МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Разработка рекомендаций по организации системы защиты персональных данных в образовательной организации высшего образования

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
87 % авторского текста

Работа рекомендована к защите
«18» 01 2021 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ЗФ-309-210-2-1
Гумен Антон Валерьевич

Научный руководитель:
Диденко Галина Александровна, к.п.н., доцент

Челябинск
2021

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.

К самим же персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Первоначально на проблему защиты персональных данных на международном уровне обратила внимание Организация по экономическому сотрудничеству и развитию (ОЭСР), принявшая в 1980 г. Директиву о защите неприкосновенности частной жизни и международных обменов персональными данными. В дальнейшем эти принципы были детализированы в Конвенции Совета Европы «Об охране личности в отношении автоматизированной обработки персональных данных» (1981 г.), в Директиве Европейского сообщества о защите граждан в плане обработки информации личного характера от 27 июля 1990 г. [55].

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных (далее - ПДн). Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального

закона от 27.07.2006 N 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов [6].

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;

− возможная подмена записей в ведомостях и чек-листах в личных целях;

− получение несанкционированного доступа к научным исследованиям и интеллектуальной собственности сотрудников вуза;

− нарушение доступа к веб-сайту.

Особое внимание уделяется вопросам защиты персональных данных (ПД) в автоматизированных информационных системах ПД - ИСПД. Требования к защите в ИСПД, в соответствии с рядом документов, учитывают категорию и количество ПД, специфику решаемых задач и ряд других

показателей. Выполнение этих требований, как правило, связано с существенными материальными и финансовыми затратами, вызванными необходимостью создания системы защиты, обеспечением высокой квалификации персонала, получением разрешительных документов, что не всегда возможно для большого числа пользователей информации и операторов, представляющих малобюджетные организации (медицинские и образовательные организации, предприятия системы ЖКХ, общественные организации).

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 дают вузам возможность ее решить, при этом не затрачивая лишние средства и не прибегая к сложным мерам [43; 29].

Специфика защиты персональных данных в вузе обусловлена техническими, кадровыми, организационными и финансовыми аспектами деятельности в нем. 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 высшего образования с учетом комплексной оценки уровня защищенности и требований нормативно-правовой базы Российской Федерации.

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

Предметом исследования является защита персональных данных.

Для достижения поставленной цели были сформулированы следующие *задачи:*

– изучить понятие «персональные данные» и значение их защиты в образовательной организации высшего образования;

– провести оценку существующей системе защиты персональных данных в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ;

– разработать рекомендации по организации системы защиты персональных данных в образовательной организации высшего образования и проверить их эффективность.

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. [26], Амелин Р.В. [28], Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. [28], Бадьина А. [30], Бархатова Е.Ю. [32], Кузнецова Т.В. [39], Лушников А. [40], Медведева Т.М. [41], Савельев А.И., Серков П.П., Ситникова Е.Г., Сенаторова Н.В., Терещенко Л.К. [68].

Практическая значимость работы заключается в разработке рекомендаций по организации системы защиты персональных данных в образовательной организации высшего образования, 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 высшего образования.

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

Ход исследования и его результаты докладывались и обсуждались на международных конференциях: Международная научно-практическая конференция «ИННОВАЦИОННОЕ РАЗВИТИЕ: ПОТЕНЦИАЛ НАУКИ И СОВРЕМЕННОГО ОБРАЗОВАНИЯ», г. Пенза, 23 декабря 2020 года. Публикация: Организация системы защиты персональных данных в образовательных организациях высшего образования [Текст] / А.В. Гумен // Сборник материалов Международной научно-практической конференции «ИННОВАЦИОННОЕ РАЗВИТИЕ: ПОТЕНЦИАЛ НАУКИ И СОВРЕМЕННОГО ОБРАЗОВАНИЯ». – Пенза, 2020. – С. 267-269.

Публикации в других научных изданиях: Гумен А.В. Практическая реализация системы защиты персональных данных в вузе / А.В. Гумен / Профессиональное образование: теория, методика, практика. Выпуск 14. – Челябинск, изд-во «Золотой Феникс», 2021. – С. 96-100.

Структура магистерской диссертации состоит из введения, трех глав, заключения, списка использованных источников, состоящего из 71 наименований, приложения.

ГЛАВА 1 ПОНЯТИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ЗАЩИТА В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ

1.1 Понятие персональных данных и значение их защиты в образовательной организации высшего образования

Персональные данные – это любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу – субъекту персональных данных. Таким образом, это могут быть любые сведения, идентифицирующие человека, в том числе: ФИО, дата рождения, место жительства, семейное положение, сведения об образовании и профессиональной деятельности, финансовое положение, факты биографии, деловые и личные качества человека и пр.

В рамках нашего исследования персональные данные рассматриваются, как различная информация, которая прямо или косвенно относятся к определенному физическому лицу, т.е. субъекту персональных данных. В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Изменения, связанные с регулированием персональных данных (информации о личной жизни человека), происходят сейчас во многих государствах, в том числе и в России, и в первую очередь данная проблема затрагивает высшее образование [55].

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.

Анализируя конституционно-правовые рамки защиты персональных данных можно отметить, что в Конституции отсутствует положение, которое напрямую бы закрепляло «право на защиту персональных данных». Вместе с тем, отдельные положения существуют, и необходимо разобраться, какие именно нормы гарантируют защиту персональных данных.

В настоящее время вопрос обработки персональных данных находится в секторе внимания абсолютно любой организации. В текущих реалиях трудно найти организацию, которая не обрабатывала бы персональные данные своих сотрудников.

С момента заключения трудовых отношений хотя бы с одним гражданином, организация становится оператором персональных данных и, соответственно, принимает на себя обязанности по защите указанной информации, становится поднадзорной контролирующим органам, т.н. «регуляторам» (которых на сегодняшний день три).

В свою очередь, любой гражданин в процессе своей жизни вступает во взаимоотношения с различными физическими и юридическими лицами. В результате данного взаимодействия накапливаются данные о конкретном индивиде, начиная с простых (фамилии, имени, отчестве) и заканчивая специфическими (сведения о здоровье, сведения о судимости, биометрические данные). При этом, гражданин может не желать, чтобы эти сведения становились известными широкому кругу лиц. В целях защиты указанной информации используется специальный правовой режим персональных данных. Для обеспечения данного правового режима в 2006 году был принять отдельный Федеральный закон «О персональных данных». Периодически, в него вносятся поправки, касающиеся обработки персональных данных и принимаются новые подзаконные нормативно-правовые акты, направленные на конкретизацию его норм, так последние поправки вступили в силу в сентябре 2015 года.

Тем не менее, по прошествии уже почти 10 лет, у сотрудников служб информационной безопасности возникают трудности в применении действующих правовых норм, регулирующих данную сферу общественных отношений, в связи с чем и представляется целесообразным рассмотрение вопросов обработки персональных данных работников и их защиты.

Термин персональные данные, в свою очередь, тесно связан с понятием обработка. Обработка персональных данных начинается тогда, когда

гражданин «свободно, своей волей и в своем интересе» (на что прямо указано в ч. 1 ст. 9 Федерального закона «О персональных данных») передает свои данные оператору для выполнения каких-либо функций (например, заключение трудового договора) или делает их общедоступными (например, регистрируясь в социальных сетях).

В соответствии с положениями закона обеспечение защиты персональных данных является прямой обязанностью операторов персональных данных, а это практически все предприятия Российской Федерации.

Под оператором понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обеспечение безопасности персональных данных является *не правом организации, а ее прямой обязанностью*. Несоблюдение организацией требований по обеспечению безопасности персональных данных может повлечь не только ущерб для самой организации, но, в первую очередь, привести к нарушению конституционных прав граждан, повлечь за собой череду гражданско-правовых исков со стороны физических лиц, чьи права могут оказаться нарушенными, и, даже привлечение к административной или уголовной ответственности.

Требования закона «О персональных данных» распространяются на все государственные и коммерческие организации, обрабатывающие персональные данные физических лиц (сотрудников, клиентов, партнеров и т.п.), независимо от размера и формы собственности.

Наиболее остро вопрос защиты персональных данных стоит в сферах здравоохранения, образования, финансов, и в государственных органах.

Эти обстоятельства предъявляют повышенные требования к системе защиты персональных данных и являются приоритетными для проведения проверок контролирующими органами.

Основными опасностями для персональных данных в образовательной организации высшего образования, по нашему мнению, выступают:

− обмен информацией между удаленными пользователями и веб-сайтом вуза;

− передача удаленным пользователем своих идентификационных данных программистам вуза;

− обмен данными пользователя с сервером информационных систем вуза;

− авторизация пользователя;

− шпионские программы, внедренные в информационную систему вуза.

Основные инструменты, которыми пользуются злоумышленники для доступа к персональным данным:

− слабые пароли, которые создают удаленные пользователи;

− уязвимость каналов передачи персональных данных;

− вредоносное программное обеспечение;

− непрофессиональная конфигурация сети передачи персональных данных;

− уязвимости средств и мер защиты [61].

Для защиты персональных данных всех субъектов образовательного процесса вуза необходимо соблюдать следующие меры:

− ведение внутренней документации по работе с персональными данными и их защите;

− внедрение современных мер защиты персональных данных;

− организация системы всесторонней защиты персональных данных.

В целом защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности любой организации. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение

положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности.

1.2 Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации

В настоящее время институт «персональных данных» в России регулируется рядом нормативных актов. При этом, как отмечают авторы, «практически во всех законах присутствуют нормы о правах граждан – субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об ответственности за нарушения в работе с персональными данными».

В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни. Обозначенная линия неприкосновенности частной жизни прослеживается и в Конституции Российской Федерации 1993 г. (ст. ст. 23, 24). Статья 23 Конституции гарантирует каждому «право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья 24 установила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия» [8].

Также для развития нормы о неприкосновенности частной жизни и в связи с ратификацией Российской Федерацией ряда международных актов, в Трудовой Кодекс была включена глава 14 «Защита персональных данных». В ней определяются общие положения защиты персональных данных

работника: понятие, требования, особенности хранения, передачи, права работников и ответственность за нарушение норм.

Кроме того, в качестве нормативно-правового источника защиты персональных данных, можно отметить: ФЗ №149 «Об информации, информационных технологиях и защите информации». Необходимо отметить, что действующее трудовое законодательство нацелено на обеспечение безопасности персональных данных, как в частном секторе, так и на государственной службе.

Помимо Конституции РФ, основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152- ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных. Не попадают под сферу регулирования закона 152-ФЗ следующие действия:

– обработка чужих персональных данных физическими лицами для собственных нужд (личных и семейных), при условии, что такая обработка не нарушает права владельца персональных данных;

– действия по организации архивов, которые попадают в сферу регуляции законодательства об архивном деле в РФ;

– обработка персональных данных, которые содержат сведения, отнесенные в соответствии с действующим законодательством РФ, к государственной тайне;

– персональные данные, относящиеся к деятельности судов, предоставленные в порядке, закрепленном соответствующими

законодательными актами. Федеральный закон № 152-ФЗ «О персональных данных» описывает организационно-правовые механизмы защиты персональной информации любого физического лица.

Однако в отношении данных закон не указывает, распространяются ли его нормы на персональные данные работников.

Опираясь на теорию права можно провести анализ института персональных данных.

Так, предметом указанного института являются общественные отношения, связанные с обработкой персональных данных осуществляемой государственными и муниципальными органами, юридическими и физическими лицами с использованием средств. Указанный институт содержит разветвленный понятийный аппарат. Так, в частности, статья 3 Федерального закона «О персональных данных» содержит в себе такие дефиниции как: «персональные данные», «оператор», «обработка персональных данных», «автоматизированная обработка персональных данных», «обезличивание персональных данных», «информационная система персональных данных», «трансграничная передача персональных данных» и т.п.

Кроме того, указанная сфера жизнедеятельности на сегодняшний день является относительно обособленной и имеет целый арсенал источников, содержащих в себе как нормы материального права (федеральные законы), так и нормы процессуального права (подзаконные нормативные акты) предписывающие процедуры, которые обязан провести оператор персональных данных по защите, обрабатываемой им информации.

Статья 5 Федерального закона «О персональных данных» содержит принципы и условия обработки персональных данных. Анализ указанных принципов и иных норм, содержащихся в указанном Федеральном законе и изданных в соответствии с ним подзаконных нормативных актов позволяет сделать вывод о том, что для данного института характерен преимущественно императивный метод правового регулирования.

Таким образом, очевидно, что рассмотренная выше совокупность правовых норм, регулирующих общественные отношения, связанные с обработкой персональных данных и их защитой, имеет все присущие самостоятельному правовому институту отличительные черты.

Для определения места данного института в системе права Российской Федерации следует обратиться к классификации. Как известно, существует деление права на частное и публичное, материальное и процессуальное.

Проведенный выше анализ показывает, что институт персональных данных относится к публичной отрасли права. В то же время, нормы данного института находят свое отражение и в такой традиционно отнесенной к частному праву отрасли как трудовое (главе 14 ТК РФ).

Таким образом, очевидно, что указанный правовой институт регулирует общественные отношения, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому, указанный правовой институт следует рассматривать как межотраслевой.

В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих положений, связанных с организационно-правовой защитой персональных данных работников.

Таким образом, обработка персональных данных обусловлена общими требованиями, которые строятся на базе принципов добровольности, обеспечения равенства возможностей, законности, не допущения дискриминации в трудовых отношениях. Соответственно этим требованиям, содержащихся в нормативно-правовых актах трудового законодательства России, должны соответствовать и не противоречить локальные нормативные акты различных организаций и предприятий, дабы не ущемлять и не нарушать законные интересы гражданина Российской Федерации.

1.3 Этапы организации защиты персональных данных в образовательной организации

Согласно ФЗ №152 «О персональных данных», образовательные организации являются операторами персональных данных**,** поскольку занимаются обработкой персональных данных обучающихся и преподавателей. Следовательно, ответственными сотрудниками этих организаций должно обеспечиваться соблюдение вышеуказанного закона.

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от: неправомерного или случайного доступа к ним; уничтожения; изменения; блокирования; копирования; предоставления; распространения; иных неправомерных действий в отношении персональных данных.

В рамках образовательных организаций должен быть выполнен комплекс работ по сбору пакета документов, предоставляемых на проверку контролирующим организациям.

Пакет документов для проверки:

1. Концепция информационной безопасности.
2. Приказ о создании СЗ ПДн.
3. План мероприятий по обеспечению защиты ПДн.
4. Отчет о результатах проведения внутренней проверки.
5. Перечень сведений, составляющих ПДн.
6. Список ИСПДн, в которых обрабатываются ПДн.
7. Разрешительная система доступа к ПДн.
8. Перечень сотрудников, допущенных к обработке ПДн.
9. Перечень защищаемой информации.
10. Положение по обработке персональных данных.
11. Политика ИБ.
12. Инструкция пользователя ИСПДн.

13. Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.

14. Инструкция администратора ИБ ИСПДн.

15. Инструкция по организации парольной защиты.

16. Инструкция по антивирусной защите.

17. Инструкция по обработке ПДн без использования средств автоматизации.

18. Перечень ПДн с местами хранения, обработки и списком допущенных лиц.

19. Приказ о введении в действие документов, регламентирующих мероприятия по защите ПДн.

20. Приказ о создании комиссии по уничтожению ПДн.

21. Журнал регистрации фактов несанкционированного доступа.

22. Журнал учета обращений субъектов ПДн в ИСПДн.

23. Журнал учета пользователей ИСПДн, прошедших обучение правилам работы с СЗИ.

24. Журнал учета мероприятий по контролю ИБ.

25. План проверочных мероприятий по обеспечению безопасности ПДн.

26. АКТ 1 классификации ИСПДн.

27. Приказ о назначении администратора ИБ.

28. Форма согласия работника на обработку его ПДн.

Организация защиты персональных данных должна производиться в несколько этапов:

- инвентаризация информационных ресурсов;
- ограничение доступа работников к персональным данным;
- документальное регламентирование работы с персональными данными;
- формирование модели угроз безопасности персональных данных;
- классификация информационных систем персональных данных (ИСПДн) образовательных организаций;

– составление и отправка в уполномоченный орган уведомления об обработке персональных данных;

– приведение системы защиты персональных данных в соответствие с требованиями регуляторов;

– создание подсистемы информационной безопасности ИСПДн и ее аттестация (сертификация) – для ИСПДн классов К1, К2;

– организация эксплуатации и контроля безопасности ИСПДн.

Этап 1. Инвентаризация информационных ресурсов.

Инвентаризация информационных ресурсов - выявление присутствия и осуществления обработки персональных данных во всех эксплуатируемых в организации информационных системах и традиционных хранилищах данных. В качестве информационных систем, относящихся к ИСПДн, могут выступать: электронный журнал (1С:Университет); 1С:Бухгалтерия; автоматизированная информационная библиотечная система и другие.

На данном этапе следует:

– утвердить положение о защите персональных данных;

– сформировать концепцию, определить политику информационной безопасности;

– составить перечень персональных данных, подлежащих защите.

Места обработки персональных данных: бухгалтерия; библиотека; кафедры; отдел кадров.

Этап 2. Ограничение доступа работников к персональным данным.

Ограничение доступа работников организации к персональным данным – неотъемлемая часть мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах. Допуск к обработке персональных данных должен быть только у тех сотрудников, которым это необходимо для выполнения служебных (трудовых) обязанностей.

На данном этапе следует: в необходимой мере ограничить как электронный, так и физический доступ к персональным данным, хранящимся в образовательной организации.

Этап 3. Документальное регламентирование работы с персональными данными.

Согласно статье 86 Трудового кодекса РФ, работники и их представители должны быть ознакомлены под роспись с теми документами работодателя, которые устанавливают порядок обработки персональных данных работников, а также их права и обязанности в этой области.

Субъект персональных данных самостоятельно решает вопрос их передачи кому-либо, оформляя свое намерение документально.

На данном этапе следует:

- собрать согласия на обработку персональных данных;
- издать приказ о назначении лиц, ответственных за обработку ПДн;
- издать положение о разграничении прав доступа к обрабатываемым ПДн;
- составить инструкции администратора ИСПДн, пользователя ИСПДн и администратора безопасности ИСПДн.

Согласия на обработку персональных данных физических лиц.

В соответствии со статьей 9 ФЗ-№152 «О персональных данных» обработка персональных данных субъекта осуществляется только при условии наличия его письменного согласия с указанием следующих данных:

- фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва;

– подпись субъекта персональных данных.

Подписанные согласия хранятся в образовательных организациях и могут быть предоставлены только по требованию регуляторов и других уполномоченных органов РФ.

Этап 4. Формирование модели угроз безопасности персональных данных.

В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками (рисунок 1):

- по виду защищаемой от УБПДн информации, содержащей ПДн;
- по видам возможных источников УБПДн;
- по типу ИСПДн, на которые направлена реализация УБПДн;
- по способу реализации УБПДн;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по используемой уязвимости;
- по объекту воздействия.

По видам возможных источников угроз безопасности ПДн выделяются

следующие классы угроз:

− угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

− угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ [39].

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

− угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

− угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);

− угрозы утечки ПДн по техническим каналам утечки информации;

− угрозы специальных воздействий на ИСПДн [39].

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

− угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

− угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

− угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

− угрозы, реализуемые с использованием уязвимости системного ПО;

− угрозы, реализуемые с использованием уязвимости прикладного ПО;

− угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

− угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

− угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

− угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

− угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

− угрозы безопасности ПДн, обрабатываемых на АРМ;

− угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

− угрозы безопасности ПДн, передаваемых по сетям связи;

− угрозы прикладным программам, с помощью которых обрабатываются ПДн;

− угрозы системному ПО, обеспечивающему функционирование ИСПДн [39].

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД), приведены на рисунке 1 и представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий [39].

Рисунок 1 – Классификация угроз безопасности ПДн, обрабатываемых в информационных системах персональных данных

Частная модель угроз безопасности персональных данных, хранящихся в информационной системе, формируется на основании следующих документов, утвержденных Федеральной службой по техническому и экспортному контролю (ФСТЭК):

1. Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн.

На данном этапе следует сформировать модель угроз безопасности персональных данных, обрабатываемых и хранящихся в образовательной организации.

Этап 5. Классификация ИСПДн.

На данном этапе следует составить акты классификации используемых в образовательной организации информационных систем персональных данных.

Этап 6. Составление и отправка в уполномоченный орган уведомления.

Уведомление об обработке персональных данных оформляется на бланке оператора и направляется в территориальный орган Роскомнадзора Министерства связи и массовых коммуникаций РФ на бумажном носителе или в форме электронного документа с подписью уполномоченного лица. В форме указываются данные об обработчике, цель обработки, категории данных, категории субъектов, данные которых обрабатываются, правовое основание обработки, дата ее начала, срок (условие) ее прекращения и прочее.

Этап 7. Приведение системы в соответствие с требованиями регуляторов.

В ФЗ №152 «О персональных данных» сказано, что оператор персональных данных обязан принимать все необходимые меры по защите безопасности ПДн. Это означает потребность оператора в использовании современных высокотехнологичных способов хранения ПДн.

На данном этапе следует:

- создать перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- создать положение о подразделении по защите информации;
- подготовить методические рекомендации для организации защиты информации при обработке персональных данных;
- создать инструкцию пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций;
- утвердить план мероприятий по защите ПДн.

Этап 8. Аттестация (сертификация) ИСПДн.

Для обеспечения безопасности ИСПДн требуется проводить мероприятия по организации и техническому сопровождению защиты обрабатываемых персональных данных. В качестве оценки соответствия ИСПДн 1 и 2 классов требованиям к безопасности ПДн используется обязательная сертификация (аттестация).

На данном этапе следует:

– создать эскизный проект системы обеспечения безопасности информации объекта вычислительной техники;

– создать типовое техническое задание на разработку системы обеспечения безопасности информации объекта вычислительной техники;

– определить порядок резервирования технических средств защиты информации.

Уполномоченными федеральными органами, регулирующими деятельность в сфере обработки персональных данных, являются:

1. *Роскомнадзор* (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) – ведет реестр операторов персональных данных, контролирует обработку персональных данных операторами и рассматривает обращения субъектов персональных данных.

2. *ФСТЭК России* (Федеральная служба по техническому и экспортному контролю) – регулирует сферу обработки и передачи персональных данных между операторами.

3. *ФСБ РФ* (Федеральная служба безопасности РФ) - регулирует сферу использования криптографических средств защиты информации при обработке персональных данных.

Перечень объектов информатизации, подлежащих аттестации

Обязательной аттестации подлежат следующие объекты информатизации:

1. Автоматизированные системы различного уровня и назначения.

2. Системы связи, приема, обработки и передачи данных.

3. Системы отображения и размножения.

4. Помещения, предназначенные для ведения конфиденциальных переговоров.

Этап 9. Организация эксплуатации ИСПДн и контроля за безопасностью.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн.

На данном этапе следует:

1. Разработать проект приказа о положении об электронном журнале обращений пользователей информационных систем персональных данных → создать журнал учета обращений субъектов ПДн о выполнении их законных прав и журнал учета мероприятий по контролю.

2. Сформировать план внутренних проверок → издать приказ о проведении внутренней проверки → составить отчет о результатах проведения внутренней проверки.

Поддержание эффективной системы защиты ПДн

Для поддержания системы защиты персональных данных на высоком уровне требуется проведение следующих мероприятий:

1. Развертывание полноценной системы обработки ПДн.

2. Полномасштабное внедрение средств защиты.

3. Аттестация ИСПДн.

4. Приведение всех процессов обработки ПДн в соответствие с требованиями закона.

5. Реакция на регулярные проверки и прочее.

Ответственность за нарушение ФЗ №152 «О персональных данных»:

1. Административная ответственность: штраф или штраф с конфискацией несертифицированных средств обеспечения безопасности и шифровальных средств. *Административный кодекс, ст. 13.11, 13.12, 13.14.*

2. Дисциплинарная ответственность: увольнение провинившегося работника. *Трудовой кодекс РФ, ст. 81 и 90.*

3. Уголовная ответственность: от исправительных работ и лишения права занимать определенные должности до ареста. *Уголовный кодекс, ст. 137, 140, 272.*

Выводы по главе 1

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.

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.

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

Основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152- ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных.

3. Описаны 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.

В целом защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности любой организации. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности.

ГЛАВА 2 АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФГБОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1 Общие сведения об 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 Министерства здравоохранения РФ» — высшее учебное заведение федерального подчинения, реализующее многоуровневую непрерывную систему подготовки специалистов: довузовская подготовка (профориентация в школах, подготовительные курсы, медико-биологические классы лицеев и гимназий), обучение в вузе, последипломная подготовка, повышение квалификации и переподготовка врачей, а также сертификация специалистов и подготовка научно-педагогических кадров.

Важнейшим направлением образовательной политики вуза является совершенствование практической подготовки студентов. Ее основу составляют клиника, клинические базы, центр практических навыков.

В соответствии с лицензией на право осуществления образовательной деятельности в университете осуществляется подготовка специалистов по следующим уровням образования:

- среднее профессиональное образование;

– высшее образование: бакалавриат, специалитет, ординатура, аспирантура;

– дополнительное образование: дополнительное образование детей и взрослых, дополнительное профессиональное образование.

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

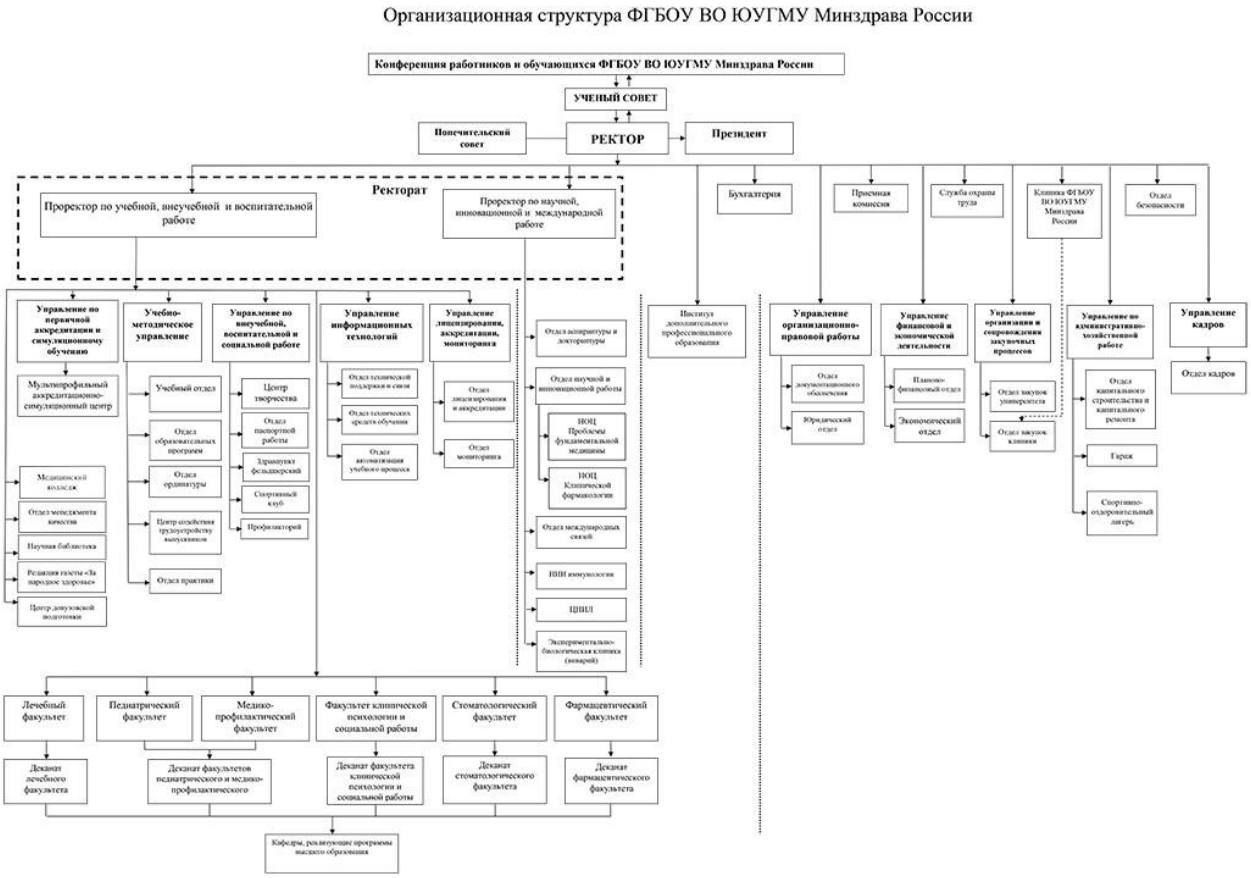

Рисунок 2 – Организационная структура [54]

Университет располагается в 4 корпусах, расположенных на улице Воровского рядом с областной больницей, первый корпус расположен по адресу ул. Воровского 64, там же находится административные подразделения вуза. В этих корпусах расположены теоретические кафедры, обучающие студентов первых 3 курсов. Студенты после 3 курса приступают к обучению на клинических кафедрах, расположенных в больницах города Челябинска. Так же в распоряжении университета имеются общежития для студентов, хозяйственные пристройки и корпус ЦНИЛ, в котором ведется научно-исследовательская работа.

Основные виды деятельности ФГБОУ ВО ЮУГМУ Минздрава России:

1) образовательная деятельность по реализации образовательных программ высшего образования, среднего общего образования, среднего профессионального образования, дополнительных профессиональных программ дополнительных общеобразовательных программ, основных: профессиональных образовательных программ послевузовского медицинского образования и фармацевтического образования в интернатуре, а также деятельность по подготовке научных кадров в докторантуре в соответствии с законодательством Российской Федерации в рамках государственного задания, устанавливаемого министерством;

2) научная деятельность в части осуществления фундаментальных поисковых и прикладных научных исследований в соответствии с законодательством Российской Федерации;

3) деятельность, связанная с правовой охраной и использованием результатов интеллектуальной деятельности в соответствии с законодательством Российской Федерации;

4) деятельность по обороту наркотических средств, психотропных веществ и их прекурсоров, культивированию наркосодержащих растений (в части оборота наркотических средств, психотропных веществ, внесенных в списки II и III перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации);

5) медицинская деятельность в части оказания населению специализированной, в том числе высокотехнологичной, медицинской помощи в объемах, устанавливаемых министерством;

6) фармацевтическая деятельность, осуществляемая в сфере обращения лекарственных средств для медицинского применения для обеспечения лечебно-диагностического и образовательного процессов Университета (изготовление лекарственных препаратов, хранение лекарственных препаратов, перевозка лекарственных препаратов, отпуск лекарственных препаратов в структурные подразделения Университета);

7) деятельность, связанная с использованием возбудителей инфекционных заболеваний, в том числе размещение, эксплуатация, техническое обслуживание, хранение оборудования и другого материально-технического оснащения, необходимого для осуществления данного вида деятельности;

8) заготовка, хранение, обеспечение безопасности и клиническое использование донорской крови и ее компонентов для обеспечения медицинской деятельности Университета;

9) деятельность, связанная с источниками ионизирующих излучений и радиоизотопов короткого действия, в том числе их наработка, размещение, эксплуатация, техническое обслуживание и хранение;

10) ветеринарная деятельность, в том числе содержание, разведение и подготовка лабораторных животных для медико-биологических исследований;

11) проведение в Университете санитарно-противоэпидемических (профилактических) мероприятий;

12) деятельность, связанная с утилизацией медицинских и биологических отходов;

13) содержание и эксплуатация информационно-вычислительной и материально-технической баз, необходимых для осуществления образовательной, научной, медицинской и иной деятельности Университета;

14) деятельность, связанная с содержанием и эксплуатацией транспортных средств, находящихся в оперативном управлении Университета;

15) издание и распространение научной, учебной, методической, справочной литературы и иной печатной продукции, содержащей результаты деятельности университета, осуществляемой за счет средств федерального бюджета;

16) деятельность, связанная с оказанием услуг по организации физкультурно-оздоровительных, спортивных и культурно-развлекательных мероприятий для обучающихся и работников Университета;

17) деятельность по защите сведений, составляющих государственную тайну, а также иной охраняемой законом информации в соответствии с возложенными на Университет задачами и в пределах его компетенции;

18) деятельность по мобилизационной подготовке, гражданской обороне, предупреждению и ликвидации чрезвычайных ситуаций в соответствии законодательством Российской Федерации [54].

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. Развитие информационных технологий в рамках административно-управленческих процессов в университете.

2. Поддержание компьютерной сети университета в работоспособном состоянии.

3. Обеспечение бесперебойной работы компьютерного оборудования университета.

4. Организация освоения и применения новых программных и технических средств, информационных технологий, накопление и

систематизация общего и тематического прикладного программного обеспечения.

5. Техническое обеспечение работ по вопросам лицензирования и аккредитации университета, ежегодной отчетности.

6. Анализ эффективности использования программных средств.

Функции отдела:

1. Обеспечение подразделения университета доступом к ресурсам сети Интернет.

2. Поддержание в рабочем состоянии и совершенствование компьютерную сети университета. Обеспечение сотрудников университета услугами электронной почты. Обеспечение комплексной защиты сети от компьютерных вирусов разных видов.

3. Развитие информационных технологий в рамках административно-управленческой деятельности.

4. Обеспечение бесперебойной работы компьютеров, компьютерной сети университета, компьютерного периферийного оборудования и пользователей.

5. Внедрение проектов системы автоматизированного управления университета.

6. Выявление и оперативное устранение перебоев в работе оборудования и пользователей.

7. Анализ и изучение проблем автоматизированных систем управления университета и ее подразделений.

8. Участие в составлении технических заданий по внедрению автоматизированной системы управления университета.

9. Подготовка планов внедрения автоматизированных систем управления университета и контроль за их выполнением.

10. Определение задач, их алгоритмизация, увязка организационного и технического обеспечения автоматизированной системы управления университета.

11. Контроль состояния и безопасности сети и сетевого оборудования.

12. Назначение пользователям сети прав доступа.

13. Установка, настройка и управление программными и аппаратными системами университета.

14. Анализ и учет случаев отказа системы.

15. Разработка и проведение мероприятий по повышению качества и надежности автоматизированных систем управления университета.

16. Модернизация применяемых технических средств.

17. Составление заявок на необходимое оборудование, ведение учета его поступлений и использования средств, выделенных на эти цели. Подготовка документации на проведение конкурсов и аукционов при закупке компьютерной и оргтехники для нужд университета.

18. Обеспечивать системами внутренней автоматической телефонной связи городка университета.

19. Обеспечивать своевременное и регулярное техническое обслуживание компьютерной техники и оргтехники подразделений университета.

20. Консультации пользователей информационно-вычислительной системы университета по вопросам использования компонентов системного программного обеспечения.

21. Техническая поддержка учебных компьютерных классов.

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

Таким образом, отдел технической поддержки и связи выполняет возложенные на него функции в тесном сотрудничестве и взаимодействии со всеми кафедрами и структурными подразделениями университета и другими ВУЗами: центрами дистанционного образования, центрами Интернет-тестирования, учебно-научными центрами по проблемам информационной безопасности в системе высшей школы.

2.2. Анализ информационных систем в ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ: структура, функционирование, средства защиты

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	Представ-ление	Передача				Использование	Хранение
		Источник	Получатель	Среда передачи	Использование шифрования		
Персональные данные сотрудников Персональные данные обучающихся	Выгрузка из БД	ПК сотрудников бухгалтерии	ПАО Челябинвестбанк	Интернет	Да, VPN-KEY-TLS	ПК сотрудников бухгалтерии	ПК сотрудников бухгалтерии
Персональные данные сотрудников Персональные данные обучающихся	Выгрузка из БД	ПК сотрудников бухгалтерии и отдела кадров	УПФР, ИФНС, ФСС	Интернет	Да, СКЗИ КриптоПро CSP 4	ПК сотрудников бухгалтерии и отдела кадров	1С: Предприятие, БД СТЭК Электронная 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.

2.3 Анализ рисков и уязвимостей системы защиты персональных данных

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.

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 [15]:

- несанкционированный доступ - 2%;
- укоренения вирусов - 3%;
- технические отказы аппаратуры сети - 20 %;
- целенаправленные действия персонала - 20 %;
- ошибки персонала (недостаточный уровень квалификации) - 55 %.

Таким образом, одной из потенциальных угроз информации в информационных системах следует считать целенаправленные или случайные деструктивные действия персонала (человеческий фактор), так как они составляют 75 % всех случаев [29, С. 7].

Рассматривая исходные ИСПДн на исходный уровень защищенности, берется в расчет технические и эксплуатационные характеристики.

Рассматриваемая ИСПДн имеет средний (Y1=5 - согласно Методике) уровень исходной защищенности, т.к. не менее 70% характеристик ИСПДн соответствуют уровню защищенности не ниже «средний».

Вероятность реализации угрозы безопасности персональных данных.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

1) маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2= 0);

2) низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

3) средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (У2 = 5);

4) высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (У2 = 10).

Показатель исходной защищенности ИСПДн.

Технические и эксплуатационные характеристики ИСПДн «Сотрудники»:

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

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

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

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

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

6. 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.

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

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 Y_1=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,

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».

На основе полученных коэффициентов реализации угрозы и параметрах опасности угроз, делается вывод о актуальности данной угрозы.

Модель угроз является неотъемлемым документов при создании системы персональных данных. Именно модель угроз указывает на приоритетные 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 1.

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 представлена в приложении 2.

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, 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.

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

Выводы по главе 2

Во второй главе магистерской диссертации проведен анализ информационных систем ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения РФ, а также рассмотрены модели угроз безопасности персональных данных при их обработке в информационных системах вуза.

«Южно-Уральский государственный медицинский университет Министерства здравоохранения РФ» — высшее учебное заведение федерального подчинения, реализующее многоуровневую непрерывную систему подготовки специалистов: довузовская подготовка (профориентация в школах, подготовительные курсы, медико-биологические классы лицеев и гимназий), обучение в вузе, последипломная подготовка, повышение квалификации и переподготовка врачей, а также сертификация специалистов и подготовка научно-педагогических кадров.

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»).

Модель угроз является неотъемлемым документов при создании системы персональных данных. Именно модель угроз указывает на приоритетные направления защиты информации в организации.

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.

ГЛАВА 3. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ

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

На основе анализа рисков и уязвимостей системы защиты персональных данных и анализа нормативно-правовых требований 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. Информационные ресурсы:

- персональные данные работников и обучающихся (исходная информация, информационные базы данных);

- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн.

2. Технические информационные системы и средства Организации, в которых обрабатывается, хранится и передается информация ПДн.

3. Помещения объектов Организации, в которых размещаются информационные ресурсы, и обрабатываются ПДн.

4. Технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Субъекты информационных отношений

1. Субъектами информационных отношений являются:

- обучающиеся (субъекты персональных данных) - физические лица, родители (законные представители) которых состоят в договорных и иных гражданско-правовых отношениях с Организацией-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом;

- сотрудники (субъекты персональных данных) - физические лица, состоящие или готовящиеся вступить в трудовые или иные гражданскоправовых отношениях с Организацией-оператором.

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.

Различают явную и неявную компрометацию ключей. Явной называется компрометация, факт которой становится известным на отрезке установленного времени действия данного ключа. Неявной называется компрометация ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

События, квалифицируемые как явная компрометация:

− утрата ключевого носителя;

− утрата ключевого носителя с последующим обнаружением;

− нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации.

К событиям, связанным с неявной компрометацией ключей и требующим их рассмотрения в каждом конкретном случае, относятся:

− навязывание заведомо ложной информации в документах, защищенных имитовставками;

− случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями, содержащими ключевую информацию, в том числе случаи, когда дискета (eToken и др.) вышла из строя и доказательно не опровергнуто, что данный факт произошел в результате несанкционированного доступа злоумышленника.

При наступлении компрометации ключа или подозрения в компрометации ключа пользователь СКЗИ обязан немедленно прекратить работу с СКЗИ и сообщить ответственному пользователю СКЗИ о факте компрометации (в том числе и предполагаемом).

По факту компрометации ключей (в том числе предполагаемому) проводится служебная проверка.

По завершению расследования оформляется письменное заключение (акт) о проведении служебной проверки. Скомпрометированные ключи по завершению расследования подлежат уничтожению.

Взамен скомпрометированных ключей ответственный пользователь СКЗИ производит замену ключей в порядке, предусмотренном технической и эксплуатационной документацией.

2. Разработать памятку пользователя СКЗИ.

3. Разработать схему криптографической защиты. В схеме криптографической защиты должны быть указаны наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются, обладатели конфиденциальной информации, реквизиты договоров на оказание услуг по криптографической защите конфиденциальной информации, а также указаны типы применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники.

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 4.

Типовая форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) расположена в приложении 5.

6. Разработать порядок уничтожения СКЗИ и ключевых документов.

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

Для обеспечения безопасности ПДн при их обработке в информационных системах необходимо провести:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн,

- определить способы и состав средств защиты информации (СЗИ), разработать техническое задание (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;

- ввод в эксплуатацию.

Исходя из этого, необходимо разработать инструкцию по проведению внутренних проверок состояния защиты персональных данных в образовательной организации высшего образования.

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

Провести обучение пользователей правилам работы 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.

Программа обучения учитывает требования:

- Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;

- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- постановления Правительства Российской Федерации от 16 апреля 2012 г. № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению

работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 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»;

- положения «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденных Приказом ФСБ России от 9 февраля 2005 г. № 66;

- инструкции о порядке работы с криптографическими средствами;

- технической и эксплуатационной документации на средства криптографической защиты информации (далее – СКЗИ).

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

Учебная программа состоит из основных разделов:

– общие вопросы защиты информации;

– организация обеспечения защиты конфиденциальной информации при использовании электронной подписи в документообороте органов исполнительной власти Челябинской области;

– правила работы с СКЗИ.

Перечень тем и их краткое содержание расположено в приложении 6.

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.

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 по защите персональных данных в вузе.

3.2. Оценка эффективности рекомендаций по орагниазции системы защиты персоналных 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.

Контроль может проводиться как администратором безопасности с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям.

После построения системы защиты персональных данных в ИСПДн необходимо оценить эффективность их защиты. Сначала составляются общие критерии гипотетической оценки с указанием средств, которые обеспечат беспристрастный и полноценный анализ.

Программа и методика оценивания.

В программе обязательно должны быть:

- оцениваемый объект;
- запротоколированная очередность мероприятий, включая список и содержание проводимых процедур;
- итоговые оценочные критерии.

Критерии проверки:

1. Полная документация по объекту.
2. Анализ структуры ИСПДн и техпроцесс обработки информации.
3. Оценка уровня защиты.
4. Проверка структуры ИСПДн согласно заявленной документации.

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

6. Вопросы охраны проверяемого объекта.

7. Есть ли штатные средства защиты, как они настроены.

8. Оценка уровня компетентности лиц, ответственных за защиту ПДн.

9. Проверка знаний персонала ИСПДн по информационной безопасности.

10. Проверка прав доступа.

11. Регистрация и учет.

12. Обеспечение целостности.

13. Антивирус и все базы.

14. Общий анализ уровня защиты.

15. Обнаружение вторжений.

16. Файрвол и его настройки.

17. Уровень защиты каналов связи.

18. Проверка защиты ИСПДн сканером безопасности.

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

Если ИСПДн не прошла испытания на соответствие требованиям по созданию эффективной защиты обрабатываемой информации, то разрабатываются предложения по устранению недостатков и, по возможности, недостатки устраняются еще до окончания процедуры оценки.

Процесс определения эффективности СЗИ начинают с выбора и обоснования критериев, а затем переходят к подбору или разработке методик расчета показателей эффективности. На практике используются следующие виды критериев [45]: экономическая эффективность; позволяющие оценивать качество СЗИ; позволяющие определить достаточность применяемых мер защиты.

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 экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной

карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым 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.			

Продолжение таблицы 3

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

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 безопасности персональных данных.	Высокий уровень	Высокий уровень	Высокий уровень
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).

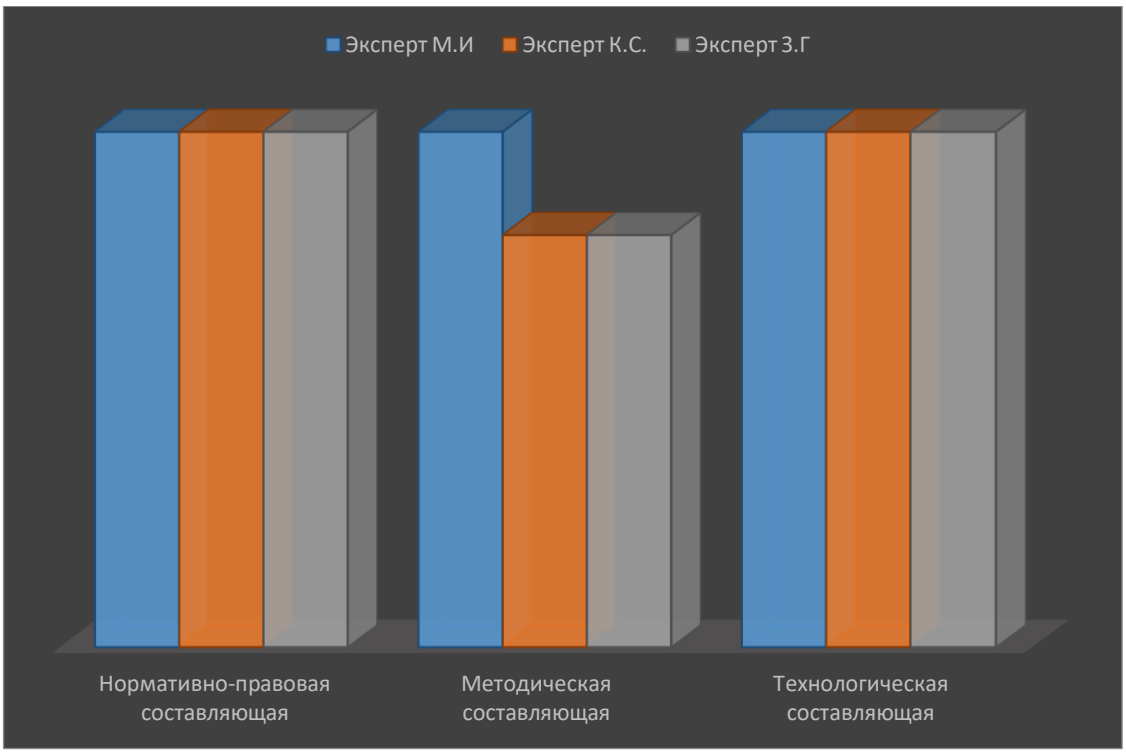

Рисунок 3 – Сводные результаты экспертной оценки эффективности разработанных рекомендаций по совершенствованию организационных и технических мер защиты персональных данных Университета

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 главе 3

В третьей главе магистерской диссертации 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

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.

Основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152- ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных.

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.

В третьей главе магистерской диссертации 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 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

Нормативно – правовые акты

1. Конституция Российской Федерации: офиц. текст. - М.: Право, 2002. - 39 с.

2. Гражданский кодекс Российской Федерации: ФЗ от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. - 2006. - №52. Ч. 1. Ст. 5496.

3. Доктрина информационной безопасности Российской Федерации от 09.09.2000: утверждена Президентом РФ В. Путиным // Известия. - 10 декабря 2002. - С.2.

4. О государственной тайне: ФЗ по состоянию на 22.08.2004. / Федер. Собр. Рос. Федерации. - М.: ГД РФ, 2004. - 12 с.

5. О коммерческой тайне: ФЗ от 29 июля 2004 № 98 // Собрание актов Президента и Правительства РФ. - № 7. - С.5.

6. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. - № 7. - 2006. - С.15.

7. Об архивном деле в Российской Федерации: ФЗ от 01 октября 2004 № 125 - ФЗ // Собрание актов Президента и Правительства РФ. - № 11. - С.12.

8. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. - №31

9. Об утверждении Перечня сведений конфиденциального характера от 06.03.97 № 188: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 23. С.12 – 14.

10. Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну: постановление правительства РФ от 03.10.2002 № 731 // Собрание актов Президента и Правительства РФ. - 2003. - № 11. - 140 с.

11. Об утверждении положения о государственной системе защиты информации от иностранной технической разведки и от ее утечки по техническим каналам от 15.09.93 № 912 - 51: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 15. - 125 с.

12. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 2002. - № 8. - С.102.

13. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. URL - https://base.garant.ru/192223/. Дата обращения: 21.09.2020.

14. Об утверждении правил оказания услуг телеграфной связи: постановление Правительства РФ от 15 апреля 2005г. № 222 // Собрание актов Президента и Правительства РФ. - 2005. - № 5. - С.45.

15. Об утверждении Перечня сведений, отнесенных к государственной тайне от 30.11.95 № 1203: с измен. и доп. от 24.01.98 № 61, от 06.06.2001 № 659, от 10.09.2001 № 1114, от 29.05.2002 № 518, от 11 февраля 2006: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 2006. - № 11.

16. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства РФ от 3 ноября 1994 г. № 1233. // Собрание актов Президента и Правительства РФ. - 1995. - № 10. - С.56.

17. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). URL - https://clck.ru/B8yGj. Дата обращения: 14.12.2020.

18. ГОСТ Р 51141. - 98. Делопроизводство и архивное дело. Термины и определения. - М.: Изд-во стандартов, 2003.

19. ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения. - М.: Изд-во стандартов, 1993.

20. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

22. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnye-terminy-i-opredeleniya.html. Дата обращения: 16.12.2020.

23. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

24. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

25. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. [Электронный ресурс]. - URL: http://www.opengost.ru/iso/13_gosty_iso/13110_gost_iso/4958-gost-r-iso_mek-to-13335-3-2007-it.-metody-i-sredstva-obespecheniya-bezopasnosti.-chast-3.-metody-menedzhmenta-bezopasnosti-informacionnyh-tehnologiy.html. Дата обращения: 16.12.2020.

Литература

26. Авдеев М.Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. №1. С. 49 – 54.

27. Ажмухамедов, И.М., Ханжина, Т.Б. Определение оптимального комплекса мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Мат. методы в технике и технологиях – ММТТ-24: сб. трудов XXII Междунар. науч. конф.: в 10 т. Т.9. Секция 13 / под общ. ред. В.С Балакирева. Саратов: Изд-во Саратовского гос. технического университета, 2011. 187с., С.73-75.

28. Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» (постатейный) // СПС КонсультантПлюс. 2013.

29. Астахова Л.В., Завадский А.О. Особенности организации защиты персональных данных в образовательной организации // Вестник УрФО. Безопасность в информационной сфере. – 2013 – № 3(9). – С.4-10.

30. Бадьина А. Обработка, порядок хранения и передвижения персональных данных // Кадровик. Кадровое делопроизводство. 2012. №1. С. 162 – 171.

31. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: [Утверждена заместителем директора ФСТЭК РФ 15.02.2008 г.]. - Режим доступа: www.fstec.ru. Дата обращения: 15.01.2021.

32. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации (постатейный). 2-е изд., перераб. и доп. Москва: Проспект, 2015. 272 с.

33. Богатырева, Ю.И. Информационная безопасность образовательных организаций: проблема и пути ее решения [Текст] / Ю.И. Богатырева // Новые информационные технологии в образовании, IX международной научно-практической конференции. 2016 Издательство: Российский государственный профессионально-педагогический университет (Екатеринбург), с. 125-130.

34. Бугров А. Международные стандарты для построения системы информационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.

35. Бурькова Е.В. Система защиты персональных данных в высшем учебном заведении // Интеллект. Инновации. Инвестиции. – 2017. – № 7. – С. 69-74.

36. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. URL - https://www.intuit.ru/studies/courses/10/10/info. Дата обращения: 20.10.2020.

37. Ильгова О. Этапы организации защиты ПДн в ОО (для администратора). – URL: https://help.dnevnik.ru/hc/ru/articles/203475268. Дата обращения: 16.12.2020.

38. Ильин К. Вопросы информационной безопасности при электронном документообороте / К. Ильин // Защита информации. INSIDE. - 2016. - № 4. - С.18 - 25.

39. Кузнецова Т. В. Организация работы с персональными данными // Делопроизводство. 2011. №2. С. 3 – 8; Трудовое право. 2011. №5. С. 77 –83.

40. Лушников А. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. 2014. № 9. С. 93–101; № 10. С. 77–82. СПС «КонсультантПлюс», 2014. Версия 4015.00.09, сборка 208002 (дата обращения: 13.01.2021).

41. Медведева Т. М. О работе с персональными данными работников // Актуальные вопросы бухгалтерского учета и налогообложения. 2014. №21. С. 77 – 88.

42. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.

43. Мельник Н.Ю. Защита персональных данных в профессиональном образовании // Современные технологии: актуальные вопросы, достижения и инновации. – 2018. – С. 55-57.

44. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

45. Меры по защите от угроз нарушения доступности [Электронный ресурс]. - URL: www.sha-danis.narod.ru. Дата обращения: 20.12.2020.

46. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008) Электронный документ. Режим доступа: http://fstec.ru/. Дата обращения: 20.12.2020.

47. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. Дата обращения: 15.01.2021.

48. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 13 декабря 2013 г.).

49. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31.03.2015 N 149/7/2/6-432). Электронный документ. Режим доступа: http://docs.cntd.ru/document/420336137. Дата обращения: 16.01.2021.

50. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). Электронный документ. Режим доступа: http://fstec.ru/. Дата обращения: 16.01.2021.

51. Методы организации защиты информации [Текст]: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2013. – 80 с.

52. Милютина О.В. Особенности защиты информации в образовательном учреждении [Текст] / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/fea

tures_information_security_in_an_educational_institution.php. Дата обращения: 10.12.2020.

53. Модели угроз информационной безопасности [Электронный ресурс]. - Режим доступа: www.arinteg.ru. Дата обращения: 19.12.2020.

54. Официальный сайт ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации. – URL: http://www.chelsma.ru/. Дата обращения: 19.12.2020.

55. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом. // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2015. – № 110. –С. 866-894.

56. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

57. Постановление Правительства РФ от 03.02.2012 N 79 (с изм. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/. Дата обращения: 16.12.2020.

58. Постановление Правительства РФ от 03.03.2012 N 171 (с изм. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/. Дата обращения: 16.12.2020.

59. Постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512 // «Российская газета», № 148, 11.07.2008.

60. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета», № 200, 24.09.2008.

61. Привалов А.Н., Богатырева Ю.И., Романов В.А. Методологические подходы к организации безопасной информационно-образовательной среды вуза // Образование и наука. – 2017. – Т. 19. – № 4. – С. 169-183.

62. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // «Российская газета», № 4637, 12.04.2008.

63. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства связи и массовых коммуникаций РФ от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/815-sovmestnyj-prikaz-fstek-rossii-fsb-rossii-i-minkomsvyazi-rossii-ot-31-dekabrya-2013-g-n-151-786-461. Дата обращения: 16.12.2020.

64. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при

использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211.

65. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.05.2013.

66. Пугачев В.П. Руководство персоналом организации: учеб. пособие / В.П. Пугачев. - М.: Аспект-Пресс, 2015. - 279 с.

67. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: [Утвержден решением председателя Гостехкомиссии при Президенте РФ 30.03.1992 г.]. - Режим доступа: www.consultant.ru. Дата обращения: 17.12.2020.

68. Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 – 13.

69. Фионова Л.Р Положение о защите персональных данных работников / Л.Р. Фионова, О.В. Касперская // Секретарское дело. - 2015. - № 10. - С.40 - 49.

70. Храмцовская Н.А. Закон о персональных данных: последствия для делопроизводства / Н.А. Храмцовская // Делопроизводство и документооборота на предприятии. - 2017. - № 2. - С.12 – 30.

71. Ярочкин В.Н. Информационная безопасность / В.Н. Ярочкин. - М.: Трикста, Академ. проект, 2015. - 542 с.

ПРИЛОЖЕНИЕ 1

**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 2

**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 3

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 4

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 5

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 выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя 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 (уничтожения)	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 6

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_____