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

Организация информационной безопасности электронного архива персональных данных обучающихся в профессиональной 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:
77,7 % авторского текста

Работа рекомендована к защите
«26» 12 2025 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Куликова Наталья Алексеевна

Научный руководитель:
д.т.н., профессор
Дмитриев Михаил Сергеевич

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. В сегодняшней цифровой эпохе, когда все больше компаний переходят к использованию технологий для улучшения своей работы, образовательные организации также не остаются в стороне. Деятельность образовательной организации (далее – ОО), как любой сложной в управленческом плане структуры, сопровождается работой с большим количеством документов. Естественно, что эти документы требуют систематизированного учета, оперативного рассмотрения и исполнения, в которых участвуют различные подразделения. При этом при работе с бумажными документами неизбежно возникают трудности, связанные с большим объемом рутинного ручного труда, сопровождающего подготовку, оформление и передачу документов. Внедрение электронного документооборота (СЭД) становится важным шагом для совершенствования управленческих процессов и обмена информацией в образовательных организациях. Электронные архивы становятся неотъемлемой частью образовательного процесса, позволяя хранить и обрабатывать большие объёмы данных, таких как персональные данные обучающихся. Однако вместе с преимуществами электронных архивов возникает необходимость обеспечения их информационной безопасности.

Персональные данные — это личная информация о человеке, которая может включать в себя имя, адрес, номер телефона, электронную почту, паспортные данные и другие сведения. Они могут быть использованы в корыстных целях или стать причиной нарушения прав и свобод человека.

Цифровой архив поддерживает полный цикл электронного документооборота: от создания или оцифровки документа до постоянного хранения или уничтожения. Соблюдаются сроки хранения документов и архивные процедуры в соответствии с законодательством.

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных (далее - ПДн). Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов [6].

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

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

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

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

Информационная безопасность электронного архива персональных данных обучающихся — это комплекс мер, направленных на защиту конфиденциальной информации от несанкционированного доступа, использования, распространения, изменения или уничтожения.

В условиях цифровизации образования и активного использования электронных систем для хранения и обработки персональных данных обучающихся вопросы обеспечения информационной безопасности становятся приоритетными. Утечка или неправомерное использование таких данных может привести к серьёзным последствиям, включая

нарушение конфиденциальности, финансовые потери и репутационный ущерб для образовательных организаций.

Изучение научных работ М.В. Ларина, О.И. Рыскова, В.Ф. Янковой, М.П. Бобылевой, Т.В. Кузнецовой, Т.А. Быковой, А.В. Пшенко, С.Л. Кузнецова предоставляет богатый материал для детального анализа законодательной базы и нормативных документов в области документоведения и архивного дела, позволяет подробно изучить вопросы управления документами в организациях, обобщить практический и теоретический опыт проектирования, выбора, внедрения системы электронного документооборота, а также выработки рекомендаций о необходимости включения в требования к корпоративным СЭД параметров по организации хранения разных видов документов в электронном виде и системы их защиты.

Анализ литературы, обобщение существующего опыта, современные тенденции позволили сформулировать *проблему исследования*, заключающуюся в разрешении противоречия между актуальностью организации защиты электронного архива персональных данных обучающихся образовательной организации**,** объективными требованиями времени, такими как рост информационного потока и динамичность информационной среды и недостаточной теоретической и практической разработанностью, а также внедрение в образовательную среду электронного документооборота, что делает возможным распространение различных злоупотреблений, связанных с использованием вычислительной техники. Для противодействия им или хотя бы для уменьшения ущерба необходимо грамотно выбирать меры и средства обеспечения защиты информации от умышленного разрушения, несанкционированного доступа, чтения и копирования. Необходимо знание основных законодательных положений в этой области, организационных, экономических и иных мер.

Актуальность, теоретическая и практическая значимость решения обозначенной выше проблемы определили тему диссертационного исследования: «*Организация информационной безопасности электронного архива персональных данных обучающихся СПО*».

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

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

Предметом исследования является защита персональных данных.

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

Для достижения поставленной цели были сформулированы следующие *задачи:*

– раскрыть понятия «персональные данные», «электронный архив» и значение их защиты в образовательной организации;

– определить общие подходы к организации информационной безопасности электронного архива персональных данных обучающихся образовательных организаций;

– проанализировать состояние системы защиты информационной системы образовательной организации;

– разработать рекомендации по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации;

– оценить экономическую эффективность разработанных рекомендации по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации.

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы, законодательных и нормативно-правовых документов РФ по теме исследования; анализ и сопоставление имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты персональных данных; методы оценки экономической эффективности.

Научная новизна заключается в комплексном анализе эффективных методов и средств совершенствования информационной безопасности электронного архива персональных данных обучающихся в ГБПОУ «Южно-Уральский государственный технический колледж» в г. Челябинске и выработке рекомендаций для повышения системы защиты ПДн.

Практическая значимость работы заключается в разработке рекомендаций по организации системы защиты персональных данных электронного архива обучающихся в образовательной организации, разработанной на основе анализа частной модели угроз ГБПОУ «Южно-Уральский государственный технический колледж», которая может быть применена в других образовательных организациях СПО.

База исследования: Государственное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (Политехнический комплекс).

Апробация исследования: Куликова Н.А. Планирование мероприятий по защите персональных данных образовательных учреждений СПО / Н.

А. Куликова // Обеспечение комплексной безопасности общества и личности: проблемы и решения: Материалы участников VII Областной студенческой научно-практической конференции, ГБПОУ «ЮУГК», 07 мая 2024 г. – Челябинск: Издательский центр ГБПОУ «ЮУГК», 2024. – С. 301-304; Куликова Н.А. Защита персональных данных в образовательной организации / Н. А. Куликова // Национальная безопасность и молодёжная политика: вызовы современности: Сборник материалов молодежного форума Международной научно-практической конференции (16-18 апреля 2024 г., г. Челябинск). – Челябинск: Изд. ЗАО «Библиотека А. Миллера», 2024. – С. 49-53.

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

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

1.1 Понятие персональных данных и значение их защиты в образовательной организации

В настоящее время в Российской Федерации вопросы, связанные с защитой прав и свобод несовершеннолетних при обработке их персональных данных, в том числе и защиты прав на неприкосновенность частной жизни, личную и семейную тайну, регулируются:

- Конституцией Российской Федерации от 12 декабря 1993 г.;
- Федеральным законом от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Центральное место в системе российского законодательства в области персональных данных занимает Федеральный закон «О персональных данных», основанный на конституционных положениях, гарантирующих защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Данный закон закрепил статус и полномочия российского уполномоченного органа, условия осуществления государственного контроля и надзора, унифицировал правила сбора и обработки персональных данных физических лиц, а также правовые, организационные и технические меры, направленные на обеспечение защиты прав граждан при сборе и обработке их персональных данных. В Федеральном законе закреплены все общепризнанные Европейским сообществом принципы обработки персональных данных.

Кроме того, во исполнение отдельных положений Федерального закона «О персональных данных» был принят ряд подзаконных нормативных правовых актов:

- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

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

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

В рамках нашего исследования персональные данные рассматриваются, как различная информация, которая прямо или косвенно

относятся к определенному физическому лицу, т.е. субъекту персональных данных. В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Изменения, связанные с регулированием персональных данных (информации о личной жизни человека), происходят сейчас во многих государствах, в том числе и в России, и в первую очередь данная проблема затрагивает высшее образование […].

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

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

Основным нормативным документом, определяющим порядок работы с персональными данными в информационных системах и компьютерных сетях, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Согласно ст.3 этого закона «персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)».

Согласно 152 ФЗ все персональные данные подразделяются на три категории:

1. Общие персональные данные: фамилия, имя отчество, дата и место рождения, паспортные данные (номера, даты и места выдачи документов, удостоверяющих личность, в т.ч. СНИЛС), домашний адрес, номера телефонов, сведения об образовании. В настоящее время очень

многие сервисы привязаны к номеру мобильного телефона, поэтому он тоже относится к персональным данным.

2. Биометрические данные: информация о физиологических и биологических особенностях человека. Статья 11 152 ФЗ определяет их «Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность». Строго говоря, к биометрическим данным относится информация о росте и весе учащихся, но скорее всего, обработка этой информации обычным педагогическим работником не осуществляется. К биометрическим данным также относятся фотографические изображения, по которым можно определить биометрические параметры конкретного человека. Это фотоснимки лиц анфас, соответствующие по информативности фотографиям на документах, удостоверяющих личность.

3. Специальные категории персональных данных: информация о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Персональные данные специальных категорий не должны обрабатываться в информационных системах, кроме специально определяемых законом случаев.

Термин персональные данные, в свою очередь, тесно связан с понятием обработка. Обработка персональных данных начинается тогда, когда гражданин «свободно, своей волей и в своем интересе» (на что прямо указано в ч. 1 ст. 9 Федерального закона «О персональных данных») передает свои данные оператору для выполнения каких-либо функций (например, заключение трудового договора) или делает их общедоступными (например, регистрируясь в социальных сетях).

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

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

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

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

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

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

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

− обмен информацией между удаленными пользователями и веб-сайтом образовательной организации;

− передача удаленным пользователем своих идентификационных данных программистам образовательной организации;

− обмен данными пользователя с сервером информационных систем образовательной организации;

− авторизация пользователя;

− шпионские программы, внедренные в информационную систему образовательной организации.

