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

Минимизация рисков нарушения безопасности в системе защиты персональных данных образовательных организаций

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
77,86 % авторского текста

Работа рекомендована к защите
«27» декабря 2025 г.
Зав. кафедрой АТ, ИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Задорожная Надежда Викторовна

Научный руководитель:
доктор технических наук, профессор
Дмитриев Михаил Сергеевич

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Защита персональных данных (далее – ПДн) сегодня - одно из важных направлений и первостепенных задач в обеспечении информационной безопасности учебного заведения, которое обрабатывает и хранит огромнейшую базу данных об абитуриентах, студентах, их родителях, сотрудниках, членах региональных органов управления, контрагентах, партнерах и просто лицах, посещающих образовательную организацию. Если раньше личные данные обрабатывались в бумажном формате, то сегодня обработка персональных сведений человека перешла в информационные системы, что предопределено появлением современных средств вычислительной техники и телекоммуникаций, которые, с одной стороны, упростили способы обработки массива данных, но с другой - породили угрозы и уязвимости, специфические для компьютерных систем и сетей.

Однако внедрение информационных технологий и распространение электронных систем документооборота способствовали и росту числа преступлений, связанных с неправомерным использованием личных данных. К ПДн как информационным ресурсам относятся следующие сведения: данные в системах бухгалтерского и кадрового учета; сведения о клиентах; контакты юридических лиц, являющихся контрагентами; данные почтовых систем клиентов и работников и др. Правонарушения в области обработки с помощью компьютера или электронных систем информации, включая персональные данные, характеризуются сложностью сбора улик, скрытностью, трудностью доказывания.

Преступления в области нарушения конфиденциальности и обеспечении неприкосновенности баз ПДн учебного заведения может стать причиной невосполнимого ущерба и привести к многочисленным рискам, среди которых могут оказаться в первую очередь финансовые риски, которые приведут к денежным потерям в связи с необходимостью

принятия срочных мер по устранению последствий данной проблемы (безусловно, это организация расследования, а также принятие мер и проведение профилактических и корректирующих мероприятий), также это потеря репутации образовательной организации или же полная остановка его деятельности.

Поэтому быстрое развитие и совершенствование информационных технологий, современного электронного обмена информацией, свободного доступа к средствам массовых коммуникаций, широкими возможностями в части копирования и распространения любой информации привело к росту важности обеспечения информационной безопасности ПДн. Это стало на сегодняшний день объективной реальностью.

Безусловно, что и раньше организации, которые обрабатывали базы персональных данных, принимали всевозможные меры по их защите, однако делали они это на основе собственных представлений в соответствии с внутренней политикой, направленной на регулирование сферы информационной безопасности. Сегодня ситуация по данному вопросу выглядит иначе. Причиной тому является федеральный закон № 152 [59], который был принят в Российской Федерации в 2006 году и закрепил на правовом уровне требования к юридическим лицам, являющимся операторами персональных данных. Кроме того, данный нормативно-правовой акт предусмотрел ответственность физических лиц, которые в соответствии с выполняемыми должностными обязанностями осуществляют сбор, обработку, хранение, передачу ПДн.

Важным шагом в развитии законодательной базы по вопросам защиты ПДн стало Постановление Правительства № 1119 [43], которое включило требования к защите персональных данных, которые должны выполняться при обработке личных сведений человека с учетом типа данных и характеристик применяемых информационных систем. При этом в указанном выше Постановлении оговаривается, что необходимо учитывать также виды угроз для разных систем и уровни защищенности

каждого типа систем. Также важно помнить, что оператор обработки ПДн должен выбирать средства защиты информации в полном соответствии с требованиями, закрепленными в нормативно-правовых актах ФСБ и ФСТЭК Российской Федерации.

В ФЗ-152 «О персональных данных» [59] закреплено, что персональные данные являются информацией ограниченного доступа, поэтому обеспечение защиты прав и свобод человека и гражданина при обработке его личных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну - цель выше указанного нормативно-правового документа.

За нарушение положений ФЗ-152 предусматриваются различные виды ответственности: административная, уголовная, гражданская, дисциплинарная и др. В некоторых случаях на основании данного закона может быть приостановлена образовательная деятельность организации или даже отозвана лицензия. Поэтому защита ПДн является важной и неотъемлемой частью успешной работы каждого учебного заведения.

Однако при существующих нормативно-правовых актах все равно правонарушения в части защиты личных данных сохраняют высокую степень распространенности. По сведениям, официально опубликованным Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, например, в Роскомнадзор за 2021 год от граждан пришло более 38 тысяч жалоб по поводу неправомерной обработки их ПДн [40]. Большая часть жалоб касалась неправомочных действия владельцев интернет-сайтов, включая социальные сети, а также организаций жилищно-коммунального хозяйства, различных кредитных учреждений и банков, коллекторских агентств. Безусловно, это объясняется в большинстве случаев тем, что граждан передавали свои персональные данные в связи с различными обязательствами, включая и обязательства финансового характера. Поэтому на действия указанных

выше категорий операторов как обычно поступает наибольшее количество жалоб.

Кроме того, необходимо отметить, что на сегодня ведется Реестр нарушителей прав субъектов ПДн, в который вошло 93 информационных ресурса и составлено больше 220 протоколов о привлечении к административной ответственности за нарушения положений Федерального закона «О персональных данных» [59] на основании судебных решений в области защиты ПДн [40].

Исходя из представленного выше анализа можно отметить следующее противоречие: наличие большого числа нормативно-правовых документов, призванных регулировать вопросы защиты ПДн при их обработке, отмечается сохранение высокого количества преступлений в этой сфере.

Среди наиболее распространенных на сегодняшний день Роскомнадзор отмечает следующие замечания и ошибки:

1) различие между фактической деятельностью оператора и сведениями, представленными в уведомлении об обработке персональных данных (учитывая изменения, указанные в информационных письмах о внесении корректировок в реестр операторов персональных данных) - часть 3 статьи 22 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных») [59];
2) игнорирование оператором мер по обеспечению неограниченного доступа к документу посредством его опубликования, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных (часть 2 статьи 18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных») [59];
3) невыполнение мер, необходимых для обеспечения осуществления обязательств, предусмотренных Федеральным законом и

принятыми в соответствии с ним нормативными правовыми актами (часть 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») [59];

4) оператором не определены места хранения персональных данных (материальных носителей) (пункт 15 постановления Правительства Российской Федерации от 15.09.2008 № 687) [45].

Все это говорит о высокой важности и актуальности темы нашего исследования «Минимизация рисков нарушения безопасности в системе защиты персональных данных образовательной организации».

Цель исследования заключается в следующем: разработать комплекс мер и мероприятий по минимизации рисков нарушения безопасности в системе защиты персональных данных образовательной организации.

Объект исследования: процесс обработки персональных данных профессиональной образовательной организацией.

Предмет исследования: комплекс мер и мероприятий минимизации рисков нарушения безопасности в системе защиты персональных данных профессиональной образовательной организации.

Гипотеза исследования заключается в предположении о том, что система защиты персональных данных образовательной организации будет устойчивее к внешним негативным воздействиям, если разработать и внедрить комплекс мероприятий и мер минимизации рисков нарушения безопасности в системе защиты персональных данных образовательной организации на основе их анализа.

Задачи исследования, поставленные в соответствии с объектом, предметом и целью работы, следующие:

– изучить различные источники информации, раскрывающие основные понятия, содержание и цели информационной безопасности, в том числе при обработке ПДн, а также состав и

классификацию методов обеспечения информационной безопасности при обработке ПДн;

- описать систему информационной безопасности при обработке ПДн профессиональной образовательной организации;
- проанализировать угрозы и риски при обработке ПДн в профессиональной образовательной организации;
- разработать и апробировать комплекс мер и мероприятий по совершенствованию методов обеспечения информационной безопасности при обработке персональных данных в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» на основании собранных данных, проверить его эффективность.

Теоретико-методологической основой исследования являются научные работы, рассматривающие вопросы информационных технологий в целом и проблемы информационной безопасности, а также защиты информации, включая персональных данных, в частности. Рассматриваемая в данной работе проблема объединяет две отрасли: с одной стороны, это необходимость нормативно-правового регулирования данного вопроса, с другой – отражение достижений и постоянное развитие информационных технологий. Большая часть научных исследований, отражающих вопросы информационной безопасности и защиты информации, касались проблемы защиты ПДн поверхностно, а многие работы, в которых рассматриваются и вопросы регулирования безопасности ПДн, отражают, как правило, общие подходы к решению проблемы без ожидаемой конкретизации.

В основу данной работы положены результаты исследований в части:

- теоретических подходов к решению вопросов информационного права и правового обеспечения информационной безопасности

(среди наиболее значимых следует назвать работы таких авторов, как И.Л. Бачило [5], В.Н. Лопатин [30], В.А. Копылов [9], М.М. Рассолов [55], В.А. Пожилых [41] и др.);

– рассмотрения вопросов обеспечения информационной безопасности с учетом достижений в области разработки технических средств и методов защиты (высоких результатов в этой сфере достигли такие ученые, как И.В. Котенко [27-29], И.Б. Саенко [28], А.А. Молдовян [34], А.Л. Балыбердин [24], В.А. Герасименко [8], М.А. Вус [24], А.А. Малюк [28] и др.).

В работах, названных выше авторов, имеются достаточные научные предпосылки для решения проблемы, стоящей в центре нашего исследования. Однако предлагаемые решения скорее носят ограниченный по областям применения и хаотичный по методам характер.

В соответствии с поставленными задачами и выдвинутой нами гипотезой в настоящей работе были использованы такие методы исследования, как: анализ теоретической, нормативно-правовой и методической литературы, законодательных документов и материалов, регулирующих процесс защиты персональных данных; обобщение и систематизация собранных данных; наблюдение и оценка системы безопасности качественным методом и методом экспертной оценки; статистическая обработка полученных данных; проектирование комплекса мер и мероприятий на основании проделанной работы.

Базой исследования является государственное бюджетное профессиональное образовательное учреждение «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

Положения, выносимые на защиту:

разработанный комплекс мероприятий и мер, представляющий собой 36 организационных и технических мер по обеспечению безопасности ПДн колледжа по 9 направлениям (идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к

объектам доступа; защита машинных носителей ПДн; регистрация событий безопасности; антивирусная защита; контроль (анализ) защищенности ПДн; защита технических средств; защита информационной системы, ее средств, систем связи и передачи данных; управление конфигурацией информационной системы и системы защиты персональных данных) и рассчитанный на реализацию в течение одного года позволит снизить количество реализованных угроз, что доказывает, что система защиты ПДн образовательной организации устойчивее к внешним негативным воздействиям при условии разработки и внедрения комплекса мероприятий и мер по минимизации рисков нарушения безопасности ИСПДн на основе их анализа.

Научная новизна состоит в обосновании возможности необходимого обновления существующей системы информационной безопасности при обработке ПДн в профессиональной образовательной организации посредством разработки комплекса мер и мероприятий минимизации рисков нарушения безопасности в системе защиты сведений личного характера граждан.

Представленное исследование имеет **теоретическую значимость**, которая состоит в обогащении и углублении научных представлений о методах обеспечения информационной безопасности при работе с персональными данными в профессиональных образовательных учреждениях.

Практическая значимость представленного исследования определяется тем, что разработанный комплекс мер и мероприятий минимизации рисков нарушения безопасности в системе защиты ПДн может применяться для совершенствования методов обеспечения информационной безопасности при обработке ПДн в других профессиональных образовательных организациях.

Основные этапы исследования. Настоящее исследование включало три этапа в период с 2022 по 2024 г.

На первом (подготовительном) этапе формулировались тема исследования, уточнялся план научной работы, а также выполнялся сбор информации по вопросу исследования из различных источников, разрабатывалась и уточнялась гипотеза, формулировались цель и задачи исследования.

Второй этап – основной – предполагал проведение комплексной работы, включающей в себя: изучение научной, нормативно-правовой, методической и технической литературы, отбор необходимых источников информации, анализ современных методов обеспечения информационной безопасности при обработке персональных данных профессиональной образовательной организации на различных уровнях защиты, публикация научных статей по теме исследования.

На третьем этапе осуществлялся анализ системы безопасности по обработке персональных данных ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», являющегося базой исследования и разработки рекомендаций по совершенствованию методов обеспечения информационной безопасности при обработке персональных данных в профессиональной образовательной организации, а также было выполнено текстовое оформление материалов исследования и сформулированы выводы.

Апробация результатов исследования.

Основные результаты данного исследования были представлены на IV Международной научно-практической конференции VIII Уральского вернисажа науки и бизнеса (г. Челябинск, 11 апреля 2024 г.), педагогическом совете, посвященном вопросам информатизации образовательного процесса ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» (г. Челябинск, 25 января 2024 г.).

Результаты работы внедрены в практику деятельности ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

Также по теме нашего исследования были опубликованы две статьи, в которых нашли отражение теоретические принципы и результаты работы:

1. Задорожная, Н. В. К вопросу о защите ПДн в эпоху цифровизации / Н. В. Задорожная // Управление, экономика и общество: проблемы и пути развития : сб. ст. участников IV Междунар. науч.-практ. конф. VIII Уральского вернисажа науки и бизнеса (Челябинск, 11 апреля 2024 г.) / под общ. ред. Е. П. Велихова ; отв. за выпуск Е. А. Колесник. - Челябинск : Изд-во Челяб. гос. ун-та, 2024. - 289 с. – С. 87-88;
2. Задорожная, Н. В. Риски нарушения безопасности в системе защиты персональных данных: методы оценки / Н. В. Задорожная // Материалы международного электронного научно-методического издания «Инновационный вестник – 2025». – Курган : изд-во Кург.гос.колледжа, 2025 *(планируется к выпуску в январе 2025 г.).*

В ходе написания данной работы был проведен анализ системы информационной безопасности при обработке ПДн образовательной организации, были выявлены угрозы и риски в информационной системе колледжа, а также разработан комплекс мер и мероприятий, позволяющий усовершенствовать уже имеющиеся методы обеспечения информационной безопасности при обработке персональных данных в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего». Это и являлось личным участием и вкладом соискателя в разработку обозначенной проблемы.

Структура работы. Представленная работа включает в себя введение, теоретическую и практическую главы, основные выводы по

каждой главе, а также заключение, список использованных источников, три приложения. Основная часть работы представлена на 109 страницах машинописного текста, в числе которых 8 рисунков и 9 таблиц. Список использованных источников состоит из 63 наименований. Приложения представлены на 38 страницах.

ГЛАВА 1 АНАЛИЗ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РИСКОВ В СИСТЕМЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Российская и зарубежная нормативно-правовая база в сфере защиты персональных данных

Нужно отметить, что в течение последних лет проблема защиты персональных данных была и остается неизменно острой. Данный вопрос поднимается среди высокопоставленных лиц и в России, и за рубежом. Причина этого кроется, думается, в том, что данная проблема касается каждого человека, вне зависимости от гражданства и должности.

История вопроса защиты личных данных человека уходит корнями в необходимость обеспечения неотъемлемых прав и свобод граждан любого государства. С приходом информационных технологий проблема защиты персональных данных приобретает с каждым днем все большую актуальность. В зарубежной практике часто используется термин privacy, буквально переводимый как «частная жизнь», «личная жизнь», «уединение», «личное пространство», «приватность», «конфиденциальность», что подчеркивает важность сохранения личных границ, включая ПДн.

Общепризнанные на международном уровне стандарты, принципы, правила обработки персональных данных, которые остаются актуальными и сегодня, заложены в «Конвенции №108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» [26], которая была внедрена в жизнь с 1981 года. Российская Федерация присоединилась к данному документу лишь спустя 20 лет - в 2001 году. Названная выше Конвенция отразила важные подходы к обработке ПДн, к числу которых относится, например, возможность использования ПДн только в соответствии с конкретными целями и в

течение ограниченного времени, неизбыточность и актуальность обрабатываемых персональных данных, защита данных и др. В названном выше документе раскрыто и содержание понятия «персональные данные».

Кратко сравним законодательство разных стран в области защиты персональных данных, для этого рассмотрим нормативно-правовую базу России, США и государств, являющихся членами Европейского Союза.

В нашем государстве действует несколько нормативных правовых документов, касающихся управления вопросами обработки личной информации, включая Федеральный закон № 152 «О персональных данных», который был принят в 2006 году (далее – ФЗ-152) [59]. Этот закон устанавливает ключевые термины и разъясняет их значение, описывает принципы и методы работы с персональными данными, а также определяет обязанности оператора по получению разрешения от граждан перед сбором их личных сведений и подчеркивает важность защиты собранных данных. Следовательно, ФЗ-152 включает положения об этичном и правомерном использовании личных данных, но при этом делается акцент на обязательное наличие согласия субъекта этих данных.

В Российской Федерации также применяются другие нормативные правовые акты в области защиты персональных данных, которые уточняют положения данного закона и регулируют, например, требования по защите персональных данных при их обработке в информационных системах ПДн [43], состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [46], требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона «О персональных данных» [47], способы оценки угроз безопасности информации [31] и др.

Анализ правовых норм европейских стран в области защиты персональных данных выявил, что существующие законы базируются на тех же принципах, что и в России, требующих от операторов обработки

данных работать в соответствии с законами, открыто, прозрачно, честно на основании имеющегося согласия субъекта данных. Важными документами в Европе являются: Общее положение о защите данных (далее - GDPR); Директивы о конфиденциальности в электронном пространстве, о защите данных, о конфиденциальности электронных сообщений; Законы Великобритании, Франции, Германии о защите данных; Органический закон Испании о защите данных и гарантии цифровых прав; Итальянский кодекс защиты данных; Закон Нидерландов о защите персональных данных и другие [38; 6].

Основным нормативным актом в области защиты персональных данных в Европе является Общий регламент по защите данных (GDPR), принятый в 2018 году. Он имеет юридическую силу во всех странах-членах ЕС. GDPR основывается на строгих, прозрачных и обязательных принципах, обеспечивающих высокий уровень защиты личной информации. Этот документ считается одним из самых всеобъемлющих и эффективных нормативных актов в этой области, получив признание за свою эффективность и требование к организациям внедрять меры по защите данных и уведомлять власти о случаях утечек в течение 72 часов. Примечательно, что GDPR предоставляет физическим лицам больше прав по сравнению с Россией и США, включая право доступа, удаления и передачи своих данных другим компаниям [38; 6].

Теперь рассмотрим законодательство США в области обработки персональных данных, которое отличается сложностью, многослойностью и фрагментированностью. Здесь отсутствует единый федеральный закон о защите персональных данных. Вместо этого существует множество федеральных законов и нормативных актов отдельных штатов, регулирующих разные аспекты обработки данных. Например, Закон о точной кредитной отчетности (FCRA) контролирует использование персональных данных в кредитных отчетах. Закон штата Калифорния о конфиденциальности потребителей (CCPA) защищает личную

информацию жителей Калифорнии. Закон о переносимости и ответственности медицинского страхования (HIPAA) регулирует обработку медицинских данных. Кроме этих законов, есть и другие, такие как Закон о защите конфиденциальности детей в Интернете (COPPA) и Закон Грэма-Лича-Блайли (GLBA).

Некоторые исследователи вопросов защиты ПДн уверены, что разрозненные законодательные акты США не могут обеспечить гражданам этой страны достаточный уровень защиты персональных данных. При этом нужно отметить, что нормативно-правовая база этого государства содержит недостаточные требования к предприятиям и организациям по реализации мер в области защиты персональных данных [9].

Таким образом, сопоставляя законодательную базу России, США и стран Европы, регулирующую вопросы обработки ПДн, можно отметить как общее, так и различное. Например, разница наблюдается в наличии или отсутствии единого, общего для всех граждан, документа в области обработки и защиты ПДн, необходимости хранения персональных данных в стране, гражданином которой является субъект ПДн, в широком или узком круге прав субъекта персональных данных, обязанности предприятий и организаций в случае обнаружения сообщать об утечке ПДн в течение 72 часов.

Однако во всех странах, нормативно-правовая база которых проанализирована в настоящем параграфе, предъявляется идентичное требование, что операторы, прежде чем обрабатывать персональные данные, должны получить согласие физических лиц, а также обязаны принимать разные меры, которые позволят обеспечить безопасность сведений личного характера. Кроме того, все указанные выше страны имеют законы и подзаконные акты, наделяющие граждан правом доступа к своим личным данным и в случае необходимости их исправления.

Также сходными являются такие основные принципы обработки персональных данных включают такие аспекты, как: правомерность,

честность и открытость процесса обработки; целевое ограничение обработки; минимизация объема данных; точность информации; ограничения по срокам хранения; а также целостность и конфиденциальность для обеспечения безопасности персональных данных.

В перспективе, думается, все страны пойдут по пути уточнения законодательной базы в отношении различных отраслей экономики. Зачатки этого мы уже наблюдаем в нормативно-правовых документах России (например, Приказ № 255 от 22 ноября 2016 г. «Об обработке ПДн в федеральном агентстве связи») и США (например, Закон о переносимости и подотчетности медицинского страхования (HIPAA)).

Итак, в ходе сравнительного анализа российской и зарубежной законодательной базы в области обработки ПДн выявлено, что имеющиеся нормативно-правовые документы в сфере защиты ПДн России, США и стран Европы имеет идентичные фундаментальные принципы, направленные на защиту прав граждан. Однако в ближайшей перспективе развитие нормативно-правовой базы в области защиты ПДн пойдет по пути конкретизации под запросы общества с учетом сферы применения.

1.2 Информационная безопасность в системе защиты персональных данных: ключевые понятия

Информационная безопасность стала важной составляющей современного общества. Она регулируется различными правовыми актами, особое место среди которых занимают те, что касаются защиты персональных данных. Существует множество законов, приказов и методических указаний, раскрывающих основы защиты ПДн, однако ключевым документом в этой области является Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ (далее – ФЗ-152) [59]. Именно он определяет основные принципы и понятия по вопросу защиты персональных данных. Предлагаем остановиться на них детальнее.

В статье 3 ФЗ-152 под *персональными данными* (далее – ПДн) понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [59]. По нашему мнению, данная дефиниция термина предоставляет общее понимание персональных данных, не детализируя конкретные элементы, которые помогут отличить одного человека от другого, увидеть уникальные идентифицирующие признаки каждой личности.

В «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» дается более конкретное определение: «персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация» [2].

Таким образом, по нашему мнению, необходимо внести ясность, что к личным данным относятся следующие виды информации: паспортные данные, такие как фамилия, имя, отчество, дата и место рождения, место жительства; данные о детях, родственниках и семейном положении; фотографии или видеозаписи, которые позволяют установить личность человека; информация о размере заработной платы; результаты оценок профессиональных навыков и личных качеств; личные данные, включающие этническую и национальную принадлежность, религиозные и политические убеждения, философские взгляды, состояние здоровья; сведения о наличии или отсутствии судимости; контактная информация, такая как номер телефона, электронная почта, IP-адрес, а также другие идентификаторы в социальных сетях и мессенджерах; серия и номер паспорта, СНИЛС, ИНН; биометрическая информация, включая цвет глаз, дактилоскопические узоры, форму ушных раковин и т.д.

При этом нужно отметить следующий факт: некоторые из этих сведений, упомянутые отдельно, без указания на другие данные человека, не являются персональными. Рассмотрим это на примере: указание только адреса электронной почты не является случаем разглашения ПДн субъекта, но если база оператора обработки ПДн эту информацию содержит вместе со сведениями о фамилии, имени и отчестве владельца, то это уже персональные данные.

Остановимся еще на одном понятии. «Совокупность программно-аппаратных, информационных элементов и информационных технологий, применяемых при обработке ПДн, называется *информационными системами ПДн* (далее – ИСПДн)» [59].

Любая ИСПДн включает в себя такие неотъемлемые, обязательные элементы, как:

1) ПДн, вносимые в базы данных в качестве совокупности информации и ее носителей, используемых в ИСПДн;
2) используемые при обработке ПДн информационные технологии;
3) различные технические средства, посредством которых обрабатываются ПДн (к примеру, они могут включать в себя средства и системы для передачи, получения и обработки персональных данных, информационно-вычислительные комплексы и сети, устройства и системы для записи звука и другие подобные компоненты.) (далее - технические средства ИСПДн);
4) программное обеспечение, такое как операционные системы, системы управления базами данных и другие;
5) средства обеспечения информационной безопасности;
6) вспомогательное техническое оборудование и системы [2].

Также необходимо раскрыть еще два существенных понятия, которые в том числе рассматриваются в ФЗ-152:

под *субъектом персональных данных* будем подразумевать «физическое лицо, сведения о котором обрабатываются оператором, то есть собираются, хранятся, передаются и т.д.» [59];

оператор – «государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными» [59].

Обработка персональных данных включает в себя следующие действия (операции) или их различное сочетание: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [59].

Важнейшей задачей при обработке ПДн считается обеспечение информационной безопасности. Предлагаем рассмотреть подробнее толкование данного термина, которое включено в «Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [2]. *Безопасность персональных данных* - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных [59].

Информационная безопасность в системе защиты персональных данных обеспечивается в зависимости от *классификации персональных данных*. В соответствии с ФЗ-152 выделяются следующие категории ПДн:

общедоступные, специальные, биометрические и иные [59]. Проанализируем этих понятиях детальнее.

К общедоступным персональным данным относится личная информация, доступ к которой разрешен субъектом персональных данных. Именно наличие согласия со стороны человека-носителя персональных данных является существенным признаком ПДн этой категории. Ошибочно считать общедоступными персональными данными сведения, которые можно обнаружить в открытом, общем доступе (чаще всего в этом случае рассматривается как источник Интернет).

Вот еще одна категория персональных данных, которая обозначается как *«специальные».* В эту категорию входят такие данные, как информация о религиозных убеждениях, национальном и / или расовом происхождении, политических и философских взглядах, состоянии здоровья, включая наличие хронических заболеваний, особенности частной жизни. Важным моментом в данной категории ПДн являются сведения о наличии или отсутствии судимости (эту информацию часто запрашивают при трудоустройстве, а при поступлении на работу в образовательные организации без нее вообще невозможно обойтись).

Биометрические персональные данные – еще одна категория - включают информацию о физиологических и биологических характеристиках субъекта ПДн, например: изображения внешности, в том числе фотографии, дактилоскопические узоры, генетическую информацию (ДНК), рисунок радужной оболочки глаз, образцы голоса. Однако в этом случае также должно быть указание на конкретное лицо, то есть другие сведения, позволяющие идентифицировать человека. Например, сканирование радужки глаза, используемое для распознавания сотрудников при входе в офис, может рассматриваться как биометрические персональные данные.

Под *иными данными* понимаются любые другие сведения о человеке, которые не были упомянуты ранее. К таким данным могут относиться,

например, номер телефона, адрес электронной почты, принадлежность к определенной социальной группе, стаж работы, место регистрации или проживания и т.д.

В Постановлении Правительства РФ от 1 ноября 2012 г. № 1119 [43] и в статье 19 ФЗ-152 [59] раскрываются меры и мероприятия, необходимые для обеспечения информационной безопасности в системе защиты ПДн. Однако при этом хочется отметить, что в статье 18.1 ФЗ-152 говорится, что оператор имеет право самостоятельно определять «состав и перечень мер, необходимых и достаточных для обеспечения информационной безопасности персональных данных» [59], и при этом уточняется, что данный перечень должен в том числе включать следующие обязательные мероприятия:

1) назначение оператором и закрепление приказом сотрудника, ответственного за организацию обработки персональных данных;
2) издание оператором политики обработки персональных данных и других внутренних регламентов, которые обязательно включают цель ПДн, категории субъектов, список обрабатываемых персональных данных, методы и сроки их обработки и хранения, а также порядок уничтожения этих сведений;
3) функционирование организации на основе правовых, организационных и технических мер, позволяющих обеспечить безопасность персональных данных;
4) внутренний контроль и (или) аудит соответствия обработки персональных данных нормативно-правовым документам, включая локальные;
5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства, а также соотношение данного вреда и мер, принимаемых оператором и направленных на обеспечение безопасности персональных данных;

6) ознакомление работников, которые непосредственно осуществляют обработку персональных данных, с законодательством Российской Федерации и локальными регламентами по вопросам обработки персональных данных, в том числе посредством освоения этими сотрудниками дополнительных образовательных программ по вопросам информационной безопасности;
7) создание условий посредством публикации на официальном сайте организации неограниченного доступа к локальным регламентам по вопросам регулирования процесса обработки ПДн.

При обработке персональных данных оператор в соответствии со статьей 19 ФЗ-152 обязан обеспечивать выполнение системы правовых, организационных и технических мер, позволяющих защитить персональные данные от любых действий, способных скомпрометировать информационные системы ПДн.

Давайте рассмотрим предложенные меры детальнее:

1) идентификация угроз безопасности персональных данных во время их обработки в информационных системах персональных данных (далее - ИСПДн);
2) разработка, утверждение и выполнение регламентов доступа к ПДн в рамках обработки в ИСПДн, включая ведение журнала и учёт всех операций с данными;
3) реализация организационных и технических мероприятий по защите персональных данных при их обработке в ИСПДн, которые необходимы для выполнения требований по защите этих данных;
4) применение сертифицированных средств защиты информации для удаления персональных данных по мере необходимости в соответствии с установленными требованиями;

5) оценка эффективности применяемых мер по защите персональных данных перед запуском информационной системы обработки персональных данных;
6) обеспечение восстановления изменённых и/или удалённых в результате несанкционированного доступа баз данных ПДн;
7) учет машинных носителей персональных данных;
8) постоянный мониторинг и регистрация случаев неправомерного доступа к персональным данным, а также реализация мероприятий, включающих выявление, предотвращение и устранение последствий кибератак на информационные системы персональных данных и реагирование на инциденты в этих системах [59];
9) организация регулярного мониторинга соблюдения мер защиты ПДн и безопасности ИСПДн согласно установленному уровню защищённости.

Детализированно состав и содержание мер по обеспечению безопасности персональных данных рассмотрен в Приказе ФСТЭК РФ от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [42].

Важно учитывать, что при работе с персональными данными возникают определённые риски, связанные с любыми несанкционированными действиями в отношении личных сведений субъекта ПДн. Это может быть намеренное уничтожение или искажение ПДн, незаконная передача третьим лицам или использование ПДн в коммерческих целях и др. Любое из данных действий способно привести к негативным последствиям. Более подробно риски при обработке ПДн мы обсудим в параграфе 1.3 представленной работы.

С рисками достаточно тесно связан термин «угроза безопасности персональных данных». В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» под *актуальными угрозами безопасности ПДн* подразумевается «совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия» [43].

Предлагаем рассмотреть более подробно три типа угроз безопасности персональных данных, при этом отметим, что для установки каждого из них оператору необходимо учитывать масштабы возможного ущерба (вреда). Так мы видим, что в первых двух случаях угрозы исходят из используемого программного обеспечения:

1) риски, обусловленные наличием скрытых функций в применяемом системном программном обеспечении;
2) угрозы, вызванные присутствием скрытых возможностей в используемом прикладном программном обеспечении;
3) в третьем случае информационная система подвержена угрозам, которые не связаны с наличием скрытых возможностей в системном и прикладном программном обеспечении.

Учитывая выше сказанное о типах угроз, можно выделить четыре уровня защиты персональных данных, которые в дальнейшем будут учитываться при обеспечении мер и мероприятий по информационной безопасности. Для большей наглядности представим их в табличном формате. Предлагаем остановиться на них более подробно (см. таблицу 1).

Таблица 1 – Уровни защищенности ПДн, их характеристика и требования к обеспечению защищенности

Уровни защищенности ПДн (УЗ)	Характеристика информационной системы (далее – ИС)	Требования к организации и обеспечению защиты ПДн
УЗ - 4	а) в обработке общедоступные ПДн, реализуются угрозы 3-его типа; б) в процессе обработки оказываются иные категории ПДн работников оператора или иные категории ПДн менее чем 100 000 субъектов ПДн, не являющихся работниками оператора, для них актуальны угрозы 3-его типа	а) организация режима обеспечения безопасности помещений, в которых размещена ИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей ПДн; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз
УЗ - 3	а) обработку проходят общедоступные ПДн работников оператора или общедоступные ПДн менее чем 100 000 субъектов ПДН, не из числа работников оператора, для которых актуальны угрозы 2-ого типа; б) обрабатываются иные категории ПДн работников оператора или иные категории ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора, и актуальны угрозы 2-ого типа; в) в обработке специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100 000 субъектов ПДн, не	см. выше пункты а), б), в), г) в третьем столбце таблицы 1, а также д) должно быть назначено ответственное за обеспечение безопасности ПДн в ИС должностное лицо из числа сотрудников организации

Продолжение таблицы 1

	из числа работников оператора, для них характерны угрозы 3-его типа; г) обработке подвергаются биометрические ПДн субъектов, для которых актуальны угрозы 3-его типа; д) в обработке иные категории ПДн более чем 100 000 субъектов ПДн, не работников оператора, и актуальны угрозы 3-его типа	
УЗ - 2	а) в обработке оказываются общедоступные ПДн субъектов, для которых актуальны угрозы 1-ого типа; б) обрабатываются специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100 000 субъектов ПДн, не являющихся работниками оператора; проявляются угрозы 2-ого типа; в) в обработке находятся биометрические ПДн субъекта, для которых актуальны угрозы 2-ого типа; г) в обработке общедо-ступные ПДн более чем 100 000 субъектов ПДн, не являющихся работниками оператора, и имеют место угрозы 2-ого типа; д) обрабатываются иные категории ПДн более чем 100 000 субъектов персональных данных, не являющихся работниками оператора, и актуальны угрозы 2-ого типа; е) обрабатываются специальные категории ПДн более чем 100 000 субъектов	см. выше пункты а), б), в), г), д) в третьем столбце таблицы 1, а также е) доступ к содержанию электронного журнала сообщений возможен исключительно для должностных лиц из числа сотрудников оператора или для уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения должностных обязанностей

Продолжение таблицы 1

	ПДн, не работников оператора, и актуальны угрозы 3-его типа	
УЗ - 1	а) в ИС обработку проходят либо специальные категории ПДн, либо биометрические ПДн, либо иные категории ПДн, и актуальны угрозы 1-ого типа; б) в ИС обрабатываются специальные категории ПДн более чем 100 000 субъектов ПДн, не являющихся работниками оператора, и актуальны угрозы 2-ого типа	см. выше пункты а), б), в), г), д), е) в третьем столбце таблицы 1, а также ж) автоматическая регистрация в электронном журнале безопасности изменения полномочий работника оператора по доступу к ИСПДн; з) создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИС, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности

Рассмотрим характеристики ИСПДн, которые являются предпосылками возникновения угроз безопасности ПДн (далее – УБПДн):

1) объем и категория обрабатываемых данных в ИСПДн, имеющих частный характер;
2) состав и строение ИСПДн;
3) наличие соединений ИСПДн с общественными сетями связи и/или международными информационными сетями;
4) атрибуты подсистемы безопасности ПДн, обрабатываемых в ИС;
5) организация способов и сроков обработки персональных данных;
6) режимы разделения прав доступа для пользователей ИСПДн;
7) местоположение;
8) условия установки технического оборудования информационных систем персональных данных.

Систематизация списка УБПДн и классификация угроз безопасности [2] позволяет разработать на их основе частные модели УБПДн для конкретного вида ИСПДн (см. подробнее об этом в главе 2).

Таким образом, в параграфе 1.2 были рассмотрены такие основные понятия в области безопасности в системе защиты ПДн, как: персональные данные, оператор обработки ПДн, субъект ПДн, ИСПДн, риски, угрозы

безопасности ПДн и др., а также проанализированы основные нормативно-правовые документы, регулирующие вопросы обеспечения защиты ПДн.

1.3 Риски нарушения безопасности в системе защиты персональных данных

Термины «риск» в широком смысле и «риск информационной безопасности» в более узком значении объемны по содержанию и по-разному раскрываются в отдельных стандартах и методиках. Рассмотрим некоторые из них.

В соответствии с таким нормативным документом, как «ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем», *риск* трактуется как «сочетание вероятности события и его последствий» [14]. Такое определение представленного термина более общее, широкое, требующее уточнения.

Однако нас в первую очередь интересует *риск информационной безопасности*, под ним понимают «потенциальную возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации» [11].

Еще один стандарт понятие *«риск»* раскрывает в виде «влияния неопределенности на цели» [12]. При этом дается пояснение, что «влияние - это отклонение от ожидаемого - положительное или отрицательное, а неопределенность - это состояние, даже частичное, недостатка информации, относящейся к событию, его последствиям или вероятности, пониманию или знанию о нем» [12]. В связи с чем термин «риск» часто связывается с потенциальными, возможными, вероятностными «событиями», а также с их «последствиями» или их различными сочетаниями, комбинациями. Другими словами, в отношении ПДн *риски информационной безопасности* могут быть растолкованы как влияние неопределенности, неизвестности на цели информационной безопасности,

в связи с чем риск информационной безопасности, так сказать, определяется вероятностью того, что угрозы смогут использовать уязвимости информационных ресурсов или их совокупности, нанося тем самым ущерб образовательной организации. Данная трактовка понятия «риск» отражено в нормативно-правовом регламенте «ГОСТ ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [12].

Рассмотрим еще одну дефиницию понятия «*риск»*, под которым подразумевается «потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов» [13]. В таком контексте риск определяется как сочетание вероятности определенного события и его возможных последствий.

Проанализируем еще одно определение термина «риск» - это «сочетание вероятности нанесения ущерба и тяжести этого ущерба» [10].

Во всех указанных выше определениях общими являются такие элементы, как потенциальность (возможность, вероятность, неопределенность, событие), угроза (опасность), уязвимость, актив / группа активов, ущерб (вред, последствия). Из данных составляющих логично выстраивается определение *риска – это потенциальное / возможное / вероятностное событие, которое в случае реализации создаст угрозу / опасность использования уязвимости актива / группы активов в целях нанесения ущерба / вреда / последствия.* Данное определение будет использовано в нашем исследовании в качестве рабочего.

Конкретизируем данное определение применительно к рискам нарушения безопасности в системе защиты ПДн. Однако требуется пояснить, что активом, то есть конкретным физическим или виртуальным объектом-источником уязвимостей, которые могут провоцировать

реализацию угроз [58], выступает ИСПДн. В этом случае понятие «*риск нарушения безопасности в системе защиты персональных данных»* может быть раскрыто как потенциальное / возможное / вероятностное нарушение безопасности в системе защиты ПДн, которое в случае реализации создаст угрозу / опасность использования уязвимости системы защиты ПДн в целях нанесения ущерба / вреда / последствия организации.

Для полного, однозначного понимания риска уточним также значения терминов «угроза» и «уязвимость». *Угроза* – «любые негативные события, которое могут нанести ущерб организации, причина нежелательных событий» [58]. *Уязвимость* – «слабость, особенность, свойство информационного актива из-за которого становится возможна реализация угрозы» [58].

При этом позволим себе отметить, что риски могут быть как личностного характера, вызванные умыслом третьих лиц, так и обезличенными, то есть техногенными, связанными с ошибками / неосторожностью персонала, обеспечивающего обработку ПДн. Рассмотрим виды информационных рисков при обработке ПДн в зависимости от сферы возникновения:

1) внутренние, инсайдерские (риски похищения или изменения сведений вследствие выполнения служебных (трудовых) обязанностей сотрудником, имеющим доступ к информационным системам);
2) внешние (субъект угроз получает несанкционированный доступ к ПДн, используя возможности информационных сетей общего пользования);
3) технические (данные риски проявляются при использовании возможностей аппаратных закладок и программ, которые предназначены для хищения электронных данных).

Существуют и другие классификации рисков [54]. Например, по природе происхождения можно выделить такие риски, как:

1) случайные, возникающие в результате непредвиденных событий, стечения обстоятельств, приводящие к нежелательным последствиям (к этой группе относятся внезапные риски, поэтому, как правило, не поддающиеся прогнозу, например: выход из строя технического оборудования в результате перебоев электроэнергии);
2) субъективные, источником происхождения которых являются ошибки и неправильные действия персонала при обработке ПДн (как правило, причина данных рисков кроется в невыполнении внутренних регламентов и правил безопасности организации, например: допущение несанкционированного доступа к конфиденциальной информации);
3) объективные, проявляющиеся по причине использования защитных систем и сопутствующего технического оборудования и возникающие в результате внедрения в ИС вредоносного программного обеспечения. Особенностью данной группы рисков является невозможность их полного исключения, так как существующие сегодня системы защиты несовершенны и, как правило, отстают от скорости развития несанционированных приемов злоумышленников.

Рассмотрим еще одну классификацию рисков по уровню проявления, в соответствии с которой выделяются такие виды риска, как допустимый, критический и катастрофический [3]. Остановимся на них подробнее:

1) допустимый, предполагающий, что потери возможны, но их размер меньше ожидаемой предпринимательской прибыли;
2) критический, связанный с опасностью потерь в размере произведенных затрат по осуществлению данного вида предпринимательской деятельности;

3) катастрофический, характеризующийся опасностью, угрозой потерь в размере, равном или превышающем все имущественное состояние предприятия [54].

При обработке ПДн может реализоваться любой из указанных выше рисков, рассмотренных в ходе анализа трех классификаций; это связано с особенностями системы защиты ПДн образовательной организации.

Однако хотелось бы остановиться еще на одной классификации, анализирующей риски с точки зрения масштаба проявления:

1) локальный, проявившийся на уровне отдельной компании или ее структурных звеньев;
2) отраслевой, характерный для конкретной отрасли;
3) региональный, охватывающий компании конкретных экономических регионов государства;
4) национальный, реализованный на уровне макроэкономики (причиной этого могут выступить непрогнозируемые изменения в политической и экономической ситуации, в законодательстве, в налогообложении, в концепции кредитования и т.п.);
5) международный, вызванный новшествами в структуре мирового рынка, во взаимоотношениях между разными государствами, различными масштабными (порой стихийными) бедствиями и т.д. [54].

В ходе написания данной работы речь пойдет о первом виде рисков из представленных в рассмотренной классификации, поскольку данное ограничение отражено в теме нашего исследования.

Таким образом, в параграфе 1.3 проанализированы следующие понятия: «риск», «риск информационной безопасности», «риск нарушения безопасности в системе защиты ПДн», «угроза», «уязвимость», «актив». Кроме того, представлены четыре классификации рисков и определены виды рисков, которые могут реализоваться при нарушении безопасности в системе защиты ПДн.

1.4 Сравнительный анализ методов оценки рисков нарушения информационной безопасности в системе защиты персональных данных

Определение информационных систем и активов, выявление их слабых мест и создание списка потенциальных угроз являются обязательными этапами перед оценкой рисков нарушения информационной безопасности при возникновении угроз. Эти действия необходимы для того, чтобы впоследствии можно было выбрать соответствующие методы и инструменты защиты данных.

В настоящее время при оценке рисков нарушения информационной безопасности в системе защиты ПДн используются такие методы, как количественный, качественный, статистический, факторный, метод экспертной оценки и др., целью которых является осознание реальных рисков нарушения информационной безопасности той или иной организации, составление актуального перечня угроз, выбор средств защиты ПДн и разработка эффективных контрмер. Каждый из названных выше методов имеет свои преимущества, но при этом можно отметить и их недостатки. Предлагаем рассмотреть данные методы подробнее.

В первую очередь остановимся на *качественном методе оценки рисков* нарушения информационной безопасности, который используется в условиях, когда невозможно представить возможный ущерб от реализации угроз и рисков в числовом формате. Это означает, что при внедрении в деятельность данного метода оценки не применяются никакие количественные показатели. В том числе при использовании этого способа оценки невозможно ущербу присвоить денежное выражение. Вместо этого оцениваемый объект получает рейтинговый показатель по трехбалльной (низкая, средняя, высокая) или, например, десятибалльной шкале (от 0 до 10).

Использование метода качественной оценки предполагает следование алгоритму, рассмотрим его более детально:

1) начинать следует с оценки значимости информационных активов по степени их критичности и возможным негативным последствиям при нарушении безопасности;
2) составить прогноз вероятности осуществления угроз для информационных активов, применяя, к примеру, трёхбалльную качественную шкалу;
3) на следующем этапе нужно определить вероятность успешной реализации угрозы, основываясь на текущем состоянии информационной безопасности и применённых мерах защиты (в этом случае также можно обратиться к трехбалльной качественной шкале);
4) сделать заключение о степени риска с учетом данных, полученных на основании пп.1-3 настоящего алгоритма (в данной ситуации лучше использовать пятибалльную или десятибалльную систему оценок и представить результаты в виде таблицы, чтобы наглядно показать, как различные сочетания показателей (ценность, вероятность, возможность) влияют на уровень риска);
5) подытожить каждую угрозу, учитывая степень риска, и на основе полученных выводов разработать набор мер, контрмер и действий для каждой актуальной угрозы, чтобы снизить уровень риска и в целом обеспечить информационную безопасность [62].

Метод качественной оценки рисков включает сбор данных с использованием анкет, интервью, опросов среди целевой аудитории, а также, при необходимости, личных встреч. Для успешного применения этого метода в области информационной безопасности необходимо привлекать сотрудников, обладающих соответствующим опытом и компетенциями в исследуемой области угроз.

Второй метод оценки рисков получил название *количественный,* что предопределено сферой его использования. Данный метод используется для определения уровня рисков и угроз, в случае реализации для которых

ущерб (негативные последствия) может быть обозначен с помощью конкретных цифр, в том числе имеющих процентное, денежное, временное выражение или в объеме человеческих ресурсов (могут использоваться и другие числовые показатели). Внедрение в практику количественного метода дает возможность точно определить размеры потенциальных убытков при возникновении информационных угроз и связанных с ними рисков. Отметим, что в этом случае объектами анализа рисков становятся элементы, которые имеют четкие числовые параметры. Это может быть, к примеру, оценка стоимости активов, пострадавших от угроз и рисков, расходы на защитные меры или же размер ущерба от реализации этих угроз и др.

Включение в работу по оценке рисков количественного метода предполагает выполнение следующего алгоритма:

1) определить денежную стоимость информационных активов;
2) оценить возможные потери для каждого информационного актива в случае возникновения угроз;
3) определить вероятность возникновения каждой угрозы, опираясь на анализ статистических данных и результаты опроса сотрудников и заинтересованных сторон; это позволит точнее установить частоту инцидентов, связанных с осуществлением различных угроз информационной безопасности в течение указанного периода;
4) выразить общий потенциальный ущерб от каждой угрозы для каждого актива за указанный период, то есть оцифровать;
5) подытожить результаты анализа в виде количественных показателей убытков для каждой угрозы, затем выбрать одно из решений: принять риск, уменьшить его или передать.

«Первый вариант решения не требует никаких мер. Во втором случае необходимо ввести дополнительные меры и средства защиты, провести обучение персонала и т.д. При этом придется произвести количественную

оценку эффективности дополнительных мер и средств защиты. В этом случае дополнительные затраты не должны превышать размера ущерба от реализации угрозы. Третье решение предполагает перекладывание последствий от реализации риска на третье лицо. Выходом в этом случае является страхование организации» [62].

В качестве итога отметим, что метод количественной оценки рисков нарушения информационной безопасности дает возможность создать полный перечень угроз информационной безопасности с учетом ущерба от каждого типа инцидентов; оценить стоимость активов в денежной форме; определить частоту возникновения различных типов угроз; спрогнозировать возможный ущерб от их реализации; а также разработать меры безопасности и контрмеры для каждой категории угроз.

Итак, анализ показал указанных выше способов оценки рисков нарушения информационной безопасности показал, что количественной метод дает возможность, во-первых, создать полный перечень угроз информационной безопасности с учетом ущерба от каждого типа инцидентов; во-вторых, оценить стоимость активов в денежной форме; в-третьих, определить частоту возникновения различных типов угроз; в-четвертых, спрогнозировать возможный ущерб от их реализации; и наконец, разработать комплекс защитных мероприятий и контрмер для каждой категории угроз.

Безусловно, второй метод оценки рисков нарушения информационной безопасности позволяет более наглядно (в цифрах) представить негативные последствия реализации угроз и рисков, но при всех своих достоинствах он имеет очевидные недостатки, которые заключаются в высокой трудоемкости и в невозможности применения в некоторых случаях (например, как оценить моральный ущерб – вопрос открытый). По сравнению с количественными методами качественные подходы могут ускорить процесс оценки рисков, однако их результаты нередко оказываются субъективными и не дают точного представления о

потенциальных убытках, затратах и преимуществах внедрения различных мер информационной безопасности.

Также при оценке рисков нарушения информационной безопасности ПДн может использоваться *метод экспертной оценки*, который заключается в следующем. Создается экспертная комиссия, задачей которой является определение объектов для анализа, включая их ключевые параметры и характеристики. Чтобы провести комплексный анализ угроз информационной безопасности компании, эксперты собирают следующие данные: общую информацию об автоматизированных системах; описание процедур работы с конфиденциальными данными; характеристику корпоративной информационной системы; обзор информационной инфраструктуры; а также оценку системы защиты данных (включая документацию по информационной безопасности, организационные и технические меры, инструменты защиты).

На основе собранной информации комиссия затем формулирует выводы относительно возможных источников риска. Для каждого идентифицированного источника определяется вероятность появления угрозы и степень его значимости. Выводы, полученные с помощью метода экспертной оценки, далее должны быть положены в основу разработки системы мер, контрмер и действий по обеспечению информационной безопасности в отношении каждой актуальной угрозы для снижения уровня риска. На наш взгляд, данный метод перекликается с методом качественной оценки рисков.

Используя такой метод, как анализ факторов риска (*метод факторного анализа рисков*), специалисты по информационным технологиям выявляют ключевые факторы, которые существенно влияют на возможность реализации потенциальных угроз различных типов. Задача специалиста заключается в изучении структуры организации и оценке того, какие уязвимости должны быть устранены, а какими можно временно пренебречь.

Еще один метод, позволяющий оценить риски нарушения информационной безопасности ПДн, это статистический анализ рисков. Этот метод позволяет выявить самые слабые звенья в системе защиты персональных данных. Тем не менее, чтобы провести такой анализ, требуется значительный объём информации об уже совершённых атаках (статистика, как правило, за достаточно продолжительный период времени) [1].

Таким образом, выбирать метод оценки рисков нарушения информационной безопасности следует с учетом специфики конкретной организации и задач, поставленных перед ее специалистами. На наш взгляд, данные методы оценки рисков нарушения информационной безопасности могут использоваться одновременно, выгодно дополняя друг друга.

Выводы по первой главе

В ходе анализа нормативно-правовой базы по вопросу минимизации рисков нарушения безопасности в системе защиты ПДн и теоретических работ, направленных на изучение данной проблемы, были сделаны следующие выводы.

Анализ нормативно-правовой базы в области защиты ПДн России, США и стран Европы показал, что, имея общие фундаментальные принципы, направленные на защиту прав граждан, в дальнейшем данный вопрос потребует конкретизации под потребности общества с учетом специфики отрасли экономики.

При достаточно высокой проработанности исследуемой проблемы на нормативно-правовом и теоретическом уровне, все равно остаются пробелы в терминологическом аппарате, в частности возникла необходимость уточнения понятия «риск нарушения безопасности в системе защиты персональных данных», а также перечня персональных данных; кроме того некоторые нормативно-правовые акты содержат

указание на неполноту закрепленных положений, например, «указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей» [31].

Ключевым термином в данной работе является «риск нарушения безопасности в системе защиты персональных данных», под которым мы будем понимать потенциальное / возможное / вероятностное нарушение безопасности в системе защиты ПДн, которое в случае реализации создаст угрозу / опасность использования уязвимости системы защиты ПДн в целях нанесения ущерба / вреда / последствия организации.

Методы оценки рисков нарушения информационной безопасности разнообразны с точки зрения особенностей применения и трудоемкости; на основе их анализа сделан вывод, что методы оценки необходимо выбирать с учетом специфики образовательной организации, а также учитывать поставленные перед специалистами задачи; на наш взгляд, описанные в настоящей работе методы оценки рисков нарушения информационной безопасности (качественный, количественный, факторный, статистический, метод экспертной оценки) могут использоваться одновременно, выгодно дополняя друг друга.

ГЛАВА 2 РАЗРАБОТКА КОМПЛЕКСА МЕР И МЕРОПРИЯТИЙ МИНИМИЗАЦИИ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Организационно-правовая структура образовательной организации

Экспериментальная часть данной работы выполнена на базе ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» (далее – колледж). Рассмотрим организационно-правовую структуру указанной выше профессиональной образовательной организации.

Полное наименование организации - государственное бюджетное профессиональное образовательное учреждение «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

Сокращенное наименование - ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

Аббревиатура - ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего».

Дата создания профессиональной образовательной организации: 7 февраля 1945 года.

Организационно-правовая форма - государственные бюджетные учреждения субъектов Российской Федерации. Учредителем колледжа является Министерство образования и науки Челябинской области.

Директором образовательного учреждения с 2010 года является Худолей Елена Сергеевна.

Юридический и фактический адреса колледжа: 454129, Российская Федерация, Уральский федеральный округ, Челябинская обл., г. Челябинск, ул. Масленникова, 21 (юридический адрес); 454129, Российская Федерация, Уральский федеральный округ, Челябинская обл.,

г. Челябинск, ул.1-ая Трубосварочная, 4 (общ.), Машиностроителей, 6 (общ.), Масленникова, 21а (общ.), Энергетиков, 2 (учебный корпус) (фактические адреса).

Основным видом экономической деятельности является «образование профессиональное среднее (85.21)» [56], дополнительными – «обучение профессиональное (85.3), образование дополнительное детей и взрослых (85.41), образование профессиональное дополнительное (85.42)» [56].

Образовательная деятельность колледжем осуществляется в соответствии с Изменениями №12 в Устав, утвержденными приказом Министерства образования и науки Челябинской области №02/2799 от 21.11.2023г., и с лицензией на право осуществления образовательной деятельности (серия 74Л02 № 0001052, регистрационный номер лицензии 11920, дата выдачи лицензии: 20.11.2015г.), срок действия лицензии – бессрочно. Кроме того, колледж зарегистрирован в реестре организаций, оказывающих услуги в области охраны труда (регистрационный номер 8742 от 31.08.2023г.).

Реализуемые колледжем образовательные программы прошли государственную аккредитацию, что подтверждено наличием свидетельства о государственной аккредитации (серия 74А04 № 0000164., регистрационный номер свидетельства 3016, дата выдачи свидетельства: 18.05.2020г.), срок действия свидетельства – бессрочно.

Структура управления колледжем относится к линейно-функциональной, особенностью которой является то, что связи и отношения субъектов управления характеризуются одновременно и субординацией, и координацией. Непосредственное управление профессиональной образовательной организацией осуществляет директор Рассмотрим подробнее структуру управления колледжа (см. рисунок 1):

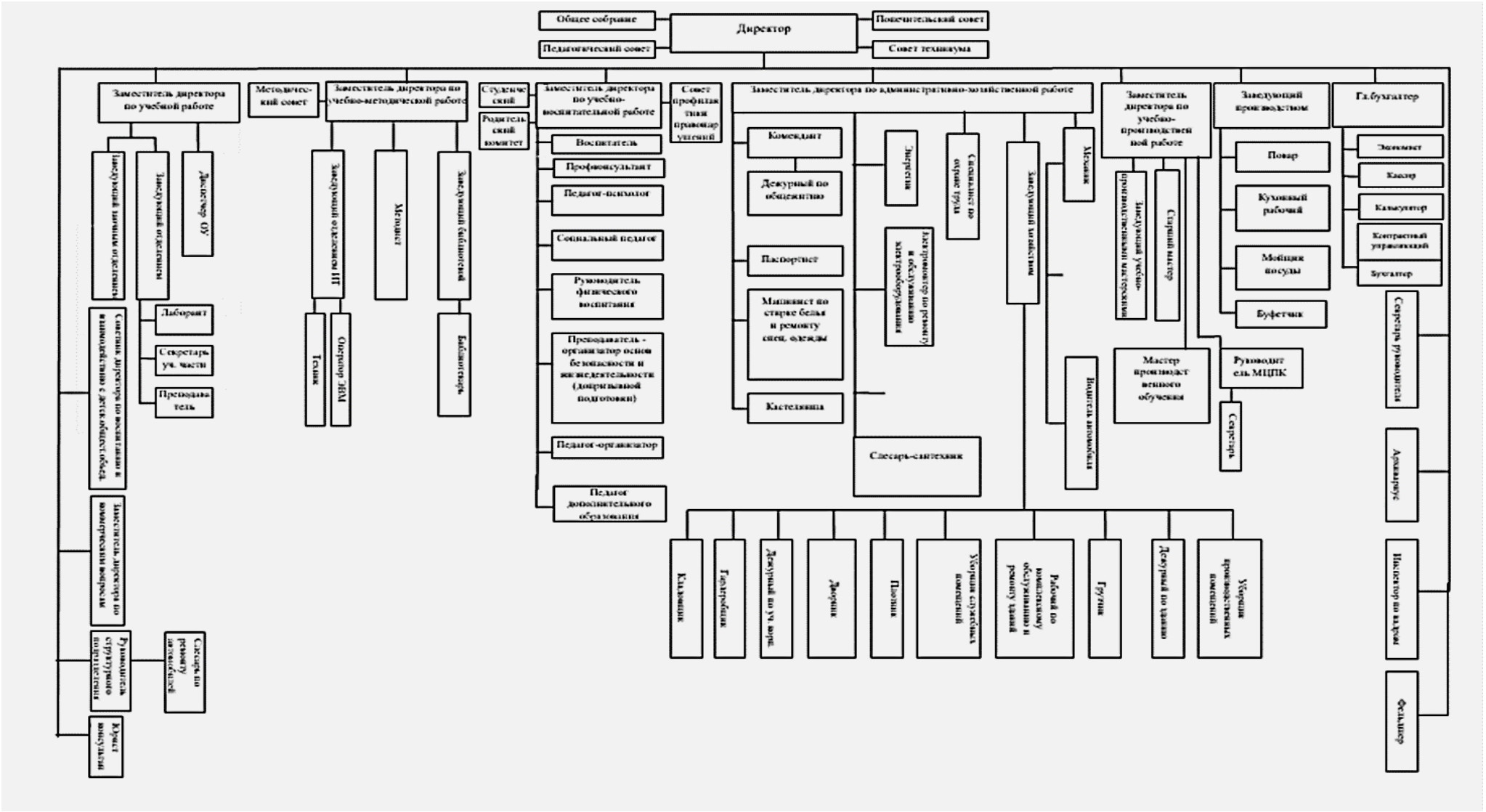


Рисунок 1 – Структура управления ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего»

Управление колледжем осуществляется на четырех уровнях, первый из которых стратегический – это уровень директора. Субъектами управления также являются такие коллегиальные органы, как общее собрание, совет колледжа, педагогический совет, попечительский совет. На этом уровне создаются условия для творческого роста педагогического персонала. Проектируется деятельность заместителей директора, педагогов, студентов.

Второй уровень – тактического управления – это уровень главного бухгалтера и заместителей директора по следующим направлениям работы: учебная, учебно-методическая, учебно-производственная, учебно-воспитательная и административно-хозяйственная. Этот уровень руководителей обеспечивает анализ, планирование, организацию, руководство, контроль и коррекцию хода реализации образовательных программ колледжем и в целом его функционирования.

Третий уровень (оперативного управления), на котором осуществляют свою деятельность заведующий отделением ИТ, заведующий библиотекой, методист, старший мастер, диспетчера, социальный педагог, психолог и т.д.

Четвёртый уровень – это уровень соуправления. Субъектами являются преподаватели, мастера производственного обучения, воспитатели общежития, студенты и их родители. То есть при линейно-функциональной структуре управления вся полнота власти сосредоточена у директора, который возглавляет коллектив колледжа.

Таким образом, структура управления колледжа соответствует функциональным задачам и Уставу профессиональной образовательной организации и позволяет обеспечить участие всех категорий сотрудников, абитуриентов, студентов, выпускников, их родителей (законных представителей) в управление образовательной организацией.

2.2 Единое информационное пространство образовательной организации

Анализ понятия «единое информационное пространство» показал различные его интерпретации, поэтому уточним, что в данной работе в понятие «единое информационное пространство» включается «совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей» [39]. Обязательными составляющими единого информационного пространства образовательной организации являются:

1) организационные структуры, которые обеспечивают функционирование и развитие единого информационного пространства учебного заведения;
2) средства информационного взаимодействия сотрудников колледжа, студентов и абитуриентов, их родителей или законных представителей, потенциальных потребителей образовательных услуг и самой организации, которая на основе соответствующих информационных технологий, включая программно-технические средства и организационно-нормативные документы, предоставляет доступ к информационным ресурсам;
3) информационные ресурсы, включая различные носители информации, используемые организацией.

Единое информационное пространство (далее – ЕИП) ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» включает в себя многочисленные компоненты.

Функционирование и развитие единого информационного пространства колледжа обеспечивается следующей *организационной*

структурой: непосредственное руководство по данному направлению осуществляет директор, именно он определяет стратегию развития образовательной организации, что отражено в Программе развития колледжа на 2024-2028 гг., включая вопросы функционирования и развития единого информационного пространства. На тактическом уровне управляет данным направлением заместитель директора по учебно-методической работе, ответственный за планирование и организацию деятельности колледжа в рамках информатизации. На уровне оперативного управления осуществляет свою деятельность заведующий отделением ИТ, в непосредственном подчинении у которого техник и оператор ЭВМ. В силу того, что в колледже реализуются образовательные программы по укрупненной группе профессий, специальностей 09.00.00 Информатика и вычислительная техника, к вопросам функционирования и развития единого информационного пространства подключается председатель предметно-цикловой комиссии «Информационные технологии».

Следующий необъемлемый компонент единого информационного пространства – это *средства информационного взаимодействия*, включая информационные технологии, программно-технические средства и организационно-нормативные документы.

Проанализируем программно-технические средства и информационные технологии, входящие в состав единого информационного пространства образовательной организации. В настоящее время колледж располагает *материально-техническим оснащением* образовательного процесса в составе:

во-первых, в колледже имеется локально-вычислительная сеть (далее – ЛВС), объединяющая 6 компьютерных классов (6 АРМ педагога и 62 АРМ студента), 38 учебных кабинетов (лабораторий, мастерских), каждый из которых оборудован 1 АРМ педагога, 2 библиотеки, имеющие 7 АРМов, 8 кабинетов администрации колледжа; 11 кабинетов обслуживающего персонала; 4 кабинета бухгалтерии; ЛВС колледжа базируется на:

– одном узле оптоволоконной связи;
– одном интернет-шлюзе, одиннадцати коммутаторах;
– VPN-канал между двумя площадками колледжа;
– двух физических серверах и 6 виртуальных серверах (включая DC, DHCP, DNS, KSC, Web-сервер);
– одном proxy-сервере Squid с модулем, DansGuardian - фильтрация web-запросов под Linux; Kaspersky endpoint security web control (контроль доступа к web-ресурсам);
– скорость доступа в Интернет составляет 95 Мбит/сек.;

во-вторых, 2 физических сервера и 6 виртуальных серверов; 137 ПК (105 ПК в образовательном процессе); главный маршрутизатор (D-Link DSR-1000N); все серверы физически соединены через ряд коммутаторов со всеми ПК по типологии подключения «звезда» (подробнее см. таблицу 2):

Таблица 2 – Материально-техническое оснащение единого информационного пространства

Наименование показателей	Всего	в т.ч. используемых в образовательных целях	
		всего	из них доступных для использования студентами после основных занятий
Персональные компьютеры, всего	137	105	74
из них: портативные персональные компьютеры, ноутбуки и другие (кроме планшетных)	3	3	0
находящиеся в составе локальных вычислительных сетей	137	100	74
имеющие доступ к Интернету	137	100	74
имеющие доступ к Интернет-порталу организации	137	100	74
поступившие в текущем году	13	13	13
Мультимедийные проекторы	26	26	0
Интерактивные доски	1	1	1
Принтеры	17	0	0
Сканеры	3	2	2
Многофункциональные устройства (МФУ, выполняющие операции печати, сканирования, копирования)	25	2	2
SmartTV	7	7	0

Таким образом, оснащенность учебных помещений вычислительной техникой составляет примерно 90%, загруженность кабинетов информатики занятиями в пределах 70%, соответствие кабинетов с компьютерной техникой санитарным и противопожарным нормам поддерживается на уровне 95%, эффективность использования сети - 55-60%.

На сегодняшний день колледжем используется такое *программное обеспечение*, как:

- MS Windows 10 pro,
- MS Windows 7 pro,
- MS Windows 2016 Server,
- MS Office от 2007-2016(19),
- WinRar - Архиватор,
- 7-ZIP - Архиватор,
- VinVNC - Удаленная поддержка пользователей,
- Kaspersky Endpoint Security - Стандартный Russian Edition - антивирус,
- KliteCodek - кодеки для воспроизведения видео файлов,
- AdobeAcrobat Reader - чтение PDF файлов,
- Yandex browser,
- Google Chrome,
- Fire Fox,
- Abby FineReader – распознавание текста на картинках,
- КриптоПро,
- Adobe Photoshop,
- ОС Linux,
- МойОфис,
- FineReader,
- 1С Предприятие 8.3.

В целях выполнения требований федерального законодательства по вопросам защиты детей при организации доступа обучающихся к сети Интернет от причиняющей вред их здоровью и / или их развитию информации, а также по противодействию экстремизму в колледже обеспечена контент-фильтрация, для чего используется программное обеспечение управления контентом DansCuardian – запретить поиск по ключевым словам, Kaspersky Веб-контроль, правило – запретить все, кроме списка разрешенного.

Анализ используемого программного обеспечение показал, что в колледже преобладают продукты иностранного происхождения, в связи с чем перед образовательной организацией остро встала проблема по установке / приобретению программного обеспечения отечественного производства. В соответствии с этим было проведено совещание по теме «ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего» в условиях цифровой трансформации», на котором рассмотрены следующие вопросы:

- Нормативно-правовая база цифровой трансформации. Тренды в образовании. Импортозамещение;
- Колледж сегодня в условиях цифровой трансформации: кадровые ресурсы, инфраструктура, информационные системы / платформы, потребности;
- Обзор зарубежного и отечественного программного обеспечения, сервисов, ресурсов и продуктов;
- Перспективы развития колледжа в соответствии с вызовами времени в области цифровой трансформации и импортозамещения.

Итогом данного совещания стал план постепенного перехода колледжа на программное обеспечение, сервисы, ресурсы и продукты отечественного происхождения.

Работа в едином информационном пространстве колледжа регламентирована следующими *организационно-нормативными документами:*

- Правила использования сети Интернет в учебном заведении;
- Положение об официальном сайте в сети «Интернет»;
- Политика обработки персональных данных;
- Положение об обработке и защите персональных данных;
- Положение о порядке применения электронного обучения, дистанционных образовательных технологий при реализации образовательных программ;
- Положение о проведении ГИА с применением электронного обучения, дистанционных образовательных технологий;
- Положение о текущем контроле успеваемости и промежуточной аттестации с применением электронного обучения, дистанционных образовательных технологий;
- Порядок учета, хранения результатов образовательного процесса и внутренний документооборот, в том числе при реализации образовательных программ и их частей с применением электронного обучения, дистанционных образовательных технологий;
- Положение об использовании средств мобильной связи;
- Регламент по организации процесса управления уязвимости;
- Положение об электронных образовательных ресурсах и портфолио обучающегося;
- Положение о работе в автоматизированной системе «Сетевой город. Образование»;
- Положение об электронном журнале;
- Приказы, распоряжения по отдельным направлениям и др.

Анализ представленных локальных нормативных актов показал, что работа колледжа в едином информационном пространстве детально регламентирована, все рассмотренные документы актуальны, при необходимости корректируются, размещены в открытом доступе (на официальном сайте колледжа) и могут быть рекомендованы в качестве образца другим образовательным организация среднего профессионального образования.

Кроме того, единое информационное пространство колледжа включает также *информационные ресурсы и информационные технологии.* Остановимся на них подробнее.

Функционирование образовательной организации обеспечивается многочисленными информационными системами (подробнее см. таблицу 3):

Таблица 3 - Информационные системы, платформы, используемые в работе колледжа

№ п/п	Наименование ИС, платформы и др.	Должность ответственного лица	Примечание
1	АСУ Procollege	Заместитель директора по учебной работе (далее – УР), секретарь учебной части, методист	обновление договора на техническую поддержку 1 раз в год
2	ФИС ГИА и приема	Заместитель директора по учебно-методической работе (далее – УМР), техник	Аттестация АРМ
3	ФИС ФРДО	Заместитель директора по УР	Аттестация АРМ, ЭЦП директора
4	ГИВЦ (статотчеты ПК-1, ПО, СПО-1, СПО-2, СПО-Мониторинг)	Заместитель директора по УМР, секретарь директора	ЭЦП директора
5	Сетевой город. Образование	Заместитель директора по УР, секретарь учебной части	
6	ГИС Образование	Заместитель директора по УР	
7	ГИС Образование. Е-услуги	Заместитель директора по учебно-воспитательной работе (далее – УВР)	

Продолжение таблицы 3

8	ИС «Аттестация педагогических кадров»	Специалист отдела кадров, заместитель директора по УМР	
9	Официальный сайт для размещения информации о государственных (муниципальных) учреждениях (https://bus.gov.ru/)	Главный бухгалтер, заместитель директора по УР, секретарь директора	ЭЦП директора
10	АИС «Навигатор дополнительного образования детей Челябинской области» https://ndo.edu-74.ru/additional-education	Заместитель директора по УВР	
11	ФИС ОКО (ВПР)	Заместитель директора по УР	
12	АЦК Финансы версия 2.0	Сотрудники бухгалтерии, отдела закупок и отдела кадров	ЭЦП
13	Барс - отчетность версия 4.2.24.0		
14	Барс - Портал СУФД имущество		
15	Свод-СМАРТ версия 20.2.0.35076		
16	Контур Экстерн		ЭЦП, 1 раз в год обновление договора
17	ЕИС «Закупки»		
18	1С:Бухгалтерия государственного учреждения 8, ред. 2.0		ЭЦП
19	1С:Зарплата и кадры 7.7		ЭЦП, 1 раз в год обновление договора на обслуживание и техническую поддержку
20	1С:Зарплата и кадры государственного учреждения 8, ред. 1.0		
21	1С:Зарплата и кадры государственного учреждения 8, ред. 2.0		
22	1С:Предприятие 8.3 (8.3.16.1814) Бухгалтерия государственного учреждения, редакция 1.0 (1.0.68.15)		
23	1С:Предприятие 8.3 (8.3.18.1289) Зарплата и кадры государственного учреждения, редакция 3.1 (3.1.20.97)		
24	Официальный сайт http://chtpgh.ru/	Заместитель директора по учебно-методической работе, техник	
25	Официальные группы в ВК, Телеграм, Рутуб, Сферум	Методист	
26	ЕГИССО	Заместитель директора по учебно-воспитательной работе	Аттестация АРМ, ЭЦП
27	ПОС (платформа обратной связи)	Директор	

Продолжение таблицы 3

28	Система электронного документооборота (СЭД) «Тезис»	Секретарь директора	
29	ФИС Меркурий	Заведующий производством	
30	ГИС Энергоэффективность	Заместитель директора по административно-хозяйственной работе	
31	Цифровая платформа WSR, тикет-система по ДЭ	Заместитель директора по учебно-производственной работе	
32	ЕИП-ФКИС (физ-ра и спорт) https://еип-фкис.рф	Руководитель физического воспитания	
33	ИС «Оценка эффективности деятельности руководителя ОО»	Секретарь директора	

Все многообразие информационных систем, используемых в работе колледжа, а также связи, существующие между ними, отражены на рисунке 2, разработанном Министерством образования и науки Челябинской области:

Рисунок 2 – Информационные системы профессиональной образовательной организации

Безусловно, в рамках представленной работы проанализировать все используемые информационные системы не получится. Остановимся подробнее на официальном сайте колледжа и АСУ Procollege.

У колледжа имеется сайт http://chtpgh.ru/ (см. рисунок 3), который функционирует в соответствии с Положением об официальном сайте в

сети «Интернет» (регистрационный №240 от 24.11.2020г.) и приказом директора №193 от 04.03.2022г. «О размещении информации на официальном сайте образовательной организации в сети «Интернет» и ее обновлении».

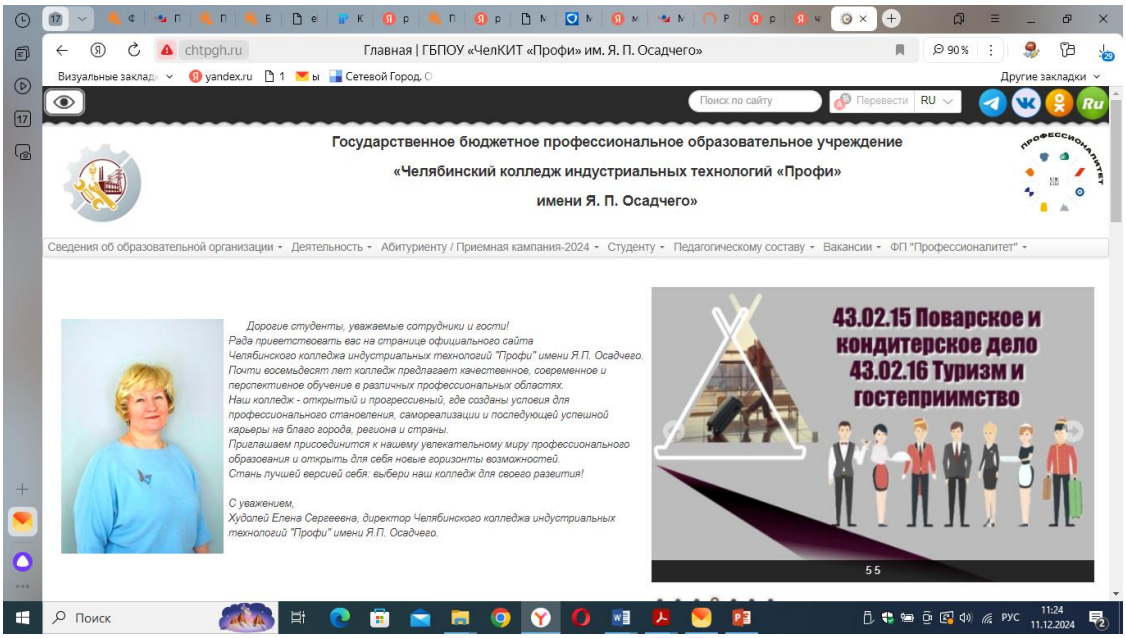


Рисунок 3 - Сайт ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего». Главная страница

Официальный сайт любой образовательной организации представляет собой информационный ресурс, созданный для увеличения информационного охвата учебного заведения и выполняющий следующие функции:

- обеспечение информацией всех участников образовательного процесса;
- повышение прозрачности и доступности образования;
- создание возможностей для внедрения современных методик обучения и воспитания;
- формирование целостной информационной инфраструктуры учебного заведения;
- укрепление позитивного имиджа образовательного учреждения;
- распространение инновационных практик учебного заведения;

– организация обратной связи с участниками образовательного процесса.

На официальном сайте колледжа сведения размещены в соответствии с Приказом Рособрнадзора от 04 августа 2023 г. № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации» [49].

Кроме того, на основании приказа директора колледжа №193 от 03 марта 2024 г. «О размещении информации на официальном сайте образовательной организации в сети «Интернет» и ее обновлении» и в связи с производственной необходимостью внесены дополнительные разделы на официальный сайт, например: «Абитуриенту», «Противодействие коррупции», «Противодействие идеологии терроризма», «Продукция и услуги» и др., что делает колледж для общественности более открытым и доступным. Информация на сайте обновляется ежедневно.

В колледже используется АСУ «ProCollege» (см. рисунки 4-7).

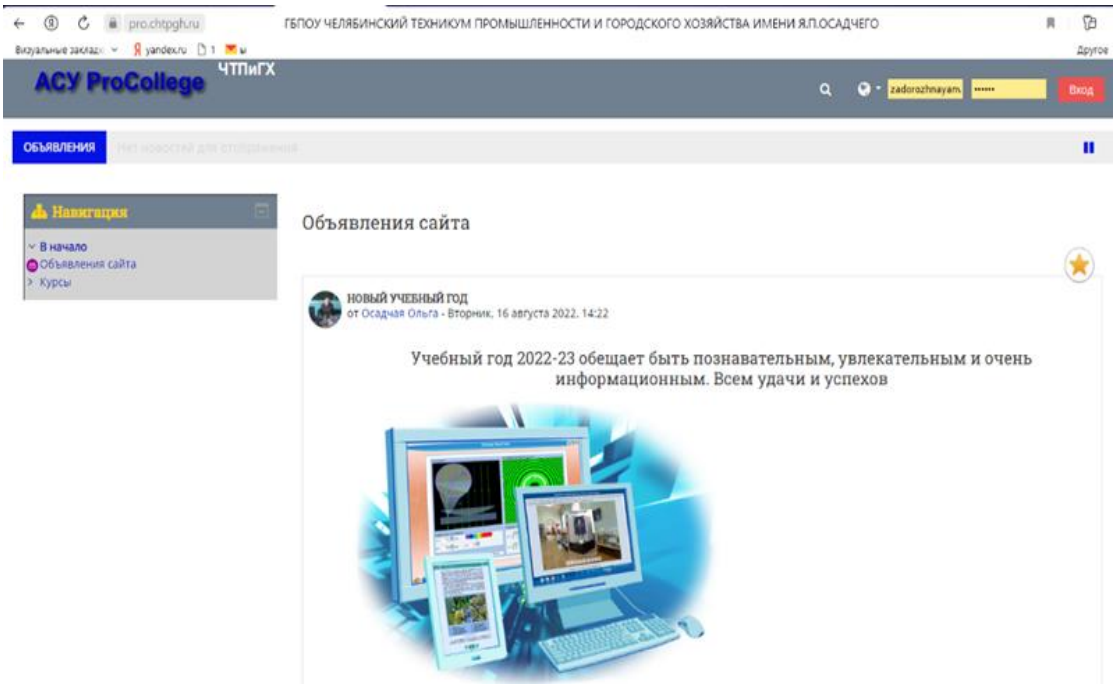


Рисунок 4 - АСУ «ProCollege». Общий вид

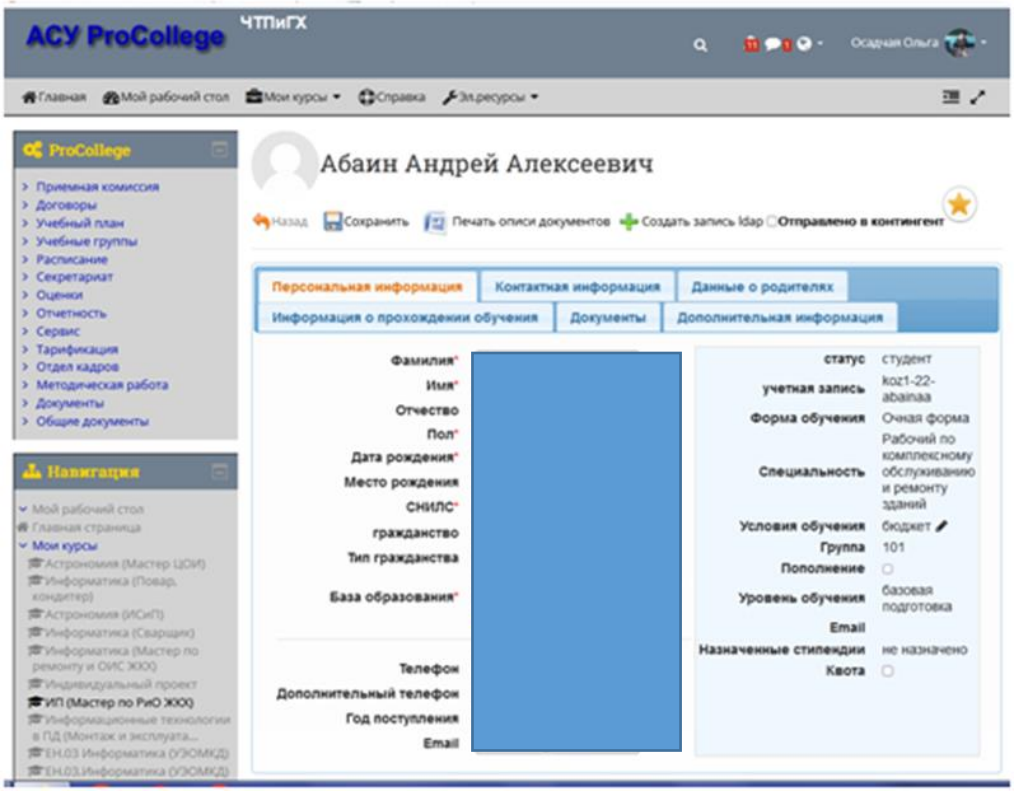
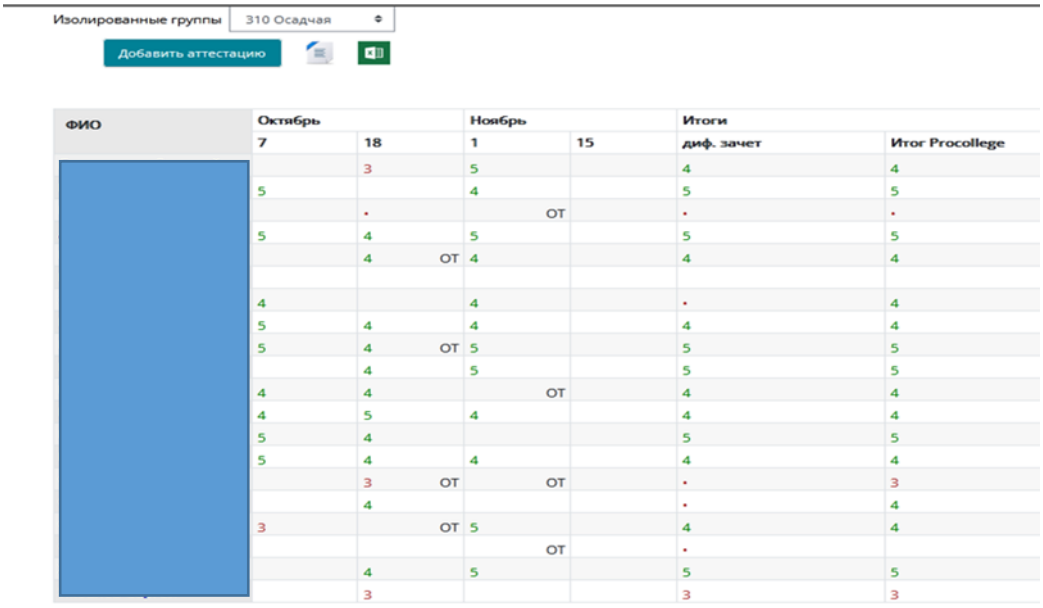


Рисунок 5 – АСУ «ProCollege». Вкладка «Управление». Личная карточка обучающегося



ФИО	Октябрь		Ноябрь		Итоги	
	7	18	1	15	диф. зачет	Итог Procollege
		3	5		4	4
	5		4		5	5
		·		ОТ	·	·
	5	4	5		5	5
		4 ОТ	4		4	4
	4		4		·	4
	5	4	4		4	4
	5	4 ОТ	5		5	5
		4	5		5	5
	4	4		ОТ	4	4
	4	5	4		4	4
	5	4			5	5
	5	4	4		4	4
		3 ОТ		ОТ	·	3
		4			·	4
	3	ОТ	5		4	4
				ОТ	·	
		4	5		5	5
		3			3	3

Рисунок 6 - АСУ «ProCollege». Вкладка «Журнал»

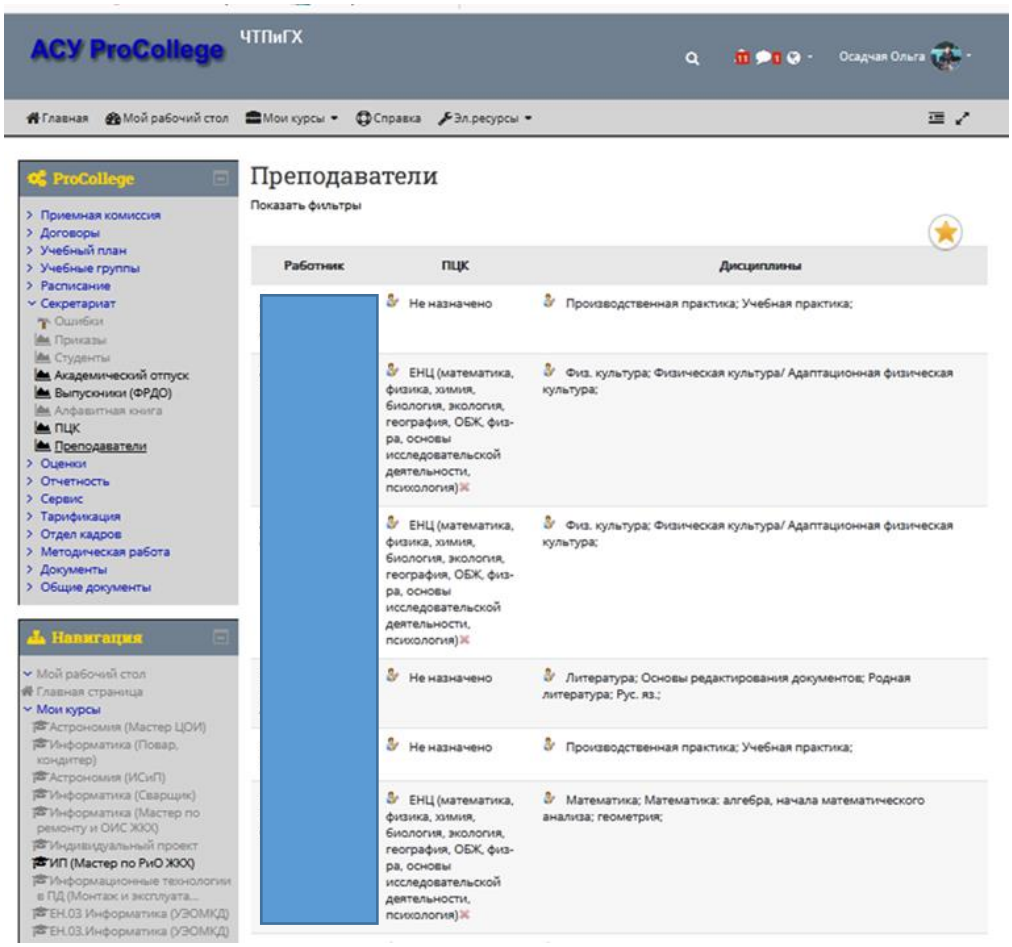


Рисунок 7 - АСУ «ProCollege». Вкладка «Управление». Список сотрудников

АСУ «ProCollege» содержит следующие разделы:

– приемную комиссию,
– годовой учебный план,
– календарный учебный график и график аттестаций,
– годовое и недельное расписание,
– рабочие программы учебных дисциплин и междисциплинарных курсов,
– электронные образовательные ресурсы по учебным дисциплинам и междисциплинарным курсам,
– личные дела обучающихся и сотрудников колледжа,
– электронный журнал с дифференцированным доступом для педагогических и административных сотрудников и обучающихся,

– обмен почтовыми сообщениями,
– форум для всех пользователей,
– доску объявлений,
– тарификация педагогов,
– отчеты, справки, приказы и др.

Внедрение в повседневную деятельность колледжа комплексной информационной системы, включающей электронный классный журнал и электронный дневник обучающегося, способствует решению еще одной задачи, поставленной государством перед образовательным учреждением: оказание образовательных услуг в электронной форме. Кроме этого единое пространство обмена информацией в условиях колледжа (база образовательных ресурсов, доска объявлений, корпоративная электронная почта, доступ к форуму колледжа, список именинников и т.п.) улучшает внутренний климат учреждения и взаимопонимание между всеми участниками учебного и воспитательного процессов.

Автоматизированная система управления «ProCollege» (информационная система) позволяет решить такие задачи, как:

для директора и заместителей директора:

– быстрый сбор и анализ данных о процессе обучения для эффективного управления;
– ведение алфавитной книги, личных дел сотрудников и обучающихся для формирования оперативных отчетов;
– составление расписаний, просмотр расписаний с различных точек зрения (по месяцам/неделям/дням, по педагогам, классам, кабинетам и т.д.), а также организация мероприятий внутри колледжа и группы;
– мониторинг перемещений обучающихся;
– разработка системы электронного документооборота;
– создание индивидуальных отчетов и др.;

для мастеров производственного обучения и преподавателей:

- ведение электронного дневника и электронного журнала;
- автоматизированное получение всех типовых отчетов по успеваемости и посещаемости в разрезе курса, группы, педагога, учебной дисциплины и т.д.;
- составление календарно-тематического планирования;
- доступ к актуальной версии своего расписания, просмотр мероприятий колледжа и групповой деятельности;
- подготовка и проведение тестирования отдельных студентов или всей группы;
- ведение социального паспорта группы и др.

для студентов колледжа:

- просмотр актуальной версии своего расписания на месяц/неделю/день, а также мероприятий внутри колледжа и группы;
- получение итоговой и текущей информации об успеваемости и посещаемости;
- доступ к электронному дневнику, где автоматически фиксируются оценки, размещаются домашние задания и задолженности по учебным дисциплинам и междисциплинарным курсам;
- возможность дистанционного обучения в рамках образовательного процесса.

Для облегчения работы в АСУ «ProCollege» разработаны инструкции для педагога и студентов по вводу данных и обмену информацией, которые опубликованы на официальном сайте колледжа.

Таким образом, анализ единого информационного пространства колледжа показал, что организационная структура и используемое многообразие информационных систем соответствует задачам открытости, доступности, прозрачности деятельности колледжа, локальные

нормативные акты, сопровождающие функционирование и развитие единого информационного пространства, выполнены на высоком уровне. Однако можно выделить такие актуальные для колледжа направления дальнейшего развития единого информационного пространства как:

1) дооснащение учебных кабинетов, лабораторий, мастерских компьютерной техникой и поддержание техники в рабочем состоянии;
2) обучение педагогов пользованию сложной техникой;
3) реализация плана перехода на отечественное программное обеспечение;
4) прохождение пользователями и администраторами обучения по работе в отечественных операционных системах;
5) включение в работу всех доступных функций АСУ «ProCollege»;
6) дальнейшее внедрение в образовательный процесс дистанционных и электронных технологий обучения;
7) создание и использование электронных образовательных ресурсов;
8) усиление контент-фильтрации на рабочих местах студентов в целях защиты детей от причиняющей вред их здоровью и / или их развитию информации.

2.3 Анализ состояния информационных систем персональных данных образовательной организации

В соответствии с основными видами экономической деятельности, а также целями и задачами любая профессиональная образовательная организация обязана работать в многочисленных и разнообразных информационных системах, каждая их которых содержит различные персональные данные, прежде всего педагогических работников, абитуриентов, студентов, выпускников, а также их родителей и / или законных представителей (подробнее см. таблицу 4):

Таблица 4 - Перечень информационных систем ПДн колледжа

№ п/п	Наименование ИСПДн	Категория субъектов ПДн	Цели обработки ПДн
1	ФИС ГИА и Приема	Абитуриенты, студенты колледжа	обеспечение проведения ГИА обучающихся, освоивших образовательные программы основного общего, среднего общего образования, и приема граждан в образовательные учреждения для получения среднего профессионального или высшего образования, а также в региональных ИС обеспечение проведения ГИА обучающихся, освоивших образовательные программы основного общего, среднего общего образования
2	ФИС ФРДО	Студенты колледжа и его выпускники	обеспечение защищенного (безопасного) канала передачи данных (сведений о документах об образовании и (или) о квалификации, документах об обучении) между сегментами виртуальной сети VipNet с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сеть связи общего пользования
3	ГИС «Образование. Е-услуги»	Абитуриенты, студенты колледжа	обеспечение предоставления муниципальных и государственных услуг в электронном виде, в т.ч. приём заявлений, постановка на учёт и зачисление детей в профессиональные учебные заведения
4	АСУ Procollege	Педагоги, студенты колледжа и их родители	управление деятельностью образовательной организации, создание открытого информационного образовательного пространства для эффективного решения задач управления воспитательно-образовательной системой посредством сетевого взаимодействия на основе информационно-коммуникационных технологий (электронный журнал, электронный дневник и др.)
5	ИС «Сетевой город. Образование»	Педагоги и студенты колледжа	управление деятельностью образовательной организации, создание открытого информационного образовательного пространства для эффективного решения задач управления воспитательно-образовательной системой

Продолжение таблицы 4

			посредством сетевого взаимодействия на основе информационно-коммуникационных технологий (электронный журнал, электронный дневник, доступ к электронным образовательным ресурсам и др.)
6	ИС «Бухгалтерия и кадры»	Сотрудники и студенты колледжа	начисление и выплата заработной платы и иных выплат, организация учета сотрудников для обеспечения соблюдения их законных прав, и исполнения обязанностей, установленных РФ, Налоговым кодексом РФ и иными нормативно-правовыми и внутренними локальными нормативными актами, материальная поддержка студентов в соответствии с ФЗ-273 от 29.12.2012
7	ИС «Аттестация педагогических кадров»	Педагогические работники колледжа	обеспечение прохождения процедуры аттестации педагогами в соответствии с ФЗ-273 от 29.12.2012 «Об образовании в РФ» и Приказом Минпросвещения России от 24.03.2023 № 196

При обработке ПДн для обеспечения безопасности выполняется защита информации, которая обрабатывается техническими средствами, а также информации, содержащейся на бумажных, оптических, магнитных и иных видах носителей в форме информационных массивов и баз данных в ИСПДн. Сотрудникам запрещается использовать съемные носители информации за исключением случаев, когда это необходимо в рамках их должностных обязанностей.

Помещения, в которых хранятся ПДн, оборудуются сейфами, надежными замками, противопожарной сигнализацией. В рабочее время при отсутствии работников помещения запираются на ключ. Проведение уборки помещений, в которых хранятся ПДн, осуществляется в присутствии сотрудников из числа лиц, несущих ответственность за сохранность ПДн.

Работники образовательной организации, назначенные ответственными за обеспечение безопасности ПДн, проводят ознакомление всех сотрудников колледжа, непосредственно

осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн (в том числе с требованиями к защите персональных данных), локальными актами, регулирующими вопросы правомерной обработки ПДн. А также не реже одного раза в год проводят внутренний аудит соответствия обработки ПДн требованиям к защите ПДн, закрепленным в ФЗ-152 и в принятых в соответствии с ним других законодательных документах и локальных актах колледжа.

В данной работе рассмотрим подробнее ИСПДн, сопровождающие образовательный процесс от момента подачи абитуриентами заявления на прием до выпуска: ФИС ГИА и Приема, ФИС ФРДО, ГИС Образование. Е-услуги, АСУ Procollege и Сетевой город. Образование. В колледже проводится обработка персональных данных сотрудников, абитуриентов, обучающихся и их родителей в соответствии со следующими локальными нормативными актами: Политика обработки и защиты персональных регистраци0нный № 277 от 16.05.2022 г., Положение об обработке и защите персональных данных, регистрационный № 278 от 16.05.2022 г. (см. приложение 1, 2). Данные документы опубликованы на официальном сайте колледжа.

В названных выше локальных нормативных актах рассмотрены: основные понятия, принципы обработки персональных данных, состав и субъекты ПДн, порядок их обработки, хранения, правила доступа к персональным данным, передача, уточнение, изменение, блокирование ПДн, уничтожение персональных данных, обязанности образовательной организации при обработке ПДн, права родителей (законных представителей), направленные на обеспечение выполнения колледжем обязанностей, предусмотренных ФЗ-152 меры, правила работы с обезличенными персональными данными, а также ответственность и наказание за нарушение закона.

Детальный анализ исходных данных об ИСПДн колледжа позволил комиссии, состав которой утвержден приказом директора, установить

уровень защищенности каждой используемой информационной системы ПДн (см. таблицу 5).

Таблица 5 – Уровень защищенности ИСПДн колледжа

Наименование ИСПДн	Объем обрабатываемых ПДн	Категория ПДн, обрабатываемых в ИС	Тип угроз безопасности	Уровень защищенности ИСПДн
ФИС ГИА и Приема	в ИС одновременно обрабатываются данные менее 100 000 субъектов ПДн	иные категории ПДн субъектов, не являющихся сотрудниками оператора	угрозы 3-его типа	4-й
ФИС ФРДО	в ИС одновременно обрабатываются данные менее 100 000 субъектов ПДн	обрабатываются общедоступные и иные ПДн субъектов, не являющихся работниками оператора	угрозы 3-его типа	4-й
ГИС «Образование. Е-услуги»	в ИС одновременно обрабатываются данные менее 100 000 субъектов ПДн	обрабатываются общедоступные и иные категории ПДн субъектов, не являющихся работниками оператора	угрозы 3-его типа	4-й
*АСУ Procollege	в ИС одновременно обрабатываются данные менее 100 000 субъектов ПДн	обрабатываются общедоступные и иные ПДн работников оператора и субъектов, не являющихся работниками оператора	угрозы 3-его типа	4-й
*ИС «Сетевой город. Образование»	в ИС одновременно обрабатываются данные менее 100 000 субъектов ПДн	обрабатываются общедоступные и иные ПДн работников оператора и субъектов, не являющихся работниками оператора	угрозы 3-его типа	4-й

*В перспективе данные информационные системы после размещения информации о состоянии здоровья обучающихся (справка 086-у и справка о группе здоровья для уроков физической культуры) перейдут в группу 3-его уровня защищенности ИСПДн.

В соответствии с представленными выше результатами (уровень защищенности у всех ИСПДн – четвертый) колледжем предусмотрены различные меры, позволяющие обеспечить необходимую степень защиты ПДн, и, отметим, все они соответствуют таким требованиям:

1) гарантированная сохранность носителей персональных данных;
2) обеспечение безопасной эксплуатации помещений, в которых размещены информационные системы, с целью предотвращения несанкционированного доступа или нахождения в них лиц без должного разрешения;
3) утверждение руководством организации списка сотрудников, которым требуется доступ к персональным данным, обрабатываемым в информационной системе, для исполнения их рабочих обязанностей;
4) использование сертифицированных средств защиты информации, соответствующих требованиям отечественного законодательства в отрасли информационной безопасности, при необходимости устранения существующих угроз [43].

В колледже имеются две защищенные сети 2458, 3660, используемые для обработки и передачи персональных данных абитуриентов, студентов и выпускников. Доступ к данным сетям осуществляется в специальном закрытом помещении в соответствии приказом директора №426 от 11.08.2016 г. «О выделении режимного помещения», ответственное лицо за работу в них назначено приказом директора колледжа № 202 от 13.03.2020 г. «О назначении ответственных за защиту информации и обеспечение защиты ПДн при их обработке в ИСПДн и обмена информацией с ИСПДн ФИС ФРДО, ГИС Образование. Е-услуги, ФИС ГИА и приема».

Для передачи ПДн по защищенным сетям в колледже используется автоматизированное рабочее место (далее – АРМ), расположенное в специальном закрытом помещении, которое прошло аттестационные испытания ИСПДн. В целях подтверждения данного факта были

оформлены протокол и заключение по результатам аттестационных испытаний. Кроме того, для запуска в работу АРМ были проведены следующие работы:

для обеспечения защиты от несанкционированного доступа:

- имеется неисключительное право на использование Dallas Lock 8.0-K (СЗИ НСД, СКН) (программное обеспечение), произведена установка и настройка Dallas Lock 8.0-K, осуществляется техническая поддержка установленных средств защиты информации;

для построения защищенного канала связи:

- передача права на использование ПО ViPNet Client for Windows 4.x (КС2), Компакт-диск с дистрибутивом ПО ViPNet Client for Windows 4.x (КС2) и Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client for Windows 4.x (КС2) на срок 1 год, расширенный уровень;

мероприятия, необходимые для выдачи аттестата соответствия:

- проведение аттестационных испытаний ИСПДн;
- разработка организационно-распорядительной и технической документации для ИСПДн.

Используемый для передачи ПДн по защищенным сетям АРМ имеет следующие программно-технические характеристики:

процессор - Intel Core 2 Duo;

- объем оперативной памяти - не менее 1 Гбайт;
- свободное место на жестком диске - более 1 Гбайт;
- сетевой интерфейс (не более 10 IP-адресов на одном сетевом интерфейсе);
- операционная система - Windows 10 (32/64 разрядная) (установлен последний накопительный пакет обновлений);
- при использовании Internet Explorer - версия 6.0 или выше.

Кроме того, для повышения уровня безопасности системы защиты персональных данных были реализованы следующие меры:

во-первых, определены категории и объемы персональных данных, которые обрабатываются в информационной системе персональных данных;

во-вторых, выявлены потенциальные угрозы безопасности для информационных систем, а также созданы модели злоумышленников, способных нарушить безопасность этих систем;

в-третьих, разработаны и утверждены:

- модель угроз безопасности персональных данных при их обработке в ИСПДн «ФИС ГИА и Приема» № 74.0464.МУ от 26 февраля 2021 г.;
- модель угроз безопасности персональных данных при их обработке в ИСПДн «Сетевой город. Образование» №74.03997.МУ от 29 октября 2020 г.;
- модель угроз безопасности персональных данных при их обработке в ИСПДн «ГИС Образование. Е-услуги» №74.03998.МУ от 29 октября 2020 г.;
- модель угроз безопасности персональных данных при их обработке в ИСПДн «ФИС ФРДО» №74.0599.МУ от 09 ноября 2023 г.;

в-четвертых, определен уровень защищенности ИСПДн на основании полученных данных (см. таблицу 5 выше);

в-пятых, комиссией по классификации подписаны соответствующие акты определения степени защищенности;

в-шестых, средства криптографической защиты информации (далее – СКЗИ), эксплуатационная и техническая документация к ним, ключевые документы, имеющиеся в колледже, взяты на учет в журнале «поэкземплярного учета СКЗИ»;

в-седьмых, руководителем колледжа:

- назначено лицо, являющееся ответственным пользователем СКЗИ (Приказ №307 от 20 ноября 2023 г.);
- утверждена инструкция по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах персональных данных колледжа;
- утверждена схема организации криптографической защиты ПДн в ИСПДн;
- утверждены функциональные обязанности ответственного пользователя СКЗИ (Приказ №308 от 20 ноября 2023 г.);
- утвержден перечень пользователей СКЗИ (Приказ №277 от 05 сентября 2024 г.
- утвержден порядок уничтожения ключевых документов СКЗИ (Приказ №309 от 20.11.2023г.);
- утвержден перечень режимных помещений, где осуществляется работа с (или хранение) СКЗИ (Приказ №426 от 11.08.2016г.);
- утвержден перечень лиц, имеющих доступ в режимные помещения (Приказ №202 от 13.03.2020г.);
- утвержден План внутренних проверок режима защиты персональных данных (Приказ №308 от 20.11.2023г.);

в-восьмых, проведен инструктаж пользователей СКЗИ правилам использования СКЗИ и обращения с ключевыми документами, составлены заключения об обучении и допуске к самостоятельной работе с СКЗИ, пользователи ознакомлены с требованиями по обеспечению безопасного функционирования шифровальных (криптографических) средств;

в-девятых, приняты меры по обеспечению безопасности помещений с ограниченным доступом:

- режимные помещения оснащены устройствами для опечатывания;

– прием и передача под охрану «закрытых» помещений / кабинетов производится согласно журналу «Приема (сдачи) под охрану режимных помещений, хранилищ и ключей от них»;
– ключи от механических замков помещений / кабинетов с ограниченным доступом зарегистрированы в журнале «Учета хранилищ, сейфов, специальных хранилищ, шкафов и ключей от них».

Контроль за реализуемыми мерами, позволяющими обеспечить безопасность персональных данных и необходимый уровень защищенности ИСПДн, выполняется на основании Плана внутренних проверок режима защиты ПДн.

Таким образом, в колледже обеспечивается безопасность в системе защиты персональных данных.

2.4 Анализ и оценка рисков нарушения безопасности в системе защиты ПДн и разработка на их основе комплекса мер и мероприятий по минимизации данных рисков

В соответствии со статьей 19 ФЗ-152 [59] для любой ИСПДн должны быть определены угрозы безопасности и разработана Модель угроз безопасности информации (далее – Модель угроз). Данный документ служит для идентификации угроз безопасности информации, реализация (возникновение) которых возможна в информационной системе персональных данных.

Применение Модели угроз позволяет решить такие задачи, как:

– проведение мер по предотвращению несанкционированного доступа к ПДн и/или передаче этой информации лицам без прав на доступ;

– создание специализированных моделей угроз безопасности персональных данных для определенных информационных систем обработки ПДн с учетом их функционального назначения, условий использования и специфики функционирования;
– анализ уязвимостей ИСПДн перед угрозами безопасности ПДн при организации и выполнении работ по защите этих данных;
– предотвращение воздействий на технические средства ИСПДн, которые могут привести к нарушениям в их работе;
– создание системы защиты ПДн, которая нейтрализует потенциальные угрозы с применением методов и средств защиты, соответствующих классу конкретной ИСПДн;
– контроль за обеспечением необходимого уровня защиты личной информации граждан.

Для каждой ИСПДн колледжа разработана модель угроз. В силу того, что ИСПДн «ФИС ГИА и Приема», «ФИС ФРДО», «ГИС Образование. Е-услуги», «АСУ Procollege» и «Сетевой город. Образование» одинаковы с точки зрения уровня защищенности, имеют близкие цели и объемы обработки ПДн, категории ПДн и тип угроз, оценим риски нарушения безопасности данных ИСПДн вместе.

Как уже написано выше, риски напрямую связаны с угрозами нарушения безопасности, уязвимостью информационной системы и активом (в нашем случае это ПДн), поэтому риск можно изобразить с помощью следующей формулы:

Степень риска = Ущерб + Вероятность + Приоритет актива,

при этом ущерб, вероятность и приоритет актива будем рассчитывать исходя из трехбалльной шкалы: 1 - низкий, 2 - средний, 3 - высокий. Таким образом, в нашей работе степень риска будем оценивать с помощью качественного метода и метода экспертной оценки (экспертная группа в составе заместителя директора по УМР, заведующего отделением ИТ,

техника, оператора ЭВМ, секретаря учебной части, утвержденная приказом директора №356 от 24 декабря 2023 г., должна была определить объекты исследования, а также их параметры и характеристики). Чем больше степень риска, тем выше его вероятность и негативные последствия в случае его реализации. Для этого построим следующую матрицу на примере четырех угроз (см. таблицу 6):

Таблица 6 – Матрица оценки риска качественным методом и методом экспертной оценки

Наименование угрозы	Объект воздействия	Негативные последствия (далее - НП)	Вероятность реализации угрозы	Степень риска
Угроза подмены доверенного пользователя	Сетевой узел, сетевое ПО	НП.2 – 3 балла НП.3 – 2 балла НП.6 – 3 балла НП.7 – 3 балла НП.8 – 2 балла НП.10 – 3 балла НП.11 – 3 балла	2	21
Угроза подмены содержимого сетевых ресурсов	Сетевое ПО, прикладное ПО и сетевой трафик	НП.1 – 1 балл НП.2 – 3 балла НП.3 – 2 балла НП.6 – 3 балла НП.7 – 3 балла НП.8 – 2 балла НП.10 – 3 балла НП.11 – 3 балла	2	22
Угроза удаления аутентификационной информации	Учетные данные ответственного пользователя, системное ПО, микропрограммное обеспечение	НП.2 – 3 балла НП.6 – 2 балла НП.7 – 3 балла НП.11 – 3 балла	2	13
Угроза форматирования носителей информации	Машинный носитель информации	НП.2 – 3 балла НП.6 – 2 балла НП.7 – 1 балла НП.11 – 3 балла	3	12

В силу того, что в качестве информационного актива будут выступать во всех случаях ПДн, в данной матрице этот показатель как постоянный не отражен. Наименование угрозы и объекты воздействия выбраны методом экспертной оценки, ущерб и вероятность реализации угрозы оценены качественным методом. Раскроем содержание негативных последствий:

НП.1 - Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах;

НП.2 - Нарушение конфиденциальности (утечка) персональных данных;

НП.3 - Разглашение персональных данных граждан;

НП.4 - Нарушение законодательства Российской Федерации;

НП.5 - Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций;

НП.6 - Необходимость дополнительных (незапланированных) затрат на восстановление деятельности;

НП.7 - Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций);

НП.8 - Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др.;

НП.9 - Увеличение количества жалоб в органы государственной власти или органы местного самоуправления;

НП.10 - Доступ к системам и сетям с целью незаконного использования вычислительных мощностей;

НП.11 - Утечка информации ограниченного доступа.

Таким образом, с помощью подсчета суммы баллов мы определили, что риск в случае реализации угрозы подмены содержимого сетевых ресурсов выше, по сравнению с другими, рассмотренными в таблице 6. Но это только в случае сравнения, представленных в этой таблице видов угроз, имеющих место при обработке ПДн.

Используя предложенную матрицу можно оценить риски всех возможных угроз и ущерба от них при нарушении безопасности в системе защиты ПДн (см. приложение 3). Угрозы, степень риска которых равна 11 и более, выделены красным цветом. Именно на них мы остановимся в данной работе детальнее.

Анализ и оценка рисков нарушения безопасности в системе защиты ПДн колледжа показал, что наибольшие риски ожидаются в случае реализации следующих угроз (см. таблицу 7):

Таблица 7 – Угрозы ПДн с высокой степенью риска

Название угрозы и ее идентификатор	Объект воздействия угрозы	Степень риска
УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации	Системное программное обеспечение, учетные данные ответственного пользователя	15
УБИ.014 Угроза длительного удержания вычислительных ресурсов пользователями	Информационная система, сетевой узел, машинный носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	21
УБИ.028 Угроза использования альтернативных путей доступа к ресурсам	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	15
УБИ.030 Угроза использования информации идентификации / аутентификации, заданной по умолчанию	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	16
УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	16
УБИ.071 Угроза несанкционированного восстановления удаленной защищаемой информации	Машинный носитель информации	14
УБИ.074 Угроза несанкционированного доступа к аутентификационной информации	Системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр, машинные носители информации	15
УБИ.085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Машинный носитель информации, объекты файловой системы	12
УБИ.086 Угроза несанкционированного изменения аутентификационной информации	Системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр	15
УБИ.088 Угроза несанкционированного копирования защищаемой информации	Объекты файловой системы, машинный носитель информации	18
УБИ.090 Угроза несанкционированного создания учетной записи пользователя	Системное программное обеспечение	15
УБИ.091 Угроза несанкционированного удаления защищаемой информации	Метаданные, объекты файловой системы, реестр	18
УБИ.113 Угроза перезагрузки	Системное программное обеспечение,	14

Продолжение таблицы 7

аппаратных и программно-аппаратных средств вычислительной техники	аппаратное обеспечение	
УБИ.121 Угроза повреждения системного реестра	Объекты файловой системы, реестр	12
УБИ.128 Угроза подмены доверенного пользователя	Сетевой узел, сетевое программное обеспечение	21
УБИ.130 Угроза подмены содержимого сетевых ресурсов	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	22
УБИ.139 Угроза преодоления физической защиты	Информационная система, машинный носитель информации, аппаратное обеспечение	16
УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Машинный носитель информации, микропрограммное обеспечение, аппаратное обеспечение, телекоммуникационное устройство	14
УБИ.152 Угроза удаления аутентификационной информации	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	13
УБИ.158 Угроза форматирования носителей информации	Машинный носитель информации	12
УБИ.190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Сетевое программное обеспечение	15
УБИ.192 Угроза использования уязвимых версий программного обеспечения	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	15
УБИ.201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Учетные данные ответственного пользователя	15
УБИ.205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Аппаратное обеспечение, программное обеспечение	13

Таким образом, в ходе оценки рисков качественным методом и методом экспертной оценки выявлено 24 угрозы с высокой степенью риска из 87 актуальных угроз, зафиксированных в Моделях угроз безопасности информации колледжа (см. выше выходные данные документов).

На основании полученных результатов, а также с учетом требований Приказа ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении

состава и содержания организационных и технических мер по обеспечению безопасности ПДн при обработке в ИСПДн» [46] нами разработан и предложен к реализации в условиях образовательной организации, являющейся базой нашего исследования, комплекс мер и мероприятий по минимизации данных рисков.

Предлагаемый комплекс мер и мероприятий свяжем с видами угроз и представим в табличном варианте для удобства (см. таблицу 8):

Таблица 8 - Комплекс мер и мероприятий по минимизации рисков с высокой степенью

№ п/п	Наименование и содержание организационных и технических мер по обеспечению безопасности ПДн	Мероприятия по реализации мер	Идентификатор угрозы	Периодичность проведения	Ответственное лицо
1.Идентификация и аутентификация субъектов доступа и объектов доступа					
1.	Аутентификация и идентификация пользователей, являющихся работниками оператора обработки ПДн	- формирование списка сотрудников, которым требуется доступ к ПДн, обрабатываемым в ИС, для исполнения их должностных обязанностей; - применение системы защиты информации Secret Net LSP; - аудит парольной и ключевой информации с регулярным обновлением данных	УБИ.201, УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152, УБИ.201	Ежемесячно	Администратор безопасности
		- аудит авторизации внутренних пользователей и входа в систему, доступа к объектам, системных событий, событий входа в систему; - аудит управления учетными записями	УБИ.071, УБИ.085, УБИ.088, УБИ.091, УБИ.121	Ежеквартально	Администратор безопасности
2.	При введении аутентификационной информации обеспечение защиты обратной связи	- применение средств защиты информации Secret Net LSP	УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152	Постоянно	Администратор безопасности
3.	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	- назначение администратора безопасности; - создание и регулярное обновление инструкций для администратора по вопросам безопасности, использования системы и управления паролями;	УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152	Ежеквартально	Администратор безопасности

Продолжение таблицы 8

4.	Менеджмент средств аутентификации, включая такие процессы, как их хранение, выдача, активация, блокировка, а также мероприятия по предотвращению и устранению последствий утраты и/или компрометации данных средств	- составление перечня лиц, доступ которых к ПДн, обрабатываемым в ИС, нужен для выполнения ими должностных обязанностей			
2.Управление доступом субъектов доступа к объектам доступа					
5.	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и принципов разграничения прав доступа	- утверждение приказом руководителя образовательной организации перечня лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей; - назначение администратора безопасности; - разработка и регулярное обновление руководства по безопасности для администраторов, матрицы прав доступа пользователей к защищенным ИС, а также инструкций по разграничению доступа пользователей к системам защиты информации и информационным ресурсам; - разработка описания технологического процесса обработки персональных данных; - использование средств защиты информации Secret Net LSP	УБИ.090, УБИ.128, УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152, УБИ.143	Постоянно	Администратор безопасности

Продолжение таблицы 8

6.	Разграничение прав доступа пользователей, администраторов и специалистов, обеспечивающих работу информационной системы	- назначение администратора безопасности; - составление перечня лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей; - разработка и постоянное обновление при необходимости инструкций администратора по безопасности, пользователя, обслуживающего персонала, по разграничению доступа пользователей к средствам защиты и информационным ресурсам, матрицы доступа пользователей к защищаемым информационным ресурсам; - разработка описания технологического процесса обработки ПДн; - использование средств защиты информации Secret Net LSP	УБИ.090, УБИ.128, УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152	Постоянно	Администратор безопасности
7.	Предоставление минимально необходимых прав и привилегий пользователям, администраторам и ответственным за работу информационной системы				
8.	Управление (фильтрация, маршрутизация, управление соединениями, однонаправленная передача и другие методы контроля и управления) информационных потоков между устройствами, сегментами информационной системы, а также между различными информационными системами	- разработка описания технологического процесса обработки информации; - использование средств защиты информации Secret Net LSP	УБИ.014, УБИ.028, УБИ.063, УБИ.113, УБИ.121, УБИ.130, УБИ.192, УБИ.205	Постоянно	Администратор безопасности

Продолжение таблицы 8

9.	Создание, администрирование, блокировка и удаление пользовательских аккаунтов, включая профили внешних пользователей	- назначение по приказу директора администратора безопасности; - разработка и поддержание в актуальном состоянии инструкции администратора по безопасности, пользователя, парольной защиты	УБИ.090, УБИ.128, УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152	Постоянно	Администратор безопасности
10.	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	- разработка и поддержание в актуальном состоянии инструкции по организации парольной защиты, инструкции пользователя; - использование средств защиты информации Secret Net LSP	УБИ.201, УБИ.008, УБИ.030, УБИ.074, УБИ.086, УБИ.152, УБИ.201	Ежемесячно	Администратор безопасности
11.	Завершение сеанса подключения к информационной системе по истечении заданного периода неактивности пользователя либо по его инициативе				
12.	Регулирование и контроль использования в ИС мобильных технических средств	- разработка и поддержание в актуальном состоянии инструкции по учету машинных носителей и регистрации их выдачи	УБИ.190, УБИ.192	Постоянно при использовании	Администратор безопасности
13.	Управление взаимодействием с информационными системами сторонних организаций (внешние ИС)	- утверждение списка лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей; - использование в работе средств защиты информации Secret Net LSP; - разработка описания технологического процесса обработки информации			
3. Защита машинных носителей ПДн					

Продолжение таблицы 8

14.	Обезличивание и при необходимости удаление (очистка) или персональных данных на электронных носителях при их передаче между пользователями, в сторонние компании для ремонта или утилизации, а также проверка удаления (очистки) или обезличивание	- разработка и постоянное обновление при необходимости инструкции по учету машинных носителей и регистрации их выдачи, инструкции по работе ответственного лица за организацию обработки ПДн; - использование средств защиты информации Secret Net LSP; - контроль порядка обращения с носителями ПДн	УБИ.152, УБИ.158	Ежеквартально	Ответственный за обеспечение безопасности ПДн
4. Регистрация событий безопасности					
15.	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	- мониторинг результатов регистрации событий безопасности и реагирование на них;- разработка и обновление при необходимости Положения об обеспечении безопасности ПДн при их обработке в ИСПДн, его неукоснительное выполнение	УБИ.008, УБИ.158	Еженедельно	Администратор безопасности
16.	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации				
17.	Сбор, запись, хранение информации о событиях безопасности на протяжении установленного времени	- внедрение в деятельность средств защиты информации Secret Net LSP; - систематическое обновление Положения об обеспечении безопасности ПДн при их обработке в ИСПДн, его выполнение			
18.	Защита информации о событиях безопасности	- использование средств защиты информации Secret Net LSP; - назначение администратора безопасности; - разработка и поддержание в актуальном состоянии инструкции администратора по безопасности			

Продолжение таблицы 8

5. Антивирусная защита					
19.	Реализация антивирусной защиты	- назначение администратора безопасности; - своевременное обновление антивирусных программ; - контроль состояния антивирусной защиты; - разработка и поддержание в актуальном состоянии инструкции администратора по безопасности, инструкции по организации антивирусной защиты	УБИ.190, УБИ.192, УБИ.014, УБИ.028, УБИ..205	Еженедельно	Администратор безопасности
20.	Актуализация базы данных признаков вредоносного программного обеспечения (вирусов)				
6. Контроль (анализ) защищенности ПДн					
21.	Постоянный мониторинг, оценка уязвимостей информационной системы и быстрое устранение новых обнаруженных уязвимостей	- назначение администратора безопасности	УБИ.128	По мере необходимости	Директор
		- проведение анализа и переоценки существующих угроз безопасности персональных данных, а также прогнозирование возникновения новых, ранее неизвестных угроз	возможность фиксации новых УБИ	Ежегодно	Администратор безопасности
		- мониторинг процесса резервного копирования (оценка функциональности инструментов для создания резервных копий, систем хранения резервных данных и средств для восстановления информации из резервных копий)	УБИ.088, УБИ.085, УБИ.071, УБИ.028	Ежемесячно	Администратор безопасности
		- контроль уровня защищенности ПДн при их обработке в ИСПДн	УБИ.190, УБИ.192, УБИ.014, УБИ.028, УБИ.008, УБИ.014	Ежегодно	Ответственный за обеспечение безопасности персональных данных
		- проверка выполнения запросов субъектов ПДн		Ежеквартально	

Продолжение таблицы 8

		- контроль нейтрализации выявленных нарушений режима обработки ПДн	все УБИ	Ежеквартально	Администратор безопасности
22.	Контроль установки обновлений ПО, включая обновление ПО средств защиты информации	- разработка и реализация плана внутренних проверок состояния защиты информационных систем персональных данных; - создание и регулярное обновление инструкций для администратора по вопросам безопасности; - контроль за соблюдением правил обработки ПДн; - контроль за обновлениями ПО и единообразия применяемого ПО на всех элементах информационных систем персональных данных	УБИ.071, УБИ.074, УБИ.085, УБИ.086, УБИ.088, УБИ.090, УБИ.091, УБИ.128, УБИ.030	Еженедельно	Администратор безопасности
		- проведение внутренних аудитов для обнаружения изменений в процедурах обработки и защиты персональных данных	УБИ.008, УБИ.014, УБИ.030, УБИ.152, УБИ.190, УБИ.192, УБИ.205	Ежегодно	Администратор безопасности
		- управление процессом разработки и внесения изменений в программное обеспечение, созданное внутри компании или стандартное ПО, которое адаптируется силами внутренних разработчиков либо с привлечением внешних организаций	УБИ.113, УБИ.139, УБИ.143, УБИ.192, УБИ.205, УБИ.063	Еженедельно	Администратор безопасности

Продолжение таблицы 8

		- регулярная проверка работы функций системы защиты персональных данных при изменениях программного окружения и состава пользователей информационной системы	УБИ.113, УБИ.139, УБИ.192, УБИ.063	Ежемесячно	Администратор безопасности
		- управление настройками технических устройств, программных приложений и средств информационной безопасности для соответствия актуальной эксплуатационной документации, включая реализацию мероприятий по устранению обнаруженных недочетов	УБИ.113, УБИ.139, УБИ.143, УБИ.192, УБИ.205, УБИ.063	Ежемесячно	Администратор безопасности
23.	Проверка функциональности, настроек и корректного выполнения задач программным обеспечением и средствами информационной безопасности	- аудит соблюдения режима защиты информации	УБИ.190, УБИ.192, УБИ.014, УБИ.028, УБИ.201	Ежедневно	Администратор безопасности
24.	Контроль средств защиты информации, ПО и состава технических средств	- проверка работоспособности и корректности работы (тестирование с использованием тестовых данных, которые приводят к ожидаемому результату) программного обеспечения и средств защиты информации, а также технических устройств; - контроль настроек ПО и средств защиты информации на соответствие параметрам конфигурации, указанным в эксплуатационной документации по системе защиты информации и средствам защиты информации	УБИ.113, УБИ.139, УБИ.143, УБИ.192, УБИ.205, УБИ.063	Ежемесячно	Администратор безопасности

Продолжение таблицы 8

		- отслеживание появления новых видов уязвимостей программного обеспечения информационных систем ПДн	УБИ.113, УБИ.139, УБИ.143, УБИ.192, УБИ.205	Еженедельно	Администратор безопасности
7. Защита технических средств					
25.	Размещение устройств отображения информации для достижения цели по предотвращению возможности несанкционированного доступа к ПДн во время их обработки	- размещение устройств отображения информации должно быть организовано так, чтобы предотвратить возможность несанкционированного доступа к данным; - занавешивание оконных проемов непрозрачными шторами	УБИ.190, УБИ.192, УБИ.014, УБИ.028, УБИ.008, УБИ.014, УБИ.201	Еженедельно	Администратор безопасности
26.	Управление и контроль физического доступа к технологическому оборудованию, системам защиты данных, обеспечивающим инфраструктуре, а также в помещения и здания, где это оборудование размещено, предотвращение несанкционированного физического проникновения к ИС, системам безопасности и поддерживающей инфраструктуре, включая те места, где они находятся	- утверждение перечня лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей, и имеющих доступ в помещение ограниченной открытости; - разработка и поддержание в актуальном состоянии инструкции по физической охране и контролю доступа к помещению; - осуществление охраны помещения собственными силами; - ведение журнала учета ключей от хранилищ, сейфов, режимного помещения			
8. Защита информационной системы, ее средств, систем связи и передачи данных					

Продолжение таблицы 8

27.	Защита персональных данных от несанкционированного доступа, изменения и внедрения ложной информации во время их передачи (или подготовки к передаче) через каналы связи, которые выходят за границы безопасной зоны, включая беспроводные сети	- использование в работе программного комплекса VipNet Client; - контроль над соблюдением режима защиты при подключении к сетям связи общего пользования; - управление доступом к приложениям информационных систем, где происходит обработка персональных данных	УБИ.086, УБИ.071, УБИ.030, УБИ.074, УБИ.088, УБИ.090, УБИ.085, УБИ.091, УБИ.128	Ежеквартально	Ответственный за обеспечение безопасности персональных данных
9. Управление конфигурацией информационной системы и системы защиты персональных данных					
28.	Оценка возможного влияния запланированных изменений в настройке информационной системы и системы защиты персональных данных на обеспечение безопасности персональных данных и координация этих изменений с уполномоченным сотрудником, отвечающим за защиту персональных данных	- утверждение приказом директора администратора безопасности; - разработка и систематическое обновление инструкции администратора по безопасности	все УБИ	Ежеквартально	Ответственный за обеспечение безопасности ПДн
29.	Ограничение круга лиц, уполномоченных вносить изменения в конфигурацию информационной системы и системы защиты персональных данных				
30.	Управление изменениями конфигурации ИС и ИСПДн				

Продолжение таблицы 8

31.	Систематическая актуализация документации по изменениям конфигурации информационной системы и системы защиты персональных данных	- назначение администратора безопасности; - создание и регулярное обновление руководства по безопасности для администратора; - своевременная переаттестация рабочего места (АРМ), на котором обрабатываются и передаются по защищенной сети ПДн; - контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков	все УБИ	Ежеквартально	Ответственный за обеспечение безопасности персональных данных
32.	Обеспечение безопасности охраняемого объекта посредством включения мер по предотвращению несанкционированного доступа и нахождения в нем лиц без соответствующего разрешения	- разработка и утверждение правил доступа в режимное помещение; - составление списка лиц, имеющих доступ в режимное помещение; - контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн; - использование в режимном помещении входной двери с замком, который обеспечивает её постоянное запирание и открытие только при санкционированном доступе, а также опечатывание этого помещения после окончания работы	УБИ.139, УБИ.128	Ежегодно	Ответственный за обеспечение безопасности персональных данных
33.	Обеспечение безопасности носителей персональных данных	- хранение съемных машинных носителей ПДн должно осуществляться в сейфах, оснащенных внутренними	УБИ.158, УБИ.143	Постоянно	Ответственный за организацию обработки

Продолжение таблицы 8

		замками с двумя комплектами ключей и устройствами для опечатывания замков; - обязательное ведение индивидуального учета машинных носителей персональных данных (заполнение журнала учета носителей ПДн)			персональных данных
34.	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных обязанностей	- составление и утверждение списка лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими должностных обязанностей	УБИ.128	По мере необходимости	Директор
35.	Применение прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации средств защиты информации, в т.ч. в случае, когда использование таких средств необходимо для нейтрализации актуальных угроз	- разработка модели нарушителя безопасности ИСПДн; - в целях обеспечения безопасности ИС применение в работе программного комплекса VipNet Client;	все УБИ	Постоянно Ежегодно	Ответственный за организацию обработки ПДн
36.	Назначение уполномоченного сотрудника, ответственного за обеспечение безопасности персональных данных в информационной системе	- назначение по приказу директора ответственного лица за обеспечение безопасности ПДн - постоянная актуализация нормативных организационных документов	все УБИ	Ежемесячно	Ответственный за организацию обработки ПДн

Реализация данного комплекса мер и мероприятий запланирована на 2024 год.

Таким образом, посредством качественного метода и метода экспертной оценки выявлены 24 угрозы с высокой степенью риска нарушения безопасности в системе защиты ПДн, в соответствии с чем разработан комплекс мер и мероприятий по их минимизации, который был реализован колледжем в течение 2024 года.

2.5 Результаты апробации комплекса мер и мероприятий по минимизации рисков нарушения безопасности в системе защиты ПДн

В целях определения эффективности предложенного нами комплекса мероприятий и мер по минимизации рисков нарушения безопасности в системе защиты ПДн, разработанного на основе анализа и оценки рисков, были выполнены констатирующие замеры в конце 2023 года, до внедрения разработанной нами системы мер и мероприятий, и контрольные замеры в середине декабря 2024, после его реализации, и охватывали календарный год, предшествующий замерам.

Оценка эффективности проводилась на основе следующей шкалы:

0 – УИБ не реализована;

1 – фиксация 1-2 случаев реализации УИБ;

2 – фиксация 3 и более случаев реализации УИБ.

Рассмотрим получившиеся результаты в таблице 9.

Таблица 9 - Результаты апробации комплекса мероприятий и мер минимизации рисков нарушения безопасности в системе защиты ПДн в условиях колледжа

Идентификатор и наименование угрозы	Степень риска	январь – декабрь 2023	январь – декабрь 2024
УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации	15	1	0

Продолжение таблицы 9

УБИ.014 Угроза длительного удержания вычислительных ресурсов пользователями	21	0	0
УБИ.028 Угроза использования альтернативных путей доступа к ресурсам	15	1	0
УБИ.030 Угроза использования информации идентификации / аутентификации, заданной по умолчанию	16	1	0
УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения	16	2	0
УБИ.071 Угроза несанкционированного восстановления удаленной защищаемой информации	14	0	0
УБИ.074 Угроза несанкционированного доступа к аутентификационной информации	15	0	0
УБИ.085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	12	0	0
УБИ.086 Угроза несанкционированного изменения аутентификационной информации	15	0	0
УБИ.088 Угроза несанкционированного копирования защищаемой информации	18	0	0
УБИ.090 Угроза несанкционированного создания учетной записи пользователя	15	0	0
УБИ.091 Угроза несанкционированного удаления защищаемой информации	18	0	0
УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	14	2	0
УБИ.121 Угроза повреждения системного реестра	12	0	0
УБИ.128 Угроза подмены доверенного пользователя	21	0	0
УБИ.130 Угроза подмены содержимого сетевых ресурсов	22	0	0
УБИ.139 Угроза преодоления физической защиты	16	1	0
УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	14	1	0
УБИ.152 Угроза удаления аутентификационной информации	13	0	0
УБИ.158 Угроза форматирования носителей информации	12	0	0
УБИ.190 Угроза внедрения вредоносного кода за счет посещения	15	2	1

Продолжение таблицы 9

зараженных сайтов в сети Интернет			
УБИ.192 Угроза использования уязвимых версий программного обеспечения	15	1	1
УБИ.201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	15	2	1
УБИ.205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	13	1	0
Количество реализованных угроз		*11*	*3*
Частота реализации угроз		*зафиксированы факты 3 и более случаев реализации*	*зафиксированы факты 1-2 случаев реализации*

Хочется отметить, что в ходе выполненных замеров не были зафиксированы случаи реализации других угроз, что свидетельствует о достоверности результатов оценки рисков посредством качественного метода и метода экспертной оценки.

Рассмотрим зависимость между степенью риска и фактами реализации угроз за 2023 и 2024 года. Для более наглядного представления информации построим гистограмму (см. рисунок 8).

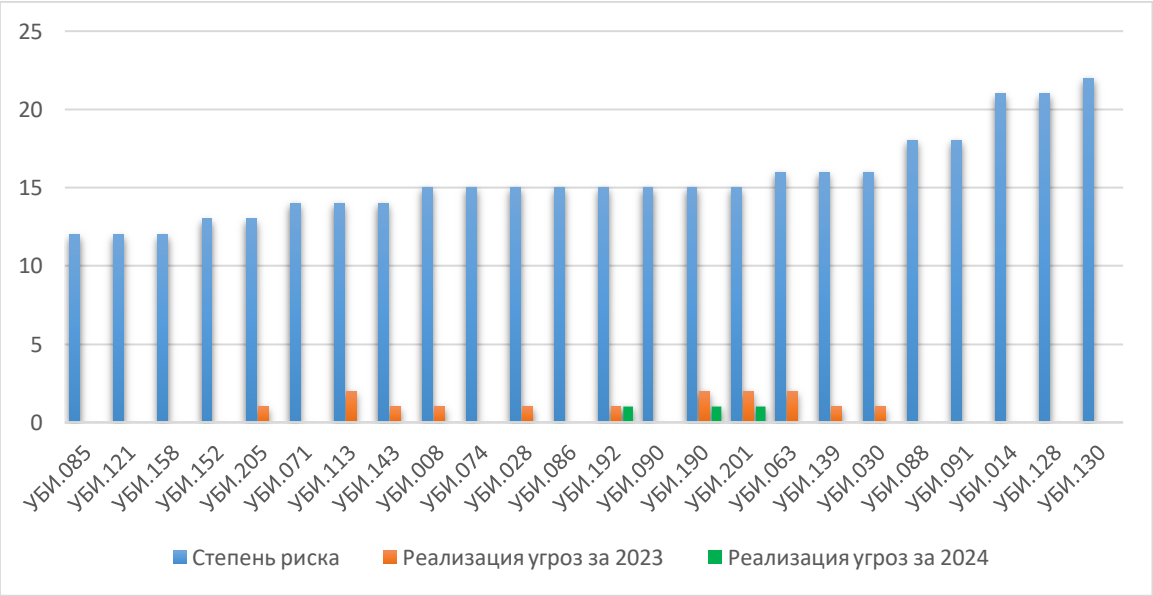


Рисунок 8 - Зависимость между степенью риска и фактами реализации угроз (по результатам анализа за 2023 и 2024 года)

Из данного рисунка можно сделать вывод, что реализация угроз приходится на те из них, степень риска которых в диапазоне от 13 до 16. Угрозы, степень риска которых менее или более указанного диапазона, за обозначенные периоды не реализовались.

Итак, анализ представленных выше результатов показал, что внедрение в колледже разработанного нами комплекса мероприятий и мер по минимизации рисков нарушения безопасности в системе защиты ПДн дало положительный эффект и позволило снизить количество реализованных угроз на 73%. Это доказывает, что система защиты ПДн образовательной организации будет устойчивее к внешним негативным воздействиям, если разработать и внедрить комплекс мероприятий и мер по минимизации рисков нарушения безопасности в системе защиты ПДн на основе их анализа. В этом и заключалась наша гипотеза.

Апробация проводилась в отношении таких информационных систем персональных данных, как «ФИС ГИА и Приема», «ФИС ФРДО», «ГИС Образование. Е-услуги», «АСУ Procollege» и «Сетевой город. Образование», но в дальнейшем, думается, этот комплекс может быть внедрен и в другие ИСПДн колледжа.

Выводы по второй главе

В ходе разработки комплекса мероприятий и мер по минимизации рисков нарушения безопасности в системе защиты ПДн ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего») сделаны следующие выводы.

Анализ единого информационного пространства колледжа показал, что организационная структура и используемое многообразие информационных систем соответствуют задачам открытости, доступности, прозрачности деятельности образовательной организации, локальные

нормативные акты, сопровождающие функционирование и развитие единого информационного пространства, выполнены на высоком уровне.

Посредством качественного метода и метода экспертной оценки выявлено 24 вида угроз, имеющих в случае реализации высокую степень риска нарушения безопасности в системе защиты ПДн, в соответствии с чем был разработан комплекс мероприятий и мер по их минимизации; данная система мероприятий и мер была внедрена в деятельность колледжа в течение 2024 года.

Анализ результатов внедрения наших предложений по минимизации рисков нарушения безопасности ИСПДн показал, что разработанный нами комплекс мероприятий и мер адекватен поставленным целям и позволил снизить количество реализованных угроз на 73%. Это доказывает, что система защиты ПДн образовательной организации устойчивее к внешним негативным воздействиям при условии разработки и внедрения комплекса мероприятий и мер по минимизации рисков нарушения безопасности ИСПДн на основе их анализа, что свидетельствует о доказательстве выдвинутой нами гипотезы.

ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования были сделаны следующие выводы.

Анализ нормативно-правовой базы по вопросу минимизации рисков нарушения безопасности в системе защиты ПДн и теоретических работ, направленных на изучение данной проблемы, показал, что законодательство в сфере защиты ПДн России, США и стран Европы имеет общие фундаментальные принципы, направленные на защиту прав граждан. Однако следует отметить, что в дальнейшем данный вопрос потребует конкретизации под потребности общества с учетом специфики отрасли экономики

Однако при достаточно высокой степени изученности данной проблемы на нормативно-правовом и теоретическом уровне по-прежнему остаются пробелы, требующие уточнения (например, понятие «риск нарушения безопасности в системе защиты персональных данных» в проанализированных источниках информации осталось нераскрытым); также нужно отметить, что некоторые нормативные правовые документы содержат информацию о неполноте закреплённых положений, что приводит в отрасли информационной безопасности к нарушениям (например, в Методике оценки угроз безопасности информации (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) написано: «указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами…» [31]). Безусловно, такие факты свидетельствуют о том, что данная отрасль правого регулирования нуждается в дальнейшей доработке и конкретизации.

В данной работе ключевым понятием является термин «риск нарушения безопасности в системе защиты персональных данных», под которым понимается «потенциальное / возможное / вероятностное

нарушение безопасности в системе защиты ПДн, которое в случае реализации создаст угрозу / опасность использования уязвимости системы защиты ПДн в целях нанесения ущерба / вреда / последствия организации».

В силу того, что риски напрямую связаны с угрозами нарушения безопасности, уязвимостью информационной системы и активом (в нашем случае это ПДн), поэтому риск может быть рассчитан по следующей формуле: **Степень риска = Ущерб + Вероятность + Приоритет актива**, при этом чем больше степень риска, тем выше его вероятность и негативные последствия в случае его реализации.

Анализ единого информационного пространства ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» показал, что организационная структура и используемое многообразие информационных систем соответствует задачам открытости, доступности, прозрачности и полноты деятельности образовательной организации, локальные нормативные акты, сопровождающие функционирование и развитие единого информационного пространства, выполнены на высоком уровне.

Однако можно выделить такие актуальные для колледжа направления дальнейшего развития единого информационного пространства как: дооснащение учебных кабинетов, лабораторий, мастерских компьютерной техникой и поддержание техники в рабочем состоянии; обучение педагогов пользованию сложной техникой; реализация плана перехода на отечественное программное обеспечение; использование всех функций АСУ «ProCollege»; дальнейшее внедрение дистанционных технологий в образовательный процесс; создание и использование электронных образовательных ресурсов и усиление контент-фильтрации на рабочих местах студентов в целях их защиты от причиняющей вред их здоровью и / или их развитию информации и др.

В образовательной организации разработаны документы, регулирующие вопросы обработки персональных данных, среди которых отметим следующие: Политика обработки персональных данных; Положение об обработке и защите персональных данных; Регламент по организации процесса управления уязвимости; Положение о работе в автоматизированной системе «Сетевой горд. Образование»; Положение об электронном журнале и др.

В колледже используются такие информационные системы ПДн, как ФИС ФРДО, ФИС ГИА и приема, ГИС Образование. Е-услуги, Сетевой город. Образование, АСУ Procollege, ИС «Аттестация педагогических кадров» и ИСПДн «Бухгалтерия и кадры». В данной работе проанализированы ИСПДн, сопровождающие образовательный процесс от момента подачи абитуриентами заявления на прием до выпуска: ФИС ГИА и Приема, ФИС ФРДО, ГИС Образование. Е-услуги, АСУ Procollege и Сетевой город. Образование, раскрыты цели обработки и объем персональных данных, субъекты ПДн, выявлены угрозы и уязвимости ИСПДн.

Анализ методов оценки рисков нарушения информационной безопасности, среди которых выделяются количественный, качественный, статистический, факторный, метод экспертной оценки, продемонстрировал, что каждый из них имеет свои достоинства и недостатки, а методы оценки необходимо выбирать с учетом специфики организации и задач, поставленных перед ее специалистами. На наш взгляд, рассмотренные методы оценки рисков нарушения информационной безопасности могут быть использованы одновременно, выгодно дополняя друг друга.

В нашей работе для оценки рисков нарушения безопасности в системе защиты ПДн использованы в комплексе качественный метод и метод экспертной оценки, преимуществом которых является высокая скорость обработки данных и объективность, так как привлекаемые

эксперты являются специалистами в области информационной безопасности. Данные методы позволили выявить 24 вида угроз, имеющих в случае реализации высокую степень риска нарушения безопасности в системе защиты ПДн (изначально в Модели угроз безопасности ПДн при их обработке в информационной системе персональных данных было зарегистрировано при первоначальном анализе 87 угроз).

Ещё необходимо отметить, что в ходе выполненных замеров не были зафиксированы случаи реализации других угроз, что свидетельствует о достоверности результатов оценки рисков посредством качественного метода и метода экспертной оценки.

В соответствии с полученными результатами был разработан комплекс мероприятий и мер по их минимизации, включающий 36 организационных и технических мер по обеспечению безопасности ПДн колледжа по 9 направлениям, а также определены ответственные лица и периодичность проведения обозначенных мероприятий. Данный комплекс мер и мероприятий рассчитан на реализацию в течение одного года и был внедрен в деятельность образовательной организации в 2024 году.

Таким образом, поставленные задачи в ходе выполнения данной работы реализованы в полном объеме, что позволило достичь обозначенную выше цель.

В целях определения эффективности предложенного нами комплекса мероприятий и мер по минимизации рисков нарушения безопасности в системе защиты ПДн, разработанной на основе анализа и оценки рисков, были выполнены констатирующие замеры в конце 2023 года, до внедрения системы мероприятий, и контрольные замеры в середине декабря 2024, после ее реализации, и охватывали календарный год, предшествующий замерам.

Анализ результатов внедрения системы мер и мероприятий по минимизации рисков нарушения безопасности ИСПДн показал, что разработанный нами комплекс мероприятий и мер адекватен

поставленным целям и позволил снизить количество реализованных угроз на 73%. Это доказывает, что система защиты ПДн образовательной организации устойчивее к внешним негативным воздействиям при условии разработки и внедрения комплекса мероприятий и мер по минимизации рисков нарушения безопасности ИСПДн на основе их анализа. Таким образом, выдвинутая нами гипотеза доказана.

Запланированные этапы исследования также реализованы в полном объеме.

В ходе выполнения работы была обоснована возможность необходимого обновления существующей системы информационной безопасности при обработке ПДн в колледже посредством разработки комплекса мер и мероприятий минимизации рисков нарушения безопасности в системе защиты ПДн.

В процессе написания данной работы были расширены научные знания в области методов обеспечения информационной безопасности при обработке ПДн образовательных организаций и достаточно глубоко изучены нормативно-правовые документы не только Российской Федерации, но и США и государств, входящих в состав Европейского Союза.

Разработанный нами в ходе представленного исследования комплекс мер и мероприятий минимизации рисков нарушения безопасности в системе защиты персональных данных может быть рекомендован для совершенствования методов обеспечения информационной безопасности при обработке ПДн в других профессиональных образовательных организациях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Анализ и оценка информационной безопасности [Электронный ресурс]. – Режим доступа https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/analiz-i-otsenka-informatsionnoy-bezopasnosti / (Дата обращения: 01.12.2024).

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.) [Электронный ресурс]. – Режим доступа https://base.garant.ru/197529/ (Дата обращения: 01.12.2024).

3. Балабанов, И. Т. Риск менеджмент [Текст] / И. Т. Балабанов. – Москва : Финансы и статистика, 2007. – 192 с.

4. Баранкова, И. И. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности [Электронный ресурс] / И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева. – Режим доступа https://cyberleninka.ru/article/n/minimizatsiya-riskov-informatsionnoy-bezopasnosti-na-osnove-modelirovaniya-ugroz-bezopasnosti/viewer (Дата обращения: 01.12.2024).

5. Бачило, И. Л. Информационное право : учебник для вузов [Текст] / И. Л. Бачило. – 5-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 419 с.

6. Волеводз, А. Г. Защита персональных данных в европейском союзе: правовое регулирование и порядок взаимодействия с третьими странами [Текст] / А. Г. Волеводз // Международное уголовное право и правосудие. – 2018. - №3 (38). - С. 303-312.

7. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов [Текст] / Е.В. Вострецова. - Екатеринбург : Изд-во Урал. ун-та, 2019- 204 с.

8. Герасименко, В. А. Основы защиты информации : Учеб. для студентов вузов обучающихся по спец. «Организация и технология защиты информации» [Текст] / В. А. Герасименко, А. А. Малюк; М-во общ. и проф. образования Рос. Федерации. Моск. гос. инж.-физ. ин-т (техн. ун-т). - Москва, 1997. - 537 с.

9. Гиш, Т. А. Анализ законодательства разных стран по обеспечению защиты персональных данных [Электронный ресурс]/ Т. А. Гиш, Н. В. Ржевская, А. С. Медведева. – Режим доступа : https://api-mag.kursksu.ru/api/v1/get_pdf/5181/ (Дата обращения: 01.12.2024).

10. ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты» (принят постановлением Госстандарта РФ от 5 июня 2002 г. №228-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/187645/ (Дата обращения: 01.12.2024).

11. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. №632-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70350582/ (Дата обращения: 01.12.2024).

12. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. №392-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/402878329/ (Дата обращения: 01.12.2024).

13. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (утв. приказом Федерального

агентства по техническому регулированию и метрологии от 19 декабря 2006 г. №317-ст) [Электронный ресурс]. - – Режим доступа: https://base.garant.ru/55171915/ (Дата обращения: 01.12.2024).

14. ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем» (принят и введен в действие постановлением Госстандарта РФ от 7 июня 2002 г. №236-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70400118/ (Дата обращения: 01.12.2024).

15. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России (принят постановлением Госстандарта РФ от 9 февраля 1995 г. № 49) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/193666/?ysclid=m4uwfr4tf9405563679 (Дата обращения: 29.11.2024).

16. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/5921891/?ysclid=m4uwin53pd791565060 (Дата обращения: 29.11.2024).

17. ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/193664/?ysclid=m4uwz6dnig232970579 (Дата обращения: 29.11.2024).

18. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и

общая модель» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/71086050/?ysclid=m4ux0m47uh830674605 (Дата обращения: 29.11.2024).

19. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. № 1339-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/71052128/?ysclid=m4ux3ocb20653682383 (Дата обращения: 29.11.2024).

20. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. « 1340-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/71052126/?ysclid=m4ux5e0531711083071 (Дата обращения: 29.11.2024).

21. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/403510768/?ysclid=m4ux70mgcz518610266 (Дата обращения: 29.11.2024).

22. ГОСТ Р ИСО/МЭК 27011-2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002» (утв. Приказом Федерального агентства по техническом урегулированию и метрологии от 24 сентября 2012г. № 424-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/71149434/?ysclid=m4uxb5s3nt801023027 (Дата обращения: 29.11.2024).

23. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 683-ст) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70246078/?ysclid=m4uxfpo0ie58485657 (Дата обращения: 29.11.2024).

24. Государственная тайна в Российской Федерации : учебно-методическое пособие [Текст] / А. Л. Балыбердин, В. С. Гусев, П. П. Аникин ; под ред. М. А. Вус; Санкт-Петербургский университет [СПбГУ], Управление Федеральной службы безопасности [ФСБ] по Санкт-Петербургу и Ленинградской области. - 2-е изд., перераб. и доп. - Санкт-Петербург : Санкт-Петербургский университет [СпбГУ], 2000. - 409 с.

25. Козин, И. С. Метод определения опасности угрозы персональным данным при их обработке в информационной системе [Текст] / И. С. Козин, С. Б. Беззатеев // Известия СПбГЭТУ «ЛЭТИ». - 2017. - № 10/2017. - С. 19-26.

26. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 (Страсбург, 28 января 1981 г.) (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/2559798/ (Дата обращения: 21.03.2024).

27. Котенко, И. В. Исследовательское моделирование бот-сетей и механизмов защиты от них [Текст] / И. В. Котенко, А. М. Коновалов, А. В. Шоров // Информационные технологии. - 2012. - № 1. - С. 3-32.

28. Котенко, И. В. Оценка рисков в компьютерных сетях критических инфраструктур [Текст] / И. В. Котенко, И. Б. Саенко, Е. В. Дойникова // Инновации в науке: сб. ст. по матер. XVI междунар. науч.-практ. конф. Часть I. – Новосибирск: СибАК, 2013. – С.84-89.

29. Котенко, И. В. Технологии больших данных для мониторинга компьютерной безопасности [Текст] / И. В. Котенко, И. А. Ушаков // Защита информации. Инсайд. - 2017. - № 3. - С. 23-33.

30. Лопатин, В. Н. Информационное право [Текст] / В. Н. Лопатин. - 3-е издание. - Москва : Проспект, 2021. – 655 с.

31. Методика оценки угроз безопасности информации (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа : // https://www.garant.ru/products/ipo/prime/doc/400325044/#review (Дата обращения: 21.03.2024).

32. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. Руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/199599/?ysclid=m4utisk1gk467149939 (Дата обращения: 29.11.2024).

33. Минзов, А. С. Безопасность персональных данных: новый взгляд на старую проблему [Текст] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов // Вопросы кибербезопасности. – 2022. - №4(50). – С. 2 – 12.

34. Молдовян, А .А. Протоколы аутентификации с нулевым разглашением секрета [Текст] / А.А. Молдовян, Д.Н. Молдовян, А.Б. Левина. – Санкт-Петербург: Университет ИТМО, 2016. – 55 с.

35. Назаров, Д. М. Основы обеспечения безопасности персональных данных в организации : учеб. пособие [Текст] / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. - Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. - 118 с.

36. Новиков, П. А. Современные аспекты обработки персональных данных: анализ и законодательное развитие [Электронный ресурс]. – Режим доступа : https://na-journal.ru/4-2024-pravo/10611-sovremennye-aspekty-obrabotki-personalnyh-dannyh-analiz-i-zakonodatelnoe-razvitie?ysclid=m4uyzirh75856829954 (Дата обращения: 21.11.2024).

37. Новосельцева, А. А. Безопасность персональных данных как элемент системы экономической безопасности в коммерческих организациях [Текст] / А. А. Новосельцева, С. С. Турбылев, Ю. Н. Руф // Экономическая безопасность страны, региона, организаций различных видов деятельности : материалы Третьего Всероссийского форума в Тюмени по экономической безопасности (г. Тюмень, 20-21 апреля 2022 г.) / ответственный редактор Д. Л. Скипин ; Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Финансово-экономический институт. – Тюмень : ТюмГУ-Press, 2022. – С. 368-375.

38. Овчинникова, Е. А. Сравнительный анализ законодательства в области защиты персональных данных в Российской Федерации и Евросоюзе // Е. А. Овчинникова [Электронный ресурс]. – Режим доступа : // https://cyberleninka.ru/article/n/sravnitelnyy-analiz-zakonodatelstva-v-oblasti-zaschity-personalnyh-dannyh-v-rossiyskoy-federatsii-i-evrosoyuze/viewer (Дата обращения: 21.11.2024).

39. Огурцова, В. С. Проблема интерпретации термина «единое информационное пространство» [Текст] / В. С. Огурцова, Ю. А. Антипина, М. Д. Голубинская и др. // Экономика и социум. – 2020. - №12-2(79). - С. 832-837.

40. Официальный сайт Рокомнадзора [Электронный ресурс]. – Режим доступа : // https://rkn.gov.ru/press/news/news74048.htm (Дата обращения: 21.03.2024).

41. Пожилых, В. А. Организационно-правовые особенности защиты информации в автоматизированных информационных системах органов внутренних дел : автореферат дис. ... кандидата юридических наук : 05.13.19 [Текст] /. 26. В. А. Пожилых,\. – Воронеж: изд-во Воронеж. ин-та МВД России, 2003. - 21 с.

42. Постановления Правительства Российской Федерации от 15 сентября 2008 № 21 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/193875/ (Дата обращения: 21.03.2024).

43. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70252506/ (Дата обращения: 21.03.2024).

44. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70152982/?ysclid=m4ust5qz8e258717589 (Дата обращения: 21.11.2024).

45. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования

средств автоматизации» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/193875/?ysclid=m4ut276hwm794897042 (Дата обращения: 24.11.2024).

46. Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70380924/ (Дата обращения: 21.03.2024).

47. Приказ от 27 октября 2022 г. № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона "о персональных данных» [Электронный ресурс]. – Режим доступа : https://www.garant.ru/products/ipo/prime/doc/405721227/ (Дата обращения: 18.12.2024).

48. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70451476/?ysclid=m4utxbdd3e917061970 (Дата обращения: 29.11.2024).

49. Приказ Рособрнадзора от 04.08.2023 № 1493 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации» [Электронный ресурс]. – Режим доступа : https://www.garant.ru/products/ipo/prime/doc/407991235 / (Дата обращения: 21.11.2024).

50. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для

выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70727118/?ysclid=m4utnl2vqn789126061 (Дата обращения: 29.11.2024).

51. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений» [Электронный ресурс]. – Режим доступа : https://www.garant.ru/products/ipo/prime/doc/70059046/?ysclid=m4utyra5ib162832007 (Дата обращения: 29.11.2024).

52. Приказ ФСТЭК России от 20 марта 2012 г. № 240/24/3095 «Об утверждении требований к средствам антивирусной защиты» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70211578/?ysclid=m4uu0fvsrx793720567 (Дата обращения: 29.11.2024).

53. Пять базовых принципов закона о персональных данных // СКБ Контур: [Электронный ресурс]. – Режим доступа : https://kontur.ru/articles/1293 (Дата обращения: 12.12.2022).

54. Раскатова, М. И. Теоретические основы управления рисками: учебное пособие [Текст] / М. И. Раскатова. – Челябинск : Издательский центр ЮУрГУ, 2019. – 46 с. – С. 8-13.

55. Рассолов, И. М. Информационное право : учебник и практикум для вузов [Текст] / И. М. Рассолов. - 7-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2024. - 427 с.

56. Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [Электронный ресурс] – Режим доступа : https://67.rkn.gov.ru/directions/p7072/p22322/ (Дата обращения: 19.12.2024).

57. Угрозы безопасности персональных данных : центр безопасности данных [Электронный ресурс] – Режим доступа : https://data-sec.ru/personal-data/threats/ (Дата обращения: 10.12.2022).

58. Управление рисками [Электронный ресурс]. – Режим доступа : https://service.securitm.ru/help/risks#assesment/ (Дата обращения: 21.11.2024).

59. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/12148567/ (Дата обращения: 21.03.2024).

60. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/12148555/?ysclid=m4usw5ocik706465296 (Дата обращения: 24.11.2024).

61. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» [Электронный ресурс]. – Режим доступа : https://base.garant.ru/12143756/?ysclid=m4usoq01ne162025573 (Дата обращения: 21.11.2024).

62. Шиляев, С. Методика оценки рисков информационной безопасности / С. Шиляев [Электронный ресурс]. – Режим доступа : https://kontur.ru/articles/1691 (Дата обращения: 01.12.2024).

63. Шинаков, К. Е. Минимизация рисков нарушения безопасности при построении системы защиты персональных данных: автореферат диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность [Текст] / К. Е. Шинаков. – Брянск, 2017. – 21с.

Приложение 1

ПОЛИТИКА
обработки и защиты персональных данных в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего»

1. Общие положения

1.1. Настоящий документ определяет политику Государственного бюджетного профессионального образовательного учреждения «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» (далее - Колледж) в отношении порядка работы с персональными данными. Политика обработки и защиты персональных данных (далее - Политика) должна быть размещена в общедоступном месте для ознакомления субъектов с процессами обработки персональных данных в Колледже.

1.2. Все мероприятия по обработке и защите персональных данных проводятся в соответствии с Федеральным Законом РФ «О персональных данных» от 27.07.2006 № 152-ФЗ и другими нормативно-правовыми актами, действующими на территории РФ.

2. Термины и определения

2.1. Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (**субъекту персональных данных**).

2.2. Оператор - Государственное бюджетное профессиональное образовательное учреждение «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

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

2.4. Распространение персональных данных - действие (операция) или совокупность действий (операций), совершаемых с персональными данными, включая передачу (предоставление, доступ) персональных данных неограниченному кругу лиц, размещенных на сайтах и в других открытых источниках.

2.5. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Информация об операторе

3.1. Полное наименование: Государственное бюджетное профессиональное образовательное учреждение «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

3.2. Сокращенное наименование: ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего»

3.3. Директор: Худолей Елена Сергеевна

3.4. Адрес местонахождения: г. Челябинск ул. Масленникова 21; Машиностроителей, 6;
1-ая Трубосварочная, 4; Энергетиков,2

3.5. Почтовый адрес: 454129, г. Челябинск, ул. Масленникова, 21
3.6. Телефон: 8(351) 253-04-52
3.7. Факс: 8(351)253-04-52
3.8. E-mail: pl10@mail.ru
3.9. Сайт: www.chtpgh.ru

4.Обработка персональных данных

4.1. При обработке персональных данных в Колледже соблюдаются конституционные права и свободы человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну.

4.2. Колледж не вправе обрабатывать персональные данные субъектов ПДн об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

4.3. Источники получения персональных данных:
- субъект ПДн;
- законный представитель субъекта;

4.4. При наличии законных оснований получателем персональных данных субъекта могут являться:
- налоговые органы;
- Пенсионный Фонд РФ;
- Фонд пенсионного и социального страхования Российской Федерации;
- Фонд обязательного медицинского страхования РФ;
- правоохранительные органы;
- банки и иные кредитные организации.

4.5. Персональные данные субъектов в Колледже обрабатываются как на бумажных носителях, так и в электронном виде – в компьютерных программах и электронных базах данных (в ИСПДн) с передачей по локальной компьютерной сети и по сети Интернет.

4.6. Обработка персональных данных по общему правилу происходит до утраты правовых оснований.

4.7. Срок хранения документов, содержащих персональные данные, определяется «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558 (ред. от 16.02.2016г.) и в иных случаях, предусмотренных законодательством РФ.

4.8. Трансграничная передача персональных данных не осуществляется.

4.9. Лицо, ответственное за организацию обработки ПДн в Колледже: техник Оглезнев Олег Леонидович.

4.10. Общие сведения об обрабатываемых в Колледже персональных данных сведены в таблицу 1.

Таблица 1 – Основные сведения об обрабатываемых данных.

Субъекты ПДн	Цели обработки	Категории ПДн	Правовые основания обработки
Сотрудники Колледжа	Реализация трудовых отношений, начисление заработной платы, передача информации в налоговые органы, Пенсионный Фонд	• фото; • фамилия, имя, отчество; • пол и возраст; • дата и место рождения; • гражданство; • паспортные данные; • адрес регистрации по местожительству и адрес фактического проживания; • номер телефона (домашний, мобильный); • почтовые и электронные адреса; • данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации; • семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым налоговым законодательством; • сведения о воинской обязанности; • сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы; • страховой номер индивидуального лицевого счета (СНИЛС); • идентификационный номер налогоплательщика (ИНН); • информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности; • сведения о банковских реквизитах (зарплатный лицевой счет); • доходы, для передачи в налоговую инспекцию по форме 2-НДФЛ и органы ПФР индивидуальных сведений о начисленных страховых взносах на обязательное медицинское страхование и данных о трудовом стаже; • сведения о судимости; • сведения о состоянии здоровья (медицинская книжка, справка о инвалидности (при наличии).	Гражданский кодекс РФ от 30.11.1994 № 51-ФЗ; Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Налоговый Кодекс РФ часть первая от 31 июля 1998 г. № 146-ФЗ и часть вторая от 5 августа 2000 г. № 117-ФЗ; Согласие на обработку персональных данных Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения
Кандидаты на вакантную должность	Принятие решения о трудоустройстве, формировани	• фамилия, имя, отчество; • дата; • контактная информация (телефон мобильный, e-mail); • сведения об образовании;	Согласие на обработку персональных данных

	е кадрового резерва	• опыт работы.	
Практиканты	Прохождение учебной, производственной практики	• фамилия, имя, отчество; • контактная информация (телефон мобильный); • сведения о месте учебы.	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ; Согласие на обработку персональных данных
Обучающиеся	Образовательная деятельность	фамилия, имя, отчество; дата и место рождения; фото; сведения об образовании (аттестат); сведения о родителях; сведения о месте регистрации, проживания; контактная информация (телефон домашний, телефон мобильный, e-mail); паспортные данные (или данные свидетельства о рождении); страховое свидетельство государственного пенсионного страхования; свидетельство о присвоении ИНН; справка с места жительства; копия страхового медицинского полиса; сведения о состоянии здоровья (справка 086у, прививочная карта ф.63, справка о инвалидности (при наличии); сведения о статусе (дети-сироты, дети, оставшиеся без попечения родителей (при наличии); характеристика; сведения о банковских реквизитах (лицевой счет для начисления стипендии).	«Основы законодательства Российской Федерации об охране здоровья граждан» № 5487-1 от 22.07.1993 г.; Федеральный закон РФ от 28.06.1991 «О медицинском страховании граждан в Российской Федерации» № 1499-1; Согласие на обработку персональных данных Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения
Законные представители обучающихся	Заключение договоров на оказание образовательных услуг	фамилия, имя, отчество; дата рождения; сведения о месте регистрации, проживания; паспортные данные; контактная информация (телефон домашний, телефон мобильный); уровень образования; сведения о статусе семьи (полная/неполная, количество детей); сведения о трудовой деятельности;	Согласие на обработку персональных данных

		сведения о прожиточном минимуме на одного члена семьи, для статистических отчетов и организации финансово-экономической деятельности «ЧКИТ «Профи» им. Я.П. Осадчего».	
Наниматель жилого помещения в общежитии	Заключение договоров найма жилого помещения в общежитии	• фамилия, имя, отчество; • дата рождения; • сведения о месте регистрации, проживания; • паспортные данные; • контактная информация (телефон домашний, телефон мобильный); • состав семьи.	Согласие на обработку персональных данных

5. Сведения об обеспечении безопасности персональных данных

5.1. Безопасность персональных данных достигается путем обеспечения их конфиденциальности, целостности и доступности.

5.2. В Колледже функционирует комплексная система защиты персональных данных, которая включает:

5.2.1. Организационные мероприятия

– действующие организационно-распорядительные документы по защите ПДн, регламентирующие порядок обработки ПДн и ответственность должностных лиц;

– осуществление внутреннего периодического контроля;

– учет машинных носителей персональных данных;

– физическая охрана зданий и помещений;

– обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

– обучение сотрудников вопросам защиты ПДн.

5.2.2. Технические меры защиты

– модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– техническое задание для ИСПДн, содержащее требования к системе защиты;

– подсистема резервного копирования информации;

– подсистема парольной защиты;

– подсистема антивирусной защиты;

– подсистема криптографической защиты;

– средства защиты информации от несанкционированного доступа;

– средства межсетевого экранирования;

– сейфы и запирающиеся шкафы для хранения носителей персональных данных;

– пожарная и охранная сигнализация.

5.3. Допуск к персональным данным субъекта имеют только те сотрудники Колледжа которым персональные данные необходимы в связи с исполнением ими своих служебных (трудовых) обязанностей.

5.4. Каждый сотрудник имеет доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

6. Права субъекта

6.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных по официальному запросу.

6.2. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных* или в судебном порядке.

6.3. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

*Примечание:

Наименование Уполномоченного органа по защите прав субъектов персональных данных: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
Наименование вышестоящего органа: Министерство связи и массовых коммуникаций Российской Федерации
Почтовый адрес для направления документов и обращений: 109992, г.Москва, Китайгородский пр., д.7, стр.2.
Телефоны:
Справочно-информационный центр: (495) 983-33-93 (тел), (495) 587-44-68 (факс)
пн-чт 8:30-17:30, пт 8.30-16:15.
Экспедиция Роскомнадзора работает: понедельник, вторник, среда, четверг - с 10.00 до 13.00 и с 14.00 до 17.00; пятница с 10.00 до 13.00 и с 14.00 до 16.00.
- в электронной форме через электронную почту (rsoc_in@rkn.gov.ru), официальный сайт (rkn.gov.ru), Портал государственных услуг (gosuslugi.ru);
- в письменной форме посредством почтовой связи.
Общий электронный адрес Роскомнадзора - rsoc_in@rkn.gov.ru

Уполномоченный орган по защите прав субъектов персональных данных - ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)
Управление Роскомнадзора по Челябинской области
Адрес: 454000, г. Челябинск, ул. Цвиллинга, 22
Телефон (351) 214-02-22
Факс (351) 214-02-23
E-mail rsockanc74@rkn.gov.ru
Руководитель Управления Оленина Марина Ивановна
Сайт 74.rkn.gov.ru

Приложение 2

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в
ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего»

1. Общие положения

1.1 Настоящее Положение об обработке и защите персональных данных (далее - Положение) государственного бюджетного профессионального образовательного учреждения «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» разработано в соответствии с Конституцией Российской Федерации от 25.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020г.), Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 №51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2 Цели разработки Положения:

1.2.1 определение порядка обработки персональных данных работников и обучающихся ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего»;

1.2.2 обеспечение защиты прав и свобод человека и гражданина, в т.ч. работников и обучающихся ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3 установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3 К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1 обезличенных персональных данных;

1.3.2 общедоступных персональных данных.

1.4 Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», если иное не определено законом Российской Федерации.

2. Термины и определения

2.1 Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.2 Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку

информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.3 Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4 Информация – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. №687
-ФЗ «Об информации, информационных технологиях и защите информации»).

2.5 Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.6 Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.7 Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 №687).

2.8 Оператор – ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

2.9 Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.10 Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3, 10.1 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

2.11 Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»).

3. Порядок получения персональных данных

3.1 Персональные данные следует получать непосредственно у субъекта либо у законного представителя.

3.2 Документы со сведениями, содержащими персональные данные, обрабатываются во всех структурных подразделениях ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

3.3 Перед началом обработки персональных данных необходимо получить у субъекта два согласия в письменной виде в соответствии с утвержденной в ГБПОУ

«Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» формой такого Согласия: Согласие на обработку персональных данных и Согласие на обработку персональных данных,
разрешенных субъектом персональных данных для распространения (ст.10.1 Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных»).

3.4 Согласия субъекта персональных данных не требуется в случаях, определенных Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11, в том числе:

3.4.1 обработка персональных данных осуществляется на основании федерального закона, устанавливающего цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего»;

3.4.2 обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

3.4.3 осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы.

3.5 Комплект документов, сопровождающий процесс оформления трудовых отношений работника ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» при его приёме, переводе и увольнении:

3.5.1 Согласие на обработку персональных данных (Приложение А) и согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приложение Б);

3.5.2 Информация, представляемая работником при поступлении на работу в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии);
- личная медицинская книжка;
- справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования;
- сведения о банковских реквизитах (зарплатный лицевой счет);
- доходы, для передачи в налоговую инспекцию по форме 2-НДФЛ и органы ПФР индивидуальных сведений о начисленных страховых взносах на обязательное медицинское страхование и данных о трудовом стаже;

- номер телефона (домашний, мобильный);
- почтовые и электронные адреса.

3.5.3 При оформлении работника в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- фото;
- общие сведения (Ф.И.О. дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;
- сведения о месте жительства и контактных телефонах.

3.5.4 В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- изменения общих сведений.

3.5.5 Необходимая информация копируется в ИСПДн: Контур Экстерн; ЕИС «Закупки»; 1С:Бухгалтерия государственного учреждения 8, ред. 2.0; 1С:Предприятие 8.3 (8.3.16.1814) Бухгалтерия государственного учреждения, редакция 1.0 (1.0.68.15); 1С:Предприятие 8.3 (8.3.18.1289) Зарплата и кадры государственного учреждения, редакция 3.1 (3.1.20.97); АСУ Procollege; ИС «Аттестация педагогических кадров», официальный сайт ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» http://chtpgh.ru/ .

3.5.6 В отделе кадров ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

- документы, содержащие персональные данные работников (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, вышестоящие органы управления и другие учреждения);
- документация по ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» о работе отделов (положения, должностные инструкции работников, приказы);
- документы по планированию, учету, анализу и отчетности в части работы с персоналом ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».
- документы, содержащие персональные данные работников, необходимые для работы: налоговые органы; Фонд пенсионного и социального страхования РФ;

Федеральная служба государственной статистики РФ; Фонд обязательного медицинского страхования РФ; правоохранительные органы; банки и иные кредитные организации (в соответствии с заключенным договором по предоставлению услуг по переводу / зачислению денежных средств на счета физических лиц).

3.6 Комплект документов, сопровождающий процесс работы с обучающимися.

3.6.1 Согласие на обработку персональных данных обучающегося (Приложение А) и согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приложение Б);

3.6.2 Информация, представляемая обучающимися, либо их представителями в структурные подразделения ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», должна иметь документальную форму. Обучающиеся, либо их представители предъявляют следующие документы:

- фамилия, имя, отчество;
- дата и место рождения;
- фото;
- сведения об образовании (аттестат);
- сведения о родителях;
- сведения о месте регистрации, проживания;
- контактная информация (телефон домашний, телефон мобильный, e-mail);
- паспортные данные (или данные свидетельства о рождении);
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- справка с места жительства;
- копия страхового медицинского полиса;
- сведения о состоянии здоровья (справка 086у, прививочная карта ф.63, справка о инвалидности (при наличии);
- сведения о статусе (дети-сироты, дети, оставшиеся без попечения родителей (при наличии);
- характеристика;

сведения о банковских реквизитах (лицевой счет для начисления стипендии).

3.6.3 Данные из документов вносятся в электронном виде в ИСПДн АСУ Procollege, ФИС ФРДО, ФИС ГИА и Приема, ГИС Образование, Сетевой город. Образование, ГИС Образование. Е-услуги, АИС «Навигатор дополнительного образования детей Челябинской области», ФИС ОКО (ВПР), ЕГИССО. В бумажном виде впоследствии создаются, хранятся и передаются следующие группы документов, содержащие персональные данные обучающихся ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» в единичном или сводном виде:

- копию документов, удостоверяющих его личность, гражданство;
- оригинал документа об образовании и его копия;
- заявление о поступлении;
- согласие на обработку персональных данных обучающегося, законного представителя (Приложение А) и согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приложение Б);
- копии документов на полное государственное обеспечение (при необходимости);
- портфолио (общие сведения, сведения о движении, результаты аттестации, квалификационные экзамены, государственная итоговая аттестация, практика, курсовые проекты, число пропущенных занятий, взыскания и поощрения);
- студенческий билет;
- зачетная книжка;

- журнал учебных занятий на группу;
- приказы о зачислении, об отчислении, о переводе, об академическом отпуске, о начислении стипендии, о организации образовательного процесса в колледже и вне его.

4. Порядок хранения персональных данных

4.1 Хранение бумажных документов, электронных носителей (дисков, флэш-накопителей и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

4.2 Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие
устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

4.3 Обработка персональных данных в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» осуществляется до утраты правовых оснований обработки персональных данных.

4.4 Срок хранения документов, содержащих персональные данные, определяется «Перечнем хранения типовых документов, управленческих содержащих архивных персональные документов, данные, образующихся определяется в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558.

4.5 По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

4.6 Обезличивания персональных данных в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» не предполагается.

5. Порядок использования персональных данных

5.1 Обработка персональных данных может осуществляться исключительно в целях предоставления среднего профессионального образования, профессионального обучения, дополнительного профессионального образования, дополнительных общеобразовательных общеразвивающих программ, услуг по содержанию и воспитанию, организации и проведению мероприятий в сфере образования, принятия решения о трудоустройстве, кадрового планирования, осуществления трудовых отношений, и в случаях, установленных законодательством Российской Федерации.

5.2 При определении объема и содержания, обрабатываемых персональных данных ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» должен руководствоваться Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

6. Порядок передачи персональных данных

6.1 Передавать персональные данные субъектов допускается только тем работникам,
которые имеют допуск к обработке персональных данных.

6.2 Предоставление персональных данных допускается в случаях передачи налоговой бухгалтерской и иной отчетности, передачи сведений о заработной плате в банковские и иные кредитные организации при официальном запросе, раскрытии данных правоохранительным органам при наличии законных оснований, а также в иных случаях, установленным законодательством РФ.

6.3 Не допускается распространение персональных данных субъекта без его согласия в письменном виде.

7. Организация защиты персональных данных

7.1 Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» за счет своих средств.

7.2 В ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

7.2.1 зафиксированные в бумажных документах;

7.2.2 зафиксированные в электронных документах на технических средствах, включая внешние носители;

7.2.3 речевая (акустическая) информация, содержащая персональные данные;

7.2.4 текстовая и графическая видовая информация, содержащая персональные данные.

7.3 Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

7.3.1 Проведение организационных мероприятий:

- разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;
- ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;
- проведение обучения работников вопросам защиты персональных данных.

7.3.2 Программно-аппаратная защита:

- внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;
- организация учёта носителей персональных данных.

7.3.3 Инженерно-техническая защита:

- установка сейфов или запирающихся шкафов для хранения носителей персональных данных;
- установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

7.4 Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-

правовыми актами ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

7.5 Организацию и контроль защиты персональных данных в структурных подразделениях ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» осуществляют их непосредственные руководители.

8. Порядок предоставления доступа к персональным данным

8.1 Допуск к персональным данным субъекта могут иметь только работники ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», которым персональные данные необходимы в связи с исполнением ими своих должностных обязанностей.

8.2 Процедура оформления допуска к персональным данным представляет собой следующую последовательность действий:

8.2.1 ознакомление работника под подпись с настоящим Положением ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», касающимися обработки персональных данных;

8.2.2 заполнение работником «Обязательства о неразглашении конфиденциальной информации» (Приложение В);

8.3 Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения должностных обязанностей.

8.4 Работникам, не имеющим допуска, доступ к персональным данным субъектов запрещается.

9. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

9.1 Персональные данные субъектов хранятся в типовых формах ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», предполагающих включение в них персональных данных.

9.2 Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» или лица, осуществляющие такую обработку по договору с ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего»), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

9.3 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

9.4 Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

9.5 При хранении материальных носителей должны соблюдаться условия,

обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом директора ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

10. Особенности обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных

10.1 В состав информационных систем персональных данных ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» входит: Контур Экстерн; ЕИС «Закупки»; 1С:Бухгалтерия государственного учреждения 8, ред. 2.0; 1С:Предприятие 8.3 (8.3.16.1814) Бухгалтерия государственного учреждения, редакция 1.0 (1.0.68.15); 1С:Предприятие 8.3 (8.3.18.1289) Зарплата и кадры государственного учреждения, редакция 3.1 (3.1.20.97); АСУ Procollege; ИС «Аттестация педагогических кадров», официальный сайт ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» http://chtpgh.ru/ , ФИС ФРДО, ФИС ГИА и Приема, ГИС Образование, Сетевой город. Образование, ГИС Образование. Е-услуги, АИС «Навигатор дополнительного образования детей Челябинской области», ФИС ОКО (ВПР), ЕГИССО.

10.2 Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплекты и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

10.3 Безопасность персональных данных достигается путем исключения 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.

10.4 Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

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

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

10.7 Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки информационных систем персональных данных.

10.8 При обработке персональных данных в информационной системе должно быть обеспечено:

10.8.1 проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

10.8.2 своевременное обнаружение фактов несанкционированного доступа к

персональным данным;
10.8.3 недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
10.8.4 возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
10.8.5 постоянный контроль над обеспечением уровня защищенности персональных данных.
10.9 Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:
10.9.1 определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
10.9.2 проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
10.9.3 установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
10.9.4 обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
10.9.5 учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
10.9.6 учет лиц, допущенных к работе с персональными данными в информационной системе;
10.9.7 контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;
10.9.8 разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
10.9.9 описание системы защиты персональных данных.
10.10 Иные требования по обеспечению безопасности информации и средств защиты информации в ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1 Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн и ответственного за организацию обработки персональных данных ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего».

11.2 Работники ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных

носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

11.3 Работник ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

11.4 Директор ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

12 Заключительные положения

12.1 Настоящее Положение утверждается директором и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

12.2 Все работники ГБПОУ «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под подпись.

ПРИЛОЖЕНИЯ А

СОГЛАСИЕ
на обработку персональных данных работника ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего»

Я,_____,

паспорт серия _____ №_____, выдан_____

адрес по прописке _____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

- фото;
- фамилия, имя, отчество;
- пол и возраст;
- дата и место рождения;
- гражданство;
- паспортные данные;
- адрес регистрации по местожительству и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- почтовые и электронные адреса;
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым налоговым законодательством;
- сведения о воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности;
- сведения о банковских реквизитах (зарплатный лицевой счет);
- доходы, для передачи в налоговую инспекцию по форме 2-НДФЛ и органы ПФР индивидуальных сведений о начисленных страховых взносах на обязательное медицинское страхование и данных о трудовом стаже;
- сведения о судимости;
- сведения о состоянии здоровья (медицинская книжка, справка о инвалидности (при наличии).

Срок действия настоящего согласия на обработку персональных данных: с момента его подписания и до достижения целей обработки. В дальнейшем - в соответствии с законодательством об архивном деле в Российской Федерации.

Настоящее согласие может быть отозвано мной в письменной форме на основании заявления, поданного на имя директора «ЧКИТ «Профи» им. Я.П. Осадчего».

Подтверждаю, что я ознакомлен(а) с Положением об обработке и защите персональных данных, действующим в «ЧКИТ «Профи» им. Я.П. Осадчего», в том числе с моими правами и обязанностями в области защиты персональных данных.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

СОГЛАСИЕ
на обработку персональных данных несовершеннолетнего обучающегося в «ЧКИТ «Профи» им. Я.П. Осадчего»

Я,_____,

паспорт серия _____ №_____, выдан _____

адрес по прописке_____,

действующий(ая) с согласия (законного

представителя)_____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «ЧКИТ «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

- фамилия, имя, отчество;
- дата и место рождения;
- фото;
- сведения об образовании (аттестат);
- сведения о родителях;
- сведения о месте регистрации, проживания;
- контактная информация (телефон домашний, телефон мобильный, e-mail);
- паспортные данные (или данные свидетельства о рождении);
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- справка с места жительства;
- копия страхового медицинского полиса;
- сведения о состоянии здоровья (справка 086у, прививочная карта ф.63, справка о инвалидности (при наличии);
- сведения о статусе (дети-сироты, дети, оставшиеся без попечения родителей (при наличии);
- характеристика;
- сведения о банковских реквизитах (лицевой счет для начисления стипендии).

Срок действия настоящего согласия на обработку персональных данных: с момента его подписания и до достижения целей обработки. В дальнейшем – в соответствии с законодательством об архивном деле в Российской Федерации. Настоящее согласие может быть отозвано мной в письменной форме на основании заявления, поданного на имя директора ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего». Подтверждаю, что я ознакомлен(а) с Положением об обработке и защите персональных данных, действующим в ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего», в том числе с моими правами и обязанностями в области защиты персональных данных.

«__» ___ 20_ _г. _____ _____
дата подпись законного представителя подпись

_____ _____
Ф.И.О. полностью законного представителя Ф.И.О. полностью

СОГЛАСИЕ
на обработку персональных данных совершеннолетнего обучающегося в «ЧКИТ «Профи» им. Я.П. Осадчего»

Я,_____,

паспорт серия _____ №_____, выдан _____

адрес по прописке_____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «ЧКИТ «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

- фамилия, имя, отчество;
- дата и место рождения;
- фото;
- сведения об образовании (аттестат);
- сведения о родителях;
- сведения о месте регистрации, проживания;
- контактная информация (телефон домашний, телефон мобильный, e-mail);
- паспортные данные (или данные свидетельства о рождении);
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- справка с места жительства;
- копия страхового медицинского полиса;
- сведения о состоянии здоровья (справка 086у, прививочная карта ф.63, справка о инвалидности (при наличии);
- сведения о статусе (дети-сироты, дети, оставшиеся без попечения родителей (при наличии);
- характеристика;
- сведения о банковских реквизитах (лицевой счет для начисления стипендии).

Срок действия настоящего согласия на обработку персональных данных: с момента его подписания и до достижения целей обработки. В дальнейшем – в соответствии с законодательством об архивном деле в Российской Федерации. Настоящее согласие может быть отозвано мной в письменной форме на основании заявления, поданного на имя директора ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего». Подтверждаю, что я ознакомлен(а) с Положением об обработке и защите персональных данных, действующим в ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего», в том числе с моими правами и обязанностями в области защиты персональных данных.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

СОГЛАСИЕ
на обработку персональных данных законных представителей обучающихся
в «ЧКИТ «Профи» им. Я.П. Осадчего».

Я,_____

дата рождения, № СНИЛС _____

паспорт серия _____ №_____, выдан _____

_____

адрес по прописке_____

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «ЧКИТ «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на обработку без использования средств автоматизации моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

- фамилия, имя, отчество;
- дата рождения;
- сведения о месте регистрации, проживания;
- паспортные данные;
- контактная информация (телефон домашний, телефон мобильный);
- уровень образования;
- сведения о статусе семьи (полная/неполная, количество детей);
- сведения о трудовой деятельности;
- сведения о прожиточном минимуме на одного члена семьи, для статистических отчетов и организации финансово-экономической деятельности «ЧКИТ «Профи» им. Я.П. Осадчего».

Срок действия настоящего согласия на обработку персональных данных: с момента его подписания и до достижения целей обработки. В дальнейшем – в соответствии с законодательством об архивном деле в Российской Федерации. Настоящее согласие может быть отозвано мной в письменной форме на основании заявления, поданного на имя директора ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего». Подтверждаю, что я ознакомлен(а) с Положением об обработке и защите персональных данных, действующим в ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего», в том числе с моими правами и обязанностями в области защиты персональных данных.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

ПРИЛОЖЕНИЕ Б

СОГЛАСИЕ
на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Я,_____,

паспорт серия _____ №_____, выдан_____

адрес по прописке _____

в соответствии со статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Персональные данные	Фамилия, Имя, Отчество	да	да		
	Дата, месяц, год рождения	да	да		
	Контактная информация (телефон, e-mail)	да	да		
	Адрес рабочий	да	да		
	Образование, специальность	да	да		
	Уровень квалификации	да	да		
	Стаж работы	да	да		
	Доходы	—	—		
	Сведения о достижениях / наградах / званиях	да	да		
Специальные категории персональных данных	Состояние здоровья	нет	нет		
	Сведения о судимости	нет	нет		
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица	да	да		

Сведения об информационных ресурсах работодателя – ГБПОУ «ЧКИТ «Профи» им.Я.П. Осадчего»,

посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
Официальный сайт колледжа http://chtpgh.ru/	- Размещение персональных данных субъекта персональных данных для поддержания функционирования информационных систем, научной, образовательной, организационной и финансово-экономической деятельности «ЧКИТ «Профи» им. Я.П. Осадчего» и в случаях, установленных нормативными документами вышестоящих органов и законодательством. - Размещение персональных данных субъекта персональных данных в новостной ленте фото, видео с указанием Ф.И.О., должности (профессии / специальности), достижений / наград / званий сотрудника
Официальные группы в социальных сетях: https://vk.com/ctpgh , https://rutube.ru/channel/25327050/ , https://t.me/chtpigh	

Настоящее согласие дано мной добровольно и действует со дня его подписания «___» _____ 20__г.
Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования работодатель обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

СОГЛАСИЕ
на обработку персональных данных, разрешенных субъектом персональных данных для распространения – несовершеннолетним обучающимся

Я,_____,

паспорт серия _____ №_____, выдан _____

адрес по прописке_____,

действующий(ая) с согласия (законного представителя)_____

_____

в соответствии со статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Персональные данные	Фамилия, Имя, Отчество	да	да		
	Дата, месяц, год рождения	да	да		
	Осваиваемая профессия / специальность	да	да		
	Номер группы	да	да		
	Сведения о достижениях / наградах	да	да		
Специальные категории персональных данных	Состояние здоровья	нет	нет		
	Сведения о судимости	нет	нет		
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица	да	да		

Сведения об информационных ресурсах работодателя – ГБПОУ «ЧКИТ «Профи» им.Я.П. Осадчего», посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
Официальный сайт колледжа http://chtpgh.ru/	- Размещение персональных данных субъекта персональных данных для поддержания функционирования информационных систем, научной, образовательной, организационной и финансово-экономической деятельности «ЧКИТ «Профи» им. Я.П. Осадчего» и в случаях, установленных нормативными документами вышестоящих органов и законодательством. - Размещение персональных данных субъекта персональных данных в новостной ленте фото, видео с указанием Ф.И.О., осваиваемой профессии / специальности, номера группы, достижений / наград
Официальные группы в социальных сетях: https://vk.com/ctpgh , https://rutube.ru/channel/25327050/ , https://t.me/chtpigh	

Настоящее согласие дано мной добровольно и действует со дня его подписания «___» _____ 20__г.
Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования работодатель обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«__» ___ 20__г. _____ _____
дата подпись законного представителя подпись

_____ _____
Ф.И.О. полностью законного представителя Ф.И.О. полностью

СОГЛАСИЕ
на обработку персональных данных, разрешенных субъектом персональных данных для распространения – совершеннолетним обучающимся

Я,_____,

паспорт серия _____ №_____, выдан_____

адрес по прописке _____

в соответствии со статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" даю свое согласие государственному бюджетному профессиональному образовательному учреждению «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего», расположенному по адресу: 454129, Челябинская область, г. Челябинск, ул. Масленникова, д.21, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных статьей 10.1 Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных": сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокировку и уничтожение сведений о фактах, событиях и обстоятельствах моей жизни, в том числе:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Персональные данные	Фамилия, Имя, Отчество	да	да		
	Дата, месяц, год рождения	да	да		
	Осваиваемая профессия / специальность	да	да		
	Номер группы	да	да		
	Сведения о достижениях / наградах	да	да		
Специальные категории персональных данных	Состояние здоровья	нет	нет		
	Сведения о судимости	нет	нет		
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица	да	да		

Сведения об информационных ресурсах работодателя – ГБПОУ «ЧКИТ «Профи» им.Я.П. Осадчего», посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
Официальный сайт колледжа http://chtpgh.ru/	- Размещение персональных данных субъекта персональных данных для поддержания функционирования информационных систем, научной, образовательной, организационной и финансово-экономической деятельности «ЧКИТ «Профи» им. Я.П. Осадчего» и в случаях, установленных нормативными документами вышестоящих органов и законодательством. - Размещение персональных данных субъекта персональных данных в новостной ленте фото, видео с указанием Ф.И.О.,
Официальные группы в социальных сетях: https://vk.com/ctpgh , https://rutube.ru/channel/25327050/ , https://t.me/chtpigh	

	осваиваемой профессии / специальности, номера группы, достижений / наград

Настоящее согласие дано мной добровольно и действует со дня его подписания «___» _____ 20__г.
Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования работодатель обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

ПРИЛОЖЕНИЕ В

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я, _____,
исполняющий(ая) должностные обязанности _____
_____
в качестве работника государственного бюджетного профессионального образовательного учреждения «Челябинский колледж индустриальных технологий «Профи» им. Я.П. Осадчего» в период трудовых отношений и в течение трех лет после их окончания обязуюсь:

- не сообщать персональные данные работников и (или) обучающихся третьей стороне без письменного согласия работника и (или) обучающегося, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровья работника и (или) обучающегося, а также в случаях, установленных федеральным законом;
- об утрате или недостаче носителей персональных данных работников и (или) обучающихся, удостоверений, пропусков, ключей от хранилищ, сейфов, металлических шкафов, паролей доступа к информационным системам и о других фактах, которые могут привести к разглашению персональных данных работников и (или) обучающихся, а также о причинах и условиях возможной утечки сведений немедленно сообщать руководителю.

До моего сведения доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных работников и (или) обучающихся. Мне известно, что нарушение этих положений может повлечь дисциплинарную, административную, гражданско-правовую, уголовную или иную ответственность в соответствии с законодательством Российской Федерации.

«___» _____ 20__г. _____ _____
дата подпись Ф.И.О. полностью

Приложение 3

Результаты оценки рисков нарушения безопасности в системе защиты ПДн

ГБПОУ «ЧКИТ «Профи» им. Я.П. Осадчего»

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/), как наиболее полный и разработанный федеральным органом исполнительной власти Российской Федерации.

В силу того, что в качестве информационного актива будут выступать во всех случаях ПДн, в данной матрице этот показатель как постоянный не отражен. Наименование угрозы и объекты воздействия выбраны методом экспертной оценки, ущерб и вероятность реализации угрозы оценены качественным методом по трехбалльной шкале.

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза внедрения кода или данных	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза воздействия на программы с высокими привилегиями	Информационная система, сетевое программное обеспечение, сетевой трафик	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	2	10
Угроза восстановления и/или повторного использования аутентификационной информации	Системное программное обеспечение, учетные данные пользователя	НП.2, НП.6, НП.7, НП.11	12	3	15
Угроза длительного удержания вычислительных ресурсов пользователями	Информационная система, сетевой узел, машинный носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	18	3	21
Угроза доступа к защищаемым файлам с использованием обходного пути	Объекты файловой системы	НП.2, НП.7, НП.11	5	2	7
Угроза доступа к локальным файлам сервера при помощи URL	Сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	7	3	10

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза доступа/перехвата/изменения HTTP cookies	Прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	6	2	8
Угроза заражения DNS-кеша	Сетевой узел, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	2	10
Угроза избыточного выделения оперативной памяти	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	8	2	10
Угроза использования альтернативных путей доступа к ресурсам	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	НП.2, НП.7, НП.10, НП.11	12	3	15
Угроза использования информации идентификации / аутентификации, заданной по умолчанию	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	14	2	16
Угроза использования поддельных цифровых подписей BIOS	Микропрограммное и аппаратное обеспечение BIOS/UEFI	НП.6, НП.7	4	1	5
Угроза использования слабостей кодирования входных данных	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	2	10
Угроза использования слабостей протоколов сетевого / локального обмена данными	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	8	2	10
Угроза исследования приложения через отчёты об ошибках	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Микропрограммное и аппаратное обеспечение BIOS/UEFI	НП.2, НП.3, НП.6, НП.7, НП.11	5	1	6
Угроза межсайтового скриптинга	Сетевой узел, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.11	5	2	6

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза межсайтовой подделки запроса	Сетевой узел, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.11	6	2	8
Угроза нарушения целостности данных кеша	Сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза некорректного использования функционала программного и аппаратного обеспечения	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	14	2	16
Угроза неправомерного / некорректного использования интерфейса взаимодействия с приложением	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза неправомерных действий в каналах связи	Сетевой трафик	НП.1, НП.2, НП.11	5	2	7
Угроза несанкционированного восстановления удаленной защищаемой информации	Машинный носитель информации	НП.2, НП.6, НП.7, НП.11	12	2	14
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза несанкционированного доступа к аутентификационной информации	Системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр, машинные носители информации	НП.2, НП.6, НП.7, НП.11	12	3	15

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Машинный носитель информации, объекты файловой системы	НП.4, НП.5, НП.11	9	3	12
Угроза несанкционированного изменения аутентификационной информации	Системное программное обеспечение, объекты файловой системы, учетные данные пользователя, реестр	НП.2, НП.6, НП.7, НП.11	12	3	15
Угроза несанкционированного копирования защищаемой информации	Объекты файловой системы, машинный носитель информации	НП.1, НП.2, НП.4, НП.5, НП.6, НП.7, НП.9, НП.11	16	2	18
Угроза несанкционированного редактирования реестра	Системное программное обеспечение, использующее реестр, реестр	НП.6, НП.7	6	3	9
Угроза несанкционированного создания учетной записи пользователя	Системное программное обеспечение	НП.2, НП.6, НП.7, НП.11	12	3	15
Угроза несанкционированного удаления защищаемой информации	Метаданные, объекты файловой системы, реестр	НП.1, НП.2, НП.4, НП.5, НП.6, НП.7, НП.9, НП.11	15	3	18
Угроза несанкционированного управления буфером	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза несанкционированного управления указателями	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Сетевой узел, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза обнаружения хостов	Сетевой узел, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза опосредованного управления группой программ через совместно используемые данные	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза определения топологии вычислительной сети	Сетевой узел, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза перебора всех настроек и параметров приложения	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза передачи данных по скрытым каналам	Сетевой узел, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.6, НП.7, НП.11	6	2	9
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Системное программное обеспечение, аппаратное обеспечение	НП.2, НП.6, НП.7, НП.11	11	3	14
Угроза переполнения целочисленных переменных	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза перехвата данных, передаваемых по вычислительной сети	Сетевой узел, сетевой трафик	НП.1, НП.2, НП.11	4	2	6
Угроза перехвата привилегированного потока	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза перехвата привилегированного процесса	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза повреждения системного реестра	Объекты файловой системы, реестр	НП.2, НП.7, НП.11	9	3	12
Угроза повышения привилегий	Системное программное обеспечение, сетевое программное обеспечение, информационная система	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза подделки записей журнала регистрации событий	Системное программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза подмены действия пользователя путем обмана	Прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	7	2	9
Угроза подмены доверенного пользователя	Сетевой узел, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	19	2	21
Угроза подмены содержимого сетевых ресурсов	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	20	2	22
Угроза подмены субъекта сетевого доступа	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза получения предварительной информации об объекте защиты	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза преодоления физической защиты	Информационная система, машинный носитель информации, аппаратное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.11	14	2	16
Угроза приведения системы в состояние «отказ в обслуживании»	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, телекоммуникационное устройство	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Машинный носитель информации, микропрограммное обеспечение, аппаратное обеспечение, телекоммуникационное устройство	НП.2, НП.6, НП.7, НП.11	11	3	14
Угроза пропуска проверки целостности программного обеспечения	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза сбоя обработки специальным образом измененных файлов	Метаданные, объекты файловой системы, системное программное обеспечение	НП.2, НП.6, НП.7, НП.11	6	2	8
Угроза удаления аутентификационной информации	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	НП.2, НП.6, НП.7, НП.11	11	2	13
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.11	8	1	9
Угроза установки уязвимых версий обновления програм-много обеспечения BIOS	Микропрограммное и аппаратное обеспечение BIOS/UEFI	НП.6, НП.7	4	2	6
Угроза утраты вычислительных ресурсов	Информационная система, сетевой узел, машинный носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Аппаратное обеспечение, машинный носитель информации	НП.2, НП.6, НП.7, НП.11	7	2	9
Угроза форматирования носителей информации	Машинный носитель информации	НП.2, НП.6, НП.7, НП.11	9	3	12
Угроза «форсированного веб-браузинга»	Сетевой узел, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Аппаратное обеспечение, машинный носитель информации	НП.2, НП.6, НП.7, НП.11	6	1	7
Угроза эксплуатации цифровой подписи программного кода	Системное программное обеспечение, прикладное программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза «кражи» учетной записи доступа к сетевым сервисам	Сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза неправомерного шифрования информации	Объект файловой системы	НП.2, НП.7, НП.11	6	1	7
Угроза скрытного включения вычислительного устройства в состав бот-сети	Сетевой узел, сетевое программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.11	7	2	9
Угроза «фарминга»	Информационная система (ПЭВМ), сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза «фишинга»	Информационная система (ПЭВМ), сетевое программное обеспечение, сетевой трафик	НП.1, НП.2, НП.3, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза нарушения технологического / производственного процесса из-за временны́х задержек, вносимых средством защиты	Средство защиты информации	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза несанкционированного использования системных и сетевых утилит	Системное программное обеспечение	НП.2, НП.6, НП.7, НП.11	5	2	7
Угроза несанкционированного изменения параметров настройки средств защиты информации	Средство защиты информации	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза несанкционированного воздействия на средство защиты информации	Средство защиты информации	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза маскирования действий вредоносного кода	Системное программное обеспечение, сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Сетевое программное обеспечение	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	12	3	15
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза использования уязвимых версий программного обеспечения	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	12	3	15
Угроза скрытной регистрации вредоносной программой учет-ных записей администраторов	Средство защиты информации	НП.2, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9
Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Учетные данные пользователя	НП.2, НП.3, НП.6, НП.11	12	3	15
Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Аппаратное обеспечение, программное обеспечение	НП.2, НП.6, НП.7, НП.11	11	2	13
Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Информационная система (ПЭВМ)	НП.2, НП.6, НП.7, НП.11	7	1	8
Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Аппаратное обеспечение	НП.2, НП.6, НП.7, НП.11	6	1	7
Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	НП.3, НП.4, НП.6, НП.7	6	1	7

Наименование угрозы	Объект воздействия	Негативные последствия (далее – НП)	Оценка ущерба (сумма по всем НП)	Вероятность реализации угрозы - оценка	Степень риска
Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Информационная система, объекты файловой системы	НП.2, НП.3, НП.6, НП.7, НП.8, НП.10, НП.11	8	1	9