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

# Анализ защищенности информационных систем персональных данных в образовательной организации

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

Проверка на объем заимствований:
40 % авторского текста

Работа рекомендована к защите
«20» января 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Щапова Юлия Дмитриевна

Научный руководитель:
к.п.н., доцент,
каф. АТ, ИТ и МОТД,
Гафарова Елена Аркадьевна

Челябинск
2024

Содержание

# ВВЕДЕНИЕ

В современном цифровом мире, где информация играет ключевую роль, защита персональных данных становится все более важной и неотъемлемой частью нашей жизни. Отправляя сообщения, делая покупки онлайн или просто используя социальные сети, мы постоянно делимся своей личной информацией. Поэтому, несомненно, важно понимать, почему защита персональных данных является нашей неотъемлемой ответственностью.

Во-первых, наше право на конфиденциальность и частную жизнь подразумевает, что наши персональные данные должны быть защищены от неконтролируемого распространения. Каждый из нас имеет право на уверенность в том, что личная информация не будет использована без нашего согласия. Это важно для поддержания нашей индивидуальности и защиты от нежелательного вмешательства в нашу личную жизнь.

Во-вторых, защита персональных данных имеет огромное значение для предотвращения финансовых мошенничеств и киберпреступности. Возрастающая цифровизация открывает новые возможности для злоумышленников, которые могут использовать нашу личную информацию в своих корыстных целях. Кража финансовых данных, идентификационных номеров, а также других персональных сведений может привести к серьезным финансовым потерям и неприятностям. Таким образом, защита наших персональных данных также является защитой нашего финансового благополучия.

Кроме того, защита персональных данных способствует сохранению нашего достоинства и самооценки. Множество организаций собирают информацию о нас и используют ее для создания персонализированных рекламных материалов или анализа наших предпочтений и поведения. Отсутствие защиты персональных данных может привести к

нежелательному контролю или манипуляциям над нами, что негативно сказывается на нашем эмоциональном состоянии и свободе выбора.

В современном обществе очень важно качественно осуществлять обработку, хранение и использование такой информации. Это обусловлено накоплением большого количества персональной информации у граждан, в том числе и студентов образовательный организаций, поэтому каждый человек находится под возможной угрозой последствий недобросовестного обращения с его персональными данными, а это, в свою очередь, может привести к вмешательству в его частную жизнь.

Образовательная организация представляет собой сложную систему, в которую входят большие объемы информации, электронные ресурсы, многочисленные внутренние и внешние информационные связи, а также происходит сетевое взаимодействие различных компонентов.

В настоящее время наблюдается мощный толчок информатизации, которая приводит к значительным изменениям в системе управления таких организаций.

В рамках образовательного учреждения создаются автоматизированные информационные системы, которые соответствуют информационным потребностям учебного заведения. Важным компонентом таких информационных систем являются персональные данные, безопасность которых необходимо обеспечить согласно законодательству Российской Федерации.

Автоматизированные информационные системы защиты персональных данных в образовательном учреждении играют ключевую роль в обеспечении безопасности конфиденциальной информации, которая связана с учебным процессом и личными данными студентов и преподавателей. В современном мире, где цифровизация проникает во все сферы деятельности, образовательные учреждения сталкиваются с необходимостью сохранять и защищать цифровые записи, содержащие важные данные обучающихся и персонала. Автоматизированные

информационные системы обеспечивают надежную защиту этих данных от несанкционированного доступа, утечек информации и других угроз.

Одним из главных преимуществ автоматизированных информационных систем является возможность эффективно управлять и контролировать доступ к данным. Системы могут предоставлять права доступа в зависимости от ролей и ответственности пользователей, что позволяет ограничить доступ к конфиденциальной информации только квалифицированным лицам. Это снижает риск утечек данных и несанкционированного использования личной информации.

Кроме того, автоматизированные информационные системы защиты персональных данных обеспечивают возможность контролировать и анализировать доступ к данным. Системы могут вести журналы аудита, в которых регистрируются все действия пользователей, связанные с доступом к информации. Это помогает в обнаружении и предотвращении потенциальных угроз, а также дает возможность проводить расследования в случае инцидентов.

Важной составляющей автоматизированных информационных систем является обеспечение защиты от внешних атак и вирусов. Технические средства и программные решения, встроенные в эти системы, позволяют обнаруживать и блокировать вредоносное программное обеспечение, а также отслеживать несанкционированный доступ. Это помогает поддерживать интегритет данных и защищать их целостность.

Наконец, автоматизированные информационные системы предоставляют возможность резервного копирования и восстановления данных. В случае сбоев или внешних атак, системы позволяют быстро восстанавливать утраченные данные, минимизируя потери и обеспечивая бесперебойность учебного процесса.

Появление возможностей реализации различных новшеств, которые должны сделать процесс обучения более динамичным, но вместе с тем

возникает и угроза попадания персональных данных, которые являются важной частью информатизации, в руки третьим лицам.

Такие данные могут храниться единой базе данных, которая может представлять собой электронный ресурс или бумажный архив и содержит персональные данные студентов, их родителей (законных представителей), а также сотрудников образовательной организации.

Персональные данные относятся к информации ограниченного доступа, так как могут содержать различного рода информацию: личную, коммерческую и т.д.

Также персональные данные могут относится к различным категориям:

— общие (ФИО, место регистрации, информация о месте работы, номер телефона, email)**;**

— специальным (сведения о состоянии здоровья);

— биометрическим (фотографии);

— иным (паспортные данные, номера страховых, налоговых, свидетельств, сведения о доходах и другие).

В условиях широкого развития сетевых информационных технологий, встал острый вопрос о безопасности персональных данных, поскольку наблюдается рост киберугроз. Угрозу также представляет халатное обращение с такой информацией, которое может привести к последующим несанкционированным действиям третьих лиц.

Отсюда следует, что к защите персональных данных предъявляется все больше требований, а также помимо федеральных законов, регулирующих данный вопрос, существуют специальные локальные нормативные акты образовательных организаций, в которых описываются правильные этапы накопления, обработки, хранения персональных данных.

*Цель исследования:* проведение анализа защищенности информационных систем персональных данных в образовательной

организации ГБПОУ «КГСТ» и разработка рекомендаций по повышению защищенности.

*Объект исследования:* информационные системы персональных данных образовательной организации ГБПОУ «КГСТ».

*Предмет исследования:* состояние защищенности информационных систем персональных данных образовательной организации ГБПОУ «КГСТ».

*Гипотеза исследования* состоит в предположении о повышении защищенности информационных систем персональных данных при применении программно-аппаратного комплекса, реализующего политику защиты персональных данных образовательной организации.

Для достижения поставленной цели предполагается решение *следующих задач:*

1. Исследовать нормативно-правовую базу защищенности персональных данных.

2. Проанализировать состояния информационной системы персональных данных на примере образовательной организации ГБПОУ «КГСТ».

3. Выявить основные приемы защиты персональных данных и их эффективность в образовательной организации

4. Описать рекомендации по достижение эффективности защиты персональных данных.

5. Выполнить экономический расчет по внедрению Secret Disk 5.

Теоретико-методологическая база исследования состоит из общенаучного системного подхода, нормативно-методических рекомендаций ФСТЭК и ФСБ, федеральных законов и правовых актов по защите персональных данных, а также обобщения практикоориентированных подходов и методик в вопросах обращения с персональными данными.

Научная новизна работы состоит в том, что в ходе исследований образовательной организации были предложены альтернативные рекомендации по защите персональных данных.

# ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

## 1.1 Нормативно-правовая база защиты персональных данных…

Нормативно-правовая база защиты персональных данных является одним из важных аспектов современного общества. В современном информационном обществе обработка и хранение персональных данных стали неотъемлемыми процессами, которые несут за собой определенные риски для конфиденциальности и приватности людей.

Для обеспечения защиты персональных данных были разработаны различные нормативно-правовые акты, которые регулируют и контролируют этот процесс. Первоначально, вопросы защиты персональных данных были отражены в понятии "права на неприкосновенность частной жизни".

Однако с появлением информационных технологий и возможностей сбора, хранения и обработки больших объемов данных, было необходимо создать специальные нормы, которые бы регулировали этот процесс.

Одним из основных документов, регулирующих защиту персональных данных, является Закон Российской Федерации "О персональных данных". Этот закон устанавливает требования к обработке, сбору, хранению и передаче персональных данных, а также определяет права и обязанности сторон, занимающихся обработкой персональных данных. В нем также содержатся механизмы принудительного соблюдения требований и меры ответственности за их нарушение.

Кроме этого, существует ряд иных нормативных актов, которые также имеют отношение к защите персональных данных. К ним относятся, например, Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и Федеральный закон "О государственной регистрации юридических лиц и индивидуальных

предпринимателей", содержащие нормы о защите персональных данных несовершеннолетних и юридических лиц соответственно.

Обширность нормативно-правовой базы защиты персональных данных позволяет обеспечить надлежащую защиту информации о гражданах и предотвратить неправомерный доступ к ней. Постоянное развитие и совершенствование законодательства в этой сфере является неотъемлемой частью обеспечения приватности личных данных и цифровой безопасности в современном информационном обществе.

Персональные данные учащихся, их родителей (представителей) и работников техникума используются в образовательной организации для создания образовательного процесса, обеспечения безопасности, обеспечения трудовых отношений и контроля качества образования. Это важный аспект, которому необходимо уделить особое внимание.

Основная задача нормативно-правовой базы защиты персональных данных заключается в обеспечении прозрачности и законности обработки персональных данных, а также предоставлении гарантий и защиты прав и интересов граждан в сфере обработки персональных данных.

Такие меры не только способствуют сохранению конфиденциальности и приватности, но и формируют сознательное отношение к обработке персональных данных и повышают уровень доверия общества к информационным технологиям и взаимодействию с ними.

Существует множество документов по защите персональных данных, которые регулируют разработку собственных нормативных документов в организациях, использующих такие данные.

При создании систем защиты персональных данных используются следующие документы:

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

—Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

—Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

—ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утверждено постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469;

—ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» утверждено постановлением Госстандарта СССР от 24 марта 1989 г. №664;

—ГОСТ РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов», утверждены постановлением Госстандарта СССР от 27.12.1990 № 3380;

—ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» утверждено постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399.

—«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено приказом ФСТЭК России от 18.02.2013 № 21.

—Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/6/6-622.

