии, общая клиника и другие.

4. Общественно-просветительская деятельность. ЮУГМУ проводит различные мероприятия, посвященные здоровью, направленные на повышение знаний общества в области медицины, профилактики заболеваний и здорового образа жизни [44].

Организацией системы защиты персональных данных в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации занимается Управление информационных технологий.

Управление информационных технологий университета расположено по адресу: 454092, г. Челябинск, ул. Воровского, 64. Начальник управления информационных технологий - Муратов И.И.

В структуру управления информационных технологий университета входят:

1. Отдел технической поддержки и связи.

2. Отдел технических средств обучения.

Отдел технической поддержки и связи.

Основные задачи отдела:

1. Разработка и выполнение программы развития информационных технологий в университете.

2. Управление инфраструктурой информационных систем, включая хранение, обработку, передачу и защиту данных.

3. Обеспечение связи и взаимодействия между различными информационными системами университета.

4. Поддержка и развитие электронных библиотек и других информационных ресурсов, необходимых для академической и научной работы.

5. Поддержка и развитие онлайн-курсов и других форм дистанционного обучения.

6. Обучение и развитие персонала университета в области информационных технологий.

7. Обеспечение эксплуатации и обслуживания компьютерной техники и программного обеспечения.

8. Контроль за использованием информационных технологий в соответствии с нормативно-правовыми актами.

9. Разработка и внедрение мер по защите информации от несанкционированного доступа и вирусных атак.

10. Оценка эффективности использования информационных технологий в университете.

Функции отдела:

1. Планирование и координация разработки, обновления и управления информационными системами и технологиями, которые поддерживают бизнес-процессы университета.

2. Разработка стратегии информационного развития, определение критериев эффективности и продвижение лучших практик, связанных с использованием IT.

3. Обеспечение надежности, безопасности, конфиденциальности, корректности и доступности информации университета для всех пользователей.

4. Закупка, установка, конфигурация и сопровождение аппаратного и программного обеспечения, используемого на территории университета, а также обучение пользователей, использующих это оборудование и программы.

5. Содействие в обеспечении эффективного использования IT-ресурсов и технологий, в том числе в области административной деятельности, научной работы и дистанционного обучения.

6. Поддержка работы серверных систем, баз данных, сетевых технологий, программного обеспечения, электронной почты, сайта университета и других систем для обмена информацией между различными группами пользователей.

7. Создание и поддержание электронных архивов, библиотек, онлайн-курсов и других электронных ресурсов, необходимых для научной и учебной деятельности университета.

8. Мониторинг и оценка производительности IT-систем и технологий, включая анализ данных для улучшения управленческих решений.

9. Обеспечение информационной поддержки мероприятий, проводимых на территории университета, включая обеспечение доступности интернета, техническую поддержку выставочных стендов и др.

10. Взаимодействие с внешними поставщиками и другими ресурсами, связанными с IT-технологиями, в целях обеспечения надежности и доступности IT-систем и технологий университета.

Ответственным за обеспечение безопасности персональных данных является начальник отдела технической поддержки и связи управления информационных технологий.

Таким образом, отдел технической поддержки и связи тесно сотрудничает и взаимодействует со всеми кафедрами и структурными подразделениями университета и другими ВУЗами.

В Университете введены в эксплуатацию следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ» (далее - ИСПДн «ФИС ФЦТ»).

2. ИСПДн «Обучающиеся и абитуриенты» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Обучающиеся и абитуриенты»).

3. ИСПДн «Сотрудники» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Сотрудники»).

4. ИСПДн «Библиотека» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Библиотека»).

Схема информационных потоков в ИСПДн представлена в таблице 1.

На ИСПДн «ФИС ФЦТ» разработана и утверждена ректором Университета и заместителем директора ООО «ИТ Энигма» «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ» № 74.02179. МУ от 03.07.2017 (далее - Модель угроз ИСПДн «ФИС ФЦТ»), а также утвержден заместителем директора ООО «ИТ Энигма» «Аттестат соответствия информационной системы персональных данных «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ» требованиям по безопасности информации № 74.02179.АС от 03.07.2017. Согласно модели угроз ИСПДн «ФИС ФЦТ» установлено, что:

– ИСПДн является информационной системой, обрабатывающей иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для ИСПДн актуальны угрозы 3-го типа;

– 3-ий уровень защищенности персональных данных при их обработке в ИСПДн.

Таблица 1 – Схема информационных потоков в ИСПДн

Тип ПДн	Представление	Передача				Использование	Хранение
		Источник	Получатель	Среда передачи	Использование шифрования		
Персональные данные сотрудников	Выгрузка из БД	ПК сотрудников бухгалтеии	ПАО Челябинвестбанк	Интернет	Да, VPN-KEY-T	ПК сотрудников бухгалтерии	ПК сотрудников бухгалтерии
Персональные данные обучающихся							
Персональные данные сотрудников	Выгрузка из БД	ПК сотрудников бухгалтерии и отдела	УПФР, ИФНС, ФСС	Интернет	Да, СКЗИ КриптоПро CSP 4	ПК сотрудников бухгалтерии и отдела	1С: Предприятие, БД СТЭК Электронная
Персона							

льные данные обучающихся		кадров				кадров	отчетность на серверах
Персональные данные обучающихся	Выгрузка из БД	ПК сотрудников	ФРМР	Интернет	Нет, авторизация через ЕСИА	ПК сотрудников	ЦОД Министерства здравоохранения РФ

На ИСПДн «Обучающиеся и абитуриенты» разработана и утверждена ректором Университета и заместителем директора ООО «ЦИТ ОЗОН» «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Обучающиеся и абитуриенты» № 0060-2019/МУ.2 от 23.09.2019, согласно которой установлено, что:

– ИСПДн является информационной системой, обрабатывающей иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для ИСПДн актуальны угрозы 3-го типа;

– 4-ый уровень защищенности персональных данных при их обработке в ИСПДн.

На ИСПДн «Сотрудники» разработана и утверждена ректором Университета и заместителем директора ООО «ЦИТ ОЗОН» «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Сотрудники» № 0060-2019/МУ.1 от 23.09.2019, согласно которой установлено, что:

– ИСПДн является информационной системой, обрабатывающей иные категории персональных данных менее чем 100 000 субъектов персональных данных, являющихся сотрудниками оператора;

– для ИСПДн актуальны угрозы 3-го типа;

– 4-ый уровень защищенности персональных данных при их обработке в ИСПДн.

На ИСПДн «Библиотека» разработана и утверждена ректором Университета и заместителем директора ООО «ЦИТ ОЗОН» «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Сотрудники» № 0060-2019/МУ.1 от 23.09.2019, согласно которой установлено, что:

– ИСПДн является информационной системой, обрабатывающей иные категории персональных данных менее чем 100 000 субъектов персональных данных, являющихся сотрудниками оператора;

– для ИСПДн актуальны угрозы 3-го типа;

– 4-ый уровень защищенности персональных данных при их обработке в ИСПДн.

Для защиты информации в ИСПДн Университета используются следующие СКЗИ:

– «ViPNet Coordinator HW 1000», сертификат соответствия ФСБ России;

– «ViPNet Client 4», сертификат соответствия ФСБ России;

– «КриптоПро CSP 4.0», сертификат соответствия ФСБ России;

– «Тунель-TLS», сертификат соответствия ФСБ России.

Приказом ректора Университета № 552л/вр от 13.08.2019 в ИСПДн: «ФИС ФЦТ», «Обучающиеся и абитуриенты», «Сотрудники» и «Библиотека» ответственным пользователем СКЗИ назначен оператор ЭВМ отдела технической поддержки и связи управления информационных технологий.

В Университете разработана «Инструкция ответственного пользователя СКЗИ» № б/н от 15.08.2019.

Охрану специальных помещений Университета осуществляют: Общество с ограниченной ответственностью Частная охранная организация «СпецОхрана», контракт № 93/2018 от 16.11.2018, Общество с ограниченной

ответственностью Частная охранная организация «Ягуар», контракт №94/2018 от 07.12.2018.

К объектам защиты относятся:

– ПДн;

– СКЗИ;

– среда функционирования СКЗИ (далее по тексту – СФ);

– информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

– носители защищаемой информации, используемые в ИС Сотрудники, ИС Обучающиеся и ИС Библиотека в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые в ИС каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы ИС Сотрудники, ИС Обучающиеся и ИС Библиотека, имеющие отношение к криптографической защите ПДн.

Работа с понятием угрозы начинается с классификации нарушения.

безопасности информации. В общем случае, угрозы безопасности информации можно разделить на четыре основных типа:

1. Нарушение конфиденциальности: это означает, что информация становится доступной неправомерным лицам, которые не имеют права ее получать. Например, кража пароля или доступ к приватным файлам.

2. Нарушение целостности: когда информация подвергается нарушениям, которые изменяют ее. Например, изменение содержания документа или внесение в него ошибок.

3. Нарушение доступности: информация становится недоступной для тех, кто имеет к ней право доступа. Например, при атаке на сетевой сервер компании, который перестает откликаться.

4. Нарушение аутентичности: это происходит, когда информация подделывается таким образом, что кажется, будто она была создана компетентным лицом, но на самом деле это не так. Например, изменение истории обслуживания выдающего кассового аппарата.

Пройдя процесс классификации и поняв, какие угрозы могут появиться при работе с информацией, можно разработать соответствующие меры безопасности, которые позволят предотвратить эти угрозы и защитить данные.

«Насколько актуальна проблема защиты информации от различных угроз, можно увидеть на примере данных, опубликованных Computer Security Institute (Сан - Франциско, штат Калифорния, США), согласно которым нарушение защиты компьютерных систем происходит по следующим причинам:

– несанкционированный доступ - 2%;

– укоренения вирусов - 3%;

– технические отказы аппаратуры сети - 20 %;

– целенаправленные действия персонала - 20 %;

– ошибки персонала (недостаточный уровень квалификации) - 55 %» [15].

Таким образом, одной из основных потенциальных угроз в информационных системах следует считать недоброжелательные действия персонала (человеческий фактор), так как этот аспект составляет 75 процентов всех случаев [29, С. 7].

Показатель исходной защищенности ИСПДн.

Информационная система персональных данных "Сотрудники" предназначена для хранения и учета информации о сотрудниках организации. Основные технические и эксплуатационные характеристики системы:

1. Платформа: система работает на любой операционной системе Windows, Linux, Mac.

2. Язык программирования: система написана на языке программирования Java.

3. Хранение данных: данные хранятся в базе данных MySQL.

4. Интерфейс: система имеет интуитивно понятный и удобный интерфейс, ориентированный на пользователя.

5. Уровень защиты: система обеспечивает высокий уровень защиты конфиденциальности персональных данных, с помощью SSL-шифрования и авторизации пользователей.

6. Функциональность: система позволяет вести учет кадровой документации, формирование пакета документов для проверки Государственной инспекции труда, формирование заявлений на отпуск и больничный лист, расчет зарплаты и налоговых отчислений.

7. Работа в онлайн-режиме: система работает в режиме онлайн с возможностью доступа к данным с любого устройства, имеющего доступ в интернет.

8. Техническая поддержка: система позволяет всегда иметь доступ к технической поддержке пользователям.

Определение исходной степени защищенности в ИСПДн «Сотрудники», «Обучающиеся», «Библиотека» описаны в таблице 2.

Таблица 2 – Исходная степень защищенности

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	1	14%
2	Средний	2	57%
3	Низкий	3	-

В соответствии полученными данными устанавливается низкий показатель исходной защищенности. Устанавливается значение коэффициента Y1=10.

Реализуемость угроз.

По итогам оценки уровня защищенности и вероятности реализации угрозы, рассчитывается коэффициент реализуемости угрозы и определяется возможность реализации угрозы:

$$Y = (Y1 + Y2)/20, \quad (1)$$

где Y – коэффициент реализуемости угроз;

Y1 – уровень защищённости;

Y2 – вероятность реализации угроз [16].

Для большинства параметров, этот показатель не превышает значения в 0.35, что является хорошим исходным показателем.

Для ИСПДн «Сотрудники» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн «Сотрудники».

Руководствуясь [3], учитывая исходные данные об ИСПДн «Сотрудники» и тип актуальных для неё угроз, необходимо обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Сотрудники».

В соответствии с [10], и определённым в модели нарушителя типом нарушителя – Н2, в ИСПДн «Сотрудники» для криптографической защиты ПДн должны применяться СКЗИ класса не ниже КС2.

Для ИСПДн «Обучающиеся и абитуриенты» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн «Обучающиеся и абитуриенты».

Руководствуясь [3], учитывая исходные данные об ИСПДн «Обучающиеся и абитуриенты» и тип актуальных для неё угроз, необходимо

обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Обучающиеся и абитуриенты».

В соответствии с [10], и определённым в модели нарушителя типом нарушителя – Н2, в ИСПДн «Обучающиеся и абитуриенты» для криптографической защиты ПДн должны применяться СКЗИ класса не ниже КС2.

Для ИСПДн «Библиотека» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном прикладном программном обеспечении, используемом в информационной системе.

Руководствуясь [3], учитывая исходные данные об ИСПДн «Библиотека» и тип актуальных для неё угроз, необходимо обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Библиотека».

Разработка документа «Актуальная модель угроз ИСПДн».

Модель угроз является одним из главных документов при создании системы персональных данных. Именно этот документ указывает на главные направления защиты информации в организации.

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Сотрудники» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации представлена в приложении Б.

Угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Обучающиеся и абитуриенты» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации представлена в приложении В.

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Библиотека» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации представлена в приложении 3.

Таким образом, когда идет обработка система защиты персональных данных , обрабатывается в информационных системах персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Южно-Уральский государственный медицинский университет» создана.

Эксплуатация используемых криптосредств, обращение с СКЗИ осуществляется с нарушениями требований нормативных документов в области защиты информации.

В Университете введены в эксплуатацию следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ» (далее - ИСПДн «ФИС ФЦТ»).

2. ИСПДн «Обучающиеся и абитуриенты» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Обучающиеся и абитуриенты»).

3. ИСПДн «Сотрудники» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Сотрудники»).

4. ИСПДн «Библиотека» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Библиотека»).

Таким образом, система защиты персональных данных при их обработке в информационных системах персональных данных в Федеральном государственном бюджетном образовательном учреждении

высшего образования «Южно-Уральский государственный медицинский университет» создана.

2.2 Рекомендации по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.

На основании рисков и уязвимостей системы защиты персональных данных, и анализируя нормативные требования действующего законодательства нами были разработаны рекомендации по организации системы защиты персональных данных в ФГБОУ ВО «ЮУГМУ» Министерства здравоохранения РФ.

Для организации системы защиты персональных данных необходимо провести ряд последовательных мероприятий.

Для устранения недостатков в существующей системе защиты ПДн, необходимо предложить образовательной организации усовершенствовать организационные, технические и физические меры.

Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты ПДн;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты ПДн;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

– организация ИСПДн в образовательной организации высшего образования;

– введение в СЗПДн новые нормативные документы для обеспечения безопасности ПДн.

Объект защиты.

Объектом защиты являются персональные данные работников и обучающихся образовательной организации высшего образования:

1. Электронная база данных – защита доступа к электронным базам данных, содержащим персональную информацию работников и студентов университета;

2. Программное обеспечение – использование защищенного программного обеспечения для хранения, обработки и передачи персональных данных;

3. Информационные сообщения – защита персональной информации в электронных письмах, мобильных сообщениях, сообщениях в социальных сетях и других формах электронной переписки;

4. Управление доступом – настройка прав доступа к персональной информации, предоставляемых сотрудникам и студентам в соответствии с их должностными обязанностями и учебными потребностями;

5. Защита физических носителей – поддержание физической безопасности при использовании компьютеров, ноутбуков, смартфонов и других носителей, содержащих персональные данные;

6. Обучение – обучение персонала учебного заведения правилам защиты персональных данных и мерам по их обеспечению;

7. Законодательство – соблюдение требований законодательства по защите персональных данных.

Субъекты информационных отношений

1. Студенты - основные потребители информации, так как они ищут материалы для учебы, общаются между собой и с преподавателями, и используют различные каналы коммуникации.

2. Преподаватели - предоставляют информацию студентам в качестве лекторов, проводят семинары, консультации и выступают в качестве научных руководителей.

3. Администрация университета - отвечает за организацию учебного процесса, предоставляет места для проведения занятий и прочие ресурсы, необходимые для учебы.

4. Научные сотрудники - занимаются научной деятельностью, получают и распространяют новые знания и информацию в университетской общественности.

5. Библиотекари - обеспечивают доступ к широкому спектру информационных ресурсов, таких как книги, статьи, электронные базы данных и прочие.

6. Лаборанты и технический персонал - занимаются обслуживанием и поддержкой техники, обучают студентов работе с различным оборудованием и помогают создавать и сохранять лабораторные работы.

7. Студенческие объединения, клубы и ассоциации - предоставляют студентам доступ к информационным ресурсам, связанным с индивидуальными интересами и целями.

Рекомендации по организации системы защиты персональных данных реализуются в 3 этапа.

Этап 1. Разработка организационно-распорядительных документов по защите персональных данных.

1. Разработать порядок действий при компрометации ключевой информации.

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Первым шагом необходимо остановить работу всех приложений и систем, использующих компрометированный ключ.

Вторым шагом следует сменить ключевую информацию во всех системах, работающих с компрометированным ключом, и заменить старый ключ на новый.

Третьим шагом необходимо выполнить аудит безопасности системы и выявить все уязвимости и ошибки, которые могли привести к компрометации ключевой информации.

Четвертым шагом следует провести обучение сотрудников и пользователей системы по правилам безопасности, используемым при работе с ключ

Пятый шаг – это регулярное мониторинг и анализ безопасности системы. Это позволит своевременно выявлять и предотвращать новые уязвимости и атаки на ключевую информацию.

Шестой шаг – это резервное копирование ключевой информации и ее защита от несанкционированного доступа.

Седьмым шагом следует рассмотреть возможность использования дополнительных методов защиты информации, таких как двухфакторная аутентификация и шифрование данных.

И наконец, последним шагом следует докладывать о случае компрометации ключевой информации ответственным лицам и органам безопасности.

2. Разработать памятку пользователя СКЗИ.

3. Разработать схему криптографической защиты.

Для разработки схемы криптографической защиты необходимо учитывать следующие основные компоненты:

– алгоритм шифрования: выбрать алгоритм, который будет использоваться для шифрования передаваемой информации, например, AES, RSA, Blowfish или другой;

– ключевой обмен: определить метод обмена ключами, который будет использоваться для создания и распределения ключей, необходимых для шифрования и дешифрования информации;

– аутентификация: выбрать метод аутентификации, чтобы быть уверенным в том, что только авторизованные пользователи имеют доступ к защищенной информации;

– защита от взлома: убедиться, что система защищена от взломов, атак и других угроз, таких как DDoS-атаки, SQL-инъекции или фишинг;

– управление ключами: определить методы управления ключами, чтобы обеспечить безопасное хранение и передачу ключей;

– обновление системы: разработать программу обновления, чтобы регулярно патчить уязвимости и обновлять систему;

– анализ инцидентов: создать методы анализа инцидентов, чтобы быстро реагировать на возможные угрозы и нападения;

– обучение пользователей: проводить регулярное обучение пользователей по правилам безопасности и использованию системы.

На основе этих компонентов можно разработать схему криптографической защиты, которая будет обеспечивать надежную и безопасную передачу информации.

4. Подготовить приказы о вводе СКЗИ в эксплуатацию.

5. Разработать журнал учета СКЗИ, эксплуатационной и технической документации к ним.

Типовая форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты) расположена в приложении Д.

Типовая форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) расположена в приложении Е.

6. Разработать порядок уничтожения СКЗИ и ключевых документов.

7. Разработать инструкцию по проведению внутренних проверок состояния защиты персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Провести обучение пользователей работе с СКЗИ.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Программа подготовки (обучения) разработана в соответствии с законодательными, нормативными и методическими документами в области информационной безопасности и рекомендациями ФСБ России.

Целью подготовки (обучения) является введение пользователей в предметную область информационной безопасности и ознакомление с правилами работы с СКЗИ.

Этап 3. Усовершенствование физических мер по защите персональных данных.

1. Разработать инструкцию по физической охране и правилам доступа в специальные помещения.

2. Разработать журнал лиц, имеющих право доступа в определенные помещения, для выполнения своих обязанностей.

3. Оборудовать двери специальных помещений и хранилищ приспособлениями для опечатывания.

4. Оборудовать сейфы, предназначенные для хранения СКЗИ, а также документации к ним и различные приспособления.

Таким образом, перед управлением информационных технологий должны стоять следующие первоочередные задачи:

– разработка организационно-распорядительных документов по защите персональных данных в Университете;

– осуществлять обучение пользователей правилам работы с СКЗИ;

– усовершенствование физических мер защиты персональных данных в учебном заведении.

2.3 Оценка эффективности рекомендаций по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска

Контроль эффективности системы защиты ИСПДн осуществляется Учреждением с периодичностью раз в полугодие. Целью контроля является своевременное выявление ненадлежащих режимов работы ИСПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Критерии проверки:

1. Документация по объекту.

2. Анализ структуры ИСПДн и технический процесс обработки информации.

3. Уровень защиты.

4. Проверка структуры ИСПДн по заявленной документации.

5. Оценка организации рабочего процесса и общего выполнения всех требований по защите.

6. Вопросы охраны проверяемого объекта.

7. Настроены ли штатные средства защиты.

8. Оценка уровня компетентности для ответственных за защиту ПДн.

9. Проверка знаний и умений персонала ИСПДн по информационной безопасности.

10. Проверка прав доступа.

11. Учет и регистрация.

12. Целостности.

13. Все,что связано с антивирусом.

14. Полный анализ уровня защиты.

15. Обнаружение посторонних вторжений.

16. Файрвол и его настройки.

17. Анализ защиты каналов связи.

18. Проверка защиты ИСПДн с помощью сканером безопасности.

По итогам вышеперечисленных действий составляется протокол оценки эффективности системы защиты ПДн. Он служит основой составления итогового заключения о состоянии защиты данных.

Расчет показателей эффективности может производиться с помощью различных методов: методы моделирования процессов защиты информации; экспертные оценки; статистический анализ; метод минимизации рисков и т.д

В рамках исследовательской работы мы выбрали метод экспертной оценки.

Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения.

Экспертная оценка эффективности рекомендаций по организации системы защиты персональных данных проводилась на базе ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Методическая составляющая рекомендаций по организации системы защиты ПДн: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн.

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений.

Данные критерии были преобразованы в информационно-оценочную карту, которая представлена в таблице 3.

Перед проведением экспертной оценкой была определена система баллов, которые выставлялись экспертом. Это было сделано для надежности оценки. То есть, чтобы другие эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к схожим выводам.

Таблица 3 – Показатели оценки эффективности рекомендаций по совершенствованию организационных и технических мер защиты персональных данных Университета

Показатели оценки эффективности	Эксперты		
	Эксперт 1	Эксперт 2	Эксперт 3
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных			
2. Методическая составляющая рекомендаций по организации системы защиты ПДн: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн.			

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений.			

Каждому эксперту предлагались рекомендации по организации системы защиты персональных данных Университета и информационно-оценочный лист с одинаковыми показателями оценки.

По итогам оценки эксперт представляет отчет, который содержит следующие сведения:

– заполненную информационно-оценочную карту;

– общие выводы.

В состав экспертной комиссии вошли: начальник управления информационных технологий, начальник управления организационно-правовой работы, системный администратор отдела технической поддержки и связи Управления информационных технологий ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ.

Результаты экспертной оценки представлены в таблице 4.

Таблица 4 – Результаты экспертной оценки эффективности предложенных рекомендаций

Показатели оценки эффективности	Эксперты		
	Эксперт М.И.	Эксперт К.С.	Эксперт З.Г.
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению	Высокий уровень	Высокий уровень	Высокий уровень

безопасности персональных данных			
2. Методическая составляющая рекомендаций по организации системы защиты ПДн: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн.	Высокий уровень	Средний уровень	Высокий уровень
3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений.	Высокий уровень	Средний уровень	Высокий уровень
Итоговая оценка экспертов:	Высокий уровень эффективности предложенных рекомендаций		

Результаты экспертной оценки эффективности представлены на результирующей диаграмме (рисунок 3).

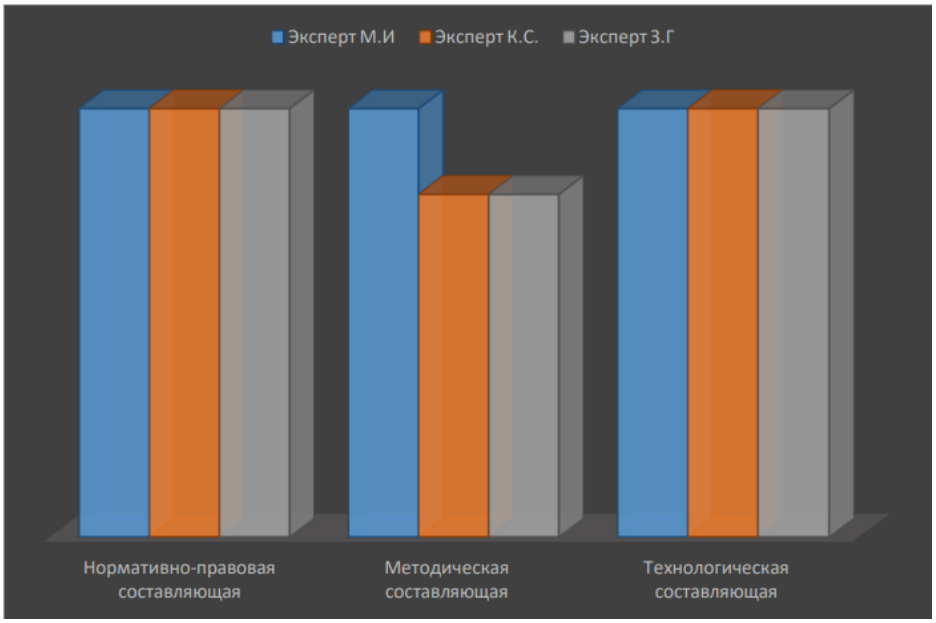

Рисунок 3 – Сводные результаты экспертной оценки эффективности разработанных рекомендаций по совершенствованию организационных и технических мер защиты персональных данных Университета

Проведенный анализ позволяет сделать вывод, что мнения экспертов относительно совпадают.