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

− слабые пароли, которые создают удаленные пользователи;

− уязвимость каналов передачи персональных данных;

− вредоносное программное обеспечение;

− непрофессиональная конфигурация сети передачи персональных данных;

− уязвимости средств и мер защиты […].

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

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

− внедрение современных мер защиты персональных данных;

− организация системы всесторонней защиты персональных данных.

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

1.2 Обеспечение защиты персональных данных обучающихся в условиях информационной открытости образовательных организаций

Сфера защиты данных юридически регулируется информационным правом (одной из подотраслей административного права), нормы которого прописаны в нескольких законодательных актах. Один из основных — Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных», цель которого заявлена как «общее обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных», таких как право на неприкосновенность частной жизни, личную и семейную тайну.

Реализация мер по защите персональных данных — это зона ответственности оператора, т. е. субъекта, осуществляющего сбор и обработку данных в информационной системе.

В образовательной организации при осуществлении образовательной деятельности повседневно обрабатываются персональные данные обучающихся, относящиеся к различным категориям данных. Эти персональные данные включают:

1. Общие персональные данные обучающихся, в т.ч. паспортные данные и данные о месте проживания, доступные широкому кругу работников образовательной организации.
2. Данные об успеваемости, текущих и итоговых оценках, прохождении учебного плана.
3. Фотографии обучающихся, позволяющие установить их личность (относятся к биометрическим данным).
4. Данные о здоровье (медицинская карта, карта прививок) – относятся к специальной категории персональных данных, должны обрабатываться отдельно лицом, имеющим допуск к медицинской документации (врачом, медсестрой, медрегистратором).

5. В определенных случаях родители (законные представители) обучающегося представляют в образовательную организацию документы, содержащие сведения, необходимые для предоставления учащемуся гарантий и компенсаций, установленных действующим законодательством: документы о составе семьи; документы о состоянии здоровья; документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством. Все эти документы должны быть категорированы в соответствии с 152 ФЗ и доступ к ним должен быть ограничен конкретным перечнем сотрудников образовательной организации.

Работники, имеющие доступ к персональным данным обучающегося, обязаны:

1. Не сообщать персональные данные обучающегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется.

2. Использовать персональные данные обучающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя).

3. Обеспечить защиту персональных данных обучающегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации.

4. Ознакомить родителя или законного представителя с их правами и обязанностями в области защиты персональных данных, под роспись.

5. Соблюдать требование конфиденциальности персональных данных учащегося.

6. Исключать или исправлять по письменному требованию одного из родителей (законного представителя) обучающегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства.

7. Ограничивать персональные данные обучающегося при передаче уполномоченным работникам правоохранительных органов или работникам органов управления образованием только той информацией, которая необходима для выполнения указанными лицами их функций.

8. Обеспечить совершеннолетнему обучающемуся или одному из родителей (законному представителю) несовершеннолетнего обучающегося свободный доступ к персональным данным обучающегося, включая право на получение копий любой записи, содержащей персональные данные.

9. Предоставить по требованию одного из родителей (законного представителя) обучающегося полную информацию о его персональных данных и обработке этих данных в образовательной организации.

В соответствии со статьей 21 Федерального закона от 29.12.2012 N 273-ФЗ (в редакции от 30.04.2021) «Об образовании в Российской Федерации» «образовательные организации формируют открытые и общедоступные информационные ресурсы, содержащие информацию об их деятельности, и обеспечивают доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети «Интернет»». Однако, указанная статья закона «Об образовании», устанавливая обязательный перечень размещаемой образовательной организацией информации, не предполагает публикации в сети персональных данных обучающихся (в отличие от персональных данных педагогических сотрудников и руководства образовательной организации). Поэтому недопустима публикация в сети в открытом доступе любых списков (групп, приглашенных на мероприятие или собеседование, принятых на обучение и т.п.). Подобное информирование может быть осуществлено либо посредством электронной почты, либо с использованием закрытых информационных систем, прежде всего электронного журнала.

Любая образовательная организация гордится успехами своих обучающихся и с удовольствием рассказывает о победах студентов на олимпиадах, спортивных соревнованиях, конкурсах. Тем не менее, в соответствии с законодательством о защите персональных данных, такая информация, содержащая персональные данные, должна публиковаться только с письменного согласия субъекта персональных данных (в случае несовершеннолетнего обучающегося – родителя/законного представителя). В случае публикации биометрической фотографии, это должно быть специально отражено в согласии. В случае отзыва согласия на публикацию со стороны субъекта персональных данных, информация должна быть немедленно удалена с общедоступного информационного ресурса. В случае отсутствия согласия субъекта персональных данных на публикацию, образовательная организация может опубликовать обезличенную информацию, например, указать только личное имя обучающегося и опубликовать коллективное фото победившей команды без указания отдельных участников.

Также допустима публикация на сайте без получения согласия родителей (законных представителей) обучающихся репортажных фотографий общего плана, без указания персональных данных обучающихся, запечатленных на фото.

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

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от: неправомерного или случайного доступа к ним; уничтожения; изменения;

блокирования; копирования; предоставления; распространения; иных неправомерных действий в отношении персональных данных.

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

Пакет документов для проверки:

1. Концепция информационной безопасности.
2. Приказ о создании СЗ ПДн.
3. План мероприятий по обеспечению защиты ПДн.
4. Отчет о результатах проведения внутренней проверки.
5. Перечень сведений, составляющих ПДн.
6. Список ИСПДн, в которых обрабатываются ПДн.
7. Разрешительная система доступа к ПДн.
8. Перечень сотрудников, допущенных к обработке ПДн.
9. Перечень защищаемой информации.
10. Положение по обработке персональных данных.
11. Политика ИБ.
12. Инструкция пользователя ИСПДн.
13. Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.
14. Инструкция администратора ИБ ИСПДн.
15. Инструкция по организации парольной защиты.
16. Инструкция по антивирусной защите.
17. Инструкция по обработке ПДн без использования средств автоматизации.
18. Перечень ПДн с местами хранения, обработки и списком допущенных лиц.
19. Приказ о введении в действие документов, регламентирующих мероприятия по защите ПДн.
20. Приказ о создании комиссии по уничтожению ПДн.

21. Журнал регистрации фактов несанкционированного доступа.

22. Журнал учета обращений субъектов ПДн в ИСПДн.

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

24. Журнал учета мероприятий по контролю ИБ.

25. План проверочных мероприятий по обеспечению безопасности ПДн.

26. АКТ 1 классификации ИСПДн.

27. Приказ о назначении администратора ИБ.

28. Форма согласия работника на обработку его ПДн.

Организация защиты персональных данных должна производиться в несколько этапов:

- инвентаризация информационных ресурсов;
- ограничение доступа работников к персональным данным;
- документальное регламентирование работы с персональными данными;
- формирование модели угроз безопасности персональных данных;
- классификация информационных систем персональных данных (ИСПДн) образовательных организаций;
- составление и отправка в уполномоченный орган уведомления об обработке персональных данных;
- приведение системы защиты персональных данных в соответствие с требованиями регуляторов;
- создание подсистемы информационной безопасности ИСПДн и ее аттестация (сертификация) – для ИСПДн классов К1, К2;
- организация эксплуатации и контроля безопасности ИСПДн.

Этап 1. Инвентаризация информационных ресурсов.

Инвентаризация информационных ресурсов - выявление присутствия и осуществления обработки персональных данных во всех эксплуатируемых в организации информационных системах и

традиционных хранилищах данных. В качестве информационных систем, относящихся к ИСПДн, могут выступать: электронный журнал (Сетевой город. Образование); 1С:Бухгалтерия; автоматизированная информационная библиотечная система и другие.

На данном этапе следует:

- утвердить положение о защите персональных данных;
- сформировать концепцию, определить политику информационной безопасности;
- составить перечень персональных данных, подлежащих защите.

Места обработки персональных данных**:** бухгалтерия; библиотека; предметно-цикловые комиссии; отдел кадров.

Этап 2. Ограничение доступа работников к персональным данным.

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

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

Этап 3. Документальное регламентирование работы с персональными данными.

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

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

На данном этапе следует:

– собрать согласия на обработку персональных данных;

– издать приказ о назначении лиц, ответственных за обработку ПДн;

– издать положение о разграничении прав доступа к обрабатываемым ПДн;

– составить инструкции администратора ИСПДн, пользователя ИСПДн и администратора безопасности ИСПДн.

Согласия на обработку персональных данных физических лиц.

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

– фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

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

– наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

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

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

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

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

– подпись субъекта персональных данных.

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

Этап 4. Формирование модели угроз безопасности персональных данных.

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

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

По видам возможных источников угроз безопасности ПДн выделяются следующие классы угроз:

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

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

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

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

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

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

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

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

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

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

По способам реализации УБПДн выделяются следующие классы угроз:

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

− угрозы утечки ПДн по техническим каналам утечки информации;

− угрозы специальных воздействий на ИСПДн [39].

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

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

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

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

По используемой уязвимости выделяются следующие классы угроз:

− угрозы, реализуемые с использованием уязвимости системного ПО;

− угрозы, реализуемые с использованием уязвимости прикладного ПО;

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

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

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

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

− угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

− угрозы безопасности ПДн, обрабатываемых на АРМ;

− угрозы безопасности ПДн, обрабатываемых в выделенных

средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

− угрозы безопасности ПДн, передаваемых по сетям связи;

− угрозы прикладным программам, с помощью которых обрабатываются ПДн;

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

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

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

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

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

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

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

Этап 5. Классификация ИСПДн.

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

Этап 6. Составление и отправка в уполномоченный орган уведомления.

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

Этап 7. Приведение системы в соответствие с требованиями регуляторов.

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

На данном этапе следует:

– создать перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– создать положение о подразделении по защите информации;

– подготовить методические рекомендации для организации защиты информации при обработке персональных данных;

– создать инструкцию пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций;

– утвердить план мероприятий по защите ПДн.

Этап 8. Аттестация (сертификация) ИСПДн.

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

На данном этапе следует:

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

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

– определить порядок резервирования технических средств защиты информации.

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

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

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

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

Перечень объектов информатизации, подлежащих аттестации.

Обязательной аттестации подлежат следующие объекты информатизации:

1. Автоматизированные системы различного уровня и назначения.

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

3. Системы отображения и размножения.

4. Помещения, предназначенные для ведения конфиденциальных переговоров.

Этап 9. Организация эксплуатации ИСПДн и контроля за безопасностью.

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

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

На данном этапе следует:

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

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

Поддержание эффективной системы защиты ПДн.

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

1. Развертывание полноценной системы обработки ПДн.

2. Полномасштабное внедрение средств защиты.

3. Аттестация ИСПДн.

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

5. Реакция на регулярные проверки и прочее.

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

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

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

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

Образовательная организация при осуществлении деятельности взаимодействует с большим количеством сторонних организаций. Это прежде всего органы управления образованием, а также органы Роспотребнадзора, соцзащиты, медицинские организации и т.д. Всем им периодически необходимо передавать какие-то персональные данные обучающихся. Так как согласие на передачу персональных данных родители обучающихся дают образовательной организации, то эти сторонние организации выступают в качестве третьих лиц в отношениях субъектов персональных данных с образовательной организацией. Образовательная организация должна включить организации, в которые регулярно передаются персональные данные, в текст согласия на обработку персональных данных, которое дается родителями учащегося при зачислении в образовательную организацию. В случае, если персональные данные надо передать организации, не включенной в этот перечень, следует получить согласие субъекта персональных данных на конкретную передачу данных.

При использовании электронных коммуникаций для передачи персональных данных, необходимо пользоваться специализированными информационными системами, такими как портал госуслуг, электронный журнал/дневник, система ведомственного электронного документооборота

и подобными. В частности, в каждой образовательной организации существует специальный компьютер с доступом к защищенному каналу связи с региональным центром обработки информации (РЦОИ) по которому передаются персональные данные участников государственной итоговой аттестации.

Следует избегать отправки персональных данных в открытом (на зашифрованном) виде по электронной почте, даже внутри корпоративной почтовой сети.

Специальные персональные данные (медицинская информация) должны обрабатываться и передаваться либо на бумажных носителях, либо внутри специализированных информационных систем, имеющих соответствующий уровень защиты и прошедших сертификацию (система электронных медкарт).

При использовании облачного хранения данных и документов общего доступа (мультипользовательских) для обработки персональных данных, надо быть уверенным, что не происходит трансграничной передачи данных. При использовании глобальных информационных сервисов (например, документов Google) такая трансграничная передача возможна, что создает риск нарушения образовательной организацией российского законодательства о защите персональных данных.

При передаче данных ответственность несет тот, кто данные передает, поэтому абсолютно недопустимо передавать любые персональные данные в ситуации, когда нет полной уверенности в том, что они попадут к надлежащему получателю. (Например, недопустимо отправлять персональные данные на электронный адрес на общедоступном почтовом сервисе (mail.ru, yandex.ru и т.п.), если нет абсолютной уверенности, что адрес администрируется надлежащим получателем).

Наиболее массовой системой обработки персональных данных в образовательной организации является электронный журнал/дневник. Педагогические работники обязаны предотвращать риски

несанкционированного доступа к данным электронного журнала, соблюдая следующие правила:

1. Использовать для входа в электронный журнал сильный пароль (не менее 8 символов, включая цифры и клавиатурные знаки) который периодически менять.

2. Не использовать в качестве пароля легко подбираемые комбинаторно или с помощью социальной инженерии символы (подряд идущие буквы алфавита, цифры даты рождения и т.п.).

3. Не хранить пароль для автозаполнения на общедоступном компьютере (на компьютере в учительской). Пользоваться автозаполнением паролей можно только на личном ноутбуке при условии непрерывного контроля над устройством со стороны владельца.

4. На школьных стационарных компьютерах установить систему индивидуальных профилей для каждого пользователя с обязательным блокированием входа (необходимостью повторного ввода пароля) через непродолжительное время отсутствия активности.

5. В случае использования для работы с информационной системой общедоступных компьютеров, включать режим «инкогнито», предполагающий уничтожение всех файлов cookie, очистку кэша и выход из всех аккаунтов при закрытии браузера.

6. Входить в информационные системы, содержащие персональные данные, только на компьютерах с установленными актуальными антивирусными системами.

7. В целях защиты персональных данных от компрометации не допускать заполнение электронного журнала неавторизованными лицами, прежде всего обучающимися.

Соблюдение этих правил, регулярное обновление паролей и антивирусных программ, очистка кэша и истории браузера позволит обеспечить надлежащий барьер несанкционированному доступу к персональным данным и конфиденциальной информации.

1.3 Общие подходы к организации информационной безопасности электронного архива персональных данных обучающихся образовательных организаций

Электронный документооборот – все более популярная форма процессов, связанных с ведением документации, во многих организациях. При этом сотрудники непросто иногда отправляют документы таким образом, они ежедневно используют на своих рабочих местах большую часть функционала систем ЭДО. В процессе ЭДО имеется одно (заключительное) звено, которое во многих организациях зачастую не развито в нужной мере, за что сегодня многие уже расплачиваются, сталкиваясь с хаосом – это проблема хранения накопленных документов.

Грамотное организованное хранение документов, содержащих персональные данные**,** — залог того, что конфиденциальная информация о сотрудниках, обучающихся и в целом деятельности образовательной организации не попадет в руки посторонних лиц. Ответственность за определение правил, места размещения и защиты информации ложится, согласно закону, на работодателя, однако не все четко понимают, о каких нюансах нужно позаботиться. Добавляют сложностей постоянные дополнения и корректировки нормативно-правовых актов, которые приходится отслеживать, чтобы не получить штраф и не попасть в эпицентр скандала, связанного с распространением личных сведений граждан.

Для того чтобы гарантировать сохранность и секретность ПДн, необходимо:

1. Четко определить условия хранения персональных данных на бумажных носителях и в электронном виде. Речь идет не только о месте, но и установлении режима доступа туда для разных категорий сотрудников.

2. Выбрать людей, которые будут отвечать за конкретные аспекты, связанные с сохранением информации.

3. Провести разъяснительную работу с персоналом, объяснив степень важности ограничений и правил использования ПДн в рамках профессиональной деятельности, а также дав четкие инструкции, как действовать в той или иной ситуации.

4. Продумать средства защиты для сейфов, шкафов с замками, а также заняться внедрением специализированного программного обеспечения.

Основная нагрузка по работе с ПДн ложится на плечи отдела кадров, бухгалтерии и учебных частей поэтому его работники должны иметь точное представление о том, что и как делать для предупреждения несанкционированного доступа. Законодательной базой является Конституция, ФЗ-152, ФЗ-149, Трудовой Кодекс и другие нормативные акты. Особое внимание должно уделяться срокам хранения, передачи и обработки персональных данных. На сегодняшний день правовые нормы определяют следующие требования:

- 3 года организация имеет право и обязано хранить заявления о трудоустройстве либо увольнении, письма с рекомендациями, автобиографии, указы о переводе на другую должность, анкеты;
- на протяжении пяти лет сохраняются докладные, служебные записки, командировочные листы, разнообразные справки (которые не включаются в личное дело), а также приказы и выписки;
- финансовая информация (связанная с выдачей зарплаты, премиальных, пособий, стипендия и т.д.) находится в архиве 75 лет.

Существует разница между сроком действия согласия на обработку ПДн и длительностью сохранения самих данных.

Хранение персональных данных — это процесс, регулируемый законодательством, решением владельца и целями использования

сведений. ФЗ-152 закрепляет обязанность оператора сразу после достижения цели обработки обезличить и уничтожить полученные данные.

Все работники, как штатные, так и внештатные, которые работают с личными сведениями, должны подписать соглашение о неразглашении. Типовой документ необходимо предварительно адаптировать под особенности деятельности образовательной организации.

Выделяют сведения о субъектах, сохраняемые в бумажном и электронном виде. Каждый вариант есть свои плюсы, минусы и особенности. Нередко информация дублируется для эффективного выполнения рабочих задач и в целях безопасности.

Бумажный архив по сей день сохраняется во многих организациях и имеет массу недостатков, которые легко решить внедрением электронного хранения документации (при этом, перевод бумажного архива в цифровую форму – сама по себе огромная проблема) (таблица 1).

Эти и другие недостатки стандартного архива делают его ведение устаревшим процессом, который давно пора заменить электронным архивом.

Электронный архив представляет собой хранилище, в котором из ЭДО или прочих цифровых источников поступает поток документации, который по определенным правилам разбивают, организуя учет и архивирование документов.

Правила регламентируются организацией, ее локальными нормативными актами и ГОСТ Р 54989-2012/ISO/TR 18492.

К основным функциям электронного архива:

– хранение личных дел, включая копии документов, результаты успеваемости, медицинские справки и другие материалы;

– удобный поиск и фильтрация данных по различным критериям;

– обмен информацией между различными подразделениями учебного заведения;

– обеспечение безопасности и конфиденциальности персональных данных.

Преимущества использования электронного архива включают:

– оптимизацию работы с документами;

– сокращение времени на поиск информации;

– повышение уровня информационной безопасности;

– снижение риска потери или повреждения данных.

Организация архива электронных документов:

– локальный архив – хранение документов в электронном виде на сервере пользователя;

– облачное хранилище – хранение документов в электронном виде на стороннем сервере и организация доступа через Интернет;

– хранилище системы ЭДО и архива – хранение документов у провайдера ЭДО. Организация и доступ оговариваются с провайдером.

Преимуществами электронного архива являются:

1. Простота и скорость работы с архивом, обусловленные доступностью любого документа за любой период в несколько кликов. Все документы хранятся в единой базе.

2. Облегчается и ускоряется поиск документов для ответа на многочисленные требования проверяющих органов.

3. Надежность и безопасность. Организация электронного архива происходит таким образом, что доступ на запись и изменение файлов, по сути, имеет только автоматизированная система, а пользователям доступно только чтение документов. Хранение документации выполняется на носителе информации, с которого создаются резервные копии на других носителях, при этом сервера должны находиться на разных (физически) машинах. Если каким-то образом сгорит или будет затоплен один сервер, то всегда есть его резервная копия, которую нетрудно было сделать. Также отсутствует возможность несанкционированного доступа к данным, поскольку работает система разграничения доступа и прав.

4. Эффективность работы. Архив электронного вида позволяет не только структурировать, но и сортировать документы относительно явных признаков, например, дата, наименование и пр.

5. Возможность масштабирования. В случае с электронным архивом достаточно приобрести дополнительный носитель информации и подключить его к системе архивирования. При этом для некоторых документов можно задавать «срок годности», после истечения которого они будут автоматически стерты.

6. Отсутствие необходимости в помещениях. В отличие от архива с бумажными носителями с ростом электронного архива не требуется расширения помещений, а значит организация получает большую экономию, сумму которой можно рассматривать как часть прибыли при переводе с бумажного варианта архива на электронный.

На рисунке 2 представлена общая схема цифрового архива в организации.

Электронное хранение предполагает создание защищенных ИСПДн, которые в автоматическом режиме фиксируют и обрабатывают большие массивы данных. В таком случае не нужно много места или закупки закрывающихся шкафов и сейфов, а отыскать интересующие сведения можно за пару секунд, к тому же при серьезном подходе к обеспечению защиты нет риска кражи или утечки ПДн. Из недостатков следует отметить наличие затрат на оснащение современным программным обеспечением, потребность в постоянном создании резервных копий, а также регулярное обновление оборудования.

Правила хранения персональных данных на бумажных носителях предполагают размещение личных дел в сейфах в алфавитном порядке в зависимости от регистрационного номера. Остальные сведения размещаются согласно внутреннему регламенту, то есть работодатель может сам выбрать место для папок-накопителей, определить ответственных за безопасность сотрудников и установить ограничение доступа. К плюсам бумажных носителей можно отнести оптимизацию учета ПДн, минимальное время поиска информации. К минусам можно отнести существенные финансовые расходы на сейфы, необходимость дополнительного обучения новых сотрудников отдела кадров, потребность в большом свободном и защищенном пространстве (если образовательная организация большая и личных дел много).

Документ преимущественно составляют по шаблону, внося некоторые корректировки в зависимости от формы, способа фиксации ПДн и других особенностей деятельности организации. Основные разделы:

- общие положения;
- способы выявления и профилактики несанкционированного доступа и распространения ПДн;
- цели обработки и содержание хранимой личной информации;
- категории субъектов;
- сроки обработки и сохранения сведений;

– механизм уничтожения информации;

– ответственность за нарушение правил.

После внедрения правил хранения персональных данных в информационных системах и на бумажных носителях необходимо убедиться в том, что:

– уровень защиты достаточно высокий и соответствует актуальным угрозам;

– все сотрудники дали согласие на совершение операций с личными сведениями;

– принятые локальные акты соответствуют федеральному законодательству;

– содержание внутреннего документа, регулирующего хранение и обработку ПДн, донесено до персонала (каждый должен поставить подпись).

Для предотвращения угроз, связанных с использованием персональных данных, необходимо разработать и внедрить комплекс мер по обеспечению информационной безопасности электронного архива.

Выводы по 1 главе

В первой главе были рассмотрены понятие персональных данных и значение их защиты в образовательной организации. Была изучены обеспечение защиты персональных данных обучающихся в условиях информационной открытости образовательных организаций, описаны общие подходы к организации информационной безопасности электронного архива персональных данных обучающихся образовательных организаций.

Персональные данные – это любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу – субъекту персональных данных. Реализация мер по защите персональных данных — это зона ответственности оператора, т. е.

субъекта, осуществляющего сбор и обработку данных в информационной системе.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя: контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией; разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн.

Грамотное организованное хранение документов, содержащих персональные данные**,** — залог того, что конфиденциальная информация о сотрудниках, обучающихся и в целом деятельности образовательной организации не попадет в руки посторонних лиц. Ответственность за определение правил, места размещения и защиты информации ложится, согласно закону, на работодателя, однако не все четко понимают, о каких нюансах нужно позаботиться. Добавляют сложностей постоянные дополнения и корректировки нормативно-правовых актов, которые приходится отслеживать, чтобы не получить штраф и не попасть в эпицентр скандала, связанного с распространением личных сведений граждан.

.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ВЫБОРУ СРЕДСТВ ЗАЩИТЫ ЭЛЕКТРОННОГО АРХИВА ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Анализ защиты персональных данных образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В качестве объекта защиты было выбрано Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж». Местонахождение главного учебного корпуса: 454007, г. Челябинск, ул. Горького, 15. Учебного комплекса №2: 454007, г. Челябинск, ул. Грибоедова, д. 45. Машиностроительного комплекса: г. Челябинск, ул. Марченко, д. 33. Политехнического комплекса: г. Челябинск, ул. Гагарина, д. 7.

В колледже реализуются образовательные программы среднего профессионального образования, основные программы профессионального обучения, дополнительные общеобразовательные и профессиональные программы, услуги по содержанию и воспитанию обучающихся в общежитии, организация и проведение мероприятий в сфере образования и науки.

Основные задачи колледжа определяются в соответствии с нормативно-правовыми актами Российской Федерации и реализуются в соответствии с Уставом колледжа [37]:

– удовлетворение потребностей граждан в получении профессионального образования в избранной профессиональной деятельности, в интеллектуальном, культурном, физическом и нравственном развитии;

– удовлетворение потребностей общества в профессионально подготовленных специалистах, создании новых рабочих мест;

– профессиональная переподготовка и повышение квалификации специалистов и рабочих;

– распространение знаний среди населения, повышение его общеобразовательного и культурного уровня, в том числе путем оказания платных образовательных услуг.

В своей образовательной деятельности колледж использует наиболее эффективные технологии обучения и воспитательные системы.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет, без ограничения времени и потребленного трафика.

Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль). Предоставление доступа осуществляется системным администратором колледжа.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте колледжа.

В ходе учебного процесса применяются дистанционные образовательные технологии с использованием таких систем как e.lanbook.ru, moodle, dom.sustec.ru.

Для осуществления дистанционной образовательной деятельности, размещения информации о предстоящих и прошедших мероприятиях и информирования студентов об актуальных событиях у ГБПОУ «Южно-Уральский государственный технический колледж» имеется собственный сайт (режим доступа: https://sustec.ru), отвечающий всем требованиям к подобным ресурсам образовательных организаций.

Педагогическим работникам обеспечивается доступ к следующим электронным базам данных: корпоративная информационная система; информационные справочные системы; поисковые системы.

Корпоративная информационная система состоит из пяти уровней:

1. Информационно-логический уровень представляет собой совокупность потоков данных и узлов возникновения, потребления и модификации информации. Уровень представляется в виде информационно-логической модели, на основании которой разрабатываются структуры баз данных, системные соглашения и организационные правила для обеспечения взаимодействия компонентов прикладного программного обеспечения.

2. Прикладной уровень представляет собой совокупность прикладных программ и программных комплексов, которые обеспечивают реализацию функций корпоративного управления. Наиболее развитые корпоративные информационные системы используют следующие прикладные программные средства:

– программные комплексы корпоративных информационных систем (1С: Предприятие 8.0, Галактика, Парус, Босс-Корпорация и др.);

– системы управления базами данных (СУБД) и программные средства для работы с хранилищами данных (MS SQL Server, Oracle, Pervasive SQL);

– программные средства для организации корпоративного управления, интерактивного общения, совместного использования справочников и документальных баз данных;

– программные средства управления документооборотом;

– программные средства календарного планирования;

– программные комплексы для ведения конструкторских работ (САПР);

– программные средства электронного офиса (MS Qffice);

– специальные системы бизнес-планирования и анализа (Project Expert, Audit Expert, Marketing Expert);

– информационно-аналитические системы (Deductor).

3. Системный уровень описывает операционные системы и сетевое программное обеспечение, которые составляют рекомендуемое программное окружение для программного комплекса корпоративных информационных систем.

4. Аппаратный уровень описывает средства вычислительной техники, требования к конфигурации серверов, рабочих станций.

5. Транспортный уровень определяет активное и пассивное сетевое оборудование, сетевые протоколы и технологии [4].

К Южно-Уральскому государственному техническому колледжу относятся различные информационные системы, которые используются для управления образовательным процессом и обеспечения коммуникации между преподавателями и студентами:

1. Система электронного документооборота – используется для обмена документами между участниками образовательного процесса.

2. Система электронного расписания – позволяет студентам и преподавателям получать доступ к расписанию занятий и изменениям в нем.

3. Система электронной почты – обеспечивает коммуникацию между преподавателями и студентами.

4. Система дистанционного обучения – позволяет студентам получать доступ к учебным материалам и заданиям в любое время и из любого места.

5. Система управления базами данных – используется для хранения и управления информацией о студентах, преподавателях и учебных материалах.

6. Система электронной библиотеки – позволяет студентам получать доступ к электронным версиям учебников и научных статей.

Согласно исследованию, защита данных информационных систем является необходимым условием при организации управления образовательным процессом и коммуникации.

Сетевой Город. Образование – комплексная автоматизированная информационная система, объединяющая в единую сеть образовательные учреждения и органы управления образования в пределах города, сельского или городского района (округа). Тем самым формируется единое информационное образовательное пространство муниципального образования**.**

Права доступа к информации разграничены и гибко настраиваются. Каждый пользователь образовательной организации (директор, зам. директор, обучающийся, преподаватели и т.д.) и родители обучающихся имеют индивидуальные имя и пароль и могут входить в систему с любого компьютера, подключенного к муниципальной сети (или сети Интернет). Например, находясь дома или на работе, родитель может отслеживать успеваемость и посещаемость, общаться с преподавателями и администрацией образовательной организации; обучающийся может удалённо получать домашние задания, просматривать свой электронный дневник и расписание, и т.д.

Параллельно, в реальном времени к обобщённой информации по ОО имеют доступ и специалисты органов управления образования для формирования статистических и иных отчетов в рамках своей компетенции, не требуя от руководителей ОО отдельных отчетов с последующей работой по своду информации.

Федеральные нормативные правовые акты:

1. Федеральный закон от 07.07.2010 г. №210 - ФЗ Об организации предоставления государственных и муниципальных услуг.

2. Распоряжение Правительства РФ от 17.12.2009 г. № 1993-р. Свободный перечень первоочередных государственных и муниципальных услуг.

3. Постановление Правительства РФ от 24.10.2011 г. №861 О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций).

4. Методические рекомендации по работе с документами в СПО.

5. Письмо МОиН Российской Федерации от 15 февраля 2012 г. № АП -147/07 О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде.

6. Методические рекомендации Системы ведения журналов успеваемости обучающихся в электронном виде в образовательных учреждениях Российской Федерации.

Региональные нормативные правовые акты:

1. Распоряжение Губернатора Челябинской области от 01.11.2010 г. №732-р «О плане мероприятий по реализации Федерального закона «Об организации предоставления государственных и муниципальных услуг».

2. Постановление Правительства Челябинской области от 13.12.2010 г. №293-П «О Порядке разработки и утверждения административных регламентов предоставления государственных услуг органами исполнительной власти Челябинской области».

3. Распоряжение Правительства Челябинской области от 11.11.2010 г. №331-рп «О Плане перехода на предоставление в электронном виде государственных услуг органами исполнительной власти Челябинской области и государственными учреждениями Челябинской области».

4. Постановление Правительства Челябинской области от 29.06.2011 г. №209-П «О Плане мероприятий по развитию информационного общества и формированию электронного правительства в Челябинской области на 2011-2013 годы».

5. Распоряжение Губернатора Челябинской области от 06.06.2011 г. №549-р «О перечне государственных услуг (функций) органов исполнительной власти Челябинской области».

6. Приказ Министерства образования и науки Челябинской области от 28.07.2016 г. № 01/2445 «О вводе в эксплуатацию автоматизированной системы «Образование Челябинской области»».

7. Приказ Министерства образования и науки Челябинской области от 25.09.2017 г. № 01/2866 «Об утверждении положения об автоматизированной информационной системе «Образование Челябинской области».

С целью формирования на территории Челябинской области единой информационно-образовательной среды, обеспечивающей автоматизацию деятельности Министерства образования и науки Челябинской области; органов местного самоуправления, осуществляющих управление в сфере образования, и образовательных организаций, организацию электронного взаимодействия всех участников образовательных отношений в 2016 году введена в эксплуатацию автоматизированная информационная система «Образование Челябинской области» (АИС «Образование»).

В состав АИС «Образование» входит АИС «Сетевой город. Образование» – модульная комплексная информационная система, предназначенная для предоставления электронных средств поддержки и сопровождения образовательной деятельности образовательных организаций, реализации государственных и муниципальных услуг в электронном виде в сфере образования, а также являющаяся инструментом сетевого взаимодействия между всеми участниками образовательных отношений и интеграции в единую сеть образовательных организаций и органов управления образованием.

АИС «Сетевой город. Образование» содержит комплект модулей, охватывающих управленческую деятельность муниципальных органов управления образованием, а также образовательную деятельность:

– дошкольных образовательных организаций.

– общеобразовательных организаций.

– организаций дополнительного образования.

– профессиональных образовательных организаций.

Модуль «Профессиональная образовательная организация» (АИС ПОО) предназначен образовательных организаций, осуществляющих образовательную деятельность по образовательным программам среднего профессионального образования и (или) по программам профессионального обучения.

Полное наименование системы: автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация». Условное обозначение системы: АИС «Сетевой Город. Образование», модуль ПОО.

Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.

Модуль предоставляет инструменты для управления: расписанием звонков, занятий, сессий; журналами текущей успеваемости, итоговой и промежуточной аттестации, а также аттестации профессиональной деятельности; курсовыми работами; движением обучающихся - зачислением, выбытием, переводом, оформлением академических отпусков и т.д.; списком дисциплин и рабочими программами по дисциплинам; образовательными программами и учебными планами; учебными календарями и календарно-тематическими планами; списками сотрудников, студентов, абитуриентов и родителей; списками учебных отделений и групп; должностями и правами доступа пользователей; статистической отчётностью и отчётностью по успеваемости и посещаемости обучающихся.

Внедрение данного модуля позволит:

– повысить качество профессионального образования и достичь новых образовательных результатов;

– автоматизировать управление системой профессионального образования и принимать обоснованные управленческие решения;

– оказывать государственные и муниципальные услуги в электронном виде в сфере образования;

– создать единое информационное пространство для взаимодействия всех участников образовательных отношений.

Установка серверов или какого-либо программного обеспечения в самих образовательных организациях не требуется. Права доступа к информации разграничены, каждый пользователь имеет доступ только к той информации, которую ему определил администратор системы.

Рассмотрим основные моменты организации учебного процесса в Системе пользователями.

1) Работа с Системой начинается с создания данных об образовательной организации.

Указывается:

1. Основная контактная информация, отражающая актуальные данные местонахождения ОО, статуса учреждения, телефоны для связи и ФИО руководителя.

2. Реквизиты, идентифицирующие учёт в налоговых органах.

3. Корпуса и аудитории, позволяющие в последующем составлять расписания занятий с учётом направлений, смен и расположения аудиторий в различных корпусах.

2) Пользователи - это следующий раздел при работе с Системой. Работа с этим меню заключается в создании данных по пунктам:

– права доступа, разграничивающие разрешение или запрещение тех или иных полномочий (например, при планировании обучения);

– должности, помогают определить кадровый состав учреждения и присвоить права доступа для последующей работы пользователей в Системе;

– Студенты, Сотрудники, Абитуриенты. Данная информация помогает в последующем вести учет пользователей, управлять группами обучения, учебными отделениями, рабочими программами дисциплин, расписаниями занятий и сессий, журналами успеваемости, сведениями промежуточной и итоговой аттестации, осуществлять контроль документооборота в части касающейся приказов и составлять отчеты.

3) Обучение. После формирования пользователей Системы следует создать учебный календарь, который необходим для организации и упорядочивания учебного процесса. Разработав учебный календарь, необходимо перейти к созданию справочника учебных дисциплин. Этот список является основой для формирования учебных планов, которые в свою очередь определяют состав учебных предметов, последовательность их изучения и общий объем отводимого на это времени.

Образовательная программа создается в виде справочника. Это форма, в которой перечисляются основные характеристики (специальность, форма обучения, база приёма, уровень подготовки, срок обучения и тип учебного периода). Сведения образовательной программы взаимоувязаны с пунктом меню Учебные группы.

Подраздел в пункте меню Образовательная программа является очередным шагом при работе с Системой.

4) Следующим шагом является формирование учебных групп.

Сведения из этого пункта меню взаимоувязаны с пунктами меню «Учебные отделения», «Перевод студентов», «Расписание занятий». Функциональными возможностями при создании групп обучения являются:

– распределение пользователей (студентов или абитуриентов по группам);

– управление подгруппами и назначение другого преподавателя;

– управление дисциплинами (эта информация взаимоувязана с данными учебных планов образовательных программ);

– редактирование журналов успеваемости и ведомостей промежуточной аттестации преподавателями-предметниками;

– учебные отделения. Этот подпункт меню позволяет объединить группы обучения по признакам (например, очное, заочное или вечернее обучение), назначить куратора (Заведующего) по отделению.

5) Рабочие программы дисциплин разграничивают авторов, соавторов рабочей программы, а также преподавателей дисциплин, использующих данную рабочую программу. Они обуславливают заполнение пункта Тематическое планирование. Однако, заполнение КТП не обязательно в Системе.

6) Заключительным разделом при работе с Системой является меню Занятия.

Расписание звонков - это одно из мероприятий по регулированию образовательного процесса. В нем заполняются все поля (название, начало и окончание действия, начало занятий, длительность занятий и перемен, количество занятий);

Расписание занятий - это форма, способствующая оптимальной организации учебной работы и повышению эффективности преподавательской деятельности. Оно составляется в соответствии с учебным планом.

Расписание сессий - это форма, регулирующая период сдачи экзаменов в учебном заведении. Система позволяет создавать расписание консультаций, экзаменов, зачётов или пересдач.

Журнал успеваемости - это форма, способствующая ведению учета и анализа учебной деятельности, повышению уровня прозрачности учебного процесса. В ней реализованы возможности:

- отображение запланированных занятий по дисциплине;

- администрирование заданий для занятий;

- выставление оценок и посещаемости. Сведения по успеваемости учитываются в ведомости промежуточной аттестации.

После окончания каждого периода обучения в Системе необходимо проводить процедуру перевода учебных групп на следующий период обучения. Информация в этот пункт меню поступает из созданного ранее учебного календаря и сортируется по фазам обучения.

Управление приказами. Этот пункт меню позволяет просматривать все созданные приказы по пользователям Системы. Сведения поступают из меню Пользователи и с помощью удобно настроенных фильтров вы можете формировать запросы на просмотры необходимых документов.

Описание работы в меню «Пользователи», «Обучение», «Занятия» - это базисные процедуры.

7) Отчёты. В Системе имеются различные формы отчетов. Сведения, представленные в этих формах, резюмируют результаты учебной и преподавательской деятельности. При создании различных категорий отчётов используются инструменты (фильтры), благодаря которым отчёт становиться наглядным и способствует созданию мотивационных элементов, влияющих на образовательный процесс.

Чтобы войти в Систему, необходимо открыть браузер и набрать в адресной строке браузера http://<имя_сервера>/, где вместо <имя_сервера> введите адрес Системы. Для перехода нажмите на клавиатуре клавишу «Enter». На открывшейся странице отображается экран входа в Систему (рисунок 3).

Для входа в Систему нужно ввести имя учётной записи (логин) и пароль и нажмите кнопку **«**Войти**»**.

После успешной авторизации открывается экран «Главная страница».

В Системе по умолчанию предусмотрены следующие роли: Абитуриент, Сотрудник, Студент, Родитель.

Для роли Сотрудник в Системе реализована возможность создания любых должностей с индивидуальным набором прав. В дальнейшем эти должности назначаются конкретным сотрудникам.

Помимо настраиваемой группы прав для роли Сотрудник предусмотрены определенные правила при работе с различными разделами системы, если данный Сотрудник является преподавателем или куратором учебной группы.

Для регистрации пользователя в Системе необходимо выбрать раздел меню «Пользователи» и один из его пунктов: «Абитуриенты», «Студенты» или «Сотрудники».

При выборе пункта меню в рабочей области отображается список пользователей выбранной категории, справа от которой отображается блок «Новый студент» («Новый сотрудник») для создания нового пользователя в Системе.

Пароли не хранятся в Системе в явном виде, поэтому в случае утери пароля его нельзя где-либо увидеть, можно только изменить пароль на новый.

В связи с тем, что в данных системах идет обработка персональных данных обучающихся (ФИО, данные свидетельства о рождении, паспорта, дата рождения, место рождения, адрес прописки и проживания, данные родителей) информация должна быть хорошо защищена.

Для этого те компьютеры, где происходит запись абитуриентов и выгрузка данных по обучающимся в АИС «Сетевой город. Образование» - должны быть аттестованы.

На них ставятся программные комлексы: VIP Net Client – создается защищенный канал связи. Также ставятся дополнительные средства защиты – программы: Dallas Lock 8.0-K и Kaspersky Endpoint Security 10.

Установка всех программ, разработка пакета документов на данное аттестованное место – ложится на плечи лицензиата ФСБ, лицензиата ФСТЭК. К данным компьютерам допускается ограниченное количество пользователей, это учитывается и в приказах, и в журналах образовательной организации.

Данные аттестованные места с СКЗИ ставятся в кабинетах, где дополнительно устанавливается сигнализация на разбив стекла и объемники (т.е. на несанкционированное перемещение после закрытия кабинета).

Кабинет после рабочего дня должен опечатываться: шток-чашка, пластилин, печать. Ключи от кабинета помещаются в пенал, пенал опечатывается и сдается на вахту. Ключи в пенале получают и вечером сдают, о чем делаются записи в соответствующем журнале.

Назначаются ответственные пользователи СКЗИ, пользователи СКЗИ и ИСПДн (информационных систем по обработке персональных данных), ответственные за опечатывание кабинета.

Описанные действия и меры прописаны в нормативных правовых актах колледжа.

Для проведения анализа уязвимостей корпоративной информационной системы ГБПОУ «Южно-Уральского государственного технического колледжа» наиболее оптимальным методом является разработка модели угроз.

Необходимость разработки модели угроз регламентирована рядом нормативных документов, таких как:

1. Часть 2 статьи 19 закона No152-ФЗ «О персональных данных», где говорится, что обеспечение безопасности персональных данных достигается, в частности: определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [27].

2. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) от 18 февраля 2013г. No 21): «Меры по обеспечению безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных» [30].

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены ФСТЭК России от 11 февраля 2013г. No 17): «Формирование требований к защите информации включает: определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации» [30].

Отсюда следует вывод: для любых корпоративных информационных систем, так или иначе подлежащих защите в соответствии с законодательством необходимо разработать модель угроз.

Таким образом, модель угроз информационной безопасности автоматизированной системы должна содержать:

- описание информационной системы;
- структурно-функциональные характеристики;
- описание угроз безопасности;
- модель нарушителя;
- возможные уязвимости;
- способы реализации угроз;
- последствия от нарушения свойств безопасности информации.

Для модели угроз изначально определяется глобальный параметр – уровень исходной защищенности. Определяется он один раз и не меняется от угрозы к угрозе. Чтобы определить уровень исходной защищенности (он же коэффициент исходной защищенности Y1) нужно для семи показателей выбрать одно из значений, которое больше всего подходит для вашей системы.

Каждому значению соответствует высокий, средний или низкий уровень защищенности. Считаем какой процент у нас получился для показателей с разными значениями. Если «высокий» и «средний» набрали 70% и выше, то определяем средний уровень исходной защищенности (Y1 = 5), если нет, то – низкий (Y1 = 10).

Далее необходимо определить частоту (вероятность) реализации угрозы (коэффициент Y2) – показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

– 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.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

– 0 – для маловероятной угрозы;

– 2 – для низкой вероятности угрозы;

– 5 – для средней вероятности угрозы;

– 10 – для высокой вероятности угрозы.

Следующий столбец – коэффициент реализуемости угрозы Y. Вычисляется по простой формуле:

$$Y = (Y1+Y2)/20.$$

Возможность реализации – это вербальный аналог коэффициента Y. Определяется в зависимости от числового значения следующим образом:

– если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признаётся низкой;

– если $0{,}3 \leq Y \leq 0{,}6$, то возможность реализации угрозы признаётся средней;

– если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признаётся высокой;

– если $Y > 0{,}8$, то возможность реализации угрозы признаётся очень высокой.

Следующий столбец – актуальность угрозы. Определяется по таблице правил отнесения угрозы безопасности ПДн к актуальной (таблица 2).

В результате была разработана модель угроз для ГБПОУ «Южно-Уральского государственного технического колледжа», представленная в приложении. В модели угроз отражены все возможные угрозы информационной системе образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

2.2 Разработка рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

Обеспечить должный уровень информационной безопасности в организации, как правило, достаточно сложно, особенно если сотрудники хранят документы на своих рабочих компьютерах и в сетевых хранилищах с общим доступом, передают по электронной почте и другим каналам коммуникации, выносят за пределы офиса на съемных носителях. По статистике, ¾ случаев утечки информации происходит из-за халатности или беспечности пользователей.

Проблема обеспечения защиты персональных данных напрямую зависит от защищенности систем электронного документооборота. Управление информацией в них происходит на протяжении всего жизненного цикла данных. Информация проходит через все процессы в организации, она создается, обрабатывается и хранится при помощи разных приложений.

В результате анализа уязвимостей информационных систем образовательной организации был определен необходимый набор механизмов защиты: безопасное хранение данных, протоколирование действий пользователей, обеспечение безопасного доступа, обеспечение подлинности документов, обеспечение доступности данных [1].

Критериями при выборе средств защиты электронного архива должны быть такие функции: разграничение прав доступа, протоколирование действий пользователя, поддержка ЭЦП, поддержка шифрования, база данных на SQL-сервере, поддержка межсетевых экранов и VPN-каналов.

При выборе средств защиты электронного архива необходимо учитывать реальный перечень основных угроз персональным данным в

образовательной организации и материальные возможности последнего. Если в образовательной организации большой штат сотрудников с постоянной сменой персонала нужно учесть малую заинтересованность людей в сохранности персональных данных обучающихся или сотрудников, таким образом, нужно обеспечить максимально функциональную подсистему управления доступом и протоколирование всех действий сотрудников. В идеале в такой системе необходимо использовать аппаратные средства аутентификации личности, такие как токены.

Использование сертифицированной версии системы особенно актуально для образовательных организаций, участвующие в тендерах на госзаказ. Действующие сертификаты ФСТЭК и ФСБ в настоящий момент имеет лишь СЭД Directum, обеспечивая защиту от НСД по 5 классу.

На основе анализа рисков и уязвимостей системы защиты персональных данных и анализа нормативно-правовых требований действующего законодательства нами были разработаны рекомендации по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж».

Практика показывает, что основными угрозами информационной безопасности являются:

- свободный доступ большого количества пользователей к электронным документам;
- отсутствие единого и надежно защищенного места хранения;
- бесконтрольное копирование и рассылка электронных документов.

При отсутствии регламентированного учета пользовательских действий в отношении документации возможны:

- несанкционированный просмотр информации сотрудниками или другими лицами, не имеющими прав доступа;
- преднамеренное или случайное уничтожение документа(ов);

– искажение информации или ошибки вследствие использования неактуальной версии;

– неправильная расстановка приоритетов при необходимости оперативного получения данных.

Оптимальным способом предупреждения и устранения возможных проблем является создание электронного архива и разработка административного регламента хранения и использования электронных документов. Для обеспечения информационной безопасности необходимо:

– создать четкие правила работы с электронным архивом, обязательные для всех сотрудников;

– разместить в электронном архиве последние, актуальные версии документов;

– после ввода данных в электронный архив удалить документы и их копии с рабочих мест;

– установить внутренний обмен документами только с помощью электронного архива;

– на аппаратно-программном уровне разграничить уровни доступа, чтобы исключить возможность несанкционированного использования информации;

– проводить регулярные проверки соблюдения правил информационной безопасности.

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

Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты хранения информации;

– организация периодической проверки соблюдения информационной безопасности сотрудниками.

Объект защиты.

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

1. Информационные ресурсы:

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

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

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

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

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

Субъекты информационных отношений:

1. Субъектами информационных отношений являются:

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

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

Проанализировав популярные на сегодняшний день технологии защиты информации, анализ рисков и уязвимостей системы защиты персональных данных, мы разработали рекомендации по выбору средств защиты электронного архива персональных данных обучающихся ГБПОУ

«Южно-Уральский государственный технический колледж» при соблюдении информационной безопасности.

Для предотвращения ошибок и взломов системы предпринимаются меры программно-технической безопасности, указанные в таблице 3.

Для обеспечения защиты личных данных используются программные и криптографические средства.

Программные средства:

- DLP-системы - комплексные системы, предотвращающие утечку данных;
- SIEM-системы - комплексные системы управления событиями и информационной безопасностью, отслеживающие в режиме реального времени событий безопасности (тревог) (MaxPatrol SIEM от Positive Technologies, КОМРАД от «НПО «Эшелон», RUSIEM).

DLP (Data Loss Prevention) — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

Предотвращение потери данных является фундаментальным принципом безопасности в компании любого масштаба.

Поскольку электронный архив представляет собой программный комплекс, включающий несколько подсистем, существует возможность разграничить доступ к каждой из них. Кроме того, электронные документы хранятся не в локальной базе данных, а на удаленном защищенном сервере, и пользователи получают для работы только их копии.

Электронный архив позволяет:

- создать централизованное хранилище электронных документов;
- разграничить права доступа к информации;

– учитывать и контролировать доступ к электронным документам, а также все изменения, производимые в электронных копиях;

– запретить изменения документов;

–зашифровать с помощью протокола SSL обмен информацией между сервером и компьютером пользователя;

–создавать резервные копии;

–защитить доступ к документам через интернет.

Хранение электронных документов в архиве организуют, соблюдая требования:

–Федерального закона от 22.10.2004 № 125-ФЗ «Об архивном деле»;

–Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

–Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

–ГОСТ Р ИСО 13008-2015. Национальный стандарт РФ. Информация и документация. Процессы конверсии и миграции электронных документов;

–Правил, утв. Приказом Росархива от 31.07.2023 № 77;

–Типовых функциональных требований к СХЭД государственных органов, утв. Приказом Росархива от 15.06.2020 № 69;

–Перечня типовых документов, утв. Приказом Росархива от 20.12.2019 № 236 — по нему определяют сроки хранения документов;

–Инструкции по применению Перечня №236, утв. Приказом Росархива от 20.12.2019 № 237;

–Положения об архиве организации.

Можно оцифровывать для облегчения поиска все бумаги, которые поступают в образовательную организацию. Но в ЭА вы будете включать только два вида документов:

1. Электронные документы, изначально созданные в цифровом виде. Это набор файлов, включающий, в том числе, описание и файл

цифровой подписи. Требования к структуре ЭАД приведены в п. 141 Правил № 77. Хранить нужно именно оригиналы – файлы в формате PDF/A с текстовыми и другими данными, созданные в системе ЭДО и подписанные электронной подписью.

2. Цифровые копии (образы) бумажных документов, относящихся к гибридным делам – делам, в которых есть электронные и бумажные документы. Например, акты выполненных работ от подрядчиков могут поступать в организацию в двух форматах – как через ЭДО, так и по Почте России. Требования к структуре цифровых копий приведены в п. 160 Правил № 77.

Все ЭАД в архиве должны быть систематизированы по схеме с уровнями систематизации *«Фонд → Опись → Раздел и подраздел описи → Электронное дело в соответствии с номенклатурой дел → Электронный документ»*.

Информация на каждом уровне оформляется в виде архивных учетных форм (АУФ) по образцам обязательных учетных документов. В приложениях к Правилам № 77 есть бланки листа и списка фондов, описей и т. д.

Цифровые оригиналы хранят столько же, сколько и бумажные версии. Сроки для каждого вида документов устанавливают по Перечню, утв. Приказом Росархива от 20.12.2019 № 236. Например, табели учета рабочего времени сотрудников и должностные инструкции работников надо держать до 75 лет.

Срок хранения считают с 1 января года, следующего за годом, когда документ завершен делопроизводством. Так подписанный 20 сентября 2023 года акт выполненных работ будет храниться 5 лет с 1 января 2024 года.

Для ЭАД действуют те же правила передачи в архив, что и для бумажных версий. Документы постоянного (свыше 10 лет) хранения

отправляют в СХЭД не ранее чем через 1 год и не позднее, чем через 3 года после завершения дел в делопроизводстве – п. 47 Правил № 77.

Электронное хранение архива предполагает создание защищенных ИСПДн, которые в автоматическом режиме фиксируют и обрабатывают большие массивы данных. В таком случае не нужно много места или закупки закрывающихся шкафов и сейфов, а отыскать интересующие сведения можно за пару секунд, к тому же при серьезном подходе к обеспечению защиты нет риска кражи или утечки ПДн. Из недостатков следует отметить наличие затрат на оснащение современным программным обеспечением, потребность в постоянном создании резервных копий, а также регулярное обновление оборудования.

Для государственных учреждений есть отдельное требование — использовать IT-решения отечественного производства. Многие частные компании тоже переходят на такие инструменты по причине их высокой эффективности.

Компания ВИАР ИТ (г. Санкт-Петербург) предлагает готовую инфраструктуру для создания и хранения цифрового архива документов. ля оцифровки и хранения электронного архива документов компания Виар ИТ предлагает программно-аппаратные комплексы собственной разработки. Сканеры-визуализаторы позволяют бережно оцифровать сшитые документы без разброшюровки.

Модуль ХАБ VIAR – приложение для передачи информации и автоматизации архивных процессов. Система использует профессиональную систему поиска с применением искусственного интеллекта, что обеспечивает быстрый доступ к информации.

ПО Редактор VIAR служит для оцифровки в соответствии с регламентами, принятыми в отрасли: повышает читабельность документов, выравнивает фон, конвертирует в необходимый формат

Оцифрованные документы загружаются в ДатаХаб VIAR, где происходит их индексация, систематизация и распознавание текста.

Собственные разработки экономят время и средства заказчика, так как не требуют обращения к внешним дорогостоящим сервисам по распознаванию текста. Электронные данные хранятся конфиденциально, при этом любой файл из цифрового архива можно за считанные секунды найти с помощью полнотекстового поиска. Оцифрованные документы быстрее находить и отправлять проверяющим органам или в ответ на запрос к архиву.

Программное обеспечение ДатаХаб VIAR позволяет связать цифровые данные в единое информационное пространство, обеспечивая сохранность документов компании. ПО, разработанное ВИАР ИТ, обеспечивает конфиденциальность и сохранность персональных данных. В любой момент пользователь может проверить содержимое архива и найти необходимые файлы через поиск. Программы для ведения электронного архива обеспечивают высокий уровень защиты, оперативный доступ, понятную структуру и правила хранения.

Программно-аппаратный комплекс VIAR представлен на рисунке 5.

1. Визуализатор VIAR SMART 800A разработан для сканирования кадровых, нотариальных, бухгалтерских и оперативных документов. Успешно справится с трудовыми книжками, товарными накладными, договорами и пр. Поможет организовать оперативную работу с документами при обращении. Незаменимый помощник для студентов и преподавателей, руководителей и сотрудников. Поставляется в комплекте с Программным обеспечением VIAR. Лицензированное ПО VIAR зарегистрировано в Министерстве цифрового развития РФ.

2. Визуализатор VIAR CLASS 40S разработан для качественной оцифровки любых сшитых документов. При оцифровке сшитый оригинал не повреждается. VIAR CLASS 40S успешно справится с

техническими чертежами, архивными делами, газетами, бухгалтерской и иной сшитой отчетностью, с форматами до А3 включительно. Визуализатор бережно оцифровывает документы длительного и постоянного сроков хранения. Поставляется в комплекте с программным обеспечением VIAR. ПО VIAR зарегистрировано в Министерстве цифрового развития РФ.

Все программные продукты VIAR имеют необходимую регистрацию в реестре отечественных ПО, рекомендованных Министерством цифрового развития РФ.

Таким образом, создание электронного архива и перевод документов в электронный вид решает большинство проблем корпоративной информационной безопасности и позволяет значительно повысить уровень защиты.

2.3 Оценка эффективности рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В комплекс рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации входили анализ нормативно-правовых требований действующего законодательства и анализ угроз образовательной организации. В результате были разработаны рекомендации по выбору современного программного обеспечения, в которые вошли ряд критериев, учитывающие специфику и цели образовательной организации, а также экспертная оценка, которая позволяет выбрать оптимальное IT-решения для хранения и защиты электронного архива в образовательной организации.

В результате была произведена экономическая оценка эффективности рекомендаций по выбору средств защиты электронного

архива персональных данных обучающихся образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж».

В экономическую оценку вошли:

1. Обследование информационных систем.
2. Перспективы внедрения программного обеспечения ДатаХаб VIAR в образовательную организацию.

В обследование информационных систем входило:

– аудит документов, обследование помещений, сети и компьютеров;

– разработка модели угроз.

Сеть образовательной организации должна быть защищена от внешних атак, вирусов и разнообразных современных киберугроз. Программное обеспечение ДатаХаб VIAR является экономически выгодным решением для образовательной организации, как в плане защиты, так и в плане ценообразования.

Согласно прайс-листу, цена на программное обеспечение ДатаХаб VIAR на 2024 год составит за 1 год до 10 пользователей/4 группы (отдела) – 170 000 руб. (таблица 4).

Данное устройство поставляется практически готовым к использованию, и его настройка может быть произведена обычным системным администратором. Срок действия: бессрочная лицензия; платформа: Windows; тип лицензии: полная версия; минимальная покупка: от 1 шт.

В результате была составлена таблица расчёта стоимости защиты электронного архива персональных данных обучающихся образовательной организации (таблица 5).

В случае выявления нарушения в области информационной безопасности образовательной организации предусмотрена уголовная, административная, дисциплинарная и гражданская ответственность (таблица 6), которая может применяться в отношении организации, руководителя организации, подразделения или виновного работника [29].

Согласно ФЗ РФ «Об образовании в Российской Федерации» всякое образовательное учреждение (учреждение, осуществляющее образовательный процесс) является юридическим лицом [34].

Таким образом максимальный штраф, который может получить образовательная организация за нарушения в области информационной безопасности составит 370 000 руб. Дополнительно возможна конфискация средств защиты, приостановление или прекращение обработки персональных данных.

После выявления нарушений выписывается предписание с указанием сроков и необходимых мер по устранению. По наступлению указанных в предписании сроков по выполнению требований, будет произведена проверка на их исполнение. В случае отрицательного результата, будут повторно применены санкции и выписано очередное предписание.

Для расчета экономической эффективности разработанных рекомендаций выбора средств защиты электронного архива персональных данных обучающихся необходимо суммарную её стоимость сравнить со стоимостью возможного ущерба со стороны регуляторных рисков (рисунок 8).

В результате сравнения экономическая эффективность разработанных рекомендаций составила 155 550 руб. Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

Таким образом, разработка рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации возможна при тщательном учёте всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь.

Выводы по 2 главе

Во второй главе были разработаны рекомендации по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации, проведена оценка эффективности разработанных рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации.

Для защиты электронного архива персональных данных обучающихся необходимо определить перечень угроз для каждого существующего в организации информационного потока; определить для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности; выбрать для существующего информационного потока надёжные средства защиты информации, позволяющие нейтрализовать «незакрытые» угрозы.

Для разработки рекомендаций было проанализировано текущее состояние системы защиты информационной системы образовательной организации ГБПОУ «ЮУрГТК» с помощью модели угроз, в результате которого было выявлено, что информационная система данной организации имеет объективные, субъективные и случайные уязвимости.

Определяя средства защиты электронного архива персональных данных обучающихся образовательной организации, мы остановили свой выбор на современном программном обеспечении ДатаХаб VIAR, как комплексное средство организации и хранения электронного архива.

В итоге была проведена экономическая оценка эффективности рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации ГБПОУ «ЮУрГТК». В данную оценку вошли расчет стоимости внедрения ПО для защиты электронного архива образовательной организации и стоимостью возможного ущерба со стороны регуляторных рисков.

На внедрение разработанных рекомендаций образовательная организация потратит 214450 рублей, а стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 000 рублей. В результате сравнения данных показателей экономическая эффективность разработанных рекомендаций составила 155 550 рублей.

Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

ЗАКЛЮЧЕНИЕ

Большинство организаций сталкиваются с необходимостью обеспечения безопасности информации только в части персональных данных сотрудников клиентов, охранять которые от утечек предписывают законы РФ. Но даже в этом, относительно легком, случае вопросы ее сохранности данных жизненно важны.

Электронный документ — это информация в цифровом виде, записанная на том или ином носителе. Человек не способен воспринимать её непосредственно — для чтения документа и работы с ним цифровой код преобразуется в изображение или текст, выводится на экран или распечатывается. После редактирования документа информация снова оцифровывается и сохраняется на носитель.

Длительное хранение электронных записей сопряжено с двумя проблемами: носители цифровой информации деградируют быстрее, чем бумага — со временем записанная на них информация считывается с ошибками или совсем перестаёт читаться; кроме физического устаревания, электронные средства хранения быстро стареют морально — носители, связанные с ними устройства записи/воспроизведения и программы выходят из обихода и заменяются другими.

Кроме этого, существуют риски, специфические для информации в цифровом виде. Например, сбои при записи или чтении информации приводят к её искажению, полной или частичной потере. Примерно такой же по последствиям вред может нанести компьютерный вирус. Документ, записанный в редком или устаревшем формате из-за отсутствия подходящего программного обеспечения может не читаться.

Для решения перечисленных проблем долговременного хранения электронных документов используют комплекс мер и технических решений.

Для защиты электронного архива персональных данных обучающихся необходимо определить перечень угроз для каждого существующего в организации информационного потока; определить для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности; выбрать для существующего информационного потока надёжные средства защиты информации, позволяющие нейтрализовать «незакрытые» угрозы.

Для разработки рекомендаций было проанализировано текущее состояние системы защиты информационной системы образовательной организации ГБПОУ «ЮУрГТК» с помощью модели угроз, в результате которого было выявлено, что информационная система данной организации имеет объективные, субъективные и случайные уязвимости.

Определяя средства защиты электронного архива персональных данных обучающихся образовательной организации, мы остановили свой выбор на современном программном обеспечении ДатаХаб VIAR, как комплексное средство организации и хранения электронного архива.

В итоге была проведена экономическая оценка эффективности рекомендаций по выбору средств защиты электронного архива персональных данных обучающихся образовательной организации ГБПОУ «ЮУрГТК». В данную оценку вошли расчет стоимости внедрения ПО для защиты электронного архива образовательной организации и стоимостью возможного ущерба со стороны регуляторных рисков.

На внедрение разработанных рекомендаций образовательная организация потратит 214450 рублей, а стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 000 рублей. В результате сравнения данных показателей экономическая эффективность разработанных рекомендаций составила 155 550 рублей.

Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

Результаты исследования рекомендуются использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности защиты электронного архива персональных данных обучающихся образовательной организации.

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