—«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства РФ от 01.11.2012 № 1119

—«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144.

—Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20. «Об утверждении Порядка проведения классификации информационных систем персональных данных» в зависимости от категории обрабатываемых данных и их количества.»

Категории персональных данных отображены в таблице №1:

Таблица №1 — Категории персональных данных

| Вид категории | Характеристика |
|---|---|
| Категория 1 | ПД, касающиеся расовой, национальной принадлежности политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни |
| Категория 2 | ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1 |
| Категория 3 | персональные данные, позволяющие идентифицировать субъекта ПД |
| Категория 4 | обезличенные и (или) общедоступные персональные данные |

Информационные системы персональных данных подразделяются на типовые и специальные. К типовым системам относятся системы, в которых требуется обеспечить только конфиденциальность персональных данных. Все остальные системы относятся к специальным.

В зависимости от последствий нарушений заданной характеристики безопасности персональных данных типовой информационной системе присваивается один из классов:

– класс 1 (К1) - информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;

– класс 2 (К2) - информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;

– класс 3 (К3) - информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;

– класс 4 (К4) - информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

—Приказ ФСТЭК № 17 от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

—Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Согласно указанным выше документам, все организации и физические лица на территории Российской Федерации должны обеспечивать необходимый уровень безопасности персональных данных в действующих информационных системах. Лица, нарушающие эти

требования, несут ответственность в соответствии с законодательством Российской Федерации.

В современном информационном обществе, защита персональных данных становится все более актуальной и важной задачей. Российская Федерация относится к государствам, где данная сфера законодательно регулируется и существует обширная система норм и правил, целью которых является обеспечение конфиденциальности и безопасности персональных данных граждан

Структура законодательства Российской Федерации по вопросам персональных данных включает ряд основных элементов, которые описываются в следующем порядке:

1. Конституционное закрепление права на защиту персональных данных. Основой для законодательного регулирования в данной сфере является Конституция Российской Федерации. Статья 24 Конституции гарантирует каждому гражданину право на неприкосновенность частной жизни, включая защиту персональных данных.

2. Федеральный закон "О персональных данных". Данный закон является основополагающим в области защиты персональных данных и определяет наиболее важные нормы, принципы и правила обработки, хранения и передачи персональных данных.

3. Подзаконные акты. Для подробной реализации положений Федерального закона "О персональных данных" принимаются подзаконные акты, такие как постановления Правительства Российской Федерации, приказы и рекомендации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и других органов государственной власти.

4. Международные соглашения. Российская Федерация является участником международных соглашений в области защиты персональных данных, таких как Конвенция Совета Европы о защите персональных данных. Нормы указанных соглашений применяются в Российской

Федерации при разрешении вопросов, касающихся защиты прав и интересов граждан при обработке и передаче их персональных данных.

5. Судебная практика. Законодательство Российской Федерации по вопросам персональных данных развивается и корректируется с учетом судебной практики. Решения судов по спорам, связанным с нарушением прав граждан в сфере персональных данных, помогают указывать на пробелы или неоднозначности в законодательстве, требующие уточнения и исправления.

Такова основная структура законодательства Российской Федерации по вопросам персональных данных. Эта система норм и правил служит беспрецедентной важности в обеспечении конфиденциальности, безопасности и защиты прав каждого гражданина на территории Российской Федерации.

На рисунке № 1 представлена схематичная структура законодательства Российской Федерации по вопросам защиты персональных данных:

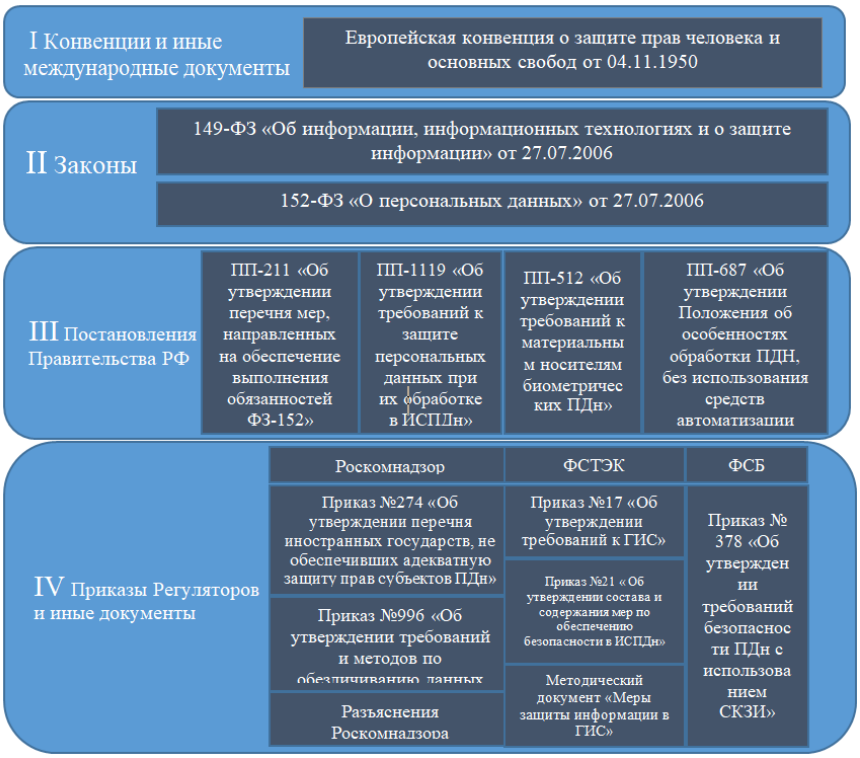


Рисунок 1 - Структура законодательства РФ по персональным данным

Операторы обязаны обеспечивать защиту персональных данных в информационных системах, которые они внедряют с момента их ввода в эксплуатацию.

Основным документом в данной области является Федеральный закон РФ № 152 "О персональных данных", принятый 27 июля 2006 года.

Данный закон определяет основные термины и критерии обработки персональных данных физических и юридических лиц, а также устанавливает требования по организации работы с этими данными оператором и его ответственность за их нарушение.

История Федерального закона номер 152 "О персональных данных" началась в далеком 1981 году, когда Совет Европы опубликовал Конвенцию о защите персональных данных граждан при их обработке с использованием электронных средств. В 1999 году конвенция была отредактирована для включения новых реалий. Россия подписала эту конвенцию 7 ноября 2001 года по требованию Всемирной торговой организации, как необходимый шаг для присоединения к организации. Таким образом, на территории России конвенция вступила в силу 1 марта 2002 года.

Конвенция предполагает, что страна, которая подписала документ, предъявляет собственные технические требования к защите персональных баз данных своих контролёров - компании, которые обрабатывают персональные данные.[2] Для реализации этого страна должна принять закон о персональных данных, который эти требования закреплял. До выпуска этого закона можно было признать обработку персональных данных незаконной по конвенции, однако прецедентов таких не известно. Таким образом, конвенция была принята формально, но по факту не действовала из-за отсутствия российских нормативных актов.

Российский закон «О персональных данных» был принят 27 июля 2006 года и получил порядковый номер 152. Он закрепил, что ответственными ведомствами за соблюдение закона является Роскомнадзор

в части организационных мер и ФСТЭК и ФСБ в части технических мер защиты. В нем также были перечислены организационные меры, такие как назначение ответственных, разработка набора корпоративных документов, регистрация в реестре операторов персональных данных, вести который доверено Роскомнадзору.

Действие данного федерального закона распространяется на отношения, связанные с обработкой персональных данных. Эта обработка может осуществляться федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами (далее - муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Настоящий федеральный закон не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством

Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Целью данного федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Процесс создания системы защиты информационной системы персональных данных – это сложная и многогранный задача, требующая тщательного и систематического подхода. Создание надежной и эффективной системы защиты информации является одной из основных приоритетов любой организации, особенно когда речь идет о персональных данных.

Далее будет приведен пример процесса создания системы защиты информационной системы персональных данных в соответствии с российским законодательством.

Первое, что необходимо сделать оператору - это определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн. На данном этапе разрабатываются и утверждаются внутренние документы, регламентирующие деятельность должностных лиц и структурных подразделений, отвечающих за информационную безопасность и закрепляющие их функциональные обязанности и права.

Далее необходимо определить состав обрабатываемых ПДн, цели и условия их обработки, а также срок хранения ПДн. Согласно федеральному закону «о персональных данных» № 152-ФЗ за исключением некоторых случаев обработка персональных данных осуществляется с согласия субъекта персональных данных. В таком случае оператор должен получить согласие субъекта на обработку его ПДн, в том числе в письменной форме.

Кроме того, необходимо определить порядок реагирования на запросы со стороны субъектов персональных данных. Затем при необходимости составляется и отправляется уведомление в уполномоченный орган по защите ПДн о начале обработки ПДн.

После этого оператор должен выделить и определить состав информационной системы персональных данных, а также провести анализ структуры информационной системы для того, чтобы определить:

– автоматизированные рабочие места, обрабатывающие персональные данные;

– серверное, коммутационное и сетевое оборудование;

– используемое в информационной системе персональных данных прикладное и общесистемное программное обеспечение;

– наличие и типы средств межсетевого экранирования в распределенных ИСПДн;[3]

– наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена.

Далее, когда собраны исходные данные о системе, наступает этап классификации ИСПДн. Оператор организует систему допуска и учета лиц, допущенных к работе с ПДн в ИСПДн. С этой целью:

– утверждают список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, нужен для выполнения служебных обязанностей;

– создается журнал учета допуска к работе пользователей в ИСПДн, в котором показываются логические имена пользователей, а также список информационных ресурсов, к которым пользователи допущены. Создание системы защиты информационной системы персональных данных – это продолжительный и ответственный процесс, требующий глубоких знаний в области информационной безопасности и постоянного обновления.

Нарушение законодательства о персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (статья 24) влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, налагаемую в судебном порядке.

## 1.2 Анализ состояния ИС персональных данных в ГБПОУ «КГСТ» на примере АИС «Сетевой город. Образование»

Состав персональных данных, обрабатываемых в ИСПДн ГБПОУ «КГСТ», определяется «Перечнем персональных данных», который утверждается директором. Он определяет перечень лиц из числа работников, уполномоченных на обработку персональных данных субъектов, обеспечивающих обработку ПДн в соответсвтии с требованиями Федерального закона от 27.06.2006г. №152-ФЗ «О персональных данных».