По результатам экспертной оценки эффективности, рекомендации по организации системы защиты (организационных и технических мер защиты) персональных данных находится в стадии исполнения в ФГБОУ ВО «Южно□Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

Выводы по второй главе

В соответствии с анализом рисков и уязвимости системы защиты персональных данных, а также выявленными нарушениями требований нормативных документов в области защиты информации в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации были предложены рекомендации организации системы защиты (организационных и технических мер защиты) персональных данных, в результате выполнения которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты ПДн;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты ПДн;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

– организация ИСПДн в образовательной организации высшего образования;

– введение в СЗПДн новые нормативные документы для обеспечения безопасности ПДн.

Рекомендации по организации системы защиты персональных данных реализуются в 3 этапа.

Этап 1. Разработка организационно-распорядительных документов по защите персональных данных.

1. Разработать порядок действий при компрометации ключевой информации.

2. Разработать памятку пользователя СКЗИ.

3. Разработать схему криптографической защиты.

4. Подготовить приказы о вводе СКЗИ в эксплуатацию.

5. Разработать журнал учета СКЗИ, эксплуатационной и технической документации к ним.

6. Разработать порядок уничтожения СКЗИ и ключевых документов.

7. Разработать инструкцию по проведению внутренних проверок состояния защиты персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Провести обучение пользователей правилам работы с СКЗИ.

Этап 3. Усовершенствование физических мер по защите персональных данных.

1. Разработать инструкцию по физической охране и правилам доступа в специальные помещения.

2. Разработать журнал лиц, имеющих право доступа в специальные помещения, для выполнения своих должностных обязанностей.

3. Оборудовать двери специальных помещений и хранилищ приспособлениями для опечатывания.

4. Оборудовать сейфы, предназначенные для хранения СКЗИ, эксплуатационной и технической документации к ним, приспособлениями для опечатывания замочных скважин.

В ходе оценки эффективности, при помощи метода экспертной оценки, были рассмотрены такие показатели качества как:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Методическая составляющая рекомендаций по организации системы защиты ПДн: содержательная и функциональная валидность предложенных

мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн.

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений.

По результатам экспертной оценки эффективности, рекомендации по организации системы защиты (организационных и технических мер защиты) персональных данных находится в стадии исполнения в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

ЗАКЛЮЧЕНИЕ

Для проведения исследования были поставлены и решены следующие задачи:

1. Рассмотрены понятие и значение защищенности информационных систем персональных данных в образовательной организации.

2. Изучены нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.

3. Определены этапы организации защищенности информационных систем персональных данных в образовательной организации.

4. Проведена оценка информационной безопасности персональных данных в ФГБОУ ВО «Южно-уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

5. Разработаны предложения по созданию системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.

6. Оценена результативность рекомендаций по организации системы надежности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ» г. Челябинска.

На сегодняшний день уровень защиты персональных данных как в государственных, так и в частных образовательных организациях высшего образования низкий и недостаточный. Проблема заключается в нехватке финансовых ресурсов, недостатке информированности руководителей организаций о необходимых мерах, сложности реализации и поддержки проектов.

В рамках нашего исследования персональные данные рассматриваются, как различная информация, которая прямо или косвенно относятся к определенному физическому лицу, т.е. субъекту персональных данных.

Под обработкой персональных данных понимается любое действие (операция) или их совокупность, с применением средств автоматизации или без них для их сбора, хранения, использования, предоставления, удаления.

Этапы организации защиты персональных данных в образовательной организации.

Этап 1. Инвентаризация информационных ресурсов.

Этап 2. Ограничение доступа работников к персональным данным.

Этап 3. Документальное регламентирование работы с персональными данными.

Этап 4. Формирование модели угроз безопасности персональных данных.

Этап 5. Классификация ИСПДн.

Этап 6. Составление и отправка в уполномоченный орган уведомления.

Этап 7. Приведение системы в соответствие с требованиями регуляторов.

Этап 8. Аттестация (сертификация) ИСПДн.

Этап 9. Организация эксплуатации ИСПДн и контроля за безопасностью.

Базой исследования являлся ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

В Университете введены в эксплуатацию следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ» (далее - ИСПДн «ФИС ФЦТ»).

2. ИСПДн «Обучающиеся и абитуриенты» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Обучающиеся и абитуриенты»).

3. ИСПДн «Сотрудники» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Сотрудники»).

4. ИСПДн «Библиотека» ФГБОУ ВО ЮУГМУ (далее - ИСПДн «Библиотека»).

Система защиты персональных данных при их обработке в информационных системах персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Южно-Уральский государственный медицинский университет» создана, но эксплуатация используемых криптосредств, обращение с СКЗИ осуществлялась с нарушениями требований нормативных документов в области защиты информации.

Во второй главе магистерской диссертации по анализу рисков и уязвимости системы защиты персональных данных, а также выявленных нарушений требований нормативных документов в области защиты информации в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации были предложены рекомендации организации системы защиты (организационных и технических мер защиты) персональных данных, в результате выполнения которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты ПДн;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты ПДн;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

– организация ИСПДн в образовательной организации высшего образования;

– введение в СЗПДн новые нормативные документы для обеспечения безопасности ПДн.

Рекомендации по организации системы защиты персональных данных состоит из 3 этапов.

В рамках рекомендаций был составлен определенный пакет документов, и внедрены внутренние приказы и распоряжения, позволившие правильно выстроить работу персонала и ответственных за обработку данных лиц.

В ходе оценки эффективности, при помощи метода экспертной оценки, были рассмотрены такие показатели качества как:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Методическая составляющая рекомендаций по организации системы защиты ПДн: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн.

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений.

По результатам экспертной оценки эффективности, рекомендации по организации системы защиты (организационных и технических мер защиты) персональных данных находится в стадии исполнения в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций высшего образования с целью совершенствования информационной безопасности.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022) (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 3

2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3451

3. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448

4. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Собрание законодательства РФ, 22.09.2008, № 38, ст. 4320

5. Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ, 02.04.2012, № 14, ст. 1626

6. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «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 № 28375) // Российская газета, № 107, 22.05.2013

7. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 № 33620) // Российская газета, № 211, 17.09.2014

8. Абдулова, Э. Д. Правовое регулирование в сфере защиты персональных данных / Э. Д. Абдулова // Молодой ученый. – 2022. – № 5(400). – С. 151-154.

9. Алимбаев, В. В. Организация защиты персональных данных и ответственность за несоблюдение требований законодательства в области защиты персональных данных / В. В. Алимбаев, Е. В. Листопадова // Природа. Человек. Культура : Материалы Третьего Международного научно-просветительского форума, Кисловодск, 04–08 октября 2022 года / Под общей редакцией С.Е. Туркулец, Е.В. Листопадовой. – Хабаровск: Дальневосточный государственный университет путей сообщения, 2022. – С. 176-182.

10. Антонова, В. В. Проблемы и решения правового регулирования защиты персональных данных / В. В. Антонова // Учет и контроль. – 2022. – № 3. – С. 15-17.

11. Бакланова, Н. А. Конституционно-правовое регулирование права на защиту персональных данных в РФ и странах Восточной Европы / Н. А. Бакланова, Д. В. Кононенко // Международный журнал гуманитарных и естественных наук. – 2022. – № 6-2(69). – С. 26-28.

12. Васильев, И. Д. Организация защиты персональных данных в будущем / И. Д. Васильев // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 34. – С. 1100-1105.

13. Воронина, И. А. Приватность в сети Интернет как способ защиты персональных данных / И. А. Воронина, А. В. Кирпичникова // Право и государство: теория и практика. – 2022. – № 12(216). – С. 95-96.

14. Газизов, А. Р. Аппаратно-программные методы защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем "сниффинг-атак / А. Р. Газизов // . – 2022. – Т. 49, № 3. – С. 52-60.

15. Гармаш, С. В. Правовые аспекты защиты персональных данных несовершеннолетних / С. В. Гармаш // Информатизация образования и науки. – 2022. – № 4(56). – С. 12-18.

16. Горбачева, С. В. Защита персональных данных в Российской Федерации: теоретико-правовые основы и перспективы развития / С. В. Горбачева // Четвертый конгресс цивилистов правоохранительных органов : Материалы Всероссийской научно-практической конференции с международным участием, Нижний Новгород - Барнаул, 24–25 марта 2022 года. – Москва: Общество с ограниченной ответственностью "Русайнс", 2022. – С. 184-188.

17. Дьячковская, Л. П. Система защиты персональных данных на предприятии / Л. П. Дьячковская, Л. Е. Яковлева // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 35. – С. 842-864.

18. Егоров, П. А. Вопросы цифровизации. Защита персональных данных в современных реалиях / П. А. Егоров // XXXV international Plekhanov readings : Юбилейный сборник статей аспирантов и молодых ученых на английском языке, Moscow, 25 марта 2022 года. – Moscow:

Российский экономический университет имени Г.В. Плеханова, 2022. – Р. 33-37.

19. Задорожний, О. Г. Правовые основы защиты персональных данных в Российской Федерации / О. Г. Задорожний // Правовая позиция. – 2022. – № 10(34). – С. 113-118.

20. Казанцев, Е. А. Защита персональных данных в рамках информационной безопасности / Е. А. Казанцев, Г. Д. Евстигнеев, В. А. Шутов // Уральский научный вестник. – 2022. – Т. 3, № 5. – С. 68-71.

21. Кайбышева, Э. Р. Законодательные акты, регламентирующие деятельность по организации защиты персональных данных / Э. Р. Кайбышева // . – 2022. – № 6-2(198). – С. 19-20.

22. Карпова, Е. В. Защита персональных данных работников / Е. В. Карпова, А. Г. Некрасова, Л. Д. Самойлова // Актуальные вопросы теории и практики финансово-хозяйственной деятельности : Сборник материалов IV Всероссийской (национальной) научно-практической конференции, Воронеж, 30 марта 2022 года. – Воронеж, 2022. – С. 154-157.

23. Ковалев, С. Д. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России в цифровую эпоху / С. Д. Ковалев // Вестник Владимирского юридического института. – 2022. – № 4(65). – С. 33-39. – EDN IBDAWL.

24. Кудина, А. А. Правовые основы защиты персональных данных / А. А. Кудина // Актуальные исследования. – 2022. – № 49-2(128). – С. 19-22.

25. Кулаченко, И. А. Угрозы безопасности персональных данных физического лица и их защита / И. А. Кулаченко // Научно-исследовательский центр "Вектор развития". – 2022. – № 8. – С. 152-156.

26. Маврин, А. В. Современные проблемы информационной безопасности, связанные с защитой персональных данных пользователя / А. В. Маврин // StudNet. – 2022. – Т. 5, № 6. – С. 109.

27. Максимова, В. С. Проблемы защиты персональных данных несовершеннолетних в цифровой действительности и пути их решения / В. С. Максимова, И. А. Гусева // Молодежный вестник ИрГТУ. – 2022. – Т. 12, № 3. – С. 640-644.

28. Полякова, Т. А. Защита прав субъектов персональных данных: новеллы правового регулирования / Т. А. Полякова, И. С. Бойченко // Информационное право. – 2022. – № 3(73). – С. 10-13.

29. Постникова, Ю. В. Меры защиты персональных данных работника / Ю. В. Постникова // Проблемы государственно-правового строительства в современной России: анализ, тенденции, перспективы : Сборник материалов VII Международной научно-практической конференции, Курск, 08 апреля 2022 года. – Курск: Юго-Западный государственный университет, 2022. – С. 114-116.

30. Прокопец, Г. К. Конституционные права человека на свободу информации и защиту персональных данных в цифровую эпоху / Г. К. Прокопец // Научный Лидер. – 2022. – № 35(80). – С. 111-113.

31. Свидетельство о государственной регистрации программы для ЭВМ № 2022664705 Российская Федерация. Программное средство "Правовые основы защиты персональных данных" : № 2022664160 : заявл. 19.07.2022 : опубл. 03.08.2022 / Э. А. Юнусов, Е. Г. Царькова, М. В. Лебедев ; заявитель Федеральное казенное учреждение «Научно-исследовательский институт Федеральной службы исполнения наказаний».

32. Свидетельство о государственной регистрации программы для ЭВМ № 2022663313 Российская Федерация. Программное обеспечение для защиты персональных данных в муниципальных информационных системах : № 2022662892 : заявл. 06.07.2022 : опубл. 13.07.2022 / В. М. Герасимов.

33. Свиридова, Е. А. Защита персональных данных в условиях цифровой трансформации общественных отношений / Е. А. Свиридова //

Проблемы экономики и юридической практики. – 2022. – Т. 18, № 6. – С. 53-58.

34. Сейдалиев, Г. Д. Правовая защита персональных данных в Российской Федерации / Г. Д. Сейдалиев, А. Е. Мун // Молодой ученый. – 2022. – № 18(413). – С. 350-352.

35. Семелькина, П. Д. Система распознавания лиц в контексте прав человека на защиту персональных данных / П. Д. Семелькина // Теория и практика современной науки. – 2022. – № 10(88). – С. 125-129.

36. Семенов, Е. Ю. Совершенствование правовых и организационных аспектов защиты персональных данных в Российской Федерации / Е. Ю. Семенов // Закон и право. – 2022. – № 1. – С. 94-96. – DOI 10.24412/2073-3313-2022-1-94-96. – EDN ZFPRGE.

37. Сивцова, А. Ю. Право на защиту персональных данных осужденных к лишению свободы: итоги анкетного исследования / А. Ю. Сивцова // Вестник Самарского юридического института. – 2022. – № 5(51). – С. 124-128.

38. Соболев, А. А. Защита персональных данных в организации, обработанных в электронном виде / А. А. Соболев // . – 2022. – № 11. – С. 134-142.

39. Соколова, А. В. Обзор методов и средств защиты персональных данных / А. В. Соколова, Д. Д. Гришкевич, И. М. Губенко // Информационное общество. – 2022. – № 3. – С. 90-97.

40. Таранов, Я. Р. Анализ защиты персональных данных и оптимизация хранения информационных ресурсов / Я. Р. Таранов // Научный Лидер. – 2022. – № 9(54). – С. 7-9.

41. Фастович, Г. Г. Защита персональных данных в системе высшего образования / Г. Г. Фастович // Наука и образование: опыт, проблемы, перспективы развития : Материалы международной научно-практической конференции, посвященной 70-летию ФГБОУ ВО Красноярский ГАУ,

Красноярск, 19–21 апреля 2022 года. – Красноярск: Красноярский государственный аграрный университет, 2022. – С. 250-252.

42. Храмцова, М. А. Защита персональных данных в Российской Федерации / М. А. Храмцова // Синергия Наук. – 2022. – № 77. – С. 228-237.

43. Шагапов, И. Р. Защита персональных данных в условиях развития цифровой экономики / И. Р. Шагапов // Международный журнал гуманитарных и естественных наук. – 2023. – № 1-3(76). – С. 153-155.

44. Шаханова, М. В. Система защиты персональных данных на предприятии / М. В. Шаханова, В. А. Белинцов, Э. С. Шаханова // Научный Альманах ассоциации France-Kazakhstan. – 2022. – № 5. – С. 252-265..

45. Шипулин, Г. Ф. Проблемы защиты персональных данных граждан в Российской Федерации / Г. Ф. Шипулин // Научный аспект. – 2022. – Т. 12, № 6. – С. 1550-1555

46. Шкуренев, Ю. С. Проблемы прокурорского надзора за соблюдением законов о защите персональных данных в сети Интернет / Ю. С. Шкуренев // Студенческий вестник. – 2022. – № 41-4(233). – С. 41-42.

47. Ястребова, А. Ю. Осуществление права человека на защиту персональных данных: отдельные международно-правовые аспекты, опыт России и СНГ / А. Ю. Ястребова, И. О. Анисимов // Вестник ученых-международников. – 2022. – № 3(21). – С. 241-266.

Приложение А

Требования законодательства Российской федерации

Название документа	Административные требования	Технические требования
Федеральный закон от 27.07.2006 №152 - ФЗ «О персональных данных»	Назначение оператором ответственного за обработку персональных данных	Обнаружение фактов несанкционированного доступа и принятие мер
	Издание оператором документов, определяющим его политику безопасности в области обработки персональных данных	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
	Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных	Создание информационной системы обработки персональных данных
	Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных	
	Публикация или осуществление беспрепятственного доступа к документу, определяющего политику безопасности в области обработки персональных данных оператора	
	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы	
	Учет машинных носителей персональных данных	Обеспечение сохранности носителей персональных данных
Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных	Организация режима обеспечения безопасности помещений	Использование средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз
	Утверждение руководителем документа, определяющего перечень лиц, допущенных к обработке персональных данных	Наличие электронного журнала безопасности
	Ограничение доступа к журналу безопасности	
	Определение класса информационной системы	

данных	персональных данных	
Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Идентификация и аутентификация субъектов доступа и объектов доступа	Ограничение программной среды
	Управление доступом субъектов доступа к объектам доступа	Защита машинных носителей
	Регистрация событий безопасности	Управление конфигурацией информационной системы
	Контроль безопасности персональных данных	Антивирусная защита
	Выявление инцидентов	Системы Обнаружения вторжений (ids/ips)
		Защита среды виртуализации
Приказ ФСБ России от 10.07.2014 №378	Утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях	Оснащение помещений входными дверьми с замками
	Утверждение перечня лиц, имеющих право доступа в Помещение	Хранение носителей персональных данных в сейфах, оборудованных внутренними замками
	Ведение журнала учета носителей персональных данных	Обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей на получение персональных данных
Приказ ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке при их обработке в информационных системах с использованием средств криптографической защиты	Поддержание в актуальном состоянии документ, определяющий перечень лиц, допущенных к работе с персональными данными	Обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений
	Назначение обладающего достаточными навыками должностного лица оператора ответственным за обеспечение безопасности персональных данных в информационной системе	Обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения
	Обеспечение периодического контроля работоспособности	Полномочий сотрудника оператора по доступу к

информации, необходимых для выполнения установленных Правительством Российской Федерации	автоматизированных средств	персональным данным, содержащимся в информационной системе
	Назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям	Оборудование окнами и дверьми Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения
Постановление Правительства от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"	Необходимо обеспечивать раздельное хранение персональных данных, обработка которых осуществляется в различных целях	
	Не допускается фиксация на одном материальном носителе персональных данных, цели обработки заведомо не совместимы	
	Лица, осуществляющие обработку, должны быть проинформированы о факте обработки ими персональных данных	
Постановление Правительства от 21.03.2012 №211 "Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами являющимися государственными или муниципальными органами	Должны быть утверждены правила обработки персональных данных, устанавливающие процедуры, направление на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных	
	Должны быть утверждены правила рассмотрения запросов субъектов персональных данных или их представителей	
	Должны быть утверждены правила обезличивания персональных данных	
	Должны быть утверждены правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	
	Должен быть утвержден должностной регламент	

	(должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных	
	Должна быть утверждена типовая форма согласия на обработку персональных данных сотрудников или иных субъектов персональных данных	
	Должен быть определен порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных	
«Трудовой кодекс Российской Федерации» от 30.12.2001 №197-ФЗ	Работники должны быть ознакомлены под роспись с документами организации, устанавливающие порядок обработки ПДн	

Приложение Б

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Обучающиеся и абитуриенты» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([7]-[8]) и ФСБ России ([6]) и нормативного правового акта ФСБ России ([10]), регламентирующих порядок обеспечения безопасности ПДн, в том числе определения актуальных угроз их безопасности и формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак.

Настоящая модель угроз безопасности ПДн при их обработке в ИСПДн «Обучающиеся и абитуриенты» (далее – Модель угроз) содержит систематизированный перечень УБПДн при их обработке в ИСПДн. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности ПДн, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по УБПДн при их обработке в ИСПДн, связанным:

- с использованием СКЗИ;
- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора ПДн, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана на основе [6] и [8] с использованием [7] для конкретной ИСПДн с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ПДн при их обработке в ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности ПДн.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов

неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

УБПДн при их обработке в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [8]. Кроме того, Модель угроз может быть пересмотрена по решению оператора (владельца) ИСПДн на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн.

Описание ИСПДн

Наименование ИСПДн и её оператора (владельца)

Наименование ИСПДн: «Обучающиеся и абитуриенты».

Наименование оператора (владельца) ИСПДн: Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

Местонахождение ИСПДн

ИСПДн «Обучающиеся и абитуриенты» размещена по адресам:

- ул. Воровского, 64 (первый корпус, второй корпус, теплый переход);
- ул. Воровского, 66 (третий корпус);
- ул. Варненская, 10 (морфокорпус).

Взаимодействие ИСПДн с внешними информационными системами

ИСПДн «Обучающиеся и абитуриенты» осуществляет однонаправленную передачу ПДн в ПАО «Челябинвестбанк» с применением СКЗИ.

Принципы модели угроз

Согласно [6] в основе Модели угроз в аспектах, касающихся использования криптосредств, лежат следующие общие принципы:

1) Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн (п. 2.2 документа [6]).

2) При формировании модели угроз необходимо учитывать, как угрозы, осуществление которых нарушает безопасность ПДн (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) ПДн обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5) Система защиты ПДн не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, криптосредство не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в [6] понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Для обеспечения безопасности ПДн при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

Модель угроз безопасности ПДн верхнего уровня

Данный раздел определяет характеристики безопасности защищаемых ПДн и других объектов защиты.

Используемые в ИСПДн информационные технологии создания и использования ПДн

Используются нижеуказанные информационные технологии:

Таблица 1. Программное обеспечение.

ПО1	Кл.-банк Челябинвестбанк, ФРМР, 1С:Предприятие 8.3, СТЭК -2011.1, БД 1С MS SQL 2017, СТЭК-Траст
ПО2	Клиентские операционные системы семейства Microsoft Windows (Microsoft Windows XP, Microsoft Windows 7 Pro, Microsoft Windows 10)
ПО3	Серверные операционные системы Microsoft Windows Server 2012 R2 Standard, 2003 R2, 2016
ПО4	Пакет офисного ПО Microsoft Office
ПО5	Браузеры
ПО6	Средство криптографической защиты информации «КриптоПро CSP» версия 4.0, Континент TLS, JINN-клиент, СКЗИ Кл.-банк Челябинвестбанк

Таблица 2. Технические средства.

ТС1	Рабочие станции
ТС2	Серверы

Формы представления ПДн в ИСПДн

ПДн имеют в ИСПДн ряд форм фиксации. Данные формы представлены в таблице.

Таблица 3. Формы фиксации.

№ п/п	Формы фиксации	Обозначение
1	Базы данных	ФФ1
2	Локальные документы	ФФ2
3	Оперативная память	ФФ3

Информация, сопутствующая процессам создания и использования ПДн

В процессе обработки ПДн используется и появляется сопутствующая информация. Типы данной информации применительно к ИСПДн приведены в таблице.

Таблица 4. Сопутствующая информация.

№ п/п	Сопутствующая информация	Обозначение
1	Информация в электронных журналах регистрации	СИ1
2	Ключевая, аутентифицирующая и парольная информация криптосредства	СИ2
3	Конфигурационная информация	СИ3

№ п/п	Сопутствующая информация	Обозначение
4	Криптографически опасная информация (КОИ)	СИ4
5	Остаточная информация на носителях информации	СИ5
6	Побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация	СИ6
7	Резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих фалов	СИ7
8	Управляющая информация	СИ8

Характеристики безопасности объектов угроз

В данном подразделе устанавливаются характеристики безопасности объектов угроз.

Список характеристик безопасности:

Таблица 5. Характеристики безопасности объектов угроз.

№ п/п	Значение	Обозначение
1	Адекватность	ХАР1
2	Аутентичность	ХАР2
3	Доступность	ХАР3
4	Конфиденциальность	ХАР4
5	Неотказуемость	ХАР5
6	Учетность	ХАР6
7	Целостность	ХАР7

а) Характеристики безопасности программного обеспечения ИСПДн:

Таблица 6. Характеристики безопасности программного обеспечения.

ПО\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ПО1	+	+	+	+	-	+	+
ПО2	+	+	+	+	-	+	+
ПО3	+	+	+	+	-	+	+
ПО4	+	+	+	+	-	+	+
ПО5	+	+	+	+	-	+	+
ПО6	+	+	+	+	+	+	+

б) Характеристики безопасности технических средств ИСПДн:

Таблица 7. Характеристики безопасности технических средств.

ТС\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ТС1	+	+	+	+	+	+	+
ТС2	+	+	+	+	-	+	+

в) Характеристики безопасности защищаемой информации (ПДн и сопутствующей информации):

Таблица 8. Характеристики безопасности защищаемой информации.

Объект\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ФФ1	+	+	+	+	+	+	+
ФФ2	+	+	+	+	+	+	+
ФФ3	+	+	+	+	-	+	+
СИ1	+	+	+	+	-	+	+

Объект\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
СИ2	+	+	+	+	+	+	+
СИ3	+	+	+	+	-	+	+
СИ4	+	+	+	+	+	+	+
СИ5	+	+	+	+	-	+	+
СИ6	+	+	+	+	-	+	+
СИ7	+	+	+	+	-	+	+
СИ8	+	+	+	+	-	+	+

Факторы угроз, не являющихся атаками

Все рассматриваемые угрозы в данном разделе могут повлечь в какой-то мере случайное нарушение характеристик безопасности объектов. Предполагается, что отсутствует заинтересованный нарушитель. Поэтому, если воздействие фактора непосредственно не приводит к нарушению характеристики, то считается, что угрозы нет.

Рассматриваются следующие факторы угроз, не являющихся атаками:

Таблица 9. Факторы угроз, не являющихся атаками.

№ п/п	Фактор	Обозначение
1	внедрение и использование неучтенных программ	ФР1
2	нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	ФР2
3	настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	ФР3
4	негативные социальные явления могут создать предпосылки для невозможности работы ИСПДн – отключения электроэнергии, нарушение работы каналов связи	ФР4
5	неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.	ФР5
6	непредумышленное искажение или удаление программных компонентов АСЗИ	ФР6
7	несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа	ФР7
8	помехи и наводки, приводящие к сбоям в работе аппаратных средств	ФР8
9	предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	ФР9
10	разрушения от ветра, попадания молнии в объекты инфраструктуры, обрывы проводов могут привести к нарушению электропитания ИСПДн, обрыву связи с сетями общего пользования	ФР10
11	техногенные аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.)	ФР11

Данные факторы могут воздействовать на объекты угроз, с нарушением характеристик безопасности.

Списки угроз, не являющихся атаками, приведены в разделе «Список угроз по модели нарушителя».

Защита от угроз, не являющихся атаками, в основном регламентируется инструкциями и распорядительными документами, разработанными с учетом особенностей эксплуатации ИСПДн и действующей нормативной базы. При этом по возможности также используются инженерно-технические меры.

Модель нарушителя

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

Объекты атак

В качестве объектов атак рассматриваются защищаемые ПДн, сопутствующая информация, ПО ИСПДн, технические средства ИСПДн, помещения, в которых размещены технические средства.

Субъекты атак

В качестве субъектов атак рассматриваются физические лица, имеющие доступ к техническим и программным средствам ИСПДн:

Таблица 10. Субъекты атак.

№ п/п	Субъект	Категория	Внутренний	Внешний	Условное обозначение
1	Администратор	2	+	+	СА1
2	Пользователь	2	+	-	СА2
3	Посетитель	2	+	-	СА3

Пояснения:

категория 1 – лица, не имеющие права доступа в контролируемую зону ИСПДн;

категория 2 – лица, имеющие право постоянного или разового доступа в контролируемую зону ИСПДн;

внешние нарушители – нарушители, осуществляющие атаки из-за пределов контролируемой зоны ИСПДн;

внутренние нарушители – нарушители, осуществляющие атаки, находясь в пределах контролируемой зоны ИСПДн.

К привилегированным пользователям ИСПДн, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями, относится администратор.

К Администраторам ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число Администраторов будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Возможность сговора субъектов атак представлена в виде таблицы:

Таблица 11. Возможность сговора.

Субъект	СА2	СА3
СА2	-	+
СА3	+	-

Пояснения:

"-" – сговор между субъектами атаки невозможен: субъекты не могут иметь общих интересов; субъекты не встречаются в реальном мире; сферы деятельности субъектов не позволяют им действовать сообща; крайне низкая вероятность сговора; ЛИБО у субъектов атаки имеется возможность организовать сговор, но сговор не позволяет им объединить знания и (или) возможности для проведения совместной атаки, либо сговор не дает новых знаний и (или) возможностей для проведения атаки;

"+" – сговор между субъектами атаки возможен.

Таким образом, получаются следующие возможности для сговора:

Таблица 12. Возможности для сговора.

Значение	Условное обозначение
Пользователь	СА2
Посетитель	СА3
Сговор(<Пользователь>, <Посетитель>)	СА4

Возможности доступа:

Таблица 13. Возможности доступа

Субъект\\объект	ФФ1	ФФ2	ФФ3	СИ1	СИ2	СИ3	СИ4	СИ5	СИ6	СИ7	СИ8
СА1	+	+	+	+	+	+	+	+	+	+	+
СА2	+	+	+	+	+	+	+	+	+	+	+
СА3	-	-	-	-	-	-	-	-	-	-	-
СА4	+	+	+	+	+	+	+	+	+	+	+

Внешний нарушитель может принимать участие в любом из сговоров с целью получения дополнительных возможностей для проведения атаки, становиться связующим звеном для любого из сговоров.

Наибольшие возможности нарушители получают при множественном сговоре. Соответственно наиболее опасны именно такие сговоры, хотя их вероятность ниже двусторонних сговоров.

Предположения об имеющейся у нарушителя информации об объектах атак

Нарушители обладают полной информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты.

Список имеющейся у нарушителя информации:

Таблица 14. Список имеющейся у нарушителя информации

№ п/п	Информация	Обозначение	Обоснование
1	Содержание технической документации на технические и программные компоненты СФК	ОИ1	-
2	Долговременные ключи криптосредства	ОИ2	-
3	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.)	ОИ3	-
4	Сведения о линиях связи, по которым передается защищаемая информация	ОИ4	-
5	Все сети связи, работающие на едином ключе	ОИ5	-

№ п/п	Информация	Обозначение	Обоснование
6	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК	ОИ6	-
7	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства и СФК	ОИ7	-
8	Сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель	ОИ8	-

Ограничения на имеющуюся у нарушителя информацию об объектах атак удобно представить в виде таблицы:

Таблица 15. Ограничения на имеющуюся у нарушителя информацию

Субъект	ОИ1	ОИ2	ОИ3	ОИ4	ОИ5	ОИ6	ОИ7	ОИ8
СА2	+	+	+	+	-	+	+	-
СА3	-	-	+	-	-	+	+	-
СА4	+	+	+	+	-	+	+	-

где:
"+" – нарушитель располагает информацией;
"-" – нарушитель не располагает информацией.
Обоснования ограничений:

Таблица 16. Обоснование ограничений на имеющуюся у нарушителя информацию

№ п/п	Субъект	Информация	Обоснование
1	СА2	ОИ5	не имеет доступа к средствам конфигурирования защищенной сети и средствам управления конфигурацией этой сети
2	СА2	ОИ8	не имеет в распоряжении специального оборудования
3	СА3	ОИ1	не располагают технической документацией и компонентами СФК
4	СА3	ОИ2	не имеет доступа к СКЗИ, носителям ключевой и аутентифицирующей информации
5	СА3	ОИ4	не располагает данной информацией
6	СА3	ОИ5	не имеет доступа к средствам конфигурирования защищенной сети, не обладают достаточными знаниями в этой области
7	СА3	ОИ8	не имеют в распоряжении специального оборудования

Предположения об имеющихся у нарушителя средствах атак

Нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Список имеющихся у нарушителя средств атак:

Таблица 17. Список имеющихся у нарушителя средств атак

№ п/п	Информация	Обозначение	Обоснование
1	Аппаратные компоненты криптосредства и СФК	СПА1	-
2	Доступные в свободной продаже технические средства и программное обеспечение	СПА2	-
3	Специально разработанные технические средства и программное обеспечение	СПА3	-
4	Штатные средства	СПА4	-

При этом имеются следующие ограничения на имеющиеся у нарушителей средства атак:

Таблица 18. Ограничения на имеющиеся у нарушителей средства атак

№ п/п	Субъект\\Средство	СПА1	СПА2	СПА3	СПА4
1	СА2	-	+	-	+
2	СА3	-	+	-	+
3	СА4	-	+	-	+

где:
"+" – нарушитель располагает средством атаки;
"-" – нарушитель не располагает средством атаки.

Обоснования ограничений:

Таблица 19. Обоснование ограничений на имеющиеся у нарушителей средства атак

№ п/п	Субъект	Информация	Обоснование
1	СА2	СПА1	доступ ограничен организационно-техническими мерами
2	СА2	СПА3	не имеет возможности использования и разработки
3	СА3	СПА1	доступ ограничен организационно-техническими мерами
4	СА3	СПА3	не имеет возможности использования и разработки

Каналы атак

Описание каналов атак.

Таблица 20. Каналы атак

№ п/п	Канал атаки	Обозначение	Обоснование
1	Каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами	КА1	-
2	Штатные средства	КА2	-
3	Каналы непосредственного доступа к объекту атаки (акустический, визуальные, физический)	КА3	-
4	Машинные носители информации	КА4	-
5	Носители информации, выведенные из употребления	КА5	-
6	Технические каналы утечки	КА6	-
7	Сигнальные цепи	КА7	-
8	Цепи электропитания	КА8	-
9	Цепи заземления	КА9	-

№ п/п	Канал атаки	Обозначение	Обоснование
10	Канал утечки за счет электронных устройств негласного получения информации	КА10	-
11	Информационные и управляющие интерфейсы СВТ	КА11	-

Ограничения на доступ к каналам атаки.

В силу действующих правил доступ и должностных обязанностей таблица доступа к каналам атаки выглядит следующим образом:

Таблица 21. Таблица доступа к каналам атаки

Субъект\\Канал	КА1	КА2	КА3	КА4	КА5	КА6	КА7	КА8	КА9	КА10	КА11
СА2	+	+	+	+	+	+	+	+	+	+	+
СА3	+	+	+	+	+	+	+	+	+	+	+
СА4	+	+	+	+	+	+	+	+	+	+	+

где:

“+” – нарушитель имеет возможность воспользоваться каналом атаки;

“-” – нарушитель не имеет возможности воспользоваться каналом атаки.

Тип нарушителя

Исходя из возможностей, устанавливаются следующие типы нарушителей:

Таблица 22. Тип нарушителя.

№ п/п	Субъект атаки	Категория	Внутренний	Внешний	Тип нарушителя
1	СА2	2	+	-	Н2
2	СА3	2	+	-	Н2
3	СА4	2	+	-	Н2

Угрозы, возникающие на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК, приведены в разделе «Список угроз по модели нарушителя».

Угрозы, связанные с моделью нарушителя и возникающие на этапе эксплуатации, приведены в разделе «Список угроз по модели нарушителя».

Список угроз по модели нарушителя

Разные факторы случайных воздействий могут приводить к реализации схожих угроз. В результате анализа характеристик факторов случайных воздействий и особенностей функционирования ИСПДн, факторы случайных воздействий сгруппированы в списки, которые представлены в таблице.

Таблица 23. Факторы случайных воздействий.

№ п/п	Название списка	Элементы списка
1	Список "Факторы 1"	ФР10, ФР4, ФР6, ФР1, ФР2, ФР9, ФР3, ФР7, ФР11, ФР5, ФР8

На разные объекты атак могут быть направлены схожие угрозы. В результате анализа характеристик объектов атак и особенностей функционирования ИСПДн, объекты атак сгруппированы в списки, которые представлены в таблице.

Таблица 24. Объекты атак.

№ п/п	Название списка	Элементы списка
1	Список "Объекты доступа 1"	ТС1, ПО2, ФФ1, СИ2, ТС2, ПО4, ФФ2, СИ4, ФФ3, СИ3, СИ8, ПО5, СИ1, ПО6, СИ6, ПО1, СИ7, ПО3, СИ5
2	Список "Объекты доступа 2"	ТС1, ПО2, ФФ1, СИ2, ПО4, ФФ2, СИ4, ФФ3, СИ3, СИ8, ПО5, СИ1, ПО6, СИ6, ПО1, СИ7, СИ5
3	Список "Объекты доступа 3"	ТС1, ФФ1, СИ2, ФФ2, СИ4, ПО6
4	Список "Объекты доступа 4"	ТС1, ПО6
5	Список "Объекты доступа 5"	ПО2, ТС2, ПО4, ПО5, ПО1
6	Список "Объекты доступа 6"	ФФ1, СИ2, ФФ2, ФФ3, СИ3, СИ1
7	Список "Объекты доступа 7"	ФФ1, ФФ2
8	Список "Объекты доступа 8"	СИ2, СИ4
9	Список "Объекты доступа 9"	СИ2, СИ4, ФФ3, СИ3, СИ8, СИ1, СИ6, СИ7, СИ5
10	Список "Объекты доступа 10"	СИ4, СИ8, СИ6, СИ7, ПО3, СИ5
11	Список "Объекты доступа 11"	СИ4, СИ8, СИ6, СИ7, СИ5
12	Список "Объекты доступа 12"	ПО3

Для разных объектов атак могут быть установлены схожие характеристики безопасности. В результате анализа характеристик безопасности и особенностей функционирования ИСПДн, характеристики безопасности сгруппированы в списки, которые представлены в таблице.

Таблица 25. Характеристики безопасности.

№ п/п	Название списка	Элементы списка
1	Список "Характеристики безопасности 1"	ХАР4, ХАР7, ХАР3, ХАР6
2	Список "Характеристики безопасности 2"	ХАР4, ХАР7, ХАР3, ХАР6, ХАР1, ХАР5, ХАР2
3	Список "Характеристики безопасности 3"	ХАР4, ХАР7, ХАР3, ХАР6, ХАР1, ХАР2
4	Список "Характеристики безопасности 4"	ХАР4, ХАР3
5	Список "Характеристики безопасности 5"	ХАР4, ХАР3, ХАР1, ХАР2
6	Список "Характеристики безопасности 6"	ХАР7, ХАР6
7	Список "Характеристики безопасности 7"	ХАР7, ХАР6, ХАР5

№ п/п	Название списка	Элементы списка
8	Список "Характеристики безопасности 8"	ХАР1, ХАР2
9	Список "Характеристики безопасности 9"	ХАР5

Разные субъекты могут пытаться осуществить схожие атаки и обладать схожими возможностями и навыками. В результате анализа характеристик субъектов атак и особенностей функционирования ИСПДн, субъекты атак сгруппированы в списки, которые представлены в таблице.

Таблица 26. Субъекты атак.

№ п/п	Название списка	Элементы списка
1	Список "Субъекты доступа 1"	СА2
2	Список "Субъекты доступа 2"	СА3

Одна и та же информация может быть известна разным субъектам атак. В результате анализа информации, известной субъектам атак, и особенностей функционирования ИСПДн, сведения сгруппированы в списки, которые представлены в таблице.

Таблица 27. Информация, известная субъектам атак.

№ п/п	Название списка	Элементы списка
1	Список "Информация 1"	ОИ2, ОИ3, ОИ4, ОИ6, ОИ7, ОИ8
2	Список "Информация 2"	ОИ3, ОИ6, ОИ7

Одни и те же средства проведения атак могут быть известны быть использованы разными субъектами атак. В результате анализа средств проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, средства проведения атак сгруппированы в списки, которые представлены в таблице.

Таблица 28. Средства проведения атак.

№ п/п	Название списка	Элементы списка
1	Список "Средства атаки 1"	СПА1, СПА2, СПА3, СПА4

Одни и те же каналы проведения атак могут быть использованы разными субъектами атак. В результате анализа каналов проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, каналы проведения атак сгруппированы в списки, которые представлены в таблице.

Таблица 29. Каналы проведения атак.

№ п/п	Название списка	Элементы списка
1	Список "Каналы атак 1"	КА1, КА2, КА3, КА4, КА5, КА6, КА7, КА8, КА9, КА10, КА11

Списки угроз, возникающих под воздействием посторонних факторов:

Таблица 30. Списки угроз, возникающих под воздействием посторонних факторов.

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
1	ПФ 1	Факторы 1	Объекты доступа 4	Характеристики безопасности 2
2	ПФ 2	Факторы 1	Объекты доступа 5	Характеристики безопасности 3

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
3	ПФ 3	Факторы 1	Объекты доступа 6	Характеристики безопасности 5
4	ПФ 4	Факторы 1	Объекты доступа 7	Характеристики безопасности 7
5	ПФ 5	Факторы 1	Объекты доступа 9	Характеристики безопасности 6
6	ПФ 6	Факторы 1	Объекты доступа 10	Характеристики безопасности 8
7	ПФ 7	Факторы 1	Объекты доступа 12	Характеристики безопасности 1
8	ПФ 8	Факторы 1	Объекты доступа 11	Характеристики безопасности 4
9	ПФ 9	Факторы 1	Объекты доступа 8	Характеристики безопасности 9

Списки угроз, возникающих по вине нарушителя (атаки):

Таблица 31. Списки угроз, возникающих по вине нарушителя (атаки).

№ п/п	Идентификатор	Субъект	Объект	Информация	Канал	Средство	Нарушаемая характеристика
1	Атака 1	Субъекты доступа 2	Объекты доступа 2	Информация 2	Каналы атак 1	Средства атаки 1	Характеристики безопасности 3
2	Атака 2	Субъекты доступа 2	Объекты доступа 3	Информация 2	Каналы атак 1	Средства атаки 1	Характеристики безопасности 9
	Атака 3	Субъекты доступа 1	Объекты доступа 1	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 3
	Атака 4	Субъекты доступа 1	Объекты доступа 3	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 9

Частная модель угроз безопасности ПДн

Настоящий раздел составлен в соответствии с [7] и [8]. В разделе определяются актуальные угрозы безопасности персональных данных, не затрагивающие вопросы, связанные с применением в ИСПДн криптосредств.

ИСПДн «Обучающиеся и абитуриенты» обрабатывает иные категории ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками ФГБОУ ВО ЮУГМУ Минздрава России.

Характеристики безопасности ПДн представлены в таблице 32.

Таблица 32. Характеристики безопасности ПДн.

№ п/п	Характеристика безопасности	Наличие характеристики безопасности
1	Конфиденциальность	Да
2	Целостность	Да
3	Доступность	Да

Режим обработки ПДн в ИСПДн «Обучающиеся и абитуриенты»: многопользовательский с разграничением прав доступа.

Показатель исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн «Обучающиеся и абитуриенты»:

а) По территориальному размещению – локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий. Уровень защищенности – средний.

б) По наличию соединения с сетями связи общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования. Уровень защищенности – низкий.

в) По встроенным (легальным) операциям с записями баз персональных данных – модификация, передача. Уровень защищенности – низкий.

г) По разграничению доступа к персональным данным – ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности – средний.

д) По наличию соединений с другими базами ПДн иных ИСПДн – ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн. Уровень защищенности – высокий.

е) По уровню обобщения (обезличивания) ПДн – ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности – низкий.

ж) По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки – ИСПДн, предоставляющая часть ПДн. Уровень защищенности – средний.

Определение исходной степени защищенности:

Таблица 33. Исходная степень защищенности.

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
4	Высокий	1	14%
5	Средний	3	57%
6	Низкий	3	-

В соответствии полученными данными устанавливается **низкий показатель исходной защищенности**. Устанавливается значение коэффициента $\mathbf{Y_1=10}$.

Опасность угроз

Согласно документу [7] угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Общее определение угрозы безопасности объекта – возможное нарушение характеристики безопасности объекта.

Определение угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Согласно данным положениям для всех угроз частной модели принимается **средняя опасность**. Для угроз утечки информации по техническим каналам принимается **низкая опасность** в связи с тем, что угроза может привести к утрате конфиденциальности незначительной части информации о субъекте и использование данного канала утечки является трудоемким (для реализации необходима дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных).

Приложение Б

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Сотрудники» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([7]-[8]) и ФСБ России ([6]) и нормативного правового акта ФСБ России ([10]), регламентирующих порядок обеспечения безопасности ПДн, в том числе определения актуальных угроз их безопасности и формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак.

Настоящая модель угроз безопасности ПДн при их обработке в ИСПДн «Сотрудники» (далее – Модель угроз) содержит систематизированный перечень УБПДн при их обработке в ИСПДн. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности ПДн, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по УБПДн при их обработке в ИСПДн, связанным:

- с использованием СКЗИ;
- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора ПДн, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана на основе [6] и [8] с использованием [7] для конкретной ИСПДн с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ПДн при их обработке в ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности ПДн.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов

неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

УБПДн при их обработке в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [8]. Кроме того, Модель угроз может быть пересмотрена по решению оператора (владельца) ИСПДн на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн.

Наименование ИСПДн и её оператора (владельца)

Наименование ИСПДн: «Сотрудники».

Наименование оператора (владельца) ИСПДн: Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

Местонахождение ИСПДн

ИСПДн «Сотрудники» размещена по адресам: ул. Воровского, 64 (первый корпус, второй корпус).

Взаимодействие ИСПДн с внешними информационными системами

ИСПДн «Сотрудники» осуществляет однонаправленную передачу ПДн в Федеральную налоговую службу, Государственное учреждение-Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации и ПАО «Челябинвестбанк» с применением СКЗИ.

Принципы модели угроз

Согласно [6] в основе Модели угроз в аспектах, касающихся использования криптосредств, лежат следующие общие принципы:

1) Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн (п. 2.2 документа [6]).

2) При формировании модели угроз необходимо учитывать, как угрозы, осуществление которых нарушает безопасность ПДн (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) ПДн обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5) Система защиты ПДн не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, криптосредство не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в [6] понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Для обеспечения безопасности ПДн при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

Модель угроз безопасности ПДн верхнего уровня

Данный раздел определяет характеристики безопасности защищаемых ПДн и других объектов защиты.

Используемые в ИСПДн информационные технологии создания и использования ПДн

Используются нижеуказанные информационные технологии:

Таблица 1. Программное обеспечение.

ПО1	1С:Предприятие 8.3, СТЭК -2011.1, ЛКФСС (Web), Кл.-банк Челябинвестбанк, БД 1С MS SQL 2017, СТЭК-Траст
ПО2	Клиентские операционные системы семейства Microsoft Windows (Microsoft Windows XP, Microsoft Windows 7 Pro, Microsoft Windows 10)
ПО3	Серверные операционные системы Microsoft Windows 2003 R2, 2016
ПО4	Пакет офисного ПО Microsoft Office
ПО5	Браузеры
ПО6	Средство криптографической защиты информации «КриптоПро CSP» версия 4.0, Континент TLS, JINN-клиент, СКЗИ Кл.-банк Челябинвестбанк

Таблица 2. Технические средства.

ТС1	Рабочие станции
ТС2	Серверы

Формы представления ПДн в ИСПДн

ПДн имеют в ИСПДн ряд форм фиксации. Данные формы представлены в таблице.

Таблица 3. Формы фиксации.

№ п/п	Формы фиксации	Обозначение
4	Базы данных	ФФ1
5	Локальные документы	ФФ2
6	Оперативная память	ФФ3

Информация, сопутствующая процессам создания и использования ПДн

В процессе обработки ПДн используется и появляется сопутствующая информация. Типы данной информации применительно к ИСПДн приведены в таблице.

Таблица 4. Сопутствующая информация.

№ п/п	Сопутствующая информация	Обозначение
9	Информация в электронных журналах регистрации	СИ1
10	Ключевая, аутентифицирующая и парольная информация криптосредства	СИ2
11	Конфигурационная информация	СИ3
12	Криптографически опасная информация (КОИ)	СИ4
13	Остаточная информация на носителях информации	СИ5

№ п/п	Сопутствующая информация	Обозначение
14	Побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация	СИ6
15	Резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих фалов	СИ7
16	Управляющая информация	СИ8

Характеристики безопасности объектов угроз

В данном подразделе устанавливаются характеристики безопасности объектов угроз.

Список характеристик безопасности:

Таблица 5. Характеристики безопасности объектов угроз.

№ п/п	Значение	Обозначение
8	Адекватность	ХАР1
9	Аутентичность	ХАР2
10	Доступность	ХАР3
11	Конфиденциальность	ХАР4
12	Неотказуемость	ХАР5
13	Учетность	ХАР6
14	Целостность	ХАР7

а) Характеристики безопасности программного обеспечения ИСПДн:

Таблица 6. Характеристики безопасности программного обеспечения.

ПО\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ПО1	+	+	+	+	-	+	+
ПО2	+	+	+	+	-	+	+
ПО3	+	+	+	+	-	+	+
ПО4	+	+	+	+	-	+	+
ПО5	+	+	+	+	-	+	+
ПО6	+	+	+	+	+	+	+

б) Характеристики безопасности технических средств ИСПДн:

Таблица 7. Характеристики безопасности технических средств.

ТС\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ТС1	+	+	+	+	+	+	+
ТС2	+	+	+	+	-	+	+

в) Характеристики безопасности защищаемой информации (ПДн и сопутствующей информации):

Таблица 8. Характеристики безопасности защищаемой информации.

Объект\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
ФФ1	+	+	+	+	+	+	+
ФФ2	+	+	+	+	+	+	+
ФФ3	+	+	+	+	-	+	+
СИ1	+	+	+	+	-	+	+
СИ2	+	+	+	+	+	+	+
СИ3	+	+	+	+	-	+	+

Объект\\Характеристика	ХАР1	ХАР2	ХАР3	ХАР4	ХАР5	ХАР6	ХАР7
СИ4	+	+	+	+	+	+	+
СИ5	+	+	+	+	-	+	+
СИ6	+	+	+	+	-	+	+
СИ7	+	+	+	+	-	+	+
СИ8	+	+	+	+	-	+	+

Факторы угроз, не являющихся атаками

Все рассматриваемые угрозы в данном разделе могут повлечь в какой-то мере случайное нарушение характеристик безопасности объектов. Предполагается, что отсутствует заинтересованный нарушитель. Поэтому, если воздействие фактора непосредственно не приводит к нарушению характеристики, то считается, что угрозы нет.

Рассматриваются следующие факторы угроз, не являющихся атаками:

Таблица 9. Факторы угроз, не являющихся атаками.

№ п/п	Фактор	Обозначение
12	внедрение и использование неучтенных программ	ФР1
13	нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	ФР2
14	настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	ФР3
15	негативные социальные явления могут создать предпосылки для невозможности работы ИСПДн – отключения электроэнергии, нарушение работы каналов связи	ФР4
16	неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.	ФР5
17	непредумышленное искажение или удаление программных компонентов АСЗИ	ФР6
18	несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа	ФР7
19	помехи и наводки, приводящие к сбоям в работе аппаратных средств	ФР8
20	предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	ФР9
21	разрушения от ветра, попадания молнии в объекты инфраструктуры, обрывы проводов могут привести к нарушению электропитания ИСПДн, обрыву связи с сетями общего пользования	ФР10
22	техногенные аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.)	ФР11

Данные факторы могут воздействовать на объекты угроз, с нарушением характеристик безопасности.

Списки угроз, не являющихся атаками, приведены в разделе «Список угроз по модели нарушителя».

Защита от угроз, не являющихся атаками, в основном регламентируется инструкциями и распорядительными документами, разработанными с учетом особенностей эксплуатации ИСПДн и действующей нормативной базы. При этом по возможности также используются инженерно-технические меры.

Модель нарушителя

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

Объекты атак

В качестве объектов атак рассматриваются защищаемые ПДн, сопутствующая информация, ПО ИСПДн, технические средства ИСПДн, помещения, в которых размещены технические средства.

Субъекты атак

В качестве субъектов атак рассматриваются физические лица, имеющие доступ к техническим и программным средствам ИСПДн:

Таблица 10. Субъекты атак.

№ п/п	Субъект	Категория	Внутренний	Внешний	Условное обозначение
4	Администратор	2	+	+	СА1
5	Пользователь	2	+	-	СА2
6	Посетитель	2	+	-	СА3

Пояснения:

категория 1 – лица, не имеющие права доступа в контролируемую зону ИСПДн;

категория 2 – лица, имеющие право постоянного или разового доступа в контролируемую зону ИСПДн;

внешние нарушители – нарушители, осуществляющие атаки из-за пределов контролируемой зоны ИСПДн;

внутренние нарушители – нарушители, осуществляющие атаки, находясь в пределах контролируемой зоны ИСПДн.

К привилегированным пользователям ИСПДн, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями, относится администратор.

К Администраторам ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число Администраторов будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Возможность сговора субъектов атак представлена в виде таблицы:

Таблица 11. Возможность сговора.

Субъект	СА2	СА3
СА2	-	+
СА3	+	-

Пояснения:

"-" – сговор между субъектами атаки невозможен: субъекты не могут иметь общих интересов; субъекты не встречаются в реальном мире; сферы деятельности субъектов не позволяют им действовать сообща; крайне низкая вероятность сговора; ЛИБО у субъектов атаки имеется возможность организовать сговор, но сговор не позволяет им объединить знания и (или) возможности для проведения совместной атаки, либо сговор не дает новых знаний и (или) возможностей для проведения атаки;

"+" – сговор между субъектами атаки возможен.

Таким образом, получаются следующие возможности для сговора:

Таблица 12. Возможности для сговора.

Значение	Условное обозначение
Пользователь	СА2
Посетитель	СА3
Сговор(<Пользователь>, <Посетитель>)	СА4

Возможности доступа:

Таблица 13. Возможности доступа.

Субъект\\объект	ФФ1	ФФ2	ФФ3	СИ1	СИ2	СИ3	СИ4	СИ5	СИ6	СИ7	СИ8
СА1	+	+	+	+	+	+	+	+	+	+	+
СА2	+	+	+	+	+	+	+	+	+	+	+
СА3	-	-	-	-	-	-	-	-	-	-	-
СА4	+	+	+	+	+	+	+	+	+	+	+

Внешний нарушитель может принимать участие в любом из сговоров с целью получения дополнительных возможностей для проведения атаки, становиться связующим звеном для любого из сговоров.

Наибольшие возможности нарушители получают при множественном сговоре. Соответственно наиболее опасны именно такие сговоры, хотя их вероятность ниже двусторонних сговоров.

Предположения об имеющейся у нарушителя информации об объектах атак

Нарушители обладают полной информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты.

Список имеющейся у нарушителя информации:

Таблица 14. Список имеющейся у нарушителя информации.

№ п/п	Информация	Обозначение	Обоснование
9	Содержание технической документации на технические и программные компоненты СФК	ОИ1	-
10	Долговременные ключи криптосредства	ОИ2	-
11	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.)	ОИ3	-
12	Сведения о линиях связи, по которым передается защищаемая информация	ОИ4	-

№ п/п	Информация	Обозначение	Обоснование
13	Все сети связи, работающие на едином ключе	ОИ5	-
14	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК	ОИ6	-
15	Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства и СФК	ОИ7	-
16	Сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель	ОИ8	-

Ограничения на имеющуюся у нарушителя информацию об объектах атак удобно представить в виде таблицы:

Таблица 15. Ограничения на имеющуюся у нарушителя информацию.

Субъект	ОИ1	ОИ2	ОИ3	ОИ4	ОИ5	ОИ6	ОИ7	ОИ8
СА2	+	+	+	+	-	+	+	-
СА3	-	-	+	-	-	+	+	-
СА4	+	+	+	+	-	+	+	-

где:
"+" – нарушитель располагает информацией;
"-" – нарушитель не располагает информацией.
Обоснования ограничений:

Таблица 16. Обоснование ограничений на имеющуюся у нарушителя информацию.

№ п/п	Субъект	Информация	Обоснование
8	СА2	ОИ5	не имеет доступа к средствам конфигурирования защищенной сети и средствам управления конфигурацией этой сети
9	СА2	ОИ8	не имеет в распоряжении специального оборудования
10	СА3	ОИ1	не располагают технической документацией и компонентами СФК
11	СА3	ОИ2	не имеет доступа к СКЗИ, носителям ключевой и аутентифицирующей информации
12	СА3	ОИ4	не располагает данной информацией
13	СА3	ОИ5	не имеет доступа к средствам конфигурирования защищенной сети, не обладают достаточными знаниями в этой области
14	СА3	ОИ8	не имеют в распоряжении специального оборудования

Предположения об имеющихся у нарушителя средствах атак

Нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Список имеющихся у нарушителя средств атак:

Таблица 17. Список имеющихся у нарушителя средств атак.

№ п/п	Информация	Обозначение	Обоснование
5	Аппаратные компоненты криптосредства и СФК	СПА1	-
6	Доступные в свободной продаже технические средства и программное обеспечение	СПА2	-
7	Специально разработанные технические средства и программное обеспечение	СПА3	-
8	Штатные средства	СПА4	-

При этом имеются следующие ограничения на имеющиеся у нарушителей средства атак:

Таблица 18. Ограничения на имеющиеся у нарушителей средства атак.

№ п/п	Субъект\\Средство	СПА1	СПА2	СПА3	СПА4
4	СА2	-	+	-	+
5	СА3	-	+	-	+
6	СА4	-	+	-	+

где:
"+" – нарушитель располагает средством атаки;
"-" – нарушитель не располагает средством атаки.

Обоснования ограничений:

Таблица 19. Обоснование ограничений на имеющиеся у нарушителей средства атак.

№ п/п	Субъект	Информация	Обоснование
5	СА2	СПА1	доступ ограничен организационно-техническими мерами
6	СА2	СПА3	не имеет возможности использования и разработки
7	СА3	СПА1	доступ ограничен организационно-техническими мерами
8	СА3	СПА3	не имеет возможности использования и разработки

Каналы атак

Описание каналов атак.

Таблица 20. Каналы атак.

№ п/п	Канал атаки	Обозначение	Обоснование
12	Каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами	КА1	-
13	Штатные средства	КА2	-
14	Каналы непосредственного доступа к объекту атаки (акустический, визуальные, физический)	КА3	-
15	Машинные носители информации	КА4	-
16	Носители информации, выведенные из употребления	КА5	-
17	Технические каналы утечки	КА6	-
18	Сигнальные цепи	КА7	-
19	Цепи электропитания	КА8	-
20	Цепи заземления	КА9	-

№ п/п	Канал атаки	Обозначение	Обоснование
21	Канал утечки за счет электронных устройств негласного получения информации	КА10	-
22	Информационные и управляющие интерфейсы СВТ	КА11	-

Ограничения на доступ к каналам атаки.

В силу действующих правил доступ и должностных обязанностей таблица доступа к каналам атаки выглядит следующим образом:

Таблица 21. Таблица доступа к каналам атаки.

Субъект\\Канал	КА1	КА2	КА3	КА4	КА5	КА6	КА7	КА8	КА9	КА10	КА11
СА2	+	+	+	+	+	+	+	+	+	+	+
СА3	+	+	+	+	+	+	+	+	+	+	+
СА4	+	+	+	+	+	+	+	+	+	+	+

где:

“+” – нарушитель имеет возможность воспользоваться каналом атаки;

“-” – нарушитель не имеет возможности воспользоваться каналом атаки.

Тип нарушителя

Исходя из возможностей, устанавливаются следующие типы нарушителей:

Таблица 22. Тип нарушителя.

№ п/п	Субъект атаки	Категория	Внутренний	Внешний	Тип нарушителя
4	СА2	2	+	-	Н2
5	СА3	2	+	-	Н2
6	СА4	2	+	-	Н2

Угрозы, возникающие на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК, приведены в разделе «Список угроз по модели нарушителя».

Угрозы, связанные с моделью нарушителя и возникающие на этапе эксплуатации, приведены в разделе «Список угроз по модели нарушителя».

Список угроз по модели нарушителя

Разные факторы случайных воздействий могут приводить к реализации схожих угроз. В результате анализа характеристик факторов случайных воздействий и особенностей функционирования ИСПДн, факторы случайных воздействий сгруппированы в списки, которые представлены в таблице.

Таблица 23. Факторы случайных воздействий.

№ п/п	Название списка	Элементы списка
2	Список "Факторы 1"	ФР10, ФР4, ФР6, ФР1, ФР2, ФР9, ФР3, ФР7, ФР11, ФР5, ФР8

На разные объекты атак могут быть направлены схожие угрозы. В результате анализа характеристик объектов атак и особенностей функционирования ИСПДн, объекты атак сгруппированы в списки, которые представлены в таблице.

Таблица 24. Объекты атак.

№ п/п	Название списка	Элементы списка
13	Список "Объекты доступа 1"	ТС1, ПО2, ФФ1, СИ2, ТС2, ПО4, ФФ2, СИ4, ФФ3, СИ3, СИ8, ПО5, СИ1, ПО6, СИ6, ПО1, СИ7, ПО3, СИ5
14	Список "Объекты доступа 2"	ТС1, ПО2, ФФ1, СИ2, ПО4, ФФ2, СИ4, ФФ3, СИ3, СИ8, ПО5, СИ1, ПО6, СИ6, ПО1, СИ7, СИ5
15	Список "Объекты доступа 3"	ТС1, ФФ1, СИ2, ФФ2, СИ4, ПО6
16	Список "Объекты доступа 4"	ТС1, ПО6
17	Список "Объекты доступа 5"	ПО2, ТС2, ПО4, ПО5, ПО1
18	Список "Объекты доступа 6"	ФФ1, СИ2, ФФ2, ФФ3, СИ3, СИ1
19	Список "Объекты доступа 7"	ФФ1, ФФ2
20	Список "Объекты доступа 8"	СИ2, СИ4
21	Список "Объекты доступа 9"	СИ2, СИ4, ФФ3, СИ3, СИ8, СИ1, СИ6, СИ7, СИ5
22	Список "Объекты доступа 10"	СИ4, СИ8, СИ6, СИ7, ПО3, СИ5
23	Список "Объекты доступа 11"	СИ4, СИ8, СИ6, СИ7, СИ5
24	Список "Объекты доступа 12"	ПО3

Для разных объектов атак могут быть установлены схожие характеристики безопасности. В результате анализа характеристик безопасности и особенностей функционирования ИСПДн, характеристики безопасности сгруппированы в списки, которые представлены в таблице.

Таблица 25. Характеристики безопасности.

№ п/п	Название списка	Элементы списка
10	Список "Характеристики безопасности 1"	ХАР4, ХАР7, ХАР3, ХАР6
11	Список "Характеристики безопасности 2"	ХАР4, ХАР7, ХАР3, ХАР6, ХАР1, ХАР5, ХАР2
12	Список "Характеристики безопасности 3"	ХАР4, ХАР7, ХАР3, ХАР6, ХАР1, ХАР2
13	Список "Характеристики безопасности 4"	ХАР4, ХАР3
14	Список "Характеристики безопасности 5"	ХАР4, ХАР3, ХАР1, ХАР2
15	Список "Характеристики безопасности 6"	ХАР7, ХАР6
16	Список "Характеристики безопасности 7"	ХАР7, ХАР6, ХАР5

№ п/п	Название списка	Элементы списка
17	Список "Характеристики безопасности 8"	ХАР1, ХАР2
18	Список "Характеристики безопасности 9"	ХАР5

Разные субъекты могут пытаться осуществить схожие атаки и обладать схожими возможностями и навыками. В результате анализа характеристик субъектов атак и особенностей функционирования ИСПДн, субъекты атак сгруппированы в списки, которые представлены в таблице.

Таблица 26. Субъекты атак.

№ п/п	Название списка	Элементы списка
3	Список "Субъекты доступа 1"	СА2
4	Список "Субъекты доступа 2"	СА3

Одна и та же информация может быть известна разным субъектам атак. В результате анализа информации, известной субъектам атак, и особенностей функционирования ИСПДн, сведения сгруппированы в списки, которые представлены в таблице.

Таблица 27. Информация, известная субъектам атак.

№ п/п	Название списка	Элементы списка
3	Список "Информация 1"	ОИ2, ОИ3, ОИ4, ОИ6, ОИ7, ОИ8
4	Список "Информация 2"	ОИ3, ОИ6, ОИ7

Одни и те же средства проведения атак могут быть известны быть использованы разными субъектами атак. В результате анализа средств проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, средства проведения атак сгруппированы в списки, которые представлены в таблице.

Таблица 28. Средства проведения атак.

№ п/п	Название списка	Элементы списка
2	Список "Средства атаки 1"	СПА1, СПА2, СПА3, СПА4

Одни и те же каналы проведения атак могут быть использованы разными субъектами атак. В результате анализа каналов проведения атак, доступных субъектам атак, и особенностей функционирования ИСПДн, каналы проведения атак сгруппированы в списки, которые представлены в таблице.

Таблица 29. Каналы проведения атак.

№ п/п	Название списка	Элементы списка
2	Список "Каналы атак 1"	КА1, КА2, КА3, КА4, КА5, КА6, КА7, КА8, КА9, КА10, КА11

Списки угроз, возникающих под воздействием посторонних факторов:

Таблица 30. Списки угроз, возникающих под воздействием посторонних факторов.

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
10	ПФ 1	Факторы 1	Объекты доступа 4	Характеристики безопасности 2
11	ПФ 2	Факторы 1	Объекты доступа 5	Характеристики безопасности 3

№ п/п	Идентификатор	Фактор угрозы	Объект угрозы	Нарушаемая характеристика
12	ПФ 3	Факторы 1	Объекты доступа 6	Характеристики безопасности 5
13	ПФ 4	Факторы 1	Объекты доступа 7	Характеристики безопасности 7
14	ПФ 5	Факторы 1	Объекты доступа 9	Характеристики безопасности 6
15	ПФ 6	Факторы 1	Объекты доступа 10	Характеристики безопасности 8
16	ПФ 7	Факторы 1	Объекты доступа 12	Характеристики безопасности 1
17	ПФ 8	Факторы 1	Объекты доступа 11	Характеристики безопасности 4
18	ПФ 9	Факторы 1	Объекты доступа 8	Характеристики безопасности 9

Списки угроз, возникающих по вине нарушителя (атаки):

Таблица 31. Списки угроз, возникающих по вине нарушителя (атаки).

№ п/п	Идентификатор	Субъект	Объект	Информация	Канал	Средство	Нарушаемая характеристика
1	Атака 1	Субъекты доступа 2	Объекты доступа 2	Информация 2	Каналы атак 1	Средства атаки 1	Характеристики безопасности 3
2	Атака 2	Субъекты доступа 2	Объекты доступа 3	Информация 2	Каналы атак 1	Средства атаки 1	Характеристики безопасности 9
	Атака 3	Субъекты доступа 1	Объекты доступа 1	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 3
	Атака 4	Субъекты доступа 1	Объекты доступа 3	Информация 1	Каналы атак 1	Средства атаки 1	Характеристики безопасности 9

Частная модель угроз безопасности ПДн

Настоящий раздел составлен в соответствии с [7] и [8]. В разделе определяются актуальные угрозы безопасности персональных данных, не затрагивающие вопросы, связанные с применением в ИСПДн криптосредств.

ИСПДн «Сотрудники» обрабатывает иные категории ПДн менее чем 100 000 субъектов ПДн, являющихся сотрудниками ФГБОУ ВО ЮУГМУ Минздрава России.

Характеристики безопасности ПДн представлены в таблице 32.

Таблица 32. Характеристики безопасности ПДн.

№ п/п	Характеристика безопасности	Наличие характеристики безопасности
4	Конфиденциальность	Да
5	Целостность	Да
6	Доступность	Да

Режим обработки ПДн в ИСПДн «Сотрудники»: многопользовательский с разграничением прав доступа.

Показатель исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн «Сотрудники»:

з) По территориальному размещению – локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий. Уровень защищенности – средний.

и) По наличию соединения с сетями связи общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования. Уровень защищенности – низкий.

к) По встроенным (легальным) операциям с записями баз персональных данных – модификация, передача. Уровень защищенности – низкий.

л) По разграничению доступа к персональным данным – ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности – средний.

м) По наличию соединений с другими базами ПДн иных ИСПДн – ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн. Уровень защищенности – высокий.

н) По уровню обобщения (обезличивания) ПДн – ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности – низкий.

о) По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки – ИСПДн, предоставляющая часть ПДн. Уровень защищенности – средний.

Определение исходной степени защищенности:

Таблица 33. Исходная степень защищенности.

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
7	Высокий	1	14%
8	Средний	2	57%
9	Низкий	3	-

В соответствии полученными данными устанавливается **низкий показатель исходной защищенности**. Устанавливается значение коэффициента $\mathbf{Y_1=10}$.

Опасность угроз

Согласно документу [7] угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Общее определение угрозы безопасности объекта – возможное нарушение характеристики безопасности объекта.

Определение угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Согласно данным положениям для всех угроз частной модели принимается **средняя опасность**. Для угроз утечки информации по техническим каналам принимается **низкая опасность** в связи с тем, что угроза может привести к утрате конфиденциальности незначительной части информации о субъекте и использование данного канала утечки является трудоемким (для реализации необходима дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных).

Приложение В

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Библиотека» Федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([4]-[6]), регламентирующих порядок обеспечения безопасности ПДн.

Настоящая «Модель угроз информационной системы персональных данных «Библиотека» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн, связанным:

с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана на основе [4] и [5] с использованием [6] для конкретной ИСПДн «Библиотека» с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [6]. Кроме того, Модель

угроз может быть пересмотрена по решению оператора (владельца) на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

Описание информационной системы персональных данных

Наименование ИСПДн

Наименование ИСПДн: – «Библиотека».

Наименование оператора (владельца) ИСПДн: Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации.

Местонахождение ИСПДн

ИСПДн «Библиотека» размещена по адресу: ул. Воровского, 64 (первый корпус, второй корпус, теплый переход).

Взаимодействие с другими ИСПДн

Взаимодействие ИСПДн «Библиотека» с другими информационными системами не предполагается.

Принципы модели угроз

В основе Модели угроз лежат следующие общие принципы:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных.

2) При формировании модели угроз необходимо учитывать, как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий.

5) Нарушитель может действовать на различных этапах жизненного цикла ИСПДн.

Частная модель угроз безопасности персональных данных

Настоящий раздел составлен в соответствии с [5] и [6]. В разделе определяются актуальные угрозы безопасности персональных данных, не затрагивающие вопросы, связанные с применением в ИСПДн криптосредств.

Исходные данные

а) Характеристика информационных систем персональных данных.

Информационная система, обрабатывающая иные категории персональных данных.

б) Обрабатываемые ПДн.

В ИСПДн обрабатываются персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

В ИСПДн обрабатываются персональные данные менее чем 100 000 субъектов персональных данных.

в) Заданные характеристики безопасности ПДн.

Устанавливаются следующие характеристики безопасности ПДн:

Таблица 1. Характеристики безопасности ПДн.

№ п/п	Характеристика безопасности	Наличие характеристики безопасности
1	Конфиденциальность	Да
2	Целостность	Да
3	Доступность	Да

г) Режим обработки ПДн.

В ИСПДн режим обработки ПДн многопользовательский с разграничением прав доступа.

Показатель исходной защищенности ИСПДн

Информационная система персональных данных (ИСПДн) «Библиотека» имеет следующие технические и эксплуатационные характеристики:

п) По территориальному размещению – локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий. Уровень защищенности – средний.

р) По наличию соединения с сетями связи общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования. Уровень защищенности – низкий.

с) По встроенным (легальным) операциям с записями баз персональных данных – запись, удаление, сортировка. Уровень защищенности – средний.

т) По разграничению доступа к персональным данным – ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности – средний.

у) По наличию соединений с другими базами ПДн иных ИСПДн – ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн. Уровень защищенности – высокий.

ф) По уровню обобщения (обезличивания) ПДн – ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности – низкий.

х) По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки – ИСПДн, не предоставляющая никакой информации. Уровень защищенности – высокий.

Определение исходной степени защищенности:

Таблица 2. Исходная степень защищенности.

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	2	28%
2	Средний	3	71%
3	Низкий	2	-

В соответствии полученными данными устанавливается **средний показатель исходной защищенности**. Устанавливается значение коэффициента $\mathbf{Y_1=5}$.

Опасность угроз

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИСПДн «Библиотека» является информационной системой, для которой нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Общее определение угрозы безопасности объекта – возможное нарушение характеристики безопасности объекта.

Определение угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Согласно данным положениям для всех угроз частной модели принимается **средняя опасность**. Для угроз утечки информации по техническим каналам принимается **низкая опасность** в связи с тем, что угроза может привести к утрате конфиденциальности незначительной части информации о субъекте и использование данного канала утечки является трудоемким (для реализации необходима дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных).

Приложение Г

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение Д

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографичес-кие номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводитель-ного письма	Ф.И.О. пользова-теля СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтоже-ния)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение Е

Программа подготовки (обучения) пользователей правилам работы с средствами криптографической защиты информации

№ п/п	Тема
I.	**Основы безопасности информационных технологий**
1.1	Основные понятия информационной безопасности
1.2	Угрозы безопасности информационных технологий
1.3	Виды мер и основные принципы обеспечения информационной безопасности
II	**Обеспечение безопасности конфиденциальных данных**
2.1.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
2.2.	Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.3	Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. № 66;
III	**Правила работы с СКЗИ**
3.1.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
3.2.	Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP
3.3.	Порядок использования электронной подписи
3.4.	Информационная система «ДелоPro». Делопроизводство и документооборот.
IV	**Тест для зачета**

Модуль 1. Основы безопасности информационных технологий

1.1 Основные понятия информационной безопасности

Что такое безопасность информационных технологий. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Определение НСД. Объекты, цели и задачи защиты информационных систем и циркулирующей в них информации.

1.2 Угрозы безопасности информационных технологий

Угрозы безопасности информации, информационных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Классификация нарушителей информационной безопасности.

1.3 Виды мер и основные принципы обеспечения информационной безопасности

Виды мер противодействия угрозам безопасности (организационные, технические, физические). Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в информационной системе.

Модуль 2. Обеспечение безопасности конфиденциальных данных

2.1. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

Основные положения. Требования, предъявляемые к оператору конфиденциальной информации. Положение о лицензировании деятельности по технической защите конфиденциальной информации.

2.2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Сфера действия. Основные понятия. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Защита информации.

2.3. Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. N 66

Общие положения. Порядок разработки СКЗИ. Порядок производства СКЗИ. Порядок реализации (распространения) СКЗИ. Порядок эксплуатации СКЗИ.

Модуль 3. Правила работы с СКЗИ

3.1. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Основные положения. Риски использования ЭП. Порядок обращения с ключевыми носителями. Инфраструктура открытых ключей. Управление своими сертификатами, их отзыв, приостановка и возобновление действия. Действия при истечении сертификата, компрометации ключей и прочих нестандартных ситуациях. Резервное копирование ключей, условия хранения и управления своими ключевыми данными.

3.2. Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP

Установка и настройка СКЗИ. Хранение, использование, учет и контроль за использованием СКЗИ. Проверка срока действия сертификата ЭП.

3.3. Порядок использования электронной подписи

Основные понятия. Сфера регулирования отношений в области использования электронных подписей. Принципы использования электронной подписи. Виды электронной подписи. Признание квалифицированной электронной подписи. Средства электронной подписи. Удостоверяющий центр. Сертификат ключа проверки электронной подписи. Аккредитация удостоверяющего центра.

Модуль 4. Тест для зачета

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ

ФИО _____

Для корректного заполнения просьба отметить один или несколько вариантов ответа

1. Какие свойства информации необходимо защищать?

a) коммерческую тайну;

b) целостность;

c) конфиденциальность;

d) полноту информации;

e) доступность.

2. Кто может быть нарушителем безопасности?

a) посетители;

b) сотрудники Вашей организации, не прошедшие обучение по работе с СКЗИ;

c) сотрудники Вашей организации, прошедшие обучение по работе с СКЗИ;

d) все вышеперечисленные.

…

15. Осуществляется ли обработка конфиденциальной информации в присутствии посторонних лиц?

a) да, если монитор расположен таким образом, что исключается возможность его обзора;

b) нет, ни в коем случае;

c) да, если это сотрудник лицензиата Управления Федеральной службы безопасности по Челябинской области.

Подпись _____

Дата _____

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

(зачтено/не зачтено)

Проверил ФИО, подпись_____