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 образовательной организации

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

Проверка на объем заимствований:
87,07 % авторского текста

Работа рекомендована к защите
«26» 12 2025 г.
Зав. кафедрой АТ, ИТ и МОТД
_____ Руднев В.В.

Выполнил:
студент группы ЗФ-309-210-2-1
Завоеванов Александр Сергеевич

Научный руководитель:
д.т.н., профессор кафедры АТ, ИТ и МОТД
Дмитриев Михаил Сергеевич

Челябинск
2026

Содержание

ВВЕДЕНИЕ

Актуальность темы исследования. На современном этапе развития, как в мире в целом, так и в России назрела необходимость изменений в сфере информации, которая не ограничивается понятиями инфраструктуры, объекта, устанавливающего режимы сбора, формирования, распространения и использования информации, но и самой системой регулирования информации. Существующие реалии с применением ставших обыденными средств вычислительной техники, с выявленными для них угрозами и уязвимостями, выявили новые формы преступлений. Это было обусловлено с одной стороны, увеличением информационного потока, что повлекло появление систем электронного документооборота, а с другой стороны, пропорционально увеличилось число преступлений, связанных с небезуспешными попытками использования персональных данных. Наиболее интересными информационными ресурсами персональных данных для завладения остаются базы данных систем кадрового и бухгалтерского учета сотрудников и учащихся; базы данных контрактов с подрядчиками; контактные данные почтовой системы и почтовых клиентов сотрудников. Преступления в сфере компьютерной обработки информации и персональных данных характеризуются скрытностью, трудностью сбора улик, сложностью доказывания.

Мониторинг данных МВД России о преступлениях, совершённых с использованием информационно–телекоммуникационных технологий, показал стабильный рост указанных правонарушений за период 2021-2024 годы. Особенно можно выделить период локдаунов 2020-2022 г.г., когда ограничения распространялись практически на все сферы жизни: были объявлены нерабочие дни для всех структур и сфер, за исключением продуктовых магазинов и аптек, закрыты рестораны и ночные клубы, для всех граждан объявлена принудительная самоизоляция. Период распространения новой коронавирусной инфекции позволил преступникам получать реквизиты банковских карт, данные электронной почты, доступ к персональным данным

в социальных сетях (Instagram, ВКонтакте и др.). Кроме того, снизился уровень раскрываемости преступлений, совершённых с использованием информационно-телекоммуникационных технологий, в среднем на 5%. [31]

Интерес к вопросам сохранности персональных данных, защиты их от случайного и преднамеренного уничтожения, повреждения и несанкционированного получения связан с введением и апробированием перевода сотрудников и учащихся образовательных учреждений на удаленный режим, что не исключает работу с персональными данными (ПДн). Общая неподготовленность оборудования и программного обеспечения информационных систем персональных данных, высокая лабильность программного обеспечения и ряд других признаков позволяют обнаружить в известной мере лёгкий доступ профессионала к ним. Утечка персональных данных в образовательных организациях – широко распространённая проблема.

Образовательные организации (ОО) обрабатывают и хранят большие объёмы информации ограниченного доступа. Реальных примеров утечек информации в образовательных организациях достаточно много. Эта тенденция набрала силу в 2023 году: образовательные организации целенаправленно подвергаются атаке не только внешних злоумышленников, но и внутренних нарушителей. Поэтому образовательные организации должны гарантировать защиту данных от несанкционированного доступа и незаконной трансграничной передачи. Одним из первых этапов защиты должны быть средства защиты от утечек со стороны внутренних нарушителей, на долю которых приходится немалая часть зафиксированных инцидентов [33].

Персональные данные представляют собой довольно сложный, формирующийся правовой институт. Перечень данных, признаваемых персональными в силу требований законодательства, неуклонно расширяется, что влечет за собой усложнение связей между субъектами правоотношений, складывающихся по поводу персональных данных. Несмотря на

определенные преимущества увеличения обмена информацией, появляются факторы, свидетельствующие об угрозах для ряда конституционных прав граждан: на неприкосновенность частной жизни, личную и семейную тайну. Для минимизации данных угроз важно решение проблемы, связанной с обработкой и защитой персональных данных, что, прежде всего, требует выявления содержания дефиниции «персональные данные» и будет способствовать обеспечению невмешательства в частную жизнь.

Теоретической основой исследования послужили труды отечественных и зарубежных ученых. Исследовались проблемы понятия персональных данных, основания проведения внеплановых проверок, риски, связанные с нарушением законодательства о персональных данных. Данные вопросы рассматривались в трудах: Добробаба М.Б., Лещинер В.Р., Цуркан Н.А., Гиш Т.А., Майорова В.И., Бачило И.В., Рассолова И.М., и др.

Нормативная основа исследования: Основным нормативным документом, определяющим порядок работы с персональными данными в информационных системах и компьютерных сетях, является Федеральный закон от27.07.2006 № 152-ФЗ «О персональных данных» [39].

Также необходимо выделить следующие нормативные документы:

- Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

- Федеральный закон от 31.07.2020 № 248-ФЗ (ред. от 06.12.2021) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»;

- Глава 14 Трудового кодекса Российской Федерации; Приказ Роскомнадзора от 30.05.2017 № 94 «Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»;

- Приказ Роскомнадзора от 30.10.2018 № 159;

- Приказ Роскомнадзора от 15.03.2013 № 274;

- Приказ Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" [4] (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ");

- Постановление Правительства Российской Федерации от 29.06.2021 № 1046 (ред. от 16.12.2021) «О федеральном государственном контроле (надзоре) за обработкой персональных данных»;

- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»[3];

- Постановление Правительства Российской Федерации от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, [2] предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, являющимися государственными или муниципальными органами»;

- Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

Согласно 152-ФЗ все персональные данные подразделяются на три категории:

1. Персональные данные, разрешенные субъектом персональных данных для распространения, это – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом (Федеральный закон от 30.12.2020 №

519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»).

2. Биометрические персональные данные[1] – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом (в ред. Федерального закона № 152-ФЗ «О персональных данных» от 25.07.2011 № 261-ФЗ).

3. Специальная категория персональных данных – обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных Федеральным законом (в ред. Федерального закона № 152-ФЗ «О персональных данных» от 24.04.2020 № 123-ФЗ).

При рассмотрении динамики изменений в сфере защиты персональных данных отмечается, что в целом она вызывает опасения. В то же время у пользователей и клиентов различных сервисов и компаний отсутствует возможность оказывать какое-либо влияние на сохранность своих персональных данных. Поскольку пользователь не может определять порядок защиты и хранения данных, его задача состоит в том, чтобы оставлять как можно меньше персональных данных. При прекращении использования тех или иных услуг необходимо отзывать согласие на обработку своих персональных данных. Угрозы информационной безопасности в наши дни обладают многообразием форм, методов и способов, направленных на искажение, раскрытие, запись, передачу и уничтожение конфиденциальной информации, полученной в результате несанкционированного доступа. Отдельно хотелось бы отметить, что, несмотря на существование

нормативных методических документов, связанных с обеспечением защиты персональных данных, их действие недостаточно эффективно.

Обработка персональных данных на основании рассматриваемой нормы Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ допускается только при одновременном соблюдении трех критериев:

- обработка производится в целях "осуществления прав и законных интересов организации или третьих лиц, либо для достижения общественно значимых целей";
- существует необходимость в обработке персональных данных для достижения поставленной оператором цели;
- обработка не нарушает "права и свободы субъекта персональных данных".

Указанные обстоятельства свидетельствуют о наличии противоречия между необходимостью обеспечения целостности, доступности и конфиденциальности персональных данных и недостаточными возможностями защиты этих данных от случайных или преднамеренных негативных воздействий в современных информационных системах. Необходимость разрешения указанного противоречия обусловливает актуальность данного исследования.[20]

Цель исследования: разработка рекомендаций по минимизации рисков нарушения безопасности в системе защиты персональных данных образовательной организации.

Объект исследования: процесс обработки и хранения персональных данных в образовательной организации.

Предмет исследования: система защиты персональных данных в образовательной организации.

Гипотеза исследования состоит в предположении о том, что минимизировать риски нарушения безопасности в системе защиты персональных данных образовательной организации возможно, если:

1. Разработана концепция информационной безопасности и схема организации информационного взаимодействия для информационных систем персональных данных ГБПОУ "Южно–Уральский агропромышленный колледж"

2. Разработана модель угроз и модель нарушителя безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

- изучить теоретические основы обработки персональных данных, функционирование информационных систем в образовательных организациях;
- исследовать риски нарушения безопасности в информационной системе персональных данных, выявить общие принципы минимизации рисков в таких системах;
- изучить текущее состояние информационной системы персональных данных на базе исследования (ГБОУ СПО ЮУрАПК)
- разработать рекомендации по минимизации рисков в информационной системе и обосновать их экономическую эффективность.

Научная новизна: усовершенствование комплекса мер, направленных на снижение рисков нарушения безопасности в системе защиты персональных данных образовательной организации.

Эмпирическая база исследования: изучение литературы и других источников. Обработка нормативно–правовых актов, связанных с обработкой персональных данных.

Методологической основой при написании работы является совокупность методов и способов научного познания. Абстрактно-логический метод позволил раскрыть теоретические аспекты обработки персональных данных и определить основные характеристики процессов и явлений, происходящих в этой сфере. Системно-структурный метод использован для анализа рисков обработки персональных данных. Применение этих методов

позволило разработать предложения по совершенствованию деятельности по защите прав субъектов персональных данных.

Теоретическая значимость исследования: в рамках исследования сформирован теоретический базис для разработки рекомендаций по совершенствованию деятельности по защите прав субъектов персональных данных.

Практическая значимость:

1. разработана Концепция информационной безопасности на основе схемы организации информационного взаимодействия для информационных систем персональных данных ГБПОУ "Южно–Уральский агропромышленный колледж» и модели угрозы ИБ.

2. разработана модель угроз и модели нарушителя безопасности.

Положения, выносимые на защиту:

1. Разработана Концепция информационной безопасности и схема организации информационного взаимодействия для информационных систем персональных данных ГБПОУ "Южно–Уральский агропромышленный колледж";

2. Разработана модель угроз и модель нарушителя безопасности для информационных систем персональных данных ГБПОУ "Южно–Уральский агропромышленный колледж".

2. Сделан вывод, что образовательные организации подпадают под действие разнообразных законодательных норм в части защиты персональных данных, а ресурсов (как финансовых, так и людских) у них, как правило, катастрофически не хватает. При этом воспользоваться всем спектром услуг по аутсорсингу функций информационной безопасности опять же мешает ограниченный бюджет[47]. Учтем также, что образовательные организации становятся объектами атак отчасти по причине недостаточной защищенности, отчасти из-за повышенного интереса к ним со стороны хакеров, использующих взломанные

инфраструктуры как своеобразный «плацдарм» для последующих атак на более крупные мишени, которые могут являться контрагентами (партнерами или, чаще всего, заказчиками) таких небольших организаций. Таким образом, потребность во внедрении процессов информационной безопасности и защиты персональных данных должна носить осознанный характер.

Итак, построение защиты персональных данных становится не только законодательным требованием, но и необходимым условием для устойчивого развития образовательной организации, что в современных реалиях цифровой экономики особенно очевидно. При этом налицо еще одна сложность - острый недостаток квалифицированных кадров в области информационной безопасности (ИБ) сужает список возможных претендентов на должность CISO (Chief Information Security Officer), то есть руководителя направления информационной безопасности, которые будут готовы трудоустроиться как в небольшую компанию, так и в образовательную организацию, обладающую ограниченным бюджетом и не имеющую возможности предложить компенсацию на уровне более крупных организаций. [49]

2. Программа повышения квалификации «Повышение осведомлённости сотрудников образовательной организации в области нарушений безопасности в системе защиты персональных данных»

Курс помогает сотрудникам образовательной организации сформировать компетенции, необходимые для профессиональной служебной деятельности и повышения профессионального уровня в рамках имеющейся квалификации (выполнения трудовых функций) слушателей в области обеспечения безопасности персональных данных. Продолжительность курса: 72 часа.

- Удостоверение о повышении квалификации
- Групповое обучение

Структура и объем работы. Работа изложена на 158 страницах и состоит из введения, двух глав (теоретической и экспериментальной), выводов по главам, заключения и списка включающего 49 использованных источников.Текст иллюстрирован 2 таблицами. Имеется 2 приложения.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МИНИМИЗАЦИИ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Информационная система персональных данных образовательной организации: общие и организационно-технические требования.

Персональные данные – новый правовой механизм, являющийся предметом особого внимания. Перечень персональных данных углубляется, усложняя отношения между субъектами. Увеличение обмена информацией вызывает угрозы для конституционных прав граждан. Важно минимизировать эти угрозы, обеспечивая защиту данных и невмешательство в частную жизнь.[34]

В ноябре 2024 года Совет Федерации РФ принял два закона, которые кардинально изменят ответственность за нарушения в области персональных данных. Эти изменения являются частью широкой реформы ответственности за неправомерную обработку персональных данных, о которой было объявлено Роскомнадзором в 2023 году.

Соблюдение требований по защите персональных данных и организация внутренних процессов становятся важными для компаний.

В Федеральном законе от 30.11.2024 № 420-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" предусмотрены новые виды нарушений [5] по статье 13.11 КоАП РФ (подробнее в таблице 1.)

Таблица 1.Составы нарушений

Нарушение	Максимальный размер штрафа для юридических лиц
Невыполнение обязанности по подаче в Роскомнадзор уведомления о намерении осуществлять обработку персональных данных или нарушение сроков такого уведомления	300 000 рублей
Невыполнение обязанности по уведомлению Роскомнадзора об утечке персональных данных или нарушение сроков такого уведомления	3 000 000 рублей

Утечка персональных данных от 1 000 до 10 000 субъектов и (или) от 10 000 до 100 000 идентификаторов* *Под идентификатором понимается уникальное обозначение сведений о физическом лице, содержащеёся в информационной системе персональных данных ГБПОУ «ЮУрАПК» и относящеёся к такому лицу	5 000 000 рублей
Утечка персональных данных от 10 000 до 100 000 субъектов и (или) от 100 000 до 1 000 000 идентификаторов	10 000 000 рублей
Утечка персональных данных болеё 100 000 субъектов и (или) болеё 1 000 000 идентификаторов	15 000 000 рублей
Утечка персональных данных, которые относятся к специальной категории	15 000 000 рублей
Утечка биометрических персональных данных	20 000 000 рублей
Повторная утечка персональных данных	До 3% совокупного размера суммы выручки за предыдущий календарный год либо размера собственных средств кредитной организации, но не менеё 20 000 000 рублей и не болеё 500 000 000 рублей
Повторная утечка биометрических персональных данных и (или) персональных данных, которые относятся к специальной категории	До 3% совокупного размера суммы выручки за предыдущий календарный год либо размера собственных средств кредитной организации, но не менеё 25 000 000 рублей и не болеё 500 000 000 рублей

Этот закон предусматривает условия для смягчения наказания.

- За последние 3 года ГБПОУ «ЮУрАПК» тратило не менее 0,1% годового дохода на мероприятия по информационной безопасности, имея соответствующую лицензию.

- Оператор доказал соответствие требованиям по защите персональных данных в течение года.[21]
- Отсутствие параметров защиты персональных данных, усугубляющих вину.

К ответственности добавляются продолжение противоправного поведения и прежние нарушения в сфере обработки персональных данных и информационной безопасности.

Если данный законопроект будет принят в настоящей редакции, он начнет действовать.по истечении 180 дней после опубликования.

Федеральный закон от 30.11.2024 № 421-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации" вносит в УК РФ статью 272.1 о незаконной обработке персональных данных.

За незаконное использование и передачу персональных данных можно лишиться свободы на 4 года.

В стратегических целях могут быть приняты меры по блокировке исходящего трафика и исключению доступа к ресурсам, введен запрет на занятие должности и деятельность до 4 лет. В целях достижения поставленных задач необходимо запланировать меры по лимитированию исходящих соединений и блокировке доступа к ресурсам.[22] Запрет сопровождает занятие некоторых определённых должностей или осуществление определённой деятельности на период до четырёх лет. Добавляются ограничения на перемещение лиц, а также использование определённых технологий связи. Отдельно рассматриваются случаи обеспечения безопасности, принимаются решения о временном или постоянном изъятии средств и носителей информации.[30]

Предлагаемые изменения существенно повлияют на оценку рисков, связанных с обработкой персональных данных. Рекомендуется провести аудит деятельности и убедиться в её соответствии законодательству и лучшим практикам перед вступлением в силу новых правил об ответственности за нарушения.[48]

Управление операционной деятельностью в образовательной организации становится все более важным соответствующих моменту условиях. Эффективное функционирование зависит от организации внутренних процессов, что помогает оптимизировать работу, улучшить удовлетворенность студентов и преподавателей, а также улучшить имидж учреждения.[25]

Внедрение систематизированного подхода к управлению процессами в образовательной среде помогает повысить эффективность защиты персональных данных. Это включает структурирование учебных программ, упрощение управления документами и использование современных технологий для автоматизации и мониторинга образовательного процесса. Управление операционной деятельностью становится неотъемлемой частью стратегии учебных заведений, направленной на минимизацию рисков нарушения безопасности персональных данных.[23]

При внесении изменений в информационную систему персональных данных важно учитывать особенности образовательной организации. Необходимо проанализировать потребности преподавателей и студентов для балансировки традиционного и инновационного подходов. Такие изменения помогут адаптировать образовательную среду к требованиям современности.

Управление персональными данными в образовательной организации направлено на оптимизацию процессов, улучшение качества образования и совершенствование взаимодействия между участниками образовательного процесса.[35] Качественное управление способствует повышению конкурентоспособности учреждений и успешной реализации образовательных программ. социально значимой миссией данный материал предназначен для стимулирования студентов и активации внутренних процессов.[38]

Эффективное управление данными в образовательных учреждениях крайне важно по нескольким причинам:

1.Повышение качества обучения:

Оптимизация процесса улучшает взаимодействие преподавателей и студентов, что способствует повышению качества образования.

2.Улучшение операционной работы:

Эффективное управление позволяет экономить и эффективно использовать ресурсы, что крайне важно для образовательных организаций при ограниченном финансировании.

3.Быстрая реакция на изменения:

Гибкие модели управления информационной безопасностью помогают образовательным учреждениям быстрее приспосабливаться к изменениям в законодательстве, технологиях и на рынке труда.

Эффективное управление защитой персональных данных крайне важно для эффективной работы образовательных учреждений.

В операционной деятельности образовательной организации выделяют несколько основных категорий.

1.Учебный процесс:

Необходимо организовать учебный процесс: составить программу, подготовить материалы, провести занятия и проверить знания студентов.

2.Управление кадрами:

Подбор, обучение и развитие педагогов, а также управление кадровой документацией **(**Положение о защите персональных данных работников, приказы по личному составу графики, таблицы, расчётные листы, табель учёта рабочего времени)**.**

3.Маркетинг и рекрутинг:

Привлечение студентов, реклама, взаимодействие с сообществом и выпускниками - основные направления работы.

4.Поддержка и сервис:

Предоставление поддержки студентам в административных вопросах: регистрация, справки, трудоустройство.

Компетентное управление системой защиты персональных данных обеспечит качественное образование. Существует много способов и средств, которые помогут уменьшить риски нарушения безопасности в образовательных организациях. Рассмотрим некоторые из них:

1.Процессный подход:

Этот подход заключается в том, чтобы сосредоточиться на процессах, а не на задачах. Необходимо понять, какие процессы происходят в учебном учреждении, их взаимосвязь и влияние на итоговый результат.

2.Система менеджмента качества (СМК):

Внедрение стандартов качества, таких как ISO 9001, помогает создать систему управления, которая контролирует и совершенствует все аспекты образовательного процесса.

3.Автоматизация процессов:

Применение IT и ПО для автоматизации рутинных задач, таких как начисление зарплат и учет посещаемости, поможет упростить работу организации.

4.Анализ и оптимизация процессов:

Изучение работы компании и её улучшение с помощью анализа данных помогут улучшить результаты и повысить эффективность.

5.Разработка и внедрение ключевых показателей эффективности (KPI):

Оценка результатов работы в образовательной организации с помощью ключевых показателей эффективности позволит выявить области для улучшения.

Для достижения стратегических целей образовательного учреждения важно правильно подобрать инструменты и методы работы, учитывая его особенности.

В образовании много примеров эффективного управления операциями, которые можно использовать как образцы.

1. Использование электронных систем для управления:

В некоторых колледжах **(**на пример в Московской области есть автомобильно-дорожный колледж, а в Ханты-Мансийске - технолого-педагогический колледж) были внедрены электронные системы управления учебным процессом, которые позволяют контролировать успеваемость студентов, вести электронные журналы и автоматизировать другие процессы.

2. Совместное обучение:

Использование смешанной модели обучения, сочетающей в себе традиционные занятия и онлайн-курсы, улучшило активность студентов и уровень образования.

3. Участие студентов в управлении:

В учебных заведениях студентов привлекают к принятию решений, что улучшает их удовлетворенность и позволяет учитывать их потребности более эффективно.

4.Аналитика данных:

Применение анализа больших данных в образовании для оценки успехов студентов, выявления проблем и создания персонализированных учебных планов, таких как в колледжах в Тамбовской области**,** Сарапульский педагогический колледж где готовят будущих педагогов. Студенты широко используют онлайн-платформы для успешной практики в учебных заведениях. Эти примеры показывают, что эффективное управление операциями может значительно улучшить образовательную среду.

Сложности и задачи в управлении операциями.

В организации без упоминания ключевых принципов и методов, управление включает в себя планирование, организацию, руководство и контроль деятельности сотрудников. Оно направлено на достижение поставленных целей и эффективное использование ресурсов. В операционной деятельности образовательные организации сталкиваются с рядом вызовов и трудностей.

1.Сопротивление изменениям: Учителя и руководство могут быть против внедрения новых процессов и неизведанных технологий, что тормозит развитие. Важно развивать гибкое мышление и готовность к переменам.

2.Недостаток финансирования:

Недостаток финансов может помешать внедрению необходимых инструментов и технологий для улучшения операционных процессов.

3.Обучение и квалификация кадров:

Постоянное обучение и повышение квалификации персонала необходимы для успешного управления. операционной деятельностью.

4.Изменения в законодательстве:

Необходимо пересматривать процессы и адаптироваться к новым условиям из-за постоянных изменений в законодательстве.

Полученные знания о проблемах помогут образовательным организациям лучше подготовиться к их решению и адаптироваться к изменяющимся условиям.

Возможные направления развития управления операциями в образовательных учреждениях.

В будущем управление операционной деятельностью образовательных организаций будет развиваться в нескольких ключевых направлениях.[44]

1. Интеграция технологий:

Применение новейших технологий, включая искусственный интеллект, блокчейн и анализ больших данных, для улучшения образовательных процессов и взаимодействия с учащимися.

2. Гибкость и адаптивность:

Разрабатываются гибкие образовательные модели для быстрой адаптации к изменениям на рынке труда и потребностям студентов.

3. Упор на компетенции:

Отказ от устаревшего метода обучения в пользу развития навыков, которые помогут студентам лучше адаптироваться к изменяющемуся миру.

Учебных программ и технологий, обеспечивает своим студентам возможность получить качественное образование и быть востребованными на рынке труда. Улучшение конкурентоспособности учебного заведения позволит обеспечить студентам современное качественное образование.

Управление операционной деятельностью:

Эффективное управление образовательной организацией - это постоянный процесс, требующий координации всех участников и готовности к переменам. Качественное управление способствует улучшению работы. учреждения. Внедрение инновационных подходов и технологий позволяет не только повысить эффективность работы школы, но и обеспечить качественное образование, соответствующеё современным требованиям и потребностям общества. учреждения в будущем.

Закон 152-ФЗ требует от всех операторов персональных данных обеспечивать защиту информации согласно статьям 18 и 19. Меры защиты должны быть описаны в организационно-распорядительной документации.

Необходимо подготовить и утвердить политику обработки персональных данных, обеспечить её хранение и выложит в публичный доступ. При ответах на запросы субъектов данных допустимо использовать внутреннюю документацию.

Изучение нормативных актов специалистом по информационной безопасности совместно с юристом позволит разработать весь комплект документов на основании законодательных актов за два месяца, что вполне достаточно для выполнения работы.

Объем документации, которую нужно разработать, зависит от типа образовательной организации и категорий обрабатываемых персональных данных. Минимальный набор включает около 28 документов. Операционная

деятельность учебного заведения включает в себя выполнение задач по реализации образовательных программ для студентов, обеспечении качественного образования и воспитания. Улучшение работы компании. современные IT-технологии, изменение структуры и анализ эффективности методов обучения помогут повысить успеваемость студентов, удовлетворенность обучающихся и преподавателей, а также оптимизировать время на административные задачи.

1.2 Риски нарушения безопасности в информационной системе персональных данных

Для обеспечения безопасности данных в образовательной организации необходимо своевременно выявлять основные уязвимости в системе защиты персональных данных, такие как фишинг, вредоносные программы и внутренние угрозы. Необходимо проводить тщательный анализ существующих систем защиты и устранять их слабые места.

Первый шаг при поиске уязвимостей - проверить актуальность политик безопасности. Важно обновлять документы, регулирующие работу с данными, чтобы соответствовать требованиям законодательства и лучшим практикам. Образовательные учреждения могут иметь устаревшие или неочень точные политики, что повышает риски утечки данных из-за некомпетентного обращения с информацией.

На этом этапе проводится проверка эффективности защитных средств, таких как антивирусные программы, брандмауэры и системы обнаружения вторжений. [37] Аудит позволяет выявить не только технические уязвимости, но и ошибки в настройках систем, которые могут быть использованы злоумышленниками. правильные настройки прав доступа могут предотвратить несанкционированный доступ к конфиденциальной информации.

Необходимо учитывать человеческий фактор в системе безопасности. Проведение опросов сотрудников и студентов поможет выявить уровень

осведомленности о правилах безопасности.[40] Низкий уровень знаний может привести к угрозам, поэтому важно проводить обучающие мероприятия и тренинги для повышения уровня информированности и формирования культуры безопасности.

Необходимо обратить внимание на физическую безопасность, чтобы защитить серверы и рабочие станции от несанкционированного доступа. Контроль перемещения сотрудников и система контроля доступа помогут минимизировать риски утечки конфиденциальной информации. Без таких мер безопасности посторонние лица могут получить доступ к данным (плечевой серфинг).[41]

Важно следить и анализировать инциденты безопасности. Собирая данные о попытках несанкционированного доступа и других инцидентах, можно выявить уязвимости. Реагирование на инциденты помогает своевременно устранять угрозы и уменьшать вред.

Исследование рассматривало развитие глобальной экономики и национальных систем в условиях активного внедрения инновационных технологий. Интеграция высокотехнологичных устройств в различные области приводит к значительному росту. рост использования технологий создает новые угрозы для безопасности персональных данных. Важно проводить анализ систем безопасности, чтобы выявить и устранить слабые места и предотвратить утечки информации.[32] Необходимо учитывать и человеческий фактор, который может привести к нарушениям безопасности. Комплексный подход к идентификации уязвимостей в системе защиты данных необходим для обеспечения надежной защиты в быстро меняющейся технологической среде.

Необходимо провести комплексный анализ системы защиты персональных данных, включая политики безопасности, аудит технических средств, оценку уровня осведомленности сотрудников и студентов, физическую безопасность и мониторинг инцидентов. Внедрение этих мер

поможет создать болеё безопасное окружение для обработки данных и снизить риски утечек и нарушений безопасности.[43]

Оценка вероятности и последствий нарушения безопасности важна для управления рисками в системе защиты данных образовательной организации. При росте информационных угроз и инцидентов с утечкой данных необходимо анализировать вероятность угроз и их последствия.

Целью определения вероятности их возникновения и потенциального вреда для системы безопасности. для оценки вероятности возникновения инцидента в образовательной организации необходимо использовать статистические данные, результаты опросов и интервью с сотрудниками. Это поможет понять, насколько высок риск в конкретном учебном заведении.

Необходимо оценить возможные последствия угроз, начиная от временных неудобств для пользователей и заканчивая утечкой конфиденциальной информации, финансовыми потерями и репутационными рисками. Важно учитывать как прямые, так и косвенные убытки, такие как потеря доверия со стороны студентов и родителей, что может негативно повлиять на репутацию образовательной организации.[29]

Для болеё точной оценки вероятности и последствий нарушения безопасности используют методы количественного и качественного анализа рисков. Качественный анализ основан на экспертных оценках и анализе сценариев, а количественный подход включает статистические модели и вероятностные расчеты. Сочетание этих методов помогает получить болеё полное представление о рисках и разработать соответствующие меры по их уменьшению.

Оценка рисков важна и должна проводиться регулярно с учетом изменений в организации, технологиях и внешней среде. Новые информационные системы или изменения законодательства могут значительно повлиять на уровень рисков.

После анализа рисков безопасности необходимо разработать стратегию их управления, включая внедрение новых политик безопасности, обучение сотрудников и улучшение технических средств защиты.[46] Необходимо разрабатывать стратегию предотвращения инцидентов и минимизации их последствий.

Исследование рассматривает важность правового регулирования защиты персональных данных для обеспечения информационной безопасности. В условиях угроз утечки данных важно разрабатывать эффективные меры защиты, такие как шифрование данных, обновление политик безопасности и обучение сотрудников.[28] Применение таких мер позволит минимизировать риски и обеспечить надежную защиту персональной информации в образовательных учреждениях.

Важно оценивать риски нарушений безопасности данных в образовательной системе. Комплексный подход к анализу, включая различные методы, поможет создать безопасную среду и снизить риски. Регулярное обновление оценок рисков необходимо для надежной защиты персональных данных.[27]

1.3 Общие принципы минимизации рисков в области информационной безопасности и информационной системы персональных данных

Принципы минимизации рисков в области информационной безопасности основаны на нормах Конституции РФ, которая закрепляет информационные права и свободы, а также особенности юридических свойств информации как объекта правоотношений.

Исходя из этого, можно выделить следующие основные принципы.

Отвечать на события в зависимости от обстоятельств.

Для снижения рисков в области информационной безопасности и предотвращения утечек информации и кибератак используются различные механизмы.

- создание актуальной модели угроз с учетом ситуации с шпионскими программами.
- организация в учебном заведении системы защиты конфиденциальной информации с установлением списка документов и данных, относящихся к этой категории, и списка сотрудников, имеющих разрешение на работу с этой информацией.
- установка и обновление защитного ПО, встроенного в операционные системы, и покупка дополнительного антивирусного программного обеспечения для обеспечения безопасности.
- иногда необходимо применять шифрование данных.

Вместе с описанными методами для снижения рисков применяются стандартные приемы безопасности и управления персоналом, направленные на обеспечение информационной безопасности.

- обучение персонала о рисках информационной безопасности.
- добавление в трудовые контракты пункта о соблюдении конфиденциальности коммерческой информации.
- поощрение сотрудников за ответственное отношение к защите персональной информации через финансовые мотивы.
- обеспечение безопасности на предприятии с помощью контроля доступа и видеонаблюдения.
- мониторинг использования мобильных устройств и USB-накопителей для безопасности данных.
- создание и утверждение правил безопасности через локальные нормативные акты.

Применение стандартных методик помогает снизить риск информационной безопасности даже без специализированных методов контроля.

В первую очередь необходимо учитывать требования регуляторов.

- Роскомнадзор;
- ФСТЭК РФ;
- ФСБ России.

Государственные органы устанавливают стандарты для защиты от угроз информационной безопасности, предписывают использование сертифицированного ПО и проведение аттестации помещений. Хотя выполнение этих требований может быть дорогостоящим для образовательных учреждений, оно упрощает процесс управления рисками и защиты информации. [47]

Международные стандарты играют важную роль в современном мире и используются повсеместно.

Внедрение стандартов включает в себя создание системы управления рисками через выявление, оценку, принятие, обработку и оценку последствий.

Каждый шаг работы с рисками имеёт свои правила, которые позволяют оценить эффективность. После внедрения системы образовательное учреждение может сертифицировать свою деятельность. Это даст конкурентное преимущество в международном образовании, где безопасность информации играет важную роль.[45]

Существуют две основные группы методик контроля рисков: качественные и количественные. Они помогают оценить вероятность возникновения рисков, опасность их последствий и потенциальный ущерб для организации.

Для получения сертификата по международной системе управления рисками информационной безопасности необходимо соблюдать два обязательных условия.

- создание специального отдела для оценки рисков.
- введение стратегии оценки и управления рисками в политику.

Этот документ содержит полный список правил по контролю информационных угроз, хотя может иметь другое название.

Обязательные разделы политики:

- основная цель управления рисками - минимизация возможных убытков или принятие рисков.
- методы управления рисками.
- критерии оценки ущерба;
- критерии оценки рисков;
- цель работы отделов.

Вся образовательная организация должна следовать политике, утвержденной руководством.

Образовательная организация оценивает риски различных объектов по группам.

- система для обработки и хранения информации.
- сервисы и приложение;
- бизнес-процессы;
- эффективность работы оборудования.
- персонал;
- облачные сервисы;
- партнеры и клиенты.

При обеспечении безопасности информационной системы важно учитывать возможные угрозы со стороны поставщиков. Рекомендуется начать внедрение системы управления рисками с ограниченного объекта, чтобы избежать ошибок и ненужных расходов. После успешного тестирования систему можно распространить на все объекты и подразделения компании.

Важно выполнять действия в определенной последовательности.

Перед началом работы над СУИБ необходимо определить риски и защищаемые активы, оценить их ценность и определить их категорию защиты, включая данные, подлежащие защите по закону.[31]

Обычно в компаниях выделяют группы активов, для которых необходимо управлять рисками информационной безопасности.

- персональные данные;
- стратегические планы ;
- ноу-хау и научные разработки;
- служебная тайна.

Для защиты информации в образовательных организациях необходимо ввести режим коммерческой тайны, чтобы привлечь нарушителей к ответственности. Список угроз безопасности персональных данных во время их обработки. необходимо определить угрозы и нарушителей информационной безопасности, указать владельца информационного актива и назначить ответственное лицо или подразделение за безопасность данных.

Вместе с определением активов и их владельцев необходимо описать операционную деятельность по защите от рисков. Использование специальных программ поможет оптимизировать процессы, сократить лишние звенья или персонал, снизить расходы. Описание процессов информационной безопасности может стать отправной точкой для оптимизации операционной деятельности организации.

Информационные активы должны оцениваться и защищаться исходя из соизмеримости уровня ущерба. Необходимо учитывать, что степень ущерба может быть разной, и она не всегда соответствует уровню конфиденциальности информации. Необходимо принимать меры защиты в зависимости от потенциального ущерба, даже если он незначителен. для

защиты объекта ценности нужно принять все возможные меры без лишней информации.

К критическим активам относятся:

- содержание, доступное образовательной организации, является государственной тайной из-за особенностей её работы.
- данные о финансовых активах, счетах, депозитах и других материальных ценностях.
- исследования и инновации в науке.
- персональные данные.

Необходимо оценить информационный актив с помощью независимого оценщика, чтобы определить его стоимость для возможного использования в судебном споре.

При оценке угроз и рисков важно учитывать два критерия.

- вероятность реализации угрозы;
- величина потенциального ущерба от возможной угрозы.

Количественная оценка рисков и их потенциала важнеё и точнеё, чем качественная. Однако некоторые информационные активы нельзя оценить только количественно. Поэтому при построении системы контроля рисков информационной безопасности в организации важно использовать сбалансированный подход, учитывающий национальные и международные стандарты. Это поможет повысить уровень информационной безопасности в организации.

Принципы конфиденциальности направлены на защиту персональных данных в информационных системах и развитие систем управления защитой данных в организациях. Эти принципы важно учитывать при работе над политикой конфиденциальности и мерами обеспечения безопасности данных. персональные данные могут быть использованы для обеспечения безопасности и эффективности программы управления конфиденциальностью в организации.

Следует использовать принципы из таблицы, но исключения должны быть минимальными.

Таблица 2. Принципы обеспечения безопасности Персональных данных

Принципы обеспечения безопасности Персональных данных
1 Согласие и выбор
2 Законность цели и ее спецификация
3 Ограничение на сбор информации
4 Минимизация данных
5 Ограничения в отношении использования, хранения и раскрытия
6 Точность и качество
7 Открытость, прозрачность и уведомление
8 Индивидуальное участие и доступ
9 Ответственность
10 Информационная безопасность
11 Соответствие безопасности Персональных данных

1. Согласие и выбор

Соблюдение принципа согласия важно.

- субъекту персональных данных предоставляется выбор между согласием на обработку своих данных или отказом от неё, за исключением случаев, когда согласие невозможно или закон разрешает обработку без него. Выбор должен быть осознанным и свободным.

- необходимо получить разрешение от человека на обработку особых категорий его персональных данных, если закон не предусматривает иное.

- субъектам персональных данных необходимо предоставлять информацию о их правах до получения их согласия в соответствии с принципом индивидуального участия и доступа.

- передача персональных данных лицу без его согласия с соблюдением принципов открытости, прозрачности и уведомления.

- объяснение важности предоставления и обработки персональных данных или отказа от этого.

Субъектам персональных данных должна быть предоставлена возможность выбора способа обработки и отзыва согласия без проблем и бесплатно. Оператор должен соблюдать законодательство о безопасности данных. Если согласие будет отозвано, данные могут быть сохранены на определенный срок по обязательствам. Если обработка данных не основана на согласии, оператор должен быть уведомлен. При необходимости отзыва согласия данные должны быть защищены от незаконной обработки.

Важно соблюдать принцип выбора персональных данных в ГБПОУ "ЮУрАПК".

- субъекту должны быть предоставлены понятные и доступные механизмы для выбора и предоставления согласия на обработку его персональных данных.

- выполнение желаний субъекта персональных данных, выраженных в его согласии.

Закон может установить дополнительные условия для обработки персональных данных, кроме согласия. Например, это может быть выполнение контракта, жизненные интересы субъекта или соблюдение закона. Некоторые законы могут предусматривать, что согласие не обязательно. для обработки персональных данных необходимо наличие юридического основания, такого как согласие подростка без одобрения родителей. Оператор персональных данных несет ответственность за соблюдение дополнительных требований при передаче данных между различными странами.

2. Законность цели и её описание

Соблюдение законности в достижении цели важно.

- гарантия соблюдения закона и выполнения целей в соответствии с правовыми обязательствами.

- субъекту персональных данных должно быть предоставлено уведомление о целях использования и сбора их информации до начала этого процесса.

- четкое и адаптированное описание цели с использованием соответствующих формулировок, приспособленных к особенностям её достижения.

- обработка специальных категорий персональных данных необходима при наличии соответствующей потребности.

Для чувствительных персональных данных требуются болеё строгие правила обработки, включая необходимость правового основания или разрешения от службы защиты данных или правительства. Важно соблюдать законность целей обработки данных.

3. Ограничение на сбор

Соблюдение ограничений на сбор информации - важный принцип.

- сбор Персональных данных должен быть ограничен законом и целью.

Компании должны собирать минимальное количество личной информации, необходимое для выполнения своих функций в рамках закона.) перед началом сбора данных, оператор должен определить необходимые персональные данные и документировать их правомерность для целей обработки информации.

Оператор может запросить дополнительные данные для маркетинга, но только с согласия субъекта. Субъекту должен быть предоставлен выбор предоставить или не предоставить эту информацию. Необязательно реагировать на запросы о дополнительных данных.[26]

4. Минимизация данных

Минимизация данных означает стремление к минимальной обработке персональных данных, в отличие от простого ограничения их сбора.

Соблюдение принципа минимизации данных включает в себя создание и применение процедур для обработки информации. и систем такими способами, чтобы:

- сократить использование личных данных и участников, заинтересованных в конфиденциальности. люди, чьи личные данные могут быть раскрыты или обработаны.

- гарантировать использование принципа "необходимости знать", то есть обработку только необходимых персональных данных для выполнения служебных обязанностей в рамках законных целей.

- использование анонимных вариантов взаимодействия и транзакций поможет снизить риск идентификации персональных данных, обеспечивая большую конфиденциальность и защиту личной информации.

- необходимо безопасно удалять персональные данные после истечения срока их обработки и отсутствия законных требований к их хранению.

Ограничения на использование, хранение и раскрытие данных.

Соблюдение ограничений в использовании, хранении и раскрытии информации.

- запрет на обработку лишних персональных данных для достижения конкретных законных целей.

- оператор не может использовать персональные данные без явного согласия до их сбора, за исключением случаев, предусмотренных законом.

- хранение личных данных будет производиться только в течение необходимого времени для достижения поставленных целей, после чего данные будут безопасно уничтожены или обезличены.

- защита персональных данных путем их блокирования и архивирования, чтобы исключить дальнейшую обработку. цели достигнуты, но нужно обеспечить хранение в соответствии с законом.

При передаче Персональных данных за границу, важно учитывать все дополнительные международные и региональные требования, касающиеся таких международных пересылок.

6.Точность и качество

Важно придерживаться точности и качества в работе.

- гарантируется корректность, полнота, актуальность и адекватность обрабатываемых персональных данных для целей использования.

- гарантируется подлинность персональных данных, полученных от третьих лиц, перед их обработкой.

- подтверждение юридической силы и корректности претензий от субъекта персональных данных перед внесением изменений в их данные.

- создание процедур сбора личных данных для обеспечения их точности и качества.

- необходимо создать системы управления для регулярной проверки точности и качества персональных данных.

Необходимо тщательно проверять данные, которые могут повлиять на получение материальной выгоды или отказ от неё. некоторые ситуации могут серьезно навредить здоровью человека.

Важно быть открытым, прозрачным и информированным.

Соблюдение принципов открытости, прозрачности и уведомления важно.

- субъектам Персональных данных должна быть предоставлена ясная информация о политиках и процедурах обработки их данных операторами.

- уведомление о обработке персональных данных включает цели обработки, типы лиц, заинтересованных в защите данных, и контактную информацию ГБПОУ «ЮУрАПК».

- оператор Персональных данных предлагает субъекту выбор и средства ограничения использования, доступа, корректировки и пересылки его информации.

- субъекты персональных данных будут уведомлены об изменениях в процедурах обработки их данных.

Необходимо обеспечить прозрачность информации о обработке персональных данных, особенно если это влияет на решения, затрагивающие субъектов данных. Участники обработки должны иметь доступ к информации о политиках и практиках защиты данных, которая доступна для общественности. необходимо документировать и утверждать процессы

обработки персональных данных, а также делать их доступными за пределами организации, чтобы обязательства были понятны и не конфиденциальны.

Необходимо четко определить цель обработки персональных данных, чтобы субъект мог понять, для чего их используют.[36]

- необходимы только те персональные данные, которые необходимы для определенной цели.

- установление конкретной цели для сбора персональных данных.

- необходимо выполнить обработку данных, включая сбор, передачу и хранение информации.

- различаются лица, которые имеют право доступа к персональным данным и те, кому могут быть переданы эти данные.

- правила хранения и удаления личной информации.

8. Индивидуальное участие и доступ

Соблюдение принципа индивидуального участия и доступа означает, что каждому должны быть предоставлены равные возможности для участия и получения информации.

- субъекту предоставляется доступ к своим персональным данным после подтверждения их идентификационных данных и при соблюдении законодательства.

- субъекты персональных данных могут оспаривать точность и полноту своих данных, требуя внесения изменений, исправлений или удаления.

- предоставление доступа к изменению или удалению персональных данных обработчикам и третьим лицам, которым данные были раскрыты.

- необходимо создать процедуры для удобного и быстрого осуществления прав субъектов персональных данных, чтобы избежать задержек и излишних расходов.

Оператор персональных данных должен гарантировать, что только сами субъекты имеют доступ к своим данным. В случае, если физическое лицо не может самостоятельно управлять своими данными, другие лица могут делать это от его имени. Закон может предоставить право доступа, просмотра и отказа

от обработки данных. Неразрешенные проблемы должны быть зарегистрированы, а третьи стороны уведомлены о их существовании.

9.Ответственность

Необходимо аккуратно обращаться с персональными данными и применять меры безопасности для их защиты.

- необходимо вести документацию и информировать о всех правилах, процедурах и способах защиты персональных данных.

- в организации определяется лицо, ответственное за обеспечение безопасности персональных данных и контроль за процедурами и методами.

- при передаче личных данных третьим лицам необходимо гарантировать, что получатель будет обеспечивать аналогичный уровень безопасности данных через договорные обязательства или другие средства, включая внутренние политики и соответствие законодательству.

- ГБПОУ «ЮУрАПК» обеспечивает обучение сотрудников для работы с персональными данными.

- установление эффективных процедур обработки претензий и возмещения ущерба для субъектов персональных данных.

- субъектам персональных данных сообщается о нарушениях безопасности, которые могут нанести им ущерб, и о принятых мерах для их устранения.

- уведомление всех заинтересованных лиц о нарушениях безопасности персональных данных в соответствии с требованиями некоторых стран и уровнем риска.

- пострадавшему субъекту персональных данных предоставляется доступ к санкциям и механизмам исправления, исключения или восстановления в случае нарушения безопасности его данных.

- изучение возможных возмещений в случаях, когда невозможно вернуть Персональные данные физического лица в первоначальное состояние.

Для устранения нарушений безопасности необходимо принимать меры, соответствующие рискам, связанным с этими нарушениями. необходимо

срочно делать что-то, за исключением случаев, когда это не разрешено, например во время расследования преступления.

Создание процедур компенсации ущерба - важная часть установления ответственности за ненадлежащеё использование персональных данных. Реституция позволяет компенсировать пострадавшему субъекту персональных данных, не только в случае кражи личности или неправильного использования данных, но и при ошибках в их модификации.

В процессе возмещения ущерба субъекты персональных данных болеё склонны к согласию, так как риск для них уменьшается. Определить компенсацию легче для некоторых услуг, чем для других, но важно, чтобы процесс был прозрачным и честным. Необходимые меры возмещения ущерба могут быть установлены законом.

10. Информационная безопасность

Соблюдение принципов информационной безопасности важно для обеспечения защиты данных.

- организация обеспечивает защиту персональных данных на всех уровнях для сохранения их конфиденциальности, целостности и доступности, а также для предотвращения рисков. незаконный доступ, повреждение, изменение или утрата информации в любое время.

- необходимо выбирать обработчиков персональных данных, которые гарантируют безопасность и соответствие организационным, физическим и техническим мерам защиты персональных данных.

- обеспечение безопасности персональных данных основывается на требованиях законодательства, стандартов безопасности, оценке рисков и анализе "затраты/выгода".

- меры безопасности должны соответствовать вероятности и серьезности возможных последствий, защищать персональные данные и учитывать количество затронутых субъектов данных и контекст реализации.

- доступ к личным данным ограничен только для сотрудников, которым это необходимо для работы, и доступ к части данных предоставляется только по мере необходимости.

- принятие решений по рискам и уязвимостям, выявленным в ходе аудита и оценки рисков данных и процессов защиты персональных данных.

- необходимо регулярно проверять и переоценивать меры безопасности персональных данных для эффективного управления рисками.

11. Гарантирование безопасности личной информации.

Соблюдение принципов безопасности персональных данных включает в себя:

- проведения проверок и демонстрации соответствия требованиям защиты персональных данных. проведение аудитов с помощью внутренних или внешних аудиторов.

- применение внутренних мер безопасности и контрольных механизмов для защиты персональных данных в соответствии с законодательством.

- проведение оценки риска нарушения безопасности персональных данных для проверки соответствия проектов, включающих обработку таких данных, требованиям безопасности.

Один или несколько наблюдательных органов могут быть ответственными за контроль соответствия закону о защите данных.[10] Соблюдение принципа безопасности персональных данных включает в себя сотрудничество с наблюдательными органами и следование их требованиям.

Выводы по первой главе.

Первая глава обсуждает два важных аспекта информационной системы персональных данных.

-усиление требований к защите персональной информации по законодательству.

-образовательные учреждения должны модернизировать свою деятельность, чтобы соответствовать современным требованиям.

Существующие процессы и системы не всегда могут обеспечить необходимый уровень защиты. Проблемы возникают из-за устаревшего ПО и недостаточной организации защиты информационных систем, включая отсутствие соответствующих регламентов обработки данных. недостаточная информированность персонала вызвана отсутствием данных и регулярного обучения.

Усовершенствование работы системы — это набор действий, цель которых принципы защиты персональных данных должны быть внедрены во все процессы работы образовательного учреждения.[11]**.** Понимание внешних регуляторных вызовов**,** так и подумай о том, как удовлетворить потребности компании.**,** образовательные организации должны принимать серьезные меры по защите персональных данных, иначе это может привести к юридическим проблемам и потере доверия со стороны студентов, родителей и сотрудников.

2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО МИНИМИЗАЦИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Текущее состояние информационной системы персональных данных в Южно–Уральском агропромышленном колледже

Для оценки эффективности информационной системы в области защиты персональных данных в Южно-Уральском агропромышленном колледже был осуществлен контроль информационной системы персональных данных, который выявил потенциал для повышения прозрачности и координирования обработки. В рамках ГБПОУ «ЮУрАПК» было проанализировано текущее состояния системы хранения и обработки персональных данных. Данный анализ направлен на повышение прозрачности и усиление надзора за процессами обработки личных данных, а также на ограничение доступа к ним. Была проведена оценка инфраструктуры на предмет соответствия установленным требованиям, в том числе с учетом последних директив Роскомнадзора.[12]

Федеральный закон от 14 июля 2022 года, который внёс изменения в законодательство о персональных данных и отменил некоторые нормы о банках и банковской деятельности.

Южно-Уральского агропромышленного колледжа в области обработки персональных данных соблюдают требования Роскомнадзора. Южно-Уральский агропромышленный колледж выступает оператором по обработке персональных данных физических лиц в соответствии с локальными нормативными актами:

- Правила работы с личными данными через компьютерные программы.
- Правила работы с личными данными без компьютерных программ.
- Регулирование доступа сотрудников ГБПОУ «ЮУрАПК» к помещениям, где происходит обработка персональной информации.
- Список сотрудников ГБПОУ «ЮУрАПК», занимающихся обезличиванием персональных данных.
- Список базы данных с личной информацией.
- Принятые правила внутреннего контроля обработки персональных данных должны соответствовать требованиям по защите персональных данных,

установленным законом "О персональных данных" и другими законодательными актами.

- Предписания о защите личной информации.

- Рекомендации о том, как реагировать на запросы субъектов персональных данных или органов, защищающих их права.

- Правила для сохранения и восстановления информации.

- Определение уровня защиты информационной системы с персональными данными.

- Руководство по обеспечению безопасности информационных систем с персональными данными.

- Документ, содержащий информацию о системе персональных данных.

- Руководство по обработке персональных данных.

- Инструкция по использованию системы для защиты персональных данных пользователей.

- Обязательство о неразглашении конфиденциальной информации в стандартной форме.

- Согласие на обработку персональных данных - обычная форма, требуемая от участников.

- Образец документа об удалении личных данных с цифровых носителей.

- Образец акта уничтожения личных данных на бумажных носителях.

- Сообщение о работе с личными данными.

- Положение о видеонаблюдении;

- Образцы документов с личной информацией.

Южно-Уральский агропромышленный колледж регулирует свою политику обработки персональных данных в соответствии с законодательством.

- Конституция России - основной закон страны.

- Трудовой кодекс Российской Федерации.

- Гражданский кодекс Российской Федерации регулирует гражданские отношения.

- Налоговый кодекс России; - это документ, который регулирует налоговые отношения в стране.

- в соответствии с Федеральным законом от 19.12.2005 №160-ФЗ, ратифицирующий Конвенцию Совета Европы о защите персональных данных.

- В законе №152-ФЗ были установлены правила обработки персональных данных.

- Согласно закону №149-ФЗ от 27.07.2006, который касается информации, информационных технологий и защиты информации.

- применительно с Федеральным законом от 29.12.2012 N 273-ФЗ - это закон о системе образования в России.

- согласно Закону о некоммерческих организациях регулирует их деятельность.

- В соответствии с законом об образовании в России регулируются все вопросы, связанные с образовательным процессом.

- 1 ноября 2012 года были утверждены требования к защите персональных данных при их обработке в информационных системах персональных данных.

- Правительство Российской Федерации приняло постановление от 15.09.2008 года № 687 о специфике обработки персональных данных без использования автоматизированных средств.

- ФСТЭК России утвердил приказ № 21 от 18.02.2013 года о мерах безопасности персональных данных при их обработке в информационных системах.

- Уставом ГБПОУ «ЮУрАПК».

- ГБПОУ «ЮУрАПК» заключает договора с субъектами персональных данных.

Руководство ГБПОУ «ЮУрАПК» приняло локальные нормативные акты в соответствии с Политикой.

- Правила обработки персональной информации с помощью компьютерных программ;

- Правила работы с персональными данными без автоматизации.

- Сотрудники ГБПОУ «ЮУрАПК» имеют доступ к помещениям с обработкой персональных данных.

- Список сотрудников ГБПОУ «ЮУрАПК», занимающихся защитой конфиденциальности персональных данных.

- Список системы хранения личных данных.

- Контроль за обработкой персональных данных должен соответствовать требованиям по их защите. согласно закону о персональных данных и дополнительным правовым актам, определяющим требования к обработке персональной информации.

- Руководство по ответственному обращению с личными сведениями.

- Инструкция о работе с запросами по персональным данным и резервному копированию данных.

- Определение уровня безопасности системы персональных данных.

- Руководство по безопасности информационных систем и защите персональных данных.

- Технический документ для обработки персональных данных.

- Руководство по обработке персональных данных.

- Рекомендации по использованию информационной системы для защиты персональных данных пользователей.

- Договор о конфиденциальности ограниченного доступа.

- Согласие на обработку персональных данных - стандартный документ.

- Образец документа об удалении личных данных с электронных носителей.

- Образец документа об уничтожении бумажных носителей личной информации.

- Уведомление о защите личных данных.

- Положение о видеонаблюдении;

- Свод документов с личной информацией.

Внутригосударственное размещение серверов неизбежно в процессе защиты персональных данных, что предотвращает их утечку и несанкционированный доступ. Мера оптимизации работы в рамках Федеральной государственной информационной системы «Единая информационная платформа национальной системы управления данными» (ФГИС «ЕИП НСУД»). При работе с персональными данными применяется обезличивания, исключающая возможность распознования конкретных лиц.

Согласно Федеральному закону № 152-ФЗ, оператор должен исполнить обязанность, если получил требование от Минцифры. Эти требования распространяются не только на государственные организации, но и на образовательные учреждения, так как они обрабатывают много персональных данных. В ГБПОУ «ЮУрАПК» данное требование утверждено в локальных нормативных актах. Персональные данные в ГБПОУ «ЮУрАПК» обезличивают работники, занимающие определенные должности. изучаем и устанавливаем правила обработки анонимных данных (после преобразования персональных данных).[13]

Роскомнадзор установил правила обезличивания персональных данных согласно постановлению Правительства Российской Федерации от 1 августа 2025 года. NПринят документ о правилах обезличивания и методах защиты персональных данных.

Приказ Роскомнадзора №140 от 19 июня 2025 года устанавливает правила обезличивания персональных данных, за исключением определенных случаев, указанных в законе №152-ФЗ "О персональных данных".

Постановление № 1154 применяется, когда оператору персональных данных необходимо обезличить информацию по требованию Минцифры России для передачи в ФГИС "ЕИП НСУД". Определенная процедура по увольнению сотрудников, что может привести к неопределенности и конфликтам в коллективе. журнал, в котором фиксируются данные о машинах, содержащих персональные данные.**,** (п. 5 ч. 2 ст. 19 Федерального закона от 27.07.2006 №152-ФЗ).

Журнал обычно включает в себя различные пункты, такие как:

- название и тип устройства для хранения данных.
- указывается уникальный номер носителя - регистрационный, серийный или инвентарный.
- люди, которым разрешен доступ к устройствам хранения данных.
- Ф. И. О. и должность сотрудника, который получил машинный носитель.
- работник подписал документ о получении носителя данных.
- уполномоченный сотрудник принял машинный носитель от работника и поставил дату и подпись.
- сотрудник подписал и уничтожил машинный носитель.
- контроль за режимами работы и административная поддержка специальных программ и аппаратных средств для защиты информации.
- проверка эффективности системы защиты после установки обновлений для информационной системы с персональными данными.[14]

Организации, необходимо получить согласие от сотрудника на обработку его персональных данных. организации, таких как:

обучение сотрудников ГБПОУ «ЮУрАПК» правилам работы с системами защиты информации. назначение администратора безопасности персональных

данных требуется в соответствии с приказом ФСТЭК России от 18.02.2013 №21.

Отсутствуют перечни лиц, согласно Приказу ФСТЭК России от 15.01.2020 № 3. Документ "Об обработке персональных данных в Федеральной службе по техническому и экспортному контролю и её территориальных органах" включает в себя "Правила обработки персональных данных в указанных органах".")

- люди, у которых есть право самостоятельно входить в информационную систему с персональными данными.
- разрешение на обработку личных данных в ИСПД.
- управление базой данных персональной информации.

Из-за неуказания класса защиты информационных систем, согласно Приказу ФСТЭК России от 30 июля 2018 года №131и, возникают проблемы с безопасностью персональных данных. Постановлению от 1 ноября 2012 г. № 1119 «Требования к защите персональных данных при обработке в ИСПД не утверждены. Определяется уровень защиты персональных данных в информационных системах, влияющий на технологический процесс. информационные системы требуют обработки данных, установки антивирусов и создания надежных паролей для защиты.

Были изучены системы защиты персональных данных в ГБПОУ «ЮУрАПК» в рамках технической оценки:

создание учетных записей для детей на портале Госуслуг может привести к возможности использования аккаунта родителями после достижения ребенком совершеннолетия. Для детей до 14 лет доступ к некоторым услугам ограничен, однако учетная запись служит для получения государственных услуг и льгот. Создание учетных записей для детей любого возраста возможно, но подтверждение происходит только после достижения 14 лет. Важно обеспечить баланс между доступом детей к услугам и защитой их

персональных данных. государственные услуги должны быть доступными для всех, но регистрация не должна быть принудительной или происходить без согласия граждан.

В Южно-Уральском агропромышленном техникуме (ЮУрАПК) для защиты данных применяются физические методы, такие как:

- Замки (включая электронные): Простые и надежные методы ограничения физического доступа к оборудованию и помещениям.
- Системы контроля и управления доступом (СКУД) предназначены для обеспечения безопасности помещений и контроля доступа сотрудников и посетителей. Устанавливаются правила доступа в определенные помещения для определенных лиц.
- Системы наблюдения и записи видео:

Сотрудники проходят наблюдение, выявляются несанкционированные проникновения.

Защита информации с использованием технических средств. эти устройства помогают защитить информацию от несанкционированного доступа и утечки через технические каналы, такие как просмотр с экранов, бумаг и прослушивание разговоров. Образовательные учреждения обычно не являются целью злоумышленников, но в организациях утечка информации может быть серьезной угрозой.[15]

Хардвер важен для защиты данных, особенно от несанкционированного доступа и утечек через технические каналы.

Метод защиты данных является крайне важным для любой организации.

Для эффективного обеспечения безопасности персональных данных, есть потребность в специализированных аппаратных средствах блокировки и обнаружения.

Предпринимаются действия для обеспечения безопасности и защиты работников в рабочих местах. На компьютерах установлена система пользовательских профилей, которая блокирует доступ при отсутствии

активности. Защита конфиденциальной информации: важность и методы обеспечения безопасности данных.

Руководитель информационного центра ЮУрАПК отвечает за ведение журналов с данными о движении персонального контента и его передачу третьим лицам.

Законы и технологии: важные аспекты.

Правовая защита персональных данных включает в себя как законодательные нормативно-правовые акты, так и функциональные характеристики компьютерного оборудования. Сбор персональных данных с использованием автоматизированных систем – это техническая процедура. Однако организация этого процесса относится скорее к обработке документов, чем к чисто юридической практике.

Спецификации и стандарты:

Специализированные документы содержат подробные описания конкретных версий программного обеспечения и моделей оборудования, созданные Министерством образования и другими органами.[16]

Необходимо соблюдать требования к Журналу учета доступа к персональным данным.

В специальном журнале регистрируются все случаи доступа к личным данным.

- Сведения о датах обработки личных данных (получение и возврат).
- Период использования документа.
- Назначение выдачи документа.
- Перечень выданных документов.
- Важное правило: Сотрудник, управляющий личным делом коллеги, не может изменять документы.

Когда организация собирает и обрабатывает персональные данные, она должна учитывать внешние факторы и обеспечить их защиту.

В Южно-Уральском агропромышленном колледже ведется журнал учета запросов по персональным данным работников.

- Кто отправил запрос в учреждение - источник информации.

- Дата начала обработки документов по запросу или отметка об отказе в предоставлении информации.
- Конкретные переданные сведения.

Эффективная система учета:

Регулярно проверяют наличие личных данных и других конфиденциальных информационных носителей для обеспечения качества системы учета персональных данных.

Состав Персональных данных :

При трудоустройстве в ГБПОУ «Южно-Уральский агропромышленный колледж» необходимо предоставить информацию о себе.

Для подтверждения личности необходимо иметь при себе паспорт или другой документ. При заключении нового трудового договора или при работе по совместительству без трудовой книжки, работнику выдается новая трудовая книжка в случае её утраты или отсутствия по другим причинам.

документ обязательного пенсионного страхования.

Документы воинского учета предназначены для военнообязанных и лиц, которые должны быть зарегистрированы в воинском учете.

при трудоустройстве на работу, где требуются специальные знания или квалификация, необходимо предоставить документы об образовании и специальной подготовке, а также свидетельство ИНН, если у работника есть.

Запрос на трудоустройство.

Получение документа о наличии или отсутствии судимости.[17]

Медицинскую книжку;

автобиографию;

фото 3х4;

справку 2-НДФЛ;

заполненный личный листок;

дубликат акта о рождении несовершеннолетних детей;

необходимо иметь водительское удостоверение.

Абитуриенты и их представители должны предоставлять документы в структурные подразделения колледжа в письменной форме.

необходимо предъявить паспорт или другой документ с фотографией для подтверждения личности.

при необходимости, предоставляется дополнительное заявление от законного представителя.

аттестат об окончании школы;

справку о составе семьи;

медицинскую справку формы №086-у;

сертификат о прививках;

характеристику из школы;

фотографии для документов;

справка по ГИА;

обязательный страховой полис здоровья.

получение санитарной книжки обязательно.

СНИЛС (при необходимости);

ИНН (при необходимости);

перечислите номер счета и банковские реквизиты, если нужно.

После зачисления абитуриент становится студентом. Данные из документов вносятся в информационную систему "Студенты". Персональные данные хранятся и передаются сотрудниками в бумажном виде.

журнал успеваемости;

книги приказов;

зачетная книжка;

студенческий билет;

диплом и его копия.

Набор документов для взаимодействия с ИП.

При заключении соглашения между частным предпринимателем и колледжем ГБПОУ «Южно-Уральский агропромышленный колледж» необходимо предоставить определенные данные.

фамилия, имя, отчество;

паспортные данные;

номер ОГРН;

номер ИНН;

адрес места регистрации;

банковские реквизиты.

С 01.09.2025 вступили в силу изменения в законодательстве о персональных данных. Теперь согласие на их обработку должно быть оформлено отдельно от других документов, подписываемых субъектом. данных. Пересмотрите свои решения перед тем, как дать согласие на обработку данных. информация о человеке представлена в простой и понятной форме. Согласие на обработку данных должно быть оформлено в отдельном документе и подписано владельцем данных.

Образовательные организации должны получать разрешения на обработку персональных данных в ходе своей работы.

- Разрешение на использование личных данных как законный повод.
- Разрешение на использование личной информации из внешних источников.
- Согласие на использование личных данных для обработки.
- Разрешение на рекламу продукции и услуг.
- Разрешение на использование личных данных для передачи третьим лицам.
- Законные представители недеёспособных лиц соглашаются на обработку их персональных данных.
- Разрешение на обработку личных данных без автоматизации.
- Разрешение на обработку чувствительных данных.
- Разрешение на использование биометрических данных.

- Разрешение на использование автоматизированных методов для принятия важных юридических решений, влияющих на правовое положение человека.
- Разрешение на публикацию личных данных в общедоступных источниках.

Для некоторых соглашений необходимо оформление в письменной или электронной форме.

В ГБПОУ «ЮУрАПК» хранятся различные категории персональной информации.

- Субъект разрешил использовать его персональные данные.
- Специальные персональные данные.

Эти данные можно собирать и использовать только в образовательной сфере в соответствии с законом. Нормативные акты Российской Федерации определяют правовые основы обработки персональных данных в учебных учреждениях.

- Биометрические**.**

Сюда включаются данные о человеке, такие как фотографии и видеозаписи.

Информационные системы хранения личных данных ГБПОУ «ЮУрАПК», как оператор обрабатывает различные категории персональных данных.

- Данные о сотрудниках собираются от самих сотрудников.
- Информация о контрагентах и их представителях получается от самих субъектов персональных данных.
- Информация о личных данных абитуриентов, студентов и их законных представителей. Как и где мы получаем эту информацию.

лица, чьи данные обрабатываются, и их законные представители.

Количество личной информации, которое хранится в системе, необходимо обеспечить её безопасность. в базе данных находится менеё 100 тысяч человек, что важно для оценки уровня безопасности системы хранения персональных данных.

ГБПОУ «ЮУрАПК» сбор информации у субъектов персональных данных проводится с учетом типа данных и наличия согласия на обработку. Это делается только при необходимости для достижения целей, с соблюдением защиты данных.

Документация, связанная с персональными данными.

- текст описывает цели использования персональных данных.
- личные данные обрабатываются с согласия субъектов, защищаются и удаляются при необходимости.

ГБПОУ «ЮУрАПК» принимаются меры по защите от случайного сбора персональных данных через системы ввода информации. Это включает использование методов обезличивания и безопасных вычислений во время обработки данных.

Каждая сторона, участвующая в обработке персональных данных, несет ответственность и подотчетность за передачу этих данных, о чем согласовано в письменной форме. Субъект данных должен быть проинформирован о передаче и её целях.

Персональные данные обрабатываются только для заявленных целей и хранятся до их выполнения, после чего уничтожаются или обезличиваются.

Уничтожение персональных данных происходит в соответствии с требованиями оператора или законодательства.

Ддля защиты личных данных были созданы специальные меры., такие как:

Система индивидуальных профилей.

Создана система индивидуальных профилей для стационарных компьютеров колледжа, которая автоматически блокирует вход при отсутствии активности пользователя.

Средства шифрования для защиты данных.для защиты данных используется шифрование, аутентификация пользователей и проверка электронных подписей.

У директора ГБПОУ «ЮУрАПК» хранятся журналы внутреннего и исходящего контроля персональных данных, содержащие информацию о конфиденциальных документах и процедурах их выдачи.

- журнал, в котором отмечаются сотрудники, имеющие доступ к персональным данным в информационных системах.
- журнал, где фиксируются машины, содержащие персональные данные.
- журнал отслеживает выполнение требований по безопасности Персональных данных при их обработке в информационной системе.
- создан журнал для записи обращений субъектов Персональных данных.
- создан журнал для отслеживания процедур резервного копирования.
- журнал отслеживания использования средств защиты информации.

Информация сохраняется на защищенных серверах, компьютеры оборудованы антивирусами, шифрованием и автоматической блокировкой экрана. Удаленная работа осуществляется через защищенные корпоративные сервисы с шифрованием доступа к базам данных..

2.2 Рекомендации по минимизации рисков информационной безопасности для информационной системы персональных данных Южно-Уральского агропромышленного колледжа.

На основе результатов анализа на данный момент информационная система персональных данных в Южно-Уральском агропромышленном колледже требует улучшения. разработаны рекомендации для снижения угроз информационной безопасности:

- оформить Необходимо подписать согласие в письменной форме.

в частности, для следующих видов:

Разрешение на использование личных данных работников из внешних источников (ст. 86 Трудового кодекса).

Одобрение на передачу личных данных работников (ст. 88 Трудового кодекса).

Разрешение на использование конфиденциальной информации (пункт 1 часть 2 статьи 10 Федерального закона № 152).

Разрешение на использование биометрических данных (статья 11 152-ФЗ).

Согласие на использование автоматизированных методов обработки персональных данных для принятия юридически значимых решений, влияющих на правовое положение субъекта.

Разрешение на публикацию личных данных в общедоступных источниках (ст. 8 152-ФЗ).

Устанавливать правила для обезличивания данных. пункт 2 статьи 13.1 Федерального закона № 152-ФЗ устанавливает.

Разработать журнал для записи информации о хранении и обработке персональных данных на электронных носителях., согласно п. 5 ч. 2 ст. 19 Федерального закона от 27.07.2006 №152-ФЗ. Для учета несъемных машинных носителей в журнале можно удалить графу 8 "Дата и подпись уполномоченного работника в получении машинного носителя от работника" и добавить новую графу "Местонахождение машинного носителя".";

Разработать перечни лиц, согласно Приказу ФСТЭК России от 15.01.2020 N Службе по техническому и экспортному контролю и её подразделениях"). Этот документ регулирует порядок обработки персональных данных в указанных организациях. органы технического и экспортного контроля и их подразделениях.

Разработать Для улучшения обработки информации и обеспечения безопасности персональных данных, проводится анализ уровня защиты информационных систем и организации парольной защиты.

Назначить администратора безопасности информационной системы Персональных данных в соответствии с Приказом ФСТЭК России от 18.02.2013 №21 о мерах по обеспечению безопасности персональных данных в информационных системах.

Разработать перечни лиц, согласно Приказу ФСТЭК России от 15.01.2020 N Правила обработки персональных данных в Федеральной службе по

техническому и экспортному контролю и её филиалах.") и утвердить перечень приказом:

- лица, имеющие право на доступ к персональным данным в информационной системе, могут самостоятельно войти в помещения.
- разрешение на обработку персональных данных в информационной системе.
- управление системой для обработки персональных данных.

Создание инструкции по защите от социальных инженеров.

- обучать сотрудников правилам информационной безопасности и проверять их на проникновение через социальную инженерию.
- регулярно проверять открытые источники на утечки конфиденциальной информации о сотрудниках.
- обновить политику информационной безопасности, включая защиту от социальной инженерии и усовершенствование парольной политики.
- создать в компании дружелюбную атмосферу, где сотрудники не стесняются задавать вопросы, признавать свои ошибки и делиться информацией о непонятных звонках и письмах.

Используйте сертифицированные средства защиты информации. — запретить использовать непроверенное программное обеспечение для защиты персональных данных, таких как антивирусы, межсетевые экраны и криптографические средства.

Сотрудники должны использовать личные учётные записи с паролями и двухфакторной аутентификацией для работы в системе. IAM-речь идет о системе, которая ограничивает права автоматически в зависимости от должности и обязанностей.[44] Отслеживание действий пользователей в журналах. действия, такие как доступ, копирование, изменение и удаление данных, облегчают процесс расследования инцидентов и проверки соблюдения правил. Для безопасного хранения информации важно делать

резервные копии, которые должны быть защищены от несанкционированного доступа. Есть необходимость в оснащении для обеспечения безопасности компьютеров используют антивирусы, шифрование и блокировку экрана. Для удалённой работы используются корпоративные сервисы с шифрованием и безопасным доступом к данным. Необходимо периодически обновлять локальные нормативные акты о защите персональных данных в соответствии с изменениями в законодательстве и внутренними процессами организации.

Необходимо регулярно проверять информацию в Реёстре на её актуальность. обработки персональных данных. Согласно закону № 152-ФЗ, необходимо обновлять реёстр до 15 числа каждого месяца, начиная с 1 марта 2023 года. необходимо уведомить о прекращении обработки в течение 10 дней после месяца, следующего за изменениями.

Желательно проводить аудиты процессов обработки персональных данных каждый год. В колледже следует создать положение о внутреннем аудите, определить формы опросных листов и назначить ответственных лиц. Такие аудиты помогут выявить новые процессы и ошибки в регулировании обработки персональных данных.

Для обработки ПД часто привлекают контрагентов, например, для информационного обеспечения. Если требуется передать данные сотрудников другим юридическим лицам (например, при командировках), можно опубликовать список таких организаций на внутреннем корпоративном ресурсе и предоставить ссылку в согласии на обработку ПД. Сотрудники смогут узнать, кому передаются их данные в любое время. данных, в каких целях.

Рекомендуется уведомления об изменениях в списке третьих лиц отправляются сотрудникам на почту или в личные кабинеты. Также ведется архив версий списка для ознакомления работодателя и работников с предыдущими и актуальными версиями. Необходимо добавить ответственность за обработку персональных данных в должностную

инструкцию.работодатель назначил нового сотрудника.. Этот специалист несёт ответственность за невыполнение своих обязанностей, нарушения и причинение ущерба.

Сотрудникам грозит наказание за неправильную обработку персональных данных, включая дисциплинарные, материальные, административные и уголовные меры ответственности. Нарушителям грозит наказание, даже если они были официально назначены для работы с данными.

2.3 Экономическая оценка эффективности предложений

При анализе рисков информационной безопасности колледжа необходимо использовать различные подходы для определения потенциального ущерба и целесообразности вложений.

Анализ затрат и выгод поможет оценить эффективность внедрения мероприятий через сравнение затрат и потенциальных выгод: снижение рисков, уменьшение потерь и повышение устойчивости к инцидентам.

Сравнение различных методов помогает выбрать наиболеё эффективные подходы. Изучив опыт других учреждений и секторов экономики, можно оценить уровень защиты информации, стойкость к атакам и скорость реагирования на инциденты. Важно также учитывать время, необходимое для достижения безопасности, так как это влияет на затраты и ресурсы.

Только финансовые показатели, но и другие выгоды от улучшения безопасности, такие как снижение риска потерь, улучшение репутации компании и повышение уровня доверия клиентов.ROI - важный инструмент для оценки эффективности мер безопасности и их влияния на бизнес. важно учитывать не только деньги, но и репутацию и доверие учебного заведения.

Метод анализа чувствительности помогает предсказать влияние изменений в ключевых показателях на общую эффективность мероприятий.

Например, можно изучить, как увеличение числа инцидентов безопасности или затрат на защитные системы отразится на общем результате.

Структурный подход к определению рисков позволяет использовать стандарты оценки на основе типовых сценариев угроз. Модель управления рисками может быть разработана с учетом вероятностей инцидентов и сравнена с имеющимися мерами защиты.

Важными критериями оценки в экономическом аспекте являются уровень готовности к реагированию на инциденты и стоимость восстановления после атак. При каждом инциденте учитывается общий ущерб, включая прямые и косвенные потери, чтобы выявить слабые места в защищенности системы и адаптировать меры к реальным потребностям колледжа.

Из текста следует, что оценка экономических мер должна быть всесторонней, учитывая затраты и выгоды. Это позволит провести анализ эффективности принятых решений в следующем разделе.

Внедрение советы по защите персональных данных в Южно-Уральском агропромышленном колледже. в Южно-Уральском агропромышленном колледже происходит улучшение защиты персональных данных. после внедрения изменений уровень утечек данных снизился, что уменьшило вероятность инцидентов. Это повысило безопасность и защиту репутации учреждения, а также обеспечило безопасность студентов и сотрудников. Сравнение данных до и после показало явное улучшение.

Улучшение системы безопасности в колледже повышает доверие студентов и их родителей, создавая положительный имидж и привлекая новых абитуриентов. Оценка стабильности через опросы и отзывы имеёт важное значение при принятии решений о приеме новых студентов и влияет на финансовый результат.

Новые методы управления информационными ресурсами снизили затраты за счет оптимизации процессов обработки данных и соответствия стандартам безопасности. Это позволило сократить расходы на обслуживание

старого оборудования и пересмотреть бюджет на обновления систем. Экономические показатели улучшились, что говорит о рентабельности инвестиций в безопасность информации.

Условий для постоянного обучения и развития являются ключевыми факторами для достижения целей в области внедрения новых технологий. специальные группы быстрого реагирования помогают обеспечить безопасность в онлайн-пространстве.

Для обеспечения безопасности в колледже необходимо внедрить систему мониторинга, которая поможет выявить нарушения и положительные изменения в учебном процессе. Это позволит сохранить целостность безопасности учебного заведения и направить дополнительные средства на развитие новых технологий и исследования.

Экономическая эффективность мероприятий по улучшению информационной безопасности важна для создания устойчивой образовательной среды и развития колледжа. Успешные шаги по минимизации рисков имеют положительное влияние на функционирование и репутацию учреждения в долгосрочной перспективе.

Для экономии средств при обеспечении информационной безопасности в колледже следует уделить внимание оптимизации расходов без ущерба для уровня защиты данных.

Требуется провести анализ затрат на информационную безопасность, выявить устаревшие системы и решения, заменить их современными и эффективными. принятие решений может уменьшить расходы на серверное оборудование и обновление программного обеспечения.

Необходимо использовать стандарты безопасности, такие как ISO 27001, чтобы структурировать процессы и улучшить прозрачность расходов. Важно обучать новых кадров, используя уже имеющиеся ресурсы и опыт сотрудников. Внутреннеё обучение с экспертами может быть болеё эффективным и экономичным, чем внешние тренинги.

Одним из важных шагов является использование открытого программного обеспечения. Оно не только дешевле лицензионного, но и обеспечивает необходимую защиту информации. Такой подход поможет сократить затраты на обслуживание и адаптировать системы под нужды колледжа.

Необходимо активно сотрудничать с другими образовательными учреждениями в области кибербезопасности, чтобы обмениваться ресурсами и опытом, что позволит снизить затраты на меры безопасности. Совместные закупки программ и тренингов упростят процесс и сэкономят деньги.

Одним из ключевых элементов оптимизации бюджета является ребалансировка ресурсов. Например, часть средств, запланированных на устранение рисков, можно перенаправить на профилактические меры, которые эффективно снижают вероятность инцидентов. Выделение эффективных резервов для обработки инцидентов и инцидентного реагирования просматривается как приоритетный шаг для управления рисками.

Сегодняшние реалии требуют от образовательных учреждений гибкого подхода к финансовым вопросам. Важно осуществлять мониторинг и пересмотр прогнозов затрат на информационную безопасность, стремясь к постоянной оптимизации. Пересмотр бюджета на основе анализа состояний информационной безопасности позволит скорректировать траты и избежать непредвиденных расходов. Эффективное использование существующих решений и ресурсов, кроме того, обеспечит устойчивый рост уровня защиты данных, что в свою очередь укрепит общую структуру информационной безопасности колледжа.

Выводы по второй главе.

При проведении анализа информационной системы персональных данных (информационной системы Персональных данных) в Южно-Уральском агропромышленном колледже (ГБПОУ «ЮУрАПК») были определены как недостатки, так и ряд преимуществ в области защиты персональных данных.

Положительные факторы:

- Политика колледжа в области обработки персональных данных в целом соответствует требованиям Роскомнадзора.
- Спектр разработанных локальных нормативных актов, таких как положения, порядки, перечни должностей, инструкции и типовые формы документов регулирующих различные аспекты обработки персональных данных свидетельствует о стремлении руководства и специалистов колледжа к регламентизации процессов связанных с защитой информационной системы Персональных данных .
- Права и обязанности оператора и физических лиц детально распределены в локально-нормативно актах.
- Колледж использует различные физические меры защиты, что является базовым уровнем безопасности.
- В соответствии современным требованиям применяются специализированные информационные системы для передачи данных (Госуслуги, электронный журнал, СЭД).

Факторы риска:

- Отсутствует четкое регулирование правил работы с обезличенными данными, не взирая на утвержденный перечень должностей, ответственных за обезличивание, что критично в свете требований ФГИС «ЕИП НСУД».
- Отсутствует журнал учета машинных носителей персональных данных, что является нарушением Федерального закона № 152-ФЗ.
- Большой проблемой является **отсутствие** администратора безопасности информационной системы Персональных данных , который бы был компетентен в принятии решения по дополнительным задачам защиты информации.

- Отсутствуют перечни лиц, имеющих право самостоятельного доступа, обработки и обслуживания информационной системы Персональных данных.
- Отсутствует Акт определения класса/уровня защищенности информационной системы Персональных данных, что мешает разработке и применению технологических процессов обработки информации, а также на антивирусную защиту и парольную политику.
- Выявлены скрытые риски, связанные с регистрацией учетных записей несовершеннолетних на портале Госуслуг, включая возможность регистрации на чужого ребенка и использование аккаунта после достижения совершеннолетия, даже при лишении родительских прав. Требуется болеё строгий контроль и, возможно, дополнительные механизмы верификации.
- Пр использовании аппаратных средства защиты, есть риск распространенных угроз (несанкционированный просмотр, утечка по техническим каналам).

Южно-Уральский агропромышленный колледж достиг положительных показателей в обеспечении защиты персональных данных, разработав локально-нормативную базу и установив надежные физические меры защиты целесообразно уделить больше внимания техническим мерам защиты.

ЗАКЛЮЧЕНИЕ

Операционная деятельность образовательных организаций становится критически важной для обеспечения безопасности персональных данных. Эффективное управление внутренними процессами в учебных заведениях напрямую влияет на минимизацию рисков нарушения безопасности персональных данных.

Систематизированный подход к управлению операционной деятельностью – ключ к повышению эффективности защиты персональных данных в образовании. Это включает в себя структурирование процессов,

упрощение документооборота, внедрение современных технологий и адаптацию к меняющимся законодательным требованиям.

Управление информационной системой персональных данных в образовательных учреждениях имеёт многогранное значение:

Повышает качество обучения.

Совершенствует операционную эффективность (снижение затрат, оптимизация ресурсов).

Обеспечивает быструю реакцию на изменения (законодательство, технологии, рынок труда).

Для эффективного управления операционной деятельностью и защиты персональных данных в образовательных организациях необходимо:

Применять процессный подход.

Внедрять системы менеджмента качества (СМК).

Использовать автоматизацию процессов.

Проводить анализ и оптимизацию процессов.

Разрабатывать и внедрять ключевые показатели эффективности (KPI).

Существуют как успешные практики, так и вызовы в управлении операционной деятельностью образовательных организаций. К успешным практикам относятся электронные системы управления, смешанное обучение, вовлечение студентов в управление и аналитика данных. Основные вызовы включают сопротивление изменениям, недостаток финансирования, потребность в обучении кадров и постоянные изменения в законодательстве.

Перспективы развития управления операционной деятельностью в образовании связаны с интеграцией технологий (ИИ, блокчейн, большие данные), повышением гибкости и адаптивности моделей, а также с акцентом на формирование компетенций.

В целом, текст подчеркивает, что в условиях растущих требований к защите персональных данных и ужесточения законодательства, образовательные организации должны активно заниматься совершенствованием своей операционной деятельности, чтобы обеспечить

соответствие нормам, минимизировать риски и повысить свою конкурентоспособность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты Российской Федерации

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) “О персональных данных” [Текст]: [Федеральный закон № 152-ФЗ: принят 27.07.2006].
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Текст]: [Постановление Правительства РФ № 1119: принято 01.11.2012].
3. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Текст]: [Постановление Правительства Российской Федерации № 687: принят 15.09.2008].
4. Приказ Роскомнадзора от 05.09.2013 N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») (Зарегистрировано в Минюсте России 10.09.2013 N 29935).
5. Кодекс об административных правонарушениях [Текст]: № 195-ФЗ: принят 30.12.2001].
6. Трудовой кодекс Российской Федерации [Текст]: [№ 197-ФЗ: принят 30.12.2001].
7. ГОСТ ISO/IEC 29100-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных Дата введения в действие: 30.11.2021
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Утверждена ФСТЭК России 15.02. 2008 г.

Международные документы

9. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных. Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 года. (официально не публиковалась) // КонсультантПлюс [сайт]. http://base.consultant.ru/cons/cgi/online.cgi ?base=INT&n=49528&req=doc (дата обращения: 16.02.2024).

Монографии, учебники и учебные пособия

10. Бабаш А.В., Баранова Е.К., Информационная безопасность и защита информации: Учебное пособие. – М.: Изд. центр РИОР, 2024. – 336 с.

11. «Стратегии противодействия угрозам экономической безопасности России: материалы Всероссийской научно-практической конференции. Вып. 1. В 3 т. Т. III» (Стратегии противодействия угрозам экономической безопасности России: материалы Всероссийской научно-практической конференции. Вып. 1 : материалы конференции : в 3 томах / под редакцией Е. Ю. Меркуловой. — Тамбов : ТГТУ, 2018 — Том 3 — 2018. — Алексеёва, Н. Г., Арзамаскова, Ю. Б. Проблемы обеспечения информационной безопасности предприятия / Н. Г. Алексеёва, Ю. Б. Арзамаскова Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/319880 (дата обращения: 22.11.2024). — Режим доступа: для авториз. пользователей. — С. 10.). — Тамбов:, 2018. — С. 9-17.

12. «Ванина А. Г., Орёл Д. В., Аникуев С. В.Персональная кибербезопасность: курс лекций» (Ванина, А. Г. Персональная кибербезопасность: курс лекций : учебное пособие / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев. — Ставрополь : СКФУ, 2022. — 137 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/386636 (дата обращения: 22.11.2024). — Режим доступа: для авториз. пользователей. — С. 1.).

13. Савельев, Александр Иванович. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А. И. Савельев. – 2-е изд., перераб. и доп. – Москва : Статут, 2021 – 468 с.

14. «Барабас А. А., Баранова Ю. Ю., Боровых И. С.Управление реализацией информационной политики в системе образования Челябинской области: модельные решения. В 2 ч. Ч.2» (Барабас, А. А. Управление реализацией информационной политики в системе образования Челябинской области: модельные решения : учебно-методическое пособие : в 2 частях / А. А. Барабас, Ю. Ю. Баранова, И. С. Боровых. — Челябинск : РЦОКИО, 2019 — Часть 2 — 2019. — ISBN 978-5-906934-38-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149031 (дата обращения: 22.11.2024). — Режим доступа: для авториз. пользователей. — С. 1.).

15. Защита персональных данных обучающихся образовательных организаций: методические рекомендации/ В.Р. Лещинер, к.п.н.; под общей

редакцией Ю.В. Федоровой, к.п.н. – М.: Московский центра развития кадрового потенциала образования, 2021 [Текст] — 17 с.

16. И.М. Рассолов Информационное право: учебник и практикум для вузов. - 7-е издание, переработанное и дополненное изд. - М. : Юрайт, 2023. - 427 с.

17. Цуканова О. А., Смирнов С. Б. Экономика защиты информации: учебное пособие, . - 2 изд. - СПб.: НИУ ИТМО, 2014 – 79 с.: НИУ ИТМО, 2014. - 79 с. (дата обращения: 29.10.2025).

Научные статьи и публикации

18. «Правовые проблемы использования виртуального пространства метавселенной в образовательном процессе вуза» (Ересько, П.В. Правовые проблемы использования виртуального пространства метавселенной в образовательном процессе вуза / П. В. Ересько, P. V. Eresko // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. — 2023. — № 4. — С. 471-477. — ISSN 1994-2540. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/349982 (дата обращения: 22.11.2024). — Режим доступа: для авториз. пользователей. — С. 1.).

19. «Правовые меры минимизации угроз информационной безопасности хозяйствующих субъектов: проблемы реализации» (правовые меры минимизации угроз информационной безопасности хозяйствующих субъектов: проблемы реализации» / Н. В. Моргунова, N. V. Morgunova, И. А. Сичкар, I. A. Sichkar // Вестник студенческого научного общества ГОУ ВПО “Донецкий национальный университет”. — 2024. — № 16. — С. 110-115. — ISSN 2522-4824. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/356819 (дата обращения: 22.11.2024). — Режим доступа: для авториз. пользователей. — С. 1.).

20. Добробаба, М. В. Понятие персональных данных: проблема правовой определенности [Текст] / М. В. Добробаба // Вестник университета (МГЮА). — 2023. — № 2. — С. 42-52.

21. Воронков Н. А. Определение персональных данных // Молодой ученый. 2022. № 27 (422). С. 78—80

22. К.А.Садыкова, Д.Е. Жонина, Е.А. Егорышева Некоторы е проблемы раскрытия и расследования преступлений в сфере информационных

технологий [Текст] / К.А.Садыкова, Д.Е. Жонина, Е.А. Егорышева // InternationalJournalofHumanitiesandNaturalSciences. — 2021. — № 12-4 (63). — С. 171-173.

23. Савинова, С. В. Защита персональных данных: проблемы и решения / С. В. Савинова. — Текст : непосредственный // Молодой ученый. — 2024. — № 9 (508). — С. 18-21. — URL: https://moluch.ru/archive/508/111591/ (дата обращения: 24.11.2024).

Интернет-ресурсы и базы данных

24. Журнал ознакомления служащих с локальными актами Управления Роскомнадзора по Уральскому федеральному округу [Текст].

25. Отчет о результатах деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2018 [Текст].

26. Отчет о результатах деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2017 [Текст].

27. Отчет о результатах деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2016 [Текст].

28. База данных российской судебной практики по информационному праву/ Раздел «Разглашение персональных данных» / URL: https://mediapravo.info (дата обращения: 05.11.2018).

29. Паспортные данные и СНИЛС 2,2 миллиона россиян попали в открытый доступ [Электронный ресурс] / https://news.mail.ru/incident/37134079/?frommail=1(дата обращения: 29.04.2019).

30. База данных российской судебной практики по информационному праву [Электронный ресурс] / Раздел «Разглашение персональных данных» URL: https://media-pravo.info (дата обращения: 05.11.2018).

31. Политика конфиденциальности Ozon.ru [Электронный ресурс] / Интернет-магазин OZON.RU URL: https://docs.ozon.ru/common/pravila-prodayoii-rekvizity/konfidentsial-nost-personal-noj-informatsii/ (дата обращения: 26.04.2019).

32. AmazonPrivacyNotice [Электронный ресурс] / Интернет-магазин Amazon.com URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (дата обращения: 26.04.2019).

33. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Портал персональных данных. Официальный сайт. URL: https://pd.rkn.gov.ru/(дата обращения: 28.01.2025).

34. В.А. Адаев, К.А. Максимов, Т.А. Жаров Концепция информационной безопасности Российской Федерации: пути реализации. / В.А. Адаев, К.А. Максимов, Т.А. Жаров [Электронный ресурс] // ResearchGate.net : [сайт]. —
URL: https://www.researchgate.net/publication/349680735_Concept_Of_Information_Security_Of_The_Russian_Federation_Ways_Of_Implementation (дата обращения: 23.11.2024).

35. Краткая характеристика состояния преступности в Российской Федерации за январь-2024 года. – [Электронный ресурс]. – Режим доступа: http://мвд.рф/ Дата обращения: 24.11.2024 г.

36. П. Друкер. Управление бизнес процессами в образовательной организации // APPTASK: управление проектами URL: https://apptask.ru/blog/upravlenie-biznes-processami-v-obrazovatelnoi-organizacii (дата обращения: 1.12.2024).

37. Дж. Леггио. Культура безопасности опирается на баланс технических знаний и понимания человеческого поведения // ItWeek URL: https://www.itweek.ru/security/article/detail.php?ID=193707 (дата обращения: 1.12.2024).

38. Р. Рахметов Управление информационной безопасностью (Менеджмент ИБ) // Security Vision URL: https://www.securityvision.ru/blog/menedzhment-informatsionnoy-bezopasnosti/ (дата обращения: 1.12.2024).

39. Е. Тутова. Путь защитника персональных данных: обучение во благо // канал “Anti-Malware” URL: https://www.anti-malware.ru/practice/methods/staff-training-to-protect-personal-data (дата обращения: 1.12.2024).

40. Новая ответственность за нарушения, связанные с оборотом персональных данных // Б1: Новые вызовы новые решения

URL: https://b1.ru/insights/law-messenger/personal-data-28-november/?lang=ru (дата обращения: 5.12.2024).

41. Основные принципы и категории средств защиты информационной безопасности // VC.RU URL: https://vc.ru/id2776479/1229369-osnovnye-principy-i-kategorii-sredstv-zashity-informacionnoi-bezopasnosti (дата обращения: 22.04.2025).

42. Магия вне Хогвартса: как повышать ИБ-грамотность сотрудников // Хабр URL: https://habr.com/ru/companies/ozontech/articles/789708/ (дата обращения: 22.04.2025).

43. Что такое Security Awareness (обучение осведомленности о кибербезопасности) и почему это так важно? // securitylab.ru URL: https://www.securitylab.ru/blog/personal/bezmaly/347850.php (дата обращения: 22.04.2025).

44. Приоритеты CISO в 2025 году // Kasperskiy daily URL: https://www.kaspersky.ru/blog/ciso-priorities-2025/39378/ (дата обращения: 27/04.2025).

45. Что произошло в 2022 году и как будет развиваться рынок информационной безопасности в 2025 году // cisoclub URL: https://cisoclub.ru/chto-proizoshlo-v-2022-godu-i-kak-budet-razvivatsja-rynok-informacionnoj-bezopasnosti-v-2025-godu/ (дата обращения: 27.04.2025).

46.Управление рисками нарушения информационной безопасности // СёрчИнформ URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/upravlenie-informatsionnoj-bezopasnostyu/upravlenie-riskami-narusheniya-informatsionnoj-bezopasnosti/ (дата обращения: 01.05.2025).

47. Как провести инвентаризацию информационных систем с персональными данными (Персональных данных) // Хабр URL: https://habr.com/ru/articles/935660/ (дата обращения: 13.09.2025).

48. Персональные данные: как настроить процесс обработки и передачи // Главбухассистент URL:&utm_campaign=red_block_content_link&utm_term=5518&utm_content=art (дата обращения: 11.10.2025).

49. Как защищать персональные данные // Контурнорматив URL: https://normativ.kontur.ru/limited/documents/240518175241?https%3A%2F%2Fnormativ.kontur.ru%2Flimited%2Fdocuments%2F240518175241= (дата обращения: 19.10.2025).

1. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

(утв. ФСТЭК РФ 14.02.2008)

ПРИЛОЖЕНИЕ 1.

Министерство образования и науки Челябинской области

Государственное бюджетное профессиональное образовательное учреждение

«Южно-Уральский агропромышленный колледж»

Обсуждено и
принято советом
Колледжа ГБПОУ
«ЮУрАПК»
Протокол № _____
от «___ »
_____20___ г

«УТВЕРЖДАЮ»
Директор ГБПОУ
«ЮУрАПК»
_____О.В. Аминева
«___»_____20___

Концепция информационной безопасности и схема организации информационного взаимодействия для информационных систем персональных данных ГБПОУ "Южно–Уральский агропромышленный колледж"

Челябинск,

2025 г.

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

***Автоматизированная система (АС)** — это система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.

***ГОСТ Р 59853-2021** "Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения" утвержден приказом Росстандарта от 19 ноября 2021 года N 1520-ст.

***Аутентификация отправителя данных** – это подтверждение того, что отправитель полученных данных соответствует заявленному.

***ГОСТ Р ИСО 7498-2-99** «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

***Безопасность персональных данных** – **это** состояние защищённости 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.

* **ГОСТ Р 59407-2021.** Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных. Дата введения в действие: 30.11.2021.

***Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

* **ГОСТ Р 59407-2021**. Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных. Дата введения в действие: 30.11.2021.[7]

***Вирус (компьютерный, программный)** – это программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей**,** а также осуществлять иные деструктивные действия.

* **ГОСТ Р 51188-98**. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Дата введения в действие: 01.07.1999.

***Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

* **ГОСТ Р 50922-2006** «Защита информации. Основные термины и определения» Дата введения в действие: 01.02.2008.

***Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными

для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

***** Словарь-справочник терминов нормативно-технической документации

***Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

* Словарь-справочник терминов нормативно-технической документации

Доступ к информации - возможность получения информации и её использования.

* **ГОСТ Р 50922-2006** «Защита информации. Основные термины и определения» Дата введения в действие: 01.02.2008.

***Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

***ГОСТ Р 51275-2006.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Дата введения в действие: 01.02.2008.

***Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

* **ГОСТ Р 50922-2006** «Защита информации. Основные термины и определения» Дата введения в действие: 01.02.2008.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

*** ГОСТ Р 58833-2020.** Защита информации. Идентификация и аутентификация. Общие положения. Дата введения в действие: 01.05.2020.

***Информативный сигнал** – это сигнал, по параметрам которого может быть определена защищаемая информация.

*** ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» Дата введения в действие: 01.10.2009

***Информационная система персональных данных (ИСПДн)** – Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

***ГОСТ Р 59407-2021.** Информационные технологии. Методы и средства обеспечения безопасности. [7]Базовая архитектура защиты персональных данных. Дата введения в **действие**: 30.11.2021.

***Информационная технология**–приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.

* **ГОСТ Р 59853-2021** «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Дата введения в действие: 9.11.2021

Использование персональных данных — это действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

* **Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» в редакции от 08.08.2024**

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление,

являющиеся причиной возникновения угрозы безопасности информации.

*ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» Дата введения в действие: 01.02.2008.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

* Словарь-справочник терминов нормативно-технической документации

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не
допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

* **Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"**

Межсетевой экран-
локальное (однокомпонентное) или функциональнораспределенное программное (программно-аппаратное) средство (комплекс), реализующеё контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

***ГОСТ Р 70860-2023** «Информационные технологии. Облачные вычисления. Общие технологии и методы». Дата введения в действие: 30.01.2024.

***Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающеё действия, следствием которых является нарушение безопасности персональных данных при их обработке

техническими средствами в информационных системах персональных данных.

***"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных"[8] (Выписка) (утв. ФСТЭК РФ 15.02.2008)**

***Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

*Постановление Правительства Российской Федерации от 15 сентября 2008 г. №687 г. "Об утверждении Положения об особенностях
персональных данных, осуществляемой без использования средств автоматизации".

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

*** Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. №114)**

Несанкционированный доступ (несанкционированные действия) - доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа**.**

**** ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» Дата введения в действие: 01.10.2009

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

***Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

*Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

*Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных

данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

*Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующеё и (или) осуществляющеё обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

*Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

* Р 50.1.053-200 Основные термины и определения в области технической защиты информации. Дата введения в действие: 01.01.

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

*Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных"

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующеё в функционировании информационной системы персональных данных или использующеё результаты её функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на

ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукГБПОУсиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенноцифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской

Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС — антивирусные средства

АИБ - администратор информационной безопасности

АРМ - автоматизированное рабочеё место

АС - автоматизированная система

ВТСС - вспомогательные технические средства и системы

ИСПДн - информационная система персональных данных

ИТ – инфраструктура – информационно-технологическая инфраструктура

КЗ - контролируемая зона

КИС – корпоративная информационная система

ЛВС - локальная вычислительная сеть

МРМ – мобильное рабочеё место

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн – персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПТК – программно-технический комплекс

ПЭМИН - побочные электромагнитные излучения и наводки

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн – система защиты персональных данных

СКЗИ – средство криптографической защиты информации

СОВ - система обнаружения вторжений

ТКУИ - технические каналы утечки информации

ТС - технические средства

УБПДн - угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Концепция информационной безопасности ИСПДн, используемая в ГБПОУ "Южно–Уральский агропромышленный колледж» (далеё – образовательное учреждение), является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности образовательное учреждение.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗ ПДн) образовательного учреждения. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам ПДн)

или инфраструктуре. Задачи информационной безопасности сводятся к минимизации рисков нарушения безопасности в системе защиты ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности образовательного учреждения, а также нормативных и методических документов, обеспечивающих её реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн образовательного учреждения;

принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

координации деятельности структурных подразделений образовательного учреждения при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн образовательного учреждения.

Область применения Концепции распространяется на все структурные подразделения образовательного учреждения, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется

автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн)

1. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) образовательного учреждения, в соответствии с Перечнем ИСПДн образовательного учреждения. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

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.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

конфиденциальность информации (защита от несанкционированного ознакомления);

целостность информации (актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения);

доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

предпроектная стадия, включающая предпроектное обследование ИСПДн,

разработку технического (частного технического) задания на её создание;

стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

Должностная инструкция администратора безопасности ИСПДн;

Должностная инструкция пользователя ИСПДн в части обеспечения безопасности

ПДн при их обработке в ИСПДн;

Инструкция пользователя на случай возникновения нештатной ситуации;

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн образовательного учреждения.

2. Задачи системы защиты персональных данных (СЗПДн)

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИСПДн;

б) к средствам вычислительной техники ИСПДн;

в) к аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

защиту ПДн от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;

защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

3.Объекты защиты

3.1. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

Перечень информационных систем

В образовательном учреждении производится обработка персональных данных с помощью используемых в ГБПОУ ИСПДн.

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки (разрабатывается индивидуально для образовательного учреждения).

3.2. Перечень объектов защиты

Объектами защиты является информация, обрабатываемая в ИСПДн, и технические средства её обработки и защиты. Персональные данные,

подлежащие защите, определены в Перечне персональных данных, подлежащих защите в ИСПДн.

Объекты защиты включают следующие компоненты:

Обрабатываемая информация.

Технологическая информация.

Программно-технические средства обработки.

Средства защиты ПДн.

Каналы информационного обмена и телекоммуникации.

Объекты и помещения, в которых размещены компоненты ИСПДн.

4. Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующеё в функционировании информационной системы персональных данных или использующеё результаты её функционирования. В образовательного учреждения пользователем ИСПДн является любой сотрудник образовательного учреждения, имеющий доступ к ИСПДн и её ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн в образовательном учреждении делятся на три основные категории:

1) Администратор ИСПДн. Сотрудники образовательного учреждения, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеёт доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

2) Программист-разработчик ИСПДн. Сотрудники образовательного учреждения или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн; - обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии её разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

3) Оператор ИСПДн. Сотрудники подразделений образовательного учреждения, участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеёт доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей, определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа пользователей к ПДн.

5. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ПДн в ИСПДн образовательного учреждения и её функционирование должны осуществляться в соответствии со следующими основными принципами:

-законность;

-системность;

-комплексность;

-непрерывность;

-своевременность;

-преёмственность и непрерывность совершенствования;

-персональная ответственность;

-минимизация полномочий;

-взаимодействие и сотрудничество;

-гибкость системы защиты;

-открытость алгоритмов и механизмов защиты;

-простота применения средств защиты;

-научная обоснованность и техническая реализуемость;

- специализация и профессионализм;

- обязательность контроля.

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн образовательного учреждения в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДн в ИСПДн образовательного учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение защиты ПДн.

5.2. Системность

Системный подход к построению СЗПДн образовательного учреждения предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн в ИСПДн образовательного учреждения.

При создании системы защиты должны учитываться все слабые и наиболеё уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно субъектов с опытом в совершении противоправных действий), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств построения целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному нарушителю

требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболеё укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

5.4. Непрерывность защиты ПДн

Защита ПДн - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы нарушителями для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления её функционирования.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию

мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и её системы защиты информации в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать болеё эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.6. Преёмственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преёмственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и её системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих функционирование ИСПДн

образовательного учреждения, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений защиты информации.

5.10. Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования.

5.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

5.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

5.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболеё подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами образовательного учреждения.

5.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения правил, которые установлены для обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль деятельности любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

6. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности.

Все меры обеспечения безопасности ИСПДн подразделяются на:

законодательные (правовые);

морально-этические;

организационные (административные);

физические;

технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в **Плане мероприятий по обеспечению защиты персональных данных.**

6.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека,

группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

6.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за её реализацию;

формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне образовательного учреждения в целом;

обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

какова область применения политики безопасности ПДн;

каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;

кто имеёт права доступа к ПДн;

какими мерами и средствами обеспечивается защита ПДн;

какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты и других защитных механизмов;

организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

Порядка допуска сотрудников к использованию ресурсов ИСПДн образовательного учреждения (Разрешительная система доступа к ПДн);

Инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);

Инструкции пользователя при возникновении нештатных ситуаций.

6.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5. Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн образовательного учреждения;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности; - криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

обеспечена физическая целостность всех компонент ИСПДн;

каждый сотрудник (пользователь ИСПДн) или группа пользователей имеёт уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

в ИСПДн образовательного учреждения разработка и отладка программ осуществляется за пределами

ИСПДн, на испытательных стендах;

все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ГБПОУ;

сетевое оборудование (концентраторы, коммутаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

специалистами ГБПОУ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Контроль эффективности системы защиты ИСПДн образовательном учреждении

Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), прогнозирование атак и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

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

8. Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является администратор информационной безопасности (далеё - АИБ), назначаемый приказом директора образовательного учреждения.

Сфера ответственности АИБ включает следующие направления обеспечения безопасности ПДн:

Планирование и реализация мер по обеспечению безопасности ПДн.

9. Анализ угроз безопасности ПДн.

Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности.

Контроль защищенности ИТ-инфраструктуры образовательного учреждения от угроз ИБ путем.

Обучение и информирование пользователей ИСПДн о порядке работы с ПДн и средствами защиты.

Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

Не реже одного раза в квартал (а при наличии необходимости и чаще) информирование руководства образовательного учреждения о состоянии информационной безопасности.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел /3/), с этими организациями должно быть заключено Соглашение о конфиденциальности, либо Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн. Подготовка типовых вариантов этих соглашений осуществляется

10. Модель нарушителя безопасности

Под нарушителем в образовательном учреждении понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел /3/).

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных ИСПДн.

11. Модель угроз безопасности

Для ИСПДн образовательного учреждения выделяются следующие основные категории угроз безопасности персональных данных:

Угрозы от утечки по техническим каналам.

Угрозы несанкционированного доступа к информации:

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программноаппаратных и программных средств (в том числе программно-математических воздействий).

Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в её составе из-за сбоев в

программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характеров.

Угрозы преднамеренных действий внутренних нарушителей.

Угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных ИСПДн.

12. Механизм реализации концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

-федеральных законов в области обеспечения информационной безопасности и защиты информации;

-постановлений Правительства Российской Федерации;

-руководящих, организационно-распорядительных и методических документов

ФСТЭК России;

-потребностей ИСПДн в средствах обеспечения безопасности информации.

12. Ожидаемый эффект от реализации концепции.

Реализация Концепции безопасности ПДн в ИСПДн позволит:

оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

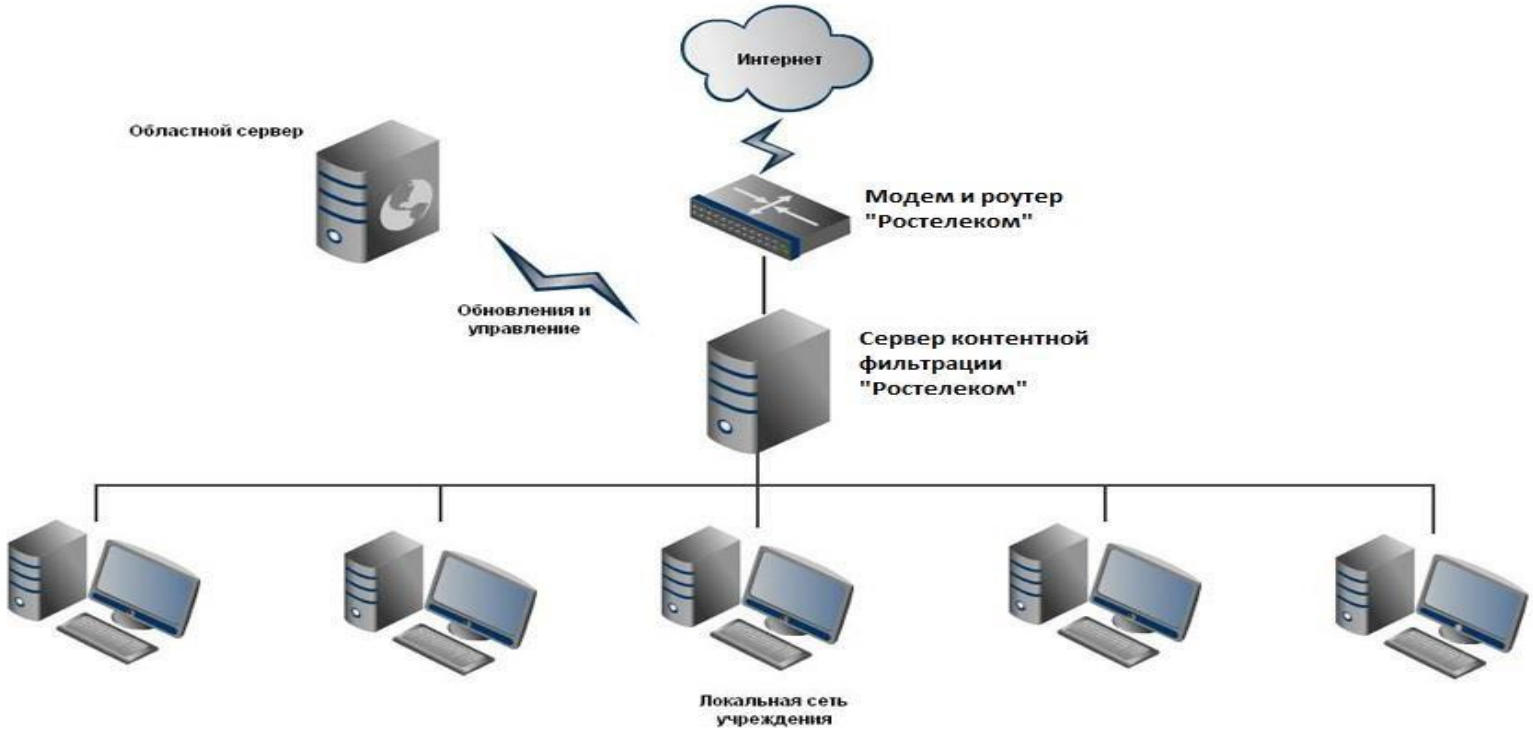
разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

провести классификацию и сертификацию ИСПДн;

провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для её дальнейшего совершенствования.


Интернет
Областной сервер
Модем и роутер
"Ростелеком"
Обновления и
управление
Сервер контентной
фильтрации
"Ростелеком"
Локальная сеть
учреждения

Государственное бюджетное профессиональное образовательное учреждение "ЮЖНО-УРАЛЬСКИЙ АГРОПРОМЫШЛЕННЫЙ КОЛЛЕДЖ" является оператором, осуществляющим обработку персональных данных

Уведомление об обработке (о намерении осуществлять обработку) персональных данных ГБПОУ «ЮУрАПК»
Регистрационный номер 74-14-001270

	Цель обработки персональных данных	Обеспечение осуществления образовательной деятельности (документирование факта, этапов, процессов воспитания и обучения учащихся, индивидуального учёта освоения образовательных программ, подтверждение достигнутого образовательного уровня, удостоверяемого соответствующим документом об образовании; предоставление мер социальной поддержки; обеспечение медицинского обслуживания; формирование баз данных информационных систем АРИСМО, ГИСЭО, ведение официального сайта ГБПОУ «Южно-Уральский агропромышленный колледж» в сети Интернет), оформление трудовых отношений, ведение кадрового и бухгалтерского учёта, регистрация обращений граждан, оформление гражданско-правовых отношений
	Правовое основание обработки персональных данных	**Трудовой Кодекс** Российской Федерации (ст. ст 85-90) [6]
		Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
		Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
		Федеральный закон от 29.12.2012 № 273 «Об образовании в Российской Федерации»
		Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
		Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
		Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
		Устав », утвержденный постановлением администрации МОГО «Инта» от 20.03.2015 № 3/819 (в ред. от 27.12.2016)
		Лицензия на осуществление образовательной деятельности № Л035-01235-74-00187704

	Правовое основание защиты персональных данных	**Федеральный закон** от 27.07.2006 № 152-ФЗ «О персональных данных»
		Кодекс Российской Федерации об административных правонарушениях (статья 13.11. «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных»)
		Уголовный кодекс Российской Федерации (статья 137 «Нарушение неприкосновенности частной жизни»)
		Уголовный кодекс Российской Федерации (статья 137 «Нарушение неприкосновенности частной жизни»)
	Политика обработки персональных данных	**Положение** об обработке персональных данных
		Инструкция ответственного лица за организацию обработки персональных данных
		Инструкция администратора информационной системы персональных данных
		Инструкция пользователя информационных систем персональных данных
		Перечень персональных данных, обрабатываемых в «Южно-Уральском агропромышленном колледже»
		Согласие на обработку персональных данных учащегося
		План мероприятий по обеспечению защиты персональных данных в ГБПОУ «Южно-Уральском агропромышленном колледже»
	ФИО лица, ответственного за обработку персональных данных	**Бухтоярова Валентина Васильевна** — инженер-программист
	Номера их контактных телефонов, почтовые адреса и адреса электронной почты	8 (35131) 2-12-90, 8 (35131) 2-17-73
	Список информационных систем и их параметры	**Категории субъектов:** учащиеся, зачисленные в родители (законные представители) учащихся; работники, состоящие в трудовых отношениях; физические лица, состоящие в договорных и иных гражданско-правовых отношениях с ГБПОУ «Южно-Уральском агропромышленном колледже»
		Перечень действий: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, персональных данных
		Обработка персональных данных: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет

	Отзыв согласия на обработку персональных данных по инициативе субъекта персональных данных	Согласие может быть отозвано в любое время на основании **письменного документа**, который может быть направлен мной в адрес ГБПОУ «Южно-Уральского агропромышленногоколледжа» по почте заказным письмом с уведомлением о вручении, либо вручен под расписку представителю ГБПОУ «Южно-Уральского агропромышленного колледжа»

ПРИЛОЖЕНИЕ 2

Министерство образования и науки Челябинской области

Государственное бюджетное профессиональное образовательное учреждение

«Южно-Уральский агропромышленный колледж»

Обсуждено и
принято советом
Колледжа ГБПОУ
«ЮУрАПК»
Протокол № _____ от
«___ »
_____20___ г

«УТВЕРЖДАЮ»
Директор ГБПОУ
«ЮУрАПК»
_____О.В.
Аминева
«___»_____20___

МОДЕЛЬ УГРОЗ И МОДЕЛИ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

с. Аргаяш, 2026

1. Перечень обозначений и сокращений

АРМ - автоматизированное рабочее место;

ИР - информационный ресурс;

ИСПДн - информационная система персональных данных;

КЗ - контролируемая зона;

ПДн - персональные данные;

ПО - программное обеспечение;

ПТС - программно-технические средства;

ПЭМИН - побочные электромагнитные излучения и наводки;

СЗИ - средства защиты информации;

СКЗИ - средства криптографической защиты информации;

ФСБ - Федеральная служба безопасности;

ФСО - Федеральная служба охраны;

ФСТЭК - Федеральная служба по техническому и экспертному контролю.

1. Общие положения

Настоящая модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн ГБПОУ «ЮУрАПК» (далее – Образовательное учреждение). Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн. Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Федеральный закон от 7 мая 2013 г. №99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона "О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных" и федерального закона "О персональных данных"[9];

[4] – Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Перечень 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, утвержденный постановлением

Правительства Российской Федерации от 21 марта 2012 г. N 211;

[5] - Указ Президента Российской Федерации от 17 марта 2008 года N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

[6] - Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и

Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом

России 3 апреля 2008 года, регистрационный № 11462);

[7] - Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован

Минюстом России 3 марта 2005 года, регистрационный № 6382);

[8] - Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6622, 2008);

[1] - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах

персональных данных с использованием средств автоматизации (ФСБ России, № 149/5-144, 2008);

[2] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[3] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[4] – Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное приказом директора ФСТЭК России от 18 февраля 2013 года № 21;

[5] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 года № 12.

2. Характеристика объекта информатизации

В Организации существуют следующие типы ИСПДн:

1. ИСПДн ведения бухгалтерского учета, управления персоналом, расчета заработной платы Организации.
2. ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

Состав ИСПДн и обрабатываемых в них персональных данных приведен в Приложении №1 к настоящему документу

В качестве объекта информатизации предприятия выступают:

1. Автономные автоматизированные рабочие места (АРМ).
2. Локальные вычислительные сети.

В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных предприятий подключена к сетям связи общего пользования.

Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

ИСПДн предполагают как распределенную (на АРМ), так и централизованную (на выделенных файловых серверах сети) обработку и хранение ПДн.

Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных сотрудников Организации, как в электронном, так и в бумажном виде.

Контролируемой зоной (КЗ) ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в Организации информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в ИСПДн Организации не обрабатываются.

Для ИСПДн Организации актуальны угрозы 2 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно подпункту «б» пункта 11 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн Организации требуется обеспечить 3-ий уровень защищенности персональных данных при их обработке в информационной системе.

4. Способы нарушения характеристик безопасности персональных данных

Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

- ✓ хищение персональных данных сотрудниками предприятия для использования в корыстных целях;
- ✓ передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- ✓ несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам предприятия;
- ✓ несанкционированное получение персональных данных третьими лицами;
- ✓ уничтожение финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ✓ модификация финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ✓ блокирование финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ✓ ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ✓ передача некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ✓ искажение архивной информации по субъекту ПДн.

- ✓ уничтожение архивной информации по субъекту Пдн.

5. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников предприятия в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

- ✓ по видам возможных источников угроз;
- ✓ по типу ИСПДн, на которые направлена реализация угроз;
- ✓ по виду нарушаемого свойства информации

(виду несанкционированных действий, осуществляемых с ПДн);

по способам реализации угроз;

по используемой уязвимости;

по объекту воздействия.

Для ПДн:

ИСПДн существуют следующие классы угроз безопасности

По видам возможных источников угроз безопасности персональных данных

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;
- угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена угроза:

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе автоматизированных рабочих мест;
- угрозы безопасности данных, обрабатываемых в ИСПДН на базе локальных информационных систем.

По способам реализации угроз:

По способам реализации угроз выделяют следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);
- угрозы специальных воздействий на ИСПДн.

По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными**):**

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
- угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);
- угрозы, реализуемые с использованием уязвимости прикладного ПО; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;

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

- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;

- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки

(принтерах, плоттерах, графопостроителях, вынесенных

мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.); угрозы безопасности ПДн, передаваемых по сетям связи;

- угрозы прикладным программам, с помощью которых обрабатываются ПДн;

- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

6. Характеристика источников угроз безопасности персональных данных в ИСПДн

В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

Антропогенные источники угроз безопасности ПДн

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними.

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезобразовательное учреждение работы, вывод систем Организации из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной

документации сотрудниками Организации, имеющих доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

– непредумышленное искажение или удаление программных компонентов;

– внедрение и использование неучтенных программ;

– игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:

- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);

- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;

- настройка и конфигурирование средств защиты информации, а также

технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников предприятия, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);

- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);

- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.

Техногенные источники угроз безопасности ПДн

Техногенные источники угроз напрямую зависят от свойств техники.

Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки.

Аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными.

Аппаратные закладки могут реализовать угрозы:

- сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла ИСПДн.

Носитель вредоносной программы

В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства – видеоадаптера, сетевой платы, устройств ввода/вывода и т . д .)
- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;
- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Стихийные источники угроз безопасности ПДн

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к Организации. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих

источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн.

8. Модели нарушителя безопасности персональных данных

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;

2. Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;

3. СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

8.1 Описание нарушителей

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

- категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;
- категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Организации;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
- представители преступных организаций.

Внешний нарушитель может осуществлять:

- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

- несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;

- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;

- атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К первой группе относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

- изменять конфигурацию технических средств обработки ПДн, вносить программноаппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

2. Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
- располагает ПДн, к которым имеет доступ.

3. К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Организации.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;
- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

4. К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
- имеет доступ ко всем техническим средствам сегмента ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

5. К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о ТС и конфигурации ИСПДн
- имеет доступ ко всем ТС ИСПДн и данным;
- обладает правами конфигурирования и административной настройки ТС ИСПДн.

6. К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Организации, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7. К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

8. К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;

- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

8.2 Предположения о возможностях нарушителя

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программнотехнических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

8.3 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;

- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;
- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационнотехнических и режимных мер.

8.4. Описание каналов атак

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
- бумажные носители информации;
- штатные программно-аппаратные средства ИСПДн;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационнотехническими мерами;
- незащищенные каналы связи; ТКУИ.

8.5. Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации

При обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

9. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы. 9.1. Уровень исходной защищенности информационной системы персональных данных

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Перечень данных характеристик и показатели защищенности ИСПДн, зависящие от них, показаны в таблице1. Показатели, относящиеся к Организации выделены жирным курсивом.

Для определения исходной защищенности ИСПДн должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для ИСПДн.

Таблица 1 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень		
	В	С	Н
По территориальному размещению			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко стоящих зданий	+		
локальная ИСПДн, развернутая в пределах одного здания	+		
По наличию соединения с сетями общего пользования		+	
ИСПДн, имеющая многоточечный выход в сеть общего		+	
ИСПДн, имеющая одноточечный выход в сеть общего пользования	+	+	
ИСПДн, физически отделенная от сети общего пользования			+
По встроенным (легальным) операциям с записями баз ПДн			
чтение, поиск	+		
запись, удаление, сортировка		+	
модификация, передача		+	
По разграничению доступа к персональным данным			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации,			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем			+
ИСПДн с открытым доступом		+	
По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (образовательное учреждение использует несколько баз ПДн ИСПДн, при этом образовательное учреждение не является владельцем всех используемых баз ПДн)		+	
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн		+	
По уровню обобщения (обезличивания) ПДн			

ИСПДн, в которой предоставляемые пользователю данные являются обезличенными			+
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и	+		
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными		+	
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без			
ИСПДн, предоставляющая всю базу данных с ПДн		+	
ИСПДн, предоставляющая часть ПДн			+
ИСПДн, не предоставляющие никакой информации		+	
Количество решений	4	11	4
Общее количество решений	19		

Принимается, что ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные уровню «средний».

В случае, если не менее 70% характеристик ИСПДн относится к уровню «не ниже среднего», а остальные к уровню «низкий», то исходная защищенность ИСПДн будет среднего уровня.

Во всех остальных случаях ИСПДн будет иметь низкий уровень защищенности.

Исходя из критериев оценки, делаем вывод, что ИСПДн Организации имеет средний уровень защищенности.

9.2. Определение актуальных угроз безопасности персональных данных

Для оценки уровня исходной защищенности вводится коэффициент исходной защищенности Y1, который может принимать значения:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Следующим параметром, необходимым для определения актуальности угроз безопасности ПДн, является частота (или вероятность) реализации угрозы, под которой понимается определенный экспертным путем показатель, характеризующий вероятность реализации конкретной угрозы безопасности ПДн для ИСПДн в

реальных условиях ее функционирования. Вводится четыре значения этого показателя, обозначаемого как Y2:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации); средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны; высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты. Данный показатель принимает следующие значения:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Используя значения приведенных выше показателей Y1 и Y2, вычисляется коэффициент реализуемости угрозы Y, определяемый соотношением $Y = (Y1+Y2)/20$. В зависимости от своего значения этот коэффициент принимает значения:

$0 < Y < 0,3$ – реализуемость угрозы признается низкой; $0,3 < Y < 0,6$ – реализуемость угрозы признается средней; $0,6 < Y < 0,8$ – реализуемость угрозы признается высокой;

$Y > 0,8$ – реализуемость угрозы признается очень высокой.

Далее дается оценка опасности каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации. Данная оценка имеет три значения: низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

После просчета всех показателей производится оценка актуальности каждой угрозы безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице 2:

Реализуемость угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таблица 2 – Матрица расчета актуальности угроз безопасности ПДн

На основании положений модели угроз, модели нарушителя, данных об исходной защищенности ИСПДн (Y1), коэффициенте реализуемости угрозы (Y), вероятности ее реализации (Y2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы безопасности ПДн, обрабатываемых в ИСПДн. (Таблица 3)

Угроза безопасности ПДн	Вероятность реализации угрозы	Коэффициент реализуемости угрозы	Оценка опасности угрозы	Оценка актуальности угрозы
Разглашение, передача или утрата атрибутов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная

Нарушение правил хранения атрибутов разграничения доступа к ИСПДн	5	0,75	низкая	актуальная
Несообщение о фактах утраты, компрометации атрибутов разграничения доступа к ИСПДн	10	1,0	высокая	актуальная
Внедрение агентов в число персонала системы	0	0,5	высокая	актуальная
Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и	2	0,6	высокая	актуальная

т.п.)				
Ввод ошибочных данных	10	1,0	низкая	актуальная
Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств	5	0,75	высокая	актуальная
Игнорирование организационных ограничений (установленных правил) при работе с ПДн	10	1	средняя	актуальная

Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов ИСПДн	0	0,5	высокая	актуальная
Закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;	0	0,5	низкая	неактуальная
Хищение носителей	2	0,6	высокая	актуальная

информации, содержащих ПДн				
То же, внешний нарушитель	2	0,6	высокая	актуальная
Незаконное получение паролей и других реквизитов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная
То же, внешний нарушитель	2	0,6	средняя	актуальная
Несанкционированная модификация программного обеспечения	5	0,75	высокая	актуальная
То же, внешний нарушитель	2	0,6	высокая	актуальная
Перехват ПД, передаваемых по каналам связи	0	0,5	высокая	актуальная
То же, внешний нарушитель	0	0,5	высокая	актуальная
Несанкционированное копирование носителей информации с ПД	5	0,75	средняя	актуальная
То же, внешний нарушитель	2	0,6	средняя	актуальная

Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств	0	0,5	низкая	неактуальная
То же, внешний нарушитель	0	0,5	низкая	неактуальная
Непреднамеренное заражение компьютера вирусами	5	0,75	низкая	актуальная
Преднамеренное заражение компьютера вирусами	10	1,0	низкая	актуальная

Вмешательство в процесс функционирования ИСПДн , сетей общего пользования с целью несанкционированной модификации данных	5	0,75	высокая	актуальная
То же, внешний нарушитель	2	0,6	высокая	актуальная
Несанкционированное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей	10	1,0	средняя	актуальна я
То же, внешний нарушитель	5	0,75	средняя	актуальная
Неумышленное повреждения внешних кабельных систем связи	2	0,6	низкая	неактуальная
Возникновение пожаров в непосредственной близости к	2	0,6	высокая	актуальная

помещениям, в которых обрабатываются ПД и архивам ПД результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.				
Разрушение зданий, отдельных помещений	0	0,5	высокая	актуальная
Воздействие атмосферного электричества	5	0,75	низкая	актуальная
Возникновение стихийных очагов пожаров	2	0,6	низкая	неактуальная
Аварии в системах электропитания	5	0,75	низкая	актуальная
Нарушение температурного режима в помещениях с критическим оборудованием результате неисправности систем кондиционирования	5	0,75	средняя	актуальная
Аварии в системах отопления и водоснабжения в непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД	2	0,75	средняя	актуальная

Таблица 3 – Актуальность угроз безопасности ПДн