Информация об учащихся, их родителях и педагогах в Коркинском горно-строительном техникуме заносится и хранится в том числе и в такой системе, как «Сетевой город.Образование».

АИС "Сетевой город. Образование" – это инновационная информационно-аналитическая система, разработанная для обеспечения эффективного управления в образовательных учреждениях. Она предлагает широкий функционал, позволяющий автоматизировать и оптимизировать многие процессы, связанные с организацией образования.

В первую очередь, АИС "Сетевой город. Образование" обеспечивает удобное и быстрое ведение учета студенческой базы данных. Она позволяет создать и поддерживать электронные журналы, в которых записываются данные о поступивших студентах, их успеваемости, посещаемости и активности в учебном процессе. Такой подход позволяет администрации и педагогам оперативно получать информацию о студентах, а также делать выводы и принимать решения на основе объективных данных.

Кроме того, АИС "Сетевой город. Образование" предоставляет возможность автоматизации процесса расписания занятий. Система учитывает особенности каждого учебного заведения и позволяет эффективно распределять группы студентов по аудиториям и времени, учитывая потребности преподавателей и студентов. Такой подход помогает избежать конфликтов и перекрывания занятий, а также оптимизирует использование ресурсов учебного заведения.

Еще одной важной функцией АИС "Сетевой город. Образование" является возможность организации электронного обучения. Система обеспечивает создание и ведение электронных курсов, что позволяет студентам получать доступ к учебным материалам, проходить тестирование и получать обратную связь от преподавателей. Такая форма обучения дает большую гибкость и доступность учебного материала, что особенно актуально в условиях современного онлайн-образования.

Кроме основного функционала, АИС "Сетевой город. Образование" предлагает и другие возможности. Среди них - возможность взаимодействия с родителями студентов через электронные дневники, организация системы электронного документооборота для учебных заведений, сбор статистических данных о работе учебного заведения и другие.

Важно отметить, что АИС "Сетевой город. Образование" обеспечивает высокий уровень конфиденциальности и безопасности персональных данных учащихся. Система строго соблюдает все требования законодательства и нормы по защите персональной информации, гарантируя ее неразглашение и надежную защиту от несанкционированного доступа.

В итоге, АИС "Сетевой город. Образование" – это передовая информационная система, которая значительно упрощает и улучшает управление образовательными процессами, повышает качество образования и позволяет эффективно работать с персональными данными учащихся. Эта

система становится незаменимым инструментом для всех участников образовательного процесса, содействуя успешному развитию и достижению высоких результатов в сфере образования.

Это мощный инструмент для эффективного управления образовательными процессами. Её функционал позволяет автоматизировать и оптимизировать множество задач, связанных с организацией и контролем образовательных процессов, что способствует повышению качества образования и удовлетворенности всех участников учебного процесса

Функционал данной системы разнообразен, ИС позволяет автоматизировать и проводить мониторинг организационно-управленческой деятельности и образовательного процесса в профессиональных образовательных организациях(Рис 3).

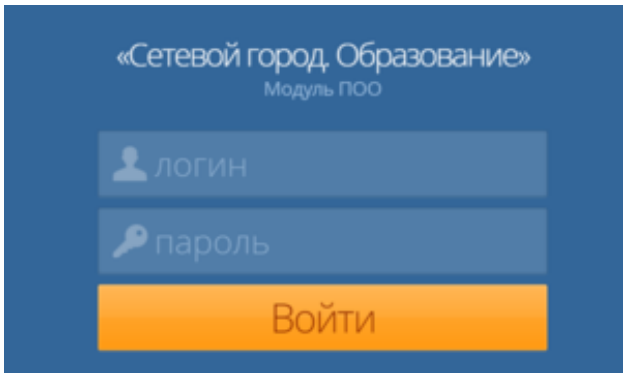


Рисунок 2 – Вход в систему «Сетевой город.Образование»

Модуль предоставляет инструменты для управления:

- расписанием звонков, занятий, сессий;
- журналы успеваемости;
- курсовыми работами;
- движением - зачислением, выбытием, переводом, оформлением академических отпусков;
- 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 отчетностью и отчетностью по успеваемости и посещаемости обучающихся.

Таким образом, формируется единое информационное образовательное пространство, где каждому пользователю присвоен определенный набор прав, который так же можно индивидуально настраивать.

Каждый пользователь образовательного учреждения и родители учащихся имеют индивидуальные имя и пароль и могут входить в систему с любого компьютера, подключенного к муниципальной сети (или сети Интернет).

Согласно ФЗ №152, ответственность за обработку персональных данных лежит полностью на операторе. В случае использования системы "Сетевой Город. Образование", таким оператором является образовательная организация. Именно оператор принимает решения о требуемом уровне защищённости своей ИСПДн, а также о способах и средствах защиты ПДн.

Для обработки персональных данных в образовательной организации необходимы письменные согласия субъектов ПДн.

Согласно требованию законодательства о персональных данных, в системе "Сетевой Город. Образование" ведётся журнал изменения персональных данных пользователей. Фиксация происходит в следующих случаях:

1) редактирование личной карточки (для сотрудников, учащихся, родителей);

2) расширенный импорт (для учащихся и родителей).

Для каждого изменения личной карточки, система сохраняет следующую информацию:

– дата и время изменений,

– пользователь, ПДн которого отредактировали,

– пользователь-автор изменения этих ПДн,

– IP-адрес, с которого было внесено изменение,

– какие поля изменились и какие значения были им установлены. (4)

В личной карточке любого пользователя (сотрудника, ученика, родителя) присутствует кнопка «Журнал изменений», которая доступна только пользователям с правом Просмотр журнала изменений сведений о пользователях (по умолчанию оно включено у роли *Администратор системы*). По данной кнопке отображается история изменений сведений о пользователе.

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.

Система позволяет создавать пользователя с ролью «Родитель». Чтобы добавить родителя конкретному студенту, необходимо выбрать его в общем списке щелчком левой кнопки мыши и в личной карточке в блоке «Родители» нажать на кнопку «+». Для доступа в систему создается логин и пароль пользователя с ролью «Родитель». Пароли не хранятся в Системе в

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

Персональные данные (ПДн) учащихся доступны только авторизованным пользователям с соответствующими правами доступа. Согласно Федеральному закону № 152-ФЗ "О персональных данных", для обработки персональных данных в образовательной организации необходимы письменные согласия субъектов ПДн. Посмотреть формы согласий на обработку ПДн для родителя и для ребёнка в разделе Ресурсы -> Документы -> Предустановленные.

Чтобы просмотреть краткие сведения об ученике, пользователю достаточно иметь право доступа «Просматривать краткие сведения об учениках и родителях». К кратким сведениям относятся:

- ФИО,
- Фотография,
- Дата рождения,
- пол,
- класс,
- e-mail,
- предпочтительный способ связи,
- домашний телефон,
- мобильный телефон,
- ФИО родителей,
- номер личного дела ученика.

В полные сведения об учащемся входят графы:

- ФИО,
- имя на экране - это то имя, которое отражается в общих списках пользователей, например, на странице Ученики. Для учеников, по умолчанию, оно выглядит так: «Иванов Иван»,

– имя пользователя - это логин, то есть имя, под которым пользователь входит в систему,

– пол,

– дата рождения,

– гражданство,

– учетная запись Windows,

– блок полей "Документы, удостоверяющие личность" (может включать паспорт РФ, свидетельство о рождении и т.д.),

– блок полей "Контактная информация": адрес проживания, адрес регистрации, домашний телефон, мобильный телефон, предпочтительный способ связи, e-mail.

– родители(ссылки на сведения о родителях),

– иностранный язык, второй иностранный язык,

– ИНН,

– группа здоровья (данные вносятся медицинским работником),

– физ.группа (данные вносятся медицинским работником),

– заболевания (данные вносятся медицинским работником),

– № личного дела,

– психолого-педагогическая характеристика,

– медицинский полис,

– социальное положение,

– дополнительное образование.

Для редактирования сведений у пользователя должно быть право доступа *редактирования сведений об учениках и родителях.* По умолчанию, им обладают пользователи с ролью *администратора*, *завуча и секретаря*. Пользователям с ролью *учителя* рекомендуется предоставить отдельное право *редактирования сведений об учениках и родителях в своем классе.*

В анкете учащегося можно указать его родителей, после чего появятся прямые ссылки на анкеты выбранных родителей.

К анкете можно присоединить и файл совершенно произвольного формата (например, характеристику ученика и т.п.).

### 1.3 Основные приемы защиты персональных данных и их эффективность в образовательной организации

Защита персональных данных является одной из наиболее важных задач в современном информационном обществе. Особенно актуальной она становится в сфере образования, где обрабатывается огромное количество личной информации учащихся, педагогов и других сотрудников образовательных организаций.

Одним из основных приемов защиты персональных данных является их классификация и маркировка. Это позволяет точно определить, какая информация относится к личным данным, и соответственно, применять соответствующие меры безопасности. Кроме того, важным элементом защиты является контроль доступа к персональным данным. Четко определенные права доступа для каждого пользователя позволяют минимизировать риски несанкционированного доступа и использования личных данных.

Следующим важным приемом является шифрование данных. Шифрование позволяет защитить информацию от несанкционированного доступа даже при их потере или краже. Использование сильных алгоритмов шифрования и системы ключей позволяет обеспечить высокую степень безопасности персональных данных.

Шифрование персональных данных является процессом преобразования информации в непонятный и неразборчивый вид, который может быть восстановлен только с помощью специального ключа или пароля. Это делается для защиты конфиденциальности персональных данных от несанкционированного доступа или использования.

Существует несколько методов шифрования персональных данных, включая симметричное шифрование, асимметричное шифрование и хеширование.

Симметричное шифрование использует один и тот же ключ для шифрования и расшифрования данных. Это означает, что отправитель и получатель должны иметь доступ к одному и тому же ключу для обмена зашифрованными данными.

Асимметричное шифрование использует пару ключей – открытый и закрытый. Открытый ключ используется для шифрования данных, а закрытый ключ – для их расшифровки. Такая система позволяет отправителю распространять открытый ключ, не раскрывая закрытый ключ, что повышает безопасность процесса.

Хеширование преобразует данные в непонятный, фиксированной длины хеш-код. Хеш-код не может быть обратно преобразован в исходные данные, поэтому он используется главным образом для проверки целостности данных.

Шифрование персональных данных является важным аспектом обеспечения безопасности информации, особенно в случае передачи по сети или хранения на незащищенных устройствах. Оно помогает предотвратить несанкционированный доступ к конфиденциальной информации и защищает права и интересы пользователей.

Дополнительные меры защиты персональных данных включают установку антивирусного программного обеспечения и систем детекции вторжений. Эти технологии позволяют обнаружить и предотвратить попытки несанкционированного доступа к персональным данным, а также предупредить утечку информации.

Установка антивирусного программного обеспечения (ПО) обладает неоспоримыми преимуществами, которые являются необходимыми для защиты компьютера и данных пользователей. Далее будут рассмотрены

основные плюсы использования антивирусного ПО и почему его установка является важной составляющей безопасности компьютерной системы.

Во-первых, антивирусное ПО способно обнаруживать и блокировать различные вредоносные программы, такие как вирусы, черви, трояны и шпионские программы. Благодаря системе постоянного мониторинга активности компьютера и поиска подозрительных файлов, антивирусная программа может реагировать на угрозы ещё до того, как они успеют нанести вред системе. Это позволяет избежать потери данных, повреждения файлов и других негативных последствий, связанных с воздействием вирусов на компьютер.

Во-вторых, установка антивирусного ПО способствует обеспечению конфиденциальности данных. Вирусы и другие вредоносные программы могут попытаться получить доступ к личным и финансовым сведениям пользователей, таким как пароли, банковские данные, личная переписка и прочее. Антивирусные программы обнаруживают и блокируют такие попытки, обеспечивая сохранность конфиденциальной информации и защищая пользователей от кражи личных данных.

Также следует отметить, что антивирусное ПО обеспечивает безопасность при работе в интернете. Современные вирусы и другие вредоносные программы активно распространяются через сеть, злоумышленники используют различные методы, чтобы получить доступ к компьютеру пользователя.

Установленное антивирусное ПО помогает выявить и блокировать такие попытки, предотвращая заражение системы во время посещения опасных веб-сайтов, скачивания ненадежных файлов или открытия вредоносной электронной почты.

Важно упомянуть, что антивирусное ПО обеспечивает регулярные обновления, которые вносят новые сигнатуры, обновленные базы данных и модули защиты. Это необходимо для борьбы с постоянно развивающимися угрозами, появляющимися в сети каждый день. Благодаря таким

обновлениям, антивирусные программы остаются актуальными и способными предотвращать новые виды вредоносного ПО, что является крайне важным для обеспечения безопасности компьютерной системы.

Наконец, установка антивирусного ПО позволяет пользователям сосредоточиться на своих задачах и работе, минимизируя риск возникновения проблем, связанных с безопасностью. Защита компьютера и данных пользователя должна быть приоритетом для всех, кто использует современные технологии в повседневной жизни.

В итоге, установка антивирусного программного обеспечения имеет множество плюсов, являясь неотъемлемой частью компьютерной безопасности. Она обеспечивает обнаружение и блокирование вредоносных программ, защиту данных, безопасность в интернете и регулярные обновления для борьбы с современными угрозами.

Эффективность применения основных приемов защиты персональных данных в образовательной организации зависит от нескольких факторов. Прежде всего, важно наличие четкой политики защиты персональных данных, политика защиты персональных данных в образовательных учреждениях, которая обязательно должна быть известна всем сотрудникам организации.

В ГБПОУ «КГСТ» защита персональных данных студентов, преподавателей и других участников образовательного процесса является одним из наших главных приоритетов. В приоритете обеспечение конфиденциальность и сохранность всех личных данных, собранных и обрабатываемых в рамках деятельности данного образовательного учреждения.

Специалисты делают всё возможное, чтобы гарантировать, что все персональные данные будут обрабатываться в соответствии с действующим законодательством о защите персональных данных. Они придерживаются таких важных принципов как легальность, прозрачность, точность и справедливость при сборе, хранении и использовании таких данных.

Соблюдаются все процедуры и меры безопасности для защиты этих данных от несанкционированного доступа, изменения или уничтожения.

Основные принципы политики защиты персональных данных в ГБПОУ «КГСТ» включают следующее:

1. Сбор и использование данных: собираются те персональные данные, которые требуются для обеспечения образовательного процесса. Данные могут включать имя, дату рождения, адрес, контактную информацию, академические результаты и другую информацию, необходимую для обучения и оценки учеников.

2. Конфиденциальность: образовательное учреждение обязуется сохранять конфиденциальность всех персональных данных, полученных от студентов, преподавателей и других участников образовательного процесса. Доступ к таким данным предоставляется только уполномоченным лицам, которым это необходимо для выполнения своих обязанностей. Также обеспечивается обучение сотрудников, чтобы они были осведомлены о важности конфиденциальности.

3. Безопасность: принимаются все необходимые меры для защиты персональных данных от несанкционированного доступа, внешних угроз и случайных утечек. Используются современные методы защиты, включая шифрование данных, системы аутентификации и ограничение физического и логического доступа к хранилищам данных.

4. Права субъектов данных: признание и уважение прав субъектов данных в отношении их персональных данных. Наличие процедур, позволяющие субъектам данных обращаться с запросами на доступ, исправление, удаление или ограничение обработки их персональных данных.

5. Сохранение данных: сохранение персональных данных только в течение необходимого времени, определенного законодательством или целями, для которых они были собраны.

Образовательное учреждение выступает в роли контроллера персональных данных, и существуют гарантии абсолютного соблюдения политики защиты персональных данных в соответствии с действующим законодательством. Происходит регулярное обновление политики и процедуры, чтобы соответствовать изменениям в законодательстве и технологиях.

Также необходимы регулярные обучающие программы, чтобы повысить осведомленность о персональных данных и методах их защиты.

Обучающие программы по сохранению персональных данных в обучающем учреждении предназначены для повышения уровня осведомленности и компетенции сотрудников, студентов и родителей в области безопасности данных. Они включают в себя широкий спектр тем, начиная от основных понятий и принципов сохранения данных, до специфических мер безопасности, применимых к конкретному обучающему учреждению.

В рамках программы студенты и сотрудники получают необходимые знания и навыки, связанные с обработкой и хранением персональных данных. Они узнают о роли технических средств защиты, а также о роли человеческого фактора в обеспечении безопасности данных. Программы также включают обучение по поводу основных законов и стандартов, регулирующих обработку и хранение персональных данных в образовательных учреждениях.

Преимущества обучающих программ очевидны. Во-первых, они помогают снизить риски утечки информации и злоупотребления персональными данными. Повышение уровня компетенции сотрудников в области безопасности данных способствует более эффективной и ответственной работе с цифровыми ресурсами, сокращает возможность возникновения ошибок при обработке данных или несанкционированного доступа к ним.

Учащиеся также становятся более информированными и осознанными пользователями, что способствует формированию правильных привычек в сфере сохранения и защиты своих персональных данных.

Обучающие программы также способствуют повышению уровня доверия родителей к образовательным учреждениям, показывая, что они принимают все необходимые меры для обеспечения безопасности данных и конфиденциальности персональной информации их детей.

Кроме того, важно иметь систему мониторинга и аудита, которая позволяет выявлять и исправлять уязвимости в системах защиты.

Система мониторинга и аудита для защиты персональных данных в образовательном учреждении является неотъемлемой частью современного образовательного процесса. С увеличением количества данных, хранимых и обрабатываемых в учебных заведениях, растет и угроза их несанкционированного доступа или утечки.

Возникает необходимость в системе, которая сможет обеспечить защиту персональных данных учащихся, преподавателей и администрации. Такая система должна быть комплексной и включать в себя инструменты для мониторинга и аудита обработки персональных данных, а также превентивные и реактивные меры по защите информации.

Мониторинг в рамках этой системы представляет собой постоянное наблюдение за обработкой персональных данных в образовательном учреждении. Он включает в себя контроль доступа к информации, регистрацию и анализ событий, а также идентификацию потенциальных угроз и проблем. Это позволяет оперативно реагировать на инциденты и предотвращать негативные последствия нарушений безопасности данных.

Аудит системы по защите персональных данных в образовательном учреждении направлен на проверку соответствия установленным требованиям и нормативам. Он включает в себя анализ деятельности учебного заведения, его политики и процедуры обработки данных, а также

оценку эффективности мер по защите информации. Аудит позволяет выявить возможные проблемы и уязвимости, а также предложить рекомендации по их устранению.

Основными задачами системы мониторинга и аудита для защиты персональных данных в образовательном учреждении являются:

1. Обеспечение конфиденциальности персональных данных. Система должна гарантировать сохранность информации и предотвращать несанкционированный доступ к ней.

2. Реагирование на инциденты. Система должна обнаруживать, анализировать и оперативно реагировать на любые инциденты, связанные с нарушением безопасности персональных данных.

3. Соблюдение законодательства и нормативных требований. Система должна быть в соответствии с действующим законодательством и регулирующими документами в области защиты персональных данных.

4. Минимизация рисков. Система должна анализировать потенциальные угрозы и проблемы, а также предоставлять возможности по их устранению и предупреждению.

Итак, система мониторинга и аудита для защиты персональных данных в образовательном учреждении является ключевым инструментом, обеспечивающим эффективную и надежную защиту информации. Она позволяет не только предотвратить утечку и несанкционированный доступ к персональным данным, но и обеспечить соблюдение требований законодательства и нормативов по защите информации.

В целом, применение основных приемов защиты персональных данных в образовательной организации является необходимым условием для обеспечения безопасности и сохранности личной информации. Однако, в связи с постоянным развитием информационных технологий, необходимо постоянно обновлять и улучшать меры защиты, чтобы эффективно справляться с новыми угрозами и рисками безопасности.

Разнообразные информационные системы достаточно давно и эффективно используются в образовательном процессе техникума, активизируя познавательную активность обучающихся, влияя на их творческие способности, на вовлеченность в образовательный процесс.

Однако это только одна из граней внедрения и введения информационных систем в образовательную организацию. Другой особенностью является использование систем не только в качестве обучающих средств, но и в поддержке организации данного процесса, и в управлении образовательной организации.

Таким образом, вопрос организации защиты информации в образовательной организации является в достаточной степени актуальным и диктует свои требования к защите ресурсов образовательных организаций и ставит задачу построения собственной интегрированной системы безопасности.

Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации в рамках образовательной организации.

Информационная безопасность образовательных организаций отличается от информационной безопасности других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан. Отсюда, особое внимание необходимо уделить защите персональных данных учащихся, абитуриентов и их родителей, работников образовательного учреждения.

Основные приемы защиты персональных данных, а также ранее разработанные ключевые положения об обработке персональных данных ГБПОУ «КГСТ» (далее – Учреждение) разработано в соответствии с

Конституцией Российской Федерации от 25.12.1993, Гражданским кодексом РФ от 30.11.1994 №51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите данных» от 27.07.2006 №152-ФЗ, а также другими нормативными правовыми актами, действующими на территории Российской Федерации.

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

- обезличенных персональных данных;
- общедоступных персональных данных.

Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении срока их хранения или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определенно законом Российской Федерации.

В положении по защите персональных данных используются следующие термины и их определения.

*Безопасность персональных данных* - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИСПДн, результатом которого могут стать: уничтожение; изменение; блокирование; копирование; предоставление; распространение персональных данных; а также иные неправомерные действия.

Таким образом, можно сделать вывод, что информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации.

*Блокирование персональных данных* – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

*Документированная информация* – зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или её материальный носитель.

*Доступ к информации* – возможность получения информации и её использования.

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

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

*Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

*Информация* – сведения (сообщения, данные) независимо от формы их представления.

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

*Конфиденциальность персональных данных* – обязательное для соблюдения оператором или иными получившими доступ к персональным

данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

*Обработка персональных данных* – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

*Оператор (персональных данных)* – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащие обработке, действия (операции), совершаемые с персональными данными.

*Персональные данные* – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

*Субъект персональных данных* – физическое лицо, которое может быть однозначно идентифицировано по персональным данным.

*Целостность информации* – состояние информации, при котором отсутствует любое её изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Порядок предоставления доступа к персональным данным предполагает, что доступ имеют только те работники, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей».

Предоставление доступа к персональным данным требует строго определенного порядка и регламента, который обеспечивает надежное хранение информации и предотвращает ее неправомерное использование.

Первоочередным принципом при предоставлении доступа к персональным данным является осознанное и добровольное согласие

субъекта данных. Это означает, что каждый человек должен иметь полную информацию о том, какие именно данные о нем собираются, для каких целей они будут использоваться и как будут храниться. Никакая информация не должна быть собрана или использована без явного согласия субъекта.

Далее, важно установить четкий порядок доступа к персональным данным. Это подразумевает определение групп лиц, которым будет разрешен доступ к информации, а также установление правил и процедур для работы с данными.

Следует предусмотреть систему разграничения доступа, чтобы обеспечить, что каждый пользователь имеет доступ только к той информации, которая необходима для выполнения своих задач.

Конфиденциальность является неразрывной составляющей порядка предоставления доступа к персональным данным. Все лица, которые могут получить доступ к информации, должны соблюдать секретность и не разглашать данные без соответствующего разрешения. Кроме того, необходимо регулярно проводить аудит доступа к данным для выявления и предотвращения возможных нарушений.

Важной частью порядка предоставления доступа является правовой аспект. Субъекты данных должны быть осведомлены о своих правах и возможностях защиты своей информации. Законодательство должно предоставить надежную правовую основу для защиты персональных данных от неправомерного доступа и использования.

Наконец, эффективная система обратной связи и обеспечения безопасности является важной составляющей порядка предоставления доступа к персональным данным. Субъекты данных должны иметь возможность связаться с ответственными лицами в случае возникновения вопросов или нарушений безопасности.

Реагирование на запросы, учет жалоб и незамедлительные меры в случае нарушений - все это необходимо для поддержания доверия к системе и обеспечения надежности хранения персональных данных.

В целом, порядок предоставления доступа к персональным данным должен быть разработан с учетом всех указанных выше факторов, обеспечивая субъектам данных полную прозрачность, контроль и защиту их конфиденциальной информации. Только таким образом можно создать надежные условия для использования персональных данных в информационном обществе.

Перечень прав оператора персональных данных представлены на рисунке №3:

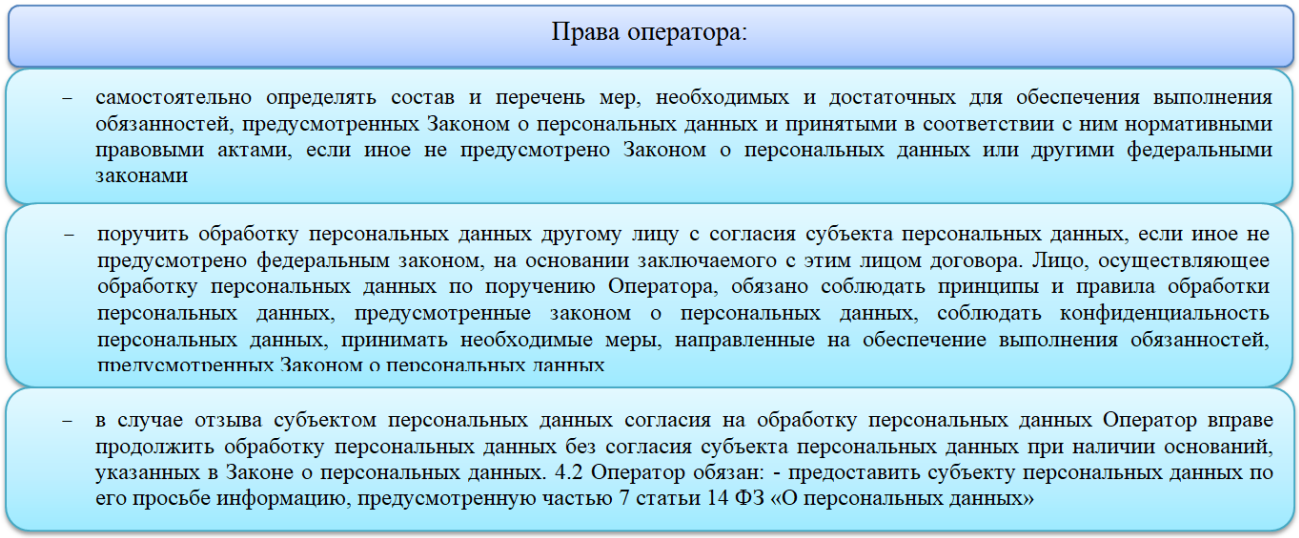


Рисунок 3 – права оператора персональных данных

Процедура оформления доступа к ПДн представляет собой следующую строгую последовательность действий:

– ознакомление работника под роспись с настоящим Положением, «перечнем персональных данных..» и другими локальными нормативно-правовыми актами, касающимися обработки персональных данных;

– истребование с работника «Обязательства о неразглашении информации ограниченного доступа»;

– внесение работника в «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей» и в «Журнал учета лиц, допущенных к работе с персональными данными в информационных системах»;

Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения работы. Остальным сотрудника, не имеющим надлежащим образом оформления допуска, доступ к персональным данным субъектов запрещается.

Имея определенный набор прав, оператор персональных данных должен придерживаться и некоторым обязанностям (рисунок №4):

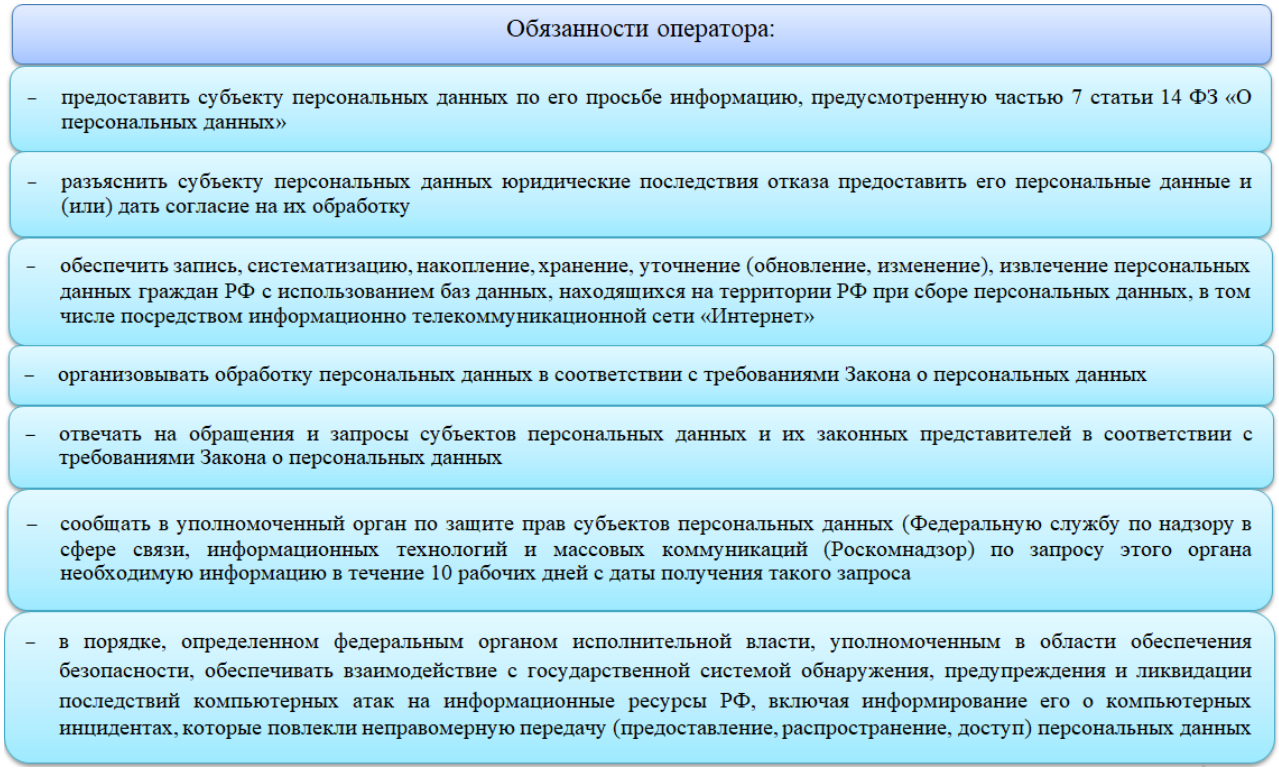


Рисунок 4 - обязанности оператора персональных данных

Субъект персональных данных имеет право:

– получать информацию, касающуюся обработки его персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

– требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– дать предварительное согласие на обработку персональных данных;

– обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

– Получить сведения об образовательном учреждении в соответствии со ст.14 ФЗ №152 от 27.06.2006г.;

Обработка персональных данных может осуществляться исключительно в целях осуществления деятельности указанной в Уставе

Учреждения, и в случае, установленных законодательством Российской Федерации.

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Обработка Оператором персональных данных осуществляется в следующих целях:

– осуществление своей деятельности в соответствии с уставом Организации, в том числе заключение и исполнение договоров с контрагентами;

– исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие работникам в трудоустройстве, получении образования и продвижении по службе, привлечение и отбор кандидатов на работу у Оператора,

обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, ведение кадрового и бухучета, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;

– осуществление пропускного режима;

– рассмотрение вопроса на соответствие кандидатуры соискателя, имеющимся вакансиям Организации;

– предоставление данных работников/соискателей в медицинские организации для прохождения обязательных медицинских осмотров;

– предоставление данных работников для участия в конкурсах на заключение контрактов, в том числе по ФЗ № 44-ФЗ, ФЗ № 223-ФЗ.

– предоставление данных работников для подтверждения соответствия продукции, системы менеджмента, услуг требованиям

– нормативной документации по различным отраслевым направлением.

Обработка и хранение персональных данных субъектов осуществляется в помещениях ГБПОУ «КГСТ» и на учтенных машинных носителях. Персональные данные могут быть получены, обработаны и переданы на хранение как на бумажных носителях, так и в электронном виде, а именно в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

При использовании типовых форм документов, обрабатываемых без использования средств автоматизации, типовая форма или связанные с ней документы должны содержать:

– сведения о цели обработке персональных данных,

– имя и адрес образовательного учреждения,

– ФИО и адрес субъекта персональных данных,

– источник получения персональных данных,

– сроки обработки персональных данных,

– перечень действий с персональными данными, которые будут совершаться в процессе их обработки,

– общее описание используемых учреждением способы обработки персональных данных.

Также типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, в тех случаях, когда существует необходимость получения письменного согласия на обработку персональных данных. Вид типовой формы должен быть понятен, чтобы при необходимости, например, будущий студент имел возможность ознакомиться со своими персональными, содержащимися в документе.

Хранение персональных данных осуществляется на бумажных и электронных носителях, доступ к которым ограничен. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Для хранения используются специально отведенная секция в сейфе, обеспечивающего защиту от несанкционированного доступа.

При передачи персональных данных субъекта представители образовательной организации должны соблюдать следующие требования:

– передавать персональные данные могут только те работники, которые имеют доступ к их обработке;

– не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта;

– предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

– не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

– передавать ПДн субъекта в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми данными, которые необходимы для выполнения указанными представителями их функций;

– все сведения о передаче персональных данных субъекта должны фиксироваться в журнале учета запросов от сторонних лиц в целях контроля правомерности использования данной информации.

## Вывод по Главе 1

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

При создании систем защиты персональных данных используются следующие документы:

1. Выявлено наличие множества документов по защите персональных данных, которые регулируют разработку собственных нормативных документов в организациях, а именно:

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

—Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

—Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

—ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утверждено постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469 и т.д.

Так же были рассмотрены основные категории персональных данных, а также классы нарушений безопасности персональных данных.

Выделены основные приемы защиты персональных данных в образовательном учреждении, главная цель которых - определение порядка обработки персональных данных граждан, обратившихся в учреждение и иных субъектов, персональные данные которых подлежат обработке на основании полномочий учреждения.

Обеспечение защиты прав и свобод человека и гражданина, в том числе того гражданина, который обратился в учреждение, является одной из главных обязанностей образовательной организации. Обработка его персональных данных, его право на неприкосновенность частой жизни, личную и семейную тайну, должна выполняться согласно закону Российской Федерации.

Был проведен анализ состояния информационной системы персональных данных в ГБПОУ «КГСТ» на примере АИС «Сетевой город. Образование».

Таким образом, в данном учебном заведении происходит достаточно активное использование данной автоматизированной системы управления. Туда вносятся различные данные учащихся, формируется расписание звонок, занятий, сессий, ведутся журналы успеваемости, вносятся учебные календари и календарно-тематические планы, вносятся списки учебных отделений и групп, ведется статистическая отчетность и отчетность по успеваемости и посещаемости обучающихся и т.д.

В современном мире сохранение персональных данных играет важную роль в образовательных учреждениях. Обучающие программы по безопасности данных являются эффективным инструментом в повышении уровня осведомленности и компетенции сотрудников, студентов и родителей. Они помогают минимизировать риски утечки информации, скачковый доступ и злоупотребление персональными данными. Внедрение таких программ является неотъемлемой частью стратегии безопасности

данных в обучающих учреждениях, гарантирующей сохранность и конфиденциальность персональной информации всех заинтересованных сторон.

# ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 2.1 Общие рекомендации для повышения защищенности персональных данных ГПБОУ «КГСТ».

Эффективность защиты персональных данных является одной из наиболее актуальных и значимых проблем в современном мире. С развитием информационных технологий и все большим количеством цифровых данных, которыми мы делимся и храним, возникает все большая потребность в надежной и эффективной системе защиты этих данных.

Однако, защита персональных данных сталкивается с рядом сложностей. Во-первых, это постоянно меняющиеся технологии и методы, которые используют злоумышленники для получения доступа к чужим данным. К сожалению, хакеры и киберпреступники становятся все более изощренными и находчивыми в своих попытках взлома защитных систем. Это означает, что системы защиты должны постоянно развиваться и обновляться, чтобы оставаться эффективными.

Во-вторых, эффективность защиты персональных данных определяется не только техническими средствами защиты, но и компетентностью сотрудников, который имеет доступ к этим данным. Часто утечки информации происходят из-за невнимательности или небрежности работников, что подчеркивает важность обучения сотрудников правилам защиты данных и строгого контроля доступа к ним.

Третьей сложностью является баланс между эффективностью защиты и удобством использования данных. Возможность передачи, обработки и хранения персональных данных является неотъемлемой частью современной жизни, особенно в контексте экономики, связанной с обработкой информации. Однако, находясь в постоянной гонке за всевозможными новшествами, нередко подвергается риску безопасности.

Поэтому здесь важно находить гармоничное решение, которое обеспечит возможность использования данных, сохраняя их надежную защиту.

Эффективность защиты персональных данных является важным элементом в нашей современной цифровой среде. Возрастающие угрозы безопасности и постоянно меняющиеся условия требуют непрерывного развития и улучшения систем защиты. Однако, эффективность не может быть обеспечена только техническими решениями, но и требует внимания к обучению персонала и поиску баланса между защитой данных и их удобством использования. Только так мы сможем обеспечить надежную защиту персональных данных и сохранить доверие пользователей к цифровым технологиям.

В настоящее время обеспечение защиты персональных данных стало актуальной и важной задачей для всех учебных заведений, работающих с личной информацией студентов, их родителей (представителей) и сотрудников. В связи с постоянным развитием информационных технологий и угроз для безопасности данных, необходимо принимать меры по улучшению эффективности защиты персональных данных.

Первым шагом в обеспечении безопасности персональных данных в образовательном учреждении является разработка политики конфиденциальности. В этом документе необходимо описать, какие персональные данные собираются, с какой целью они используются, а также каким образом они хранятся и защищаются. Следует обратить особое внимание на важность конфиденциальности, а также на процедуры получения согласия на обработку персональных данных.

Рекомендуется разработать и внедрить политику информационной безопасности, которая будет охватывать все аспекты обработки персональных данных: от сбора до удаления. Политика должна быть четкой и понятной для всех, кого это будет касаться, а также должна соответствовать законодательству в области защиты персональных данных.

Политика защиты персональных данных должна включать в себя не только меры технической безопасности, но и правовые, организационные и культурные аспекты. С одной стороны, необходимо создать надежные системы и механизмы, которые обеспечат защиту персональных данных от несанкционированного доступа, утечки или модификации. С другой стороны, важно формировать уровень осведомленности и ответственности среди пользователей и организаций, чтобы они сами принимали меры по защите своих персональных данных.

Важно отметить, что политика защиты персональных данных должна основываться на принципах прозрачности, согласия и минимизации. Это означает, что субъекты данных должны иметь ясное понимание о том, как и для каких целей их персональные данные используются, а также иметь возможность согласиться или отказаться от использования своих данных. Кроме того, собираемая информация должна быть минимальной и необходимой для достижения заданных целей, а хранение данных должно быть ограничено по времени и доступу.

Политика защиты персональных данных также должна быть соответствующей законодательным нормам и регуляциям, действующим в конкретной стране или регионе. Законы о защите данных устанавливают основные правила и требования, которые организации должны соблюдать при обработке персональных данных. Это включает в себя обязательное информирование субъектов данных о целях обработки, обеспечение безопасности хранения и передачи данных, а также предоставление прав на доступ, изменение или удаление своих персональных данных.

Наконец, эффективная политика защиты персональных данных должна регулярно оцениваться и обновляться с учетом изменяющихся технологий, угроз безопасности и законодательных изменений. Обучение и поддержка персонала являются неотъемлемыми частями успешной реализации политики защиты персональных данных, поскольку это гарантирует соблюдение установленных правил и процедур.

В современном цифровом мире, где персональные данные важнее прежнего, образовательные учреждения должны обеспечивать надежную защиту этих данных. Это особенно важно в контексте использования интернет-платформ и онлайн-обучения, которые стали незаменимой частью образовательного процесса. Однако, традиционные методы аутентификации, такие как пароль или учетные данные, не всегда гарантируют уровень безопасности, достаточный для защиты персональных данных. В этой связи, механизмы многофакторной аутентификации (МФА) начинают приобретать определеную популярность.

МФА - это метод безопасности, который требует от пользователя предоставления нескольких независимых форм идентификации для доступа к конкретным системам или ресурсам. Он обеспечивает более высокий уровень безопасности, так как для успешного доступа необходимо пройти несколько этапов аутентификации, включающих что-то, что пользователь знает (например, пароль), что-то, что пользователь имеет (например, физическое устройство) и что-то, что пользователь является (например, биометрические данные). Такое сочетание факторов делает процесс аутентификации более сложным для злоумышленников и повышает уровень защиты персональных данных.

Механизмы МФА могут включать в себя различные технологии, такие как одноразовые пароли, SMS-коды, биометрические данные, аппаратные и программные токены и др. Использование нескольких факторов идентификации позволяет образовательным учреждениям создавать надежные системы безопасности, которые помогают предотвращать несанкционированный доступ к персональным данным, таким как аккаунты пользователей, оценки, личная информация и др.

Однако, несмотря на все преимущества многофакторной аутентификации, ее реализация может иметь некоторые сложности. Дополнительные факторы аутентификации могут быть неудобны для пользователей и требовать дополнительных ресурсов для их внедрения.

Поэтому, для успешной реализации МФА необходимо провести анализ рисков, определить потребности и возможности образовательного учреждения, а также провести обучение пользователей и четкую коммуникацию относительно новых механизмов защиты персональных данных.

В заключение, многофакторная аутентификация представляет собой мощный инструмент для защиты персональных данных в образовательных учреждениях. Этот механизм обеспечивает повышенный уровень безопасности и помогает предотвратить несанкционированный доступ к конфиденциальным информационным ресурсам. Реализация МФА требует тщательной проработки, чтобы найти баланс между безопасностью и удобством пользователей. Однако, ее применение является необходимым шагом в обеспечении надежной защиты персональных данных в образовательной сфере.

Одной из важнейших рекомендаций является осуществление регулярного обучения и тренировок сотрудников по вопросам безопасности данных. Это должно способствовать освению основных правил и процедур по обработке и хранению персональных данных, а также быть в курсе последних угроз безопасности и методов их предотвращения. Такое обучение должно проводиться как при приеме на работу новых сотрудников, так и периодически для существующего персонала.

Далее, необходимо обеспечить безопасность хранения данных. Образовательные учреждения должны использовать надежные системы хранения данных, оснащенные современными механизмами шифрования и авторизации. Важно убедиться, что только авторизованный персонал имеет доступ к персональным данным, и проводить регулярное обучение по вопросам безопасности информации для сотрудников.

Для обеспечения эффективной защиты персональных данных также требуется использование современных технических средств. Это включает в себя применение средств антивирусной защиты, систем обнаружения

вторжений и шифрования данных. Кроме того, необходимо регулярно обновлять программное обеспечение и операционные системы, чтобы устранить известные уязвимости.

Важным аспектом улучшения эффективности защиты персональных данных является контроль доступа к информации. Организации должны разработать строгую систему управления доступом, определяющую, кто имеет право доступа к каким данным и на каких условиях. Дополнительно рекомендуется вести журналы доступа, чтобы иметь возможность отслеживать и контролировать все действия с персональными данными.

Не менее важным является регулярный аудит системы защиты персональных данных. Аудит позволяет выявить потенциальные слабые места в системе и своевременно принять меры по их устранению. Рекомендуется проводить аудиты не реже одного раза в год, а также после любых существенных изменений в системе.

Наконец, для обеспечения эффективности защиты персональных данных, необходимо установить процедуры реагирования на нарушения безопасности. В случае обнаружения инцидента, организация должна иметь готовый план действий, который будет максимально оперативным и эффективным для минимизации ущерба. План должен включать шаги по обнаружению, реагированию, восстановлению и предотвращению повторного нарушения безопасности.

При утечке персональных данных необходимо немедленно принимать решительные меры для минимизации возможных последствий и обеспечения безопасности информации. Ниже представлен план действий, который следует соблюдать в случае утечки персональных данных:

1. Сообщение о нарушении безопасности: Первым шагом необходимо немедленно сообщить о случившемся нарушении безопасности всем заинтересованным сторонам. Это может включать команду по защите данных, руководство учебной организации и т.д. Четкое и оперативное

информирование позволит координировать действия для минимизации ущерба.

2. Анализ причин утечки: Сразу же после обнаружения утечки следует провести тщательный анализ причин нарушения безопасности и определить охват и масштаб инцидента. Это поможет выяснить, каким образом данные могли быть скомпрометированы и какие меры предпринять для устранения возможных уязвимостей.

3. Остановка дальнейшей утечки: При обнаружении утечки персональных данных необходимо не только устранить причины нарушения безопасности, но и прекратить дальнейшую утечку информации. Это может включать отключение серверов, временное закрытие доступа к системам или любые другие доступные меры для предотвращения дальнейшего распространения данных.

4. Анализ и оценка ущерба: Проведение анализа ущерба является ключевым этапом плана действий. Необходимо выяснить, какие конкретно данные были скомпрометированы, кто мог получить к ним доступ и какие меры необходимо предпринять для предотвращения негативных последствий для пострадавших лиц.

5. Информирование пострадавших: После проведения анализа ущерба следует связаться с пострадавшими лицами, уведомить их о случившемся, предоставить им информацию о масштабе утечки и предложить конкретные действия для защиты их персональных данных. Это может включать рекомендации по смене паролейиили любые другие меры, которые помогут предотвратить злоупотребление украденной информацией.

6. Сотрудничество с внешними организациями: В случае серьезной утечки персональных данных может быть целесообразным сотрудничество с внешними организациями и экспертами в области кибербезопасности. Они могут помочь провести расследование, обеспечить техническую поддержку и предложить рекомендации по повышению уровня безопасности в будущем.

7. Анализ и улучшение систем безопасности: После решения утечки персональных данных важно провести анализ существующих систем безопасности и принять меры для их улучшения. Это может включать обновление программного обеспечения, усиление контроля доступа или реорганизацию процессов сбора и хранения персональных данных.

8. Учебные мероприятия и осведомление персонала: Утечка персональных данных может указывать на недостатки в обучении и осведомленности сотрудников о принципах безопасности информации. Необходимо провести учебные мероприятия, направленные на повышение культуры безопасности и осведомленности сотрудников о возможных рисках и мерах предотвращения утечки данных.

План действий при утечке персональных данных представляет собой комплексный подход к решению проблемы и требует немедленной реакции, тщательного анализа и принятия соответствующих мер для обеспечения безопасности и защиты пострадавших лиц.

Применение данных рекомендаций позволить повысить эффективность защиты персональных данных и минимизировать риски утечки или несанкционированного доступа к личной информации.

## 2.2. Обзор средств для повышения защищенности ИС ПДн

Существует множество комплексов защиты ИС ПДн от несанкционированного доступа.

Первым из списка возможных вариантов является программный комплекс «Страж ЭТ» от ООО «РУБИНТЕХ».

Этот продукт включает в себя все необходимое для обеспечения безопасности информации, начиная от двухфакторной аутентификации и загрузки операционной системы, заканчивая маркировкой документов независимо от используемого приложения. Основные преимущества программы включают:

— Возможность использования шв-ключа Guardant ГО, который обеспечивает безопасную двухфакторную аутентификацию и работает только с Stazh NT.

— Низкие системные требования.

— Бесплатная поддержка через телефон или электронную почту.

— Не требуется установка дополнительного программного обеспечения или серверной лицензии (СУБД).

— Возможность обеспечения безопасности не только критической информации, но и государственной тайны.

— Основные недостатки программы:

— Не поддерживаются операционные системы Microsoft Windows XP с пакетом обновлений SP3 (32-разрядная), Microsoft Windows Vista с пакетом обновлений SP2 (32- и 64-разрядная), Microsoft Windows Server 2003 (32- и 64-разрядная). Однако, некоторые предприятия все еще продолжают использовать эти операционные системы, поэтому данное ограничение может быть проблемой. Кроме того, Stazh NT не поддерживает самую новую версию Microsoft Windows Server 2016 (32- и 64-разрядная).

— Отсутствие поддержки смарт-карт.

— Необходимость проверки наличия актуальной версии на сервере производителя.

— Отсутствие поддержки обновления контрольных сумм в конце рабочего сеанса пользователя с программой.

— Не встроена функция антивирусной защиты.

— Отсутствует возможность интеграции с системами и комплексами антивирусной активности.

Ценовая политика(таблица 2)на СЗИ Страж NT 4.0

Таблица №2 - Ценовая политика на СЗИ Страж NT 4.0

| Параметры использования и лицензирования программного продукта | Цена (руб.) за лицензии | | | | | |
|---|---|---|---|---|---|---|
| | 1-10 | 11-25 | 26-100 | 101-250 | 251-1000 | >1000 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Право на использование Стандартноой лицензии НДС „Страж NT“ Версия 4.0. Лицензируется количество АРМ, на которые может быть установлен СЗИ. | 7500р | 6900р | 6400р | 5900р | 5500р | 5000р |
| Установочный комплекс, в который входят cd-r диск с ПО и эксплуатационная документация, защитный футляр для диска, копия сертификата соответствия ФСТЭК, формулятор | 250р | | | | | |
| Обновление предыдущих версий | 3750р | | | 2950р | | |

Следующим продуктом, который мы рассмотрим, является Secret Net от компании "Код Безопасности". Основные плюсы данного продукта:

— Кроссплатформенность, возможность работы в операционных системах Windows и Linux.

— Поддержка смарт-карт Jacarta.

— Возможность контроля неизменности аппаратной конфигурации компьютера и блокировки при подключении или отключении заданных устройств.

— Поддержка теневого копирования информации, выводимой на внешние носители.

Недостатки этой программы:

— Техническая поддержка предоставляется на 1 год и имеет различные пакеты с приоритетом обслуживания, которые приобретаются за дополнительную плату, за исключением базового пакета

— Разработчик предлагает отдельное программное решение для защиты сведений, являющихся государственной тайной (Secret Net Studio-C)

— Высокие системные требования для автоматизированных рабочих мест.

Ценовая политика(таблица 3)Secret Net от компании "Код Безопасности"

Таблица №3 - Ценовая политикаSecret Net от компании "Код Безопасности"

| Параметры использования и лицензирования программного продукта | Цена |
|---|---|
| | За 1-50 лицензий |
| Право на использование комплекта «Максимальная защита» | 6200р |
| Право на использование комплекта «Оптимальная защита» | 5300р |
| Право на использование комплекта «Постоянная защита» | 9100р |
| Право на использование комплекта «Дополнительная защита» | 2800р |
| Установочный комплект | 275р |
| Установочный комлект. Сертифицированное СЗИ Secret Net Studio-С 8 | 275р |
| Установочный комлект. Сертифицированное СЗИ Secret Net Studio - 8 | 275р |
| Дубликат формулятора (для ПО) или паспорта (для аппратаных средств) без голограммы | 1100р |
| Ключ активации сервиса прямой технической поддержки уровня «Стандартный» | 20% |
| Ключ активации сервиса прямой технической поддержки уровня «Расширенный» | 30% |

КриптоАРМ предназначена для защиты корпоративной и личной информации, передаваемой по сети Интернет, электронной почте и на съемных носителях (дисках, флэш-картах).

Криптоарм ГОСТ - мощный инструмент, разработанный для создания и проверки усиленной квалифицированной электронной подписи. Он позволяет значительно сократить временные и финансовые расходы на обмен документами, а также безусловно подтвердить авторство документа. Благодаря возможности шифрования файлов, Криптоарм ГОСТ гарантирует

полную конфиденциальность информации, хранящейся в электронном виде и передаваемой по незащищенным каналам связи, предоставляя доступ только тому, кто обладает закрытым ключом. Кроме того, Криптоарм ГОСТ - кроссплатформенная программа с простым и понятным интерфейсом, что делает его использование максимально удобным и эффективным. Однако для безупречной работы программы необходимо наличие криптоконтейнера КриптоПро CSP с версией не ниже 4, что влечет за собой некоторые дополнительные затраты. Также важно учесть, что для взаимодействия с ключевыми носителями потребуется установка соответствующих драйверов.

Приобретение данного продукта с неограниченной лицензией на 1 компьютер будет стоить 2900 рублей 00 копеек. Учитывая то, что как минимум на 4 компьютера необходимо будет произвести установку, в итоге получится 11600 рублей 00 копеек.

Достоинства:

— Кроссплатформенность — поддержка Microsoft Windows, macOS и Linux, iOS, Android. Поддержка стандартов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 для хеширования и электронной подписи.

— Поддержка современных ключевых носителей.

Недостатки:

— Интерфейс может вызвать трудности у неподготовленного пользователя.

— Для работы требуется наличие СКЗИ КриптоПро CSP со своей лицензией, что приводит к дополнительным тратам.

Secret Disk 5 в первую очередь это:

— Защита от несанкционированного доступа и утечки конфиденциальной информации, хранящейся и обрабатываемой на персональном компьютере или ноутбуке

— Разграничение прав пользователей на доступ к защищённой информации с использованием надёжной двухфакторной аутентификации (владение электронным ключом и знание пароля)

— Защита информации на съёмных носителях

— Сокрытие наличия на персональном компьютере конфиденциальных данных

— Шифрование данных. Secret Disk 5 обеспечивает защиту данных путём шифрования разделов на жёстких дисках, томов на динамических дисках, виртуальных дисков и съёмных носителей.

Минусы:

К минусам продукта следует отнести ориентацию только на технологии Microsoft, в построении базы данных, в административном Web-сервере, в корпоративном каталоге и в поддержки клиентских рабочих станций. Все компоненты могут работать только под управлением операционных систем Windows. В случае ГБПОУ «КГСТ» это не совсем минус, поскольку на всех компьютерах используется именно эта ОС. Общая стоимость приобретения будет составлять 9120 рублей 00 копеек.

Таким образом, самым оптимальным продуктом по стоимости и фунционалу является Secret Disk 5.

Одной из основных причин выбора Secret Disk 5 является его эффективность в защите от несанкционированного доступа к конфиденциальным данным. Программа позволяет создавать зашифрованные виртуальные диски, которые невидимы для других пользователей. Это означает, что даже если злоумышленники получат физический доступ к вашему компьютеру, они не смогут найти и расшифровать защищенные данные. Secret Disk 5 обеспечивает надежную защиту ваших файлов и папок от несанкционированного доступа.

Еще одним фактором, делающим Secret Disk 5 оптимальным выбором, является его простота использования. Программа обладает интуитивно понятным интерфейсом, что позволяет даже новичкам быстро и легко

создавать и управлять зашифрованными дисками. Благодаря удобной навигации и понятным инструкциям, пользователи могут легко освоить все функции программы и настроить ее под свои потребности.

Secret Disk 5 обладает также впечатляющей скоростью работы, что является еще одним веским аргументом в его пользу. Программа эффективно работает на всех типах жестких дисков и не замедляет процесс чтения и записи данных. Она позволяет вам оставаться проактивным и продуктивным, несмотря на наличие зашифрованных дисков.

Кроме того, Secret Disk 5 обеспечивает множество дополнительных функций, которые делают его еще более привлекательным для использования. Пользователи могут установить пароли на созданные виртуальные диски, а также указать время автозакрытия при неактивности. Это позволяет избежать случайной утечки информации и обеспечить дополнительный уровень безопасности.

В заключение, Secret Disk 5 является надежным и эффективным решением для защиты конфиденциальной информации. Его простота использования, высокая производительность и дополнительные функции делают его идеальным выбором. Необходимость выбирать Secret Disk 5 становится очевидной, когда речь идет о защите персональных данных.

## 2.3. Экономический расчет повышения защищенности ИС персональных данных в ГБПОУ «КГСТ»

В современном информационном обществе обеспечение безопасности персональных данных является одним из наиболее важных аспектов во всех сферах деятельности. Особое внимание к этому вопросу уделяется в образовательных учреждениях, где хранятся большие объемы личной информации учащихся, преподавателей и сотрудников.

Целью данного экономического расчета является определение финансовых затрат, необходимых для улучшения защиты персональных данных в образовательном учреждении. Уровень безопасности информации

напрямую влияет на репутацию учебного заведения и доверие к нему со стороны обучающихся, родителей и общественности в целом.

В первую очередь необходимо провести анализ текущего уровня защиты персональных данных в образовательном учреждении. Это включает оценку существующей системы хранения, передачи и доступа к информации, а также выявление возможных уязвимостей и рисков. Для этого могут быть задействованы специалисты в области информационной безопасности.

На основе проведенного анализа необходимо составить план мероприятий по улучшению защиты персональных данных. Возможные меры могут включать в себя:

1. Обновление программного обеспечения, включая операционные системы и антивирусные программы, для обеспечения актуальной защиты от новых угроз.

2. Внедрение системы шифрования данных для защиты информации от несанкционированного доступа.

3. Тщательное обучение сотрудников учебного заведения правилам безопасного хранения и обработки персональных данных.

4. Модернизация сетевой инфраструктуры для обеспечения стабильной и безопасной передачи информации.

5. Создание резервных копий данных для предотвращения их потери при возможных сбоях или атаках.

6. Проведение регулярных проверок и аудитов системы безопасности для выявления и устранения возможных уязвимостей.

Расчет финансовых затрат на улучшение защиты персональных данных в образовательном учреждении включает оценку стоимости необходимых технических средств, программного обеспечения, обучения персонала и возможных консультаций со специалистами. Также следует учесть потенциальные экономические выгоды от повышения уровня

безопасности, такие как уменьшение риска утечки данных или штрафов за нарушение законодательства о защите персональных данных.

В итоге, реализация мер по улучшению защиты персональных данных в образовательном учреждении позволит повысить уровень безопасности информации и защитить конфиденциальность личных данных. Это также способствует созданию доверительной атмосферы среди всех участников образовательного процесса и повышению репутации учебного заведения, что имеет положительный экономический эффект в долгосрочной перспективе.

В ходе анализа по улучшению защиты персональных данных, был выбран вариант установки на рабочие компьютеры сотрудников программного обеспечения Secret Disk 5. Почему же выбор пал на данное ПО?

Это одна из самых совершенных систем шифрования и скрытия файлов на персональных компьютерах. Разработана уже пятая версия этого революционного программного обеспечения, подарившего пользователям по всему миру незаметное хранение личной информации и превосходную защиту от несанкционированного доступа.

Возникновение и развитие Secret Disk обрамлены декадами разработки ведущих инженерных команд и константного совершенствования алгоритмов шифрования и механизмов скрытого хранения данных. История всей системы уходит корнями в прошлое, когда компания Disk Security Ldt., вдохновленная жаждой эффективной безопасности, начала свой путь в реставрации файлов на поврежденных носителях. История создания Secret Disk 5 была переполнена моментами настойчивости, трудностей и мгновений вдохновения. Каждая сделанная кнопка, каждый кусочек кода были продуманы до мельчайших деталей, чтобы обеспечить безупречную работу и защиту самой конфиденциальности пользователей.

Первые версии позволяли пользователю создать скрытый раздел на компьютере, в который можно было замаскировать конфиденциальные

файлы. Но с ростом сложности задач, стоявших перед программистами, Secret Disk 5 превзошел все ожидания.

Мастерски соединяя безупречный дизайн с передовыми криптографическими методами, разработчики Secret Disk 5 создали шедевральную систему для защиты конфиденциальных данных. Этот продукт сразу был востребован в кругу узких специалистов по информационной безопасности, проникая постепенно в индустрию и превращаясь в неотъемлемый атрибут многих пользователей.

Одной из самых важных черт Secret Disk 5 стало то, что он обеспечивал шифрование не только данных, но и служебных файлов операционной системы, предотвращая возможность идентификации самой программы в системе.

Основное назначение Secret Disk 5 - это защита личных данных, конфиденциальных файлов и ценной информации от посторонних глаз. Создание виртуального диска займет всего несколько минут. Можно выбрать необходимое имя и букву диска, на которой виртуальный диск будет отображаться. После создания виртуального диска есть возможность добавить на него все необходимые файлы и папки, которые необходимо скрыть от остальных пользователей.

Так же сущесвует возможность установить пароль для доступа к виртуальному диску. Только ответсвтенное лицо и те сотрудники, которым был передан пароль, смогут открыть диск и просматривать его содержимое. Это обеспечит максимальную безопасность персональных данных и избавит от вохможной утечках информации.

Secret Disk 5 также предлагает функцию автоматического скрытия виртуального диска. Это возможность позволяет установить определенные горячие клавиши, которые позволят мгновенно скрыть весь виртуальный диск и его содержимое.

Также одной из главных преимуществ Secret Disk 5 является его простота использования. Чтобы создать виртуальный диск, не понадобятся специальные навыки или знания компьютерной техники.

При загрузке операционной системы пользователю предъявляется электронный ключ, который обеспечивает доступ к персональному компьютеру. Однако злоумышленники или недобросовестные сотрудники могут потенциально использовать этот ключ для несанкционированного доступа к закрытым ресурсам, таким как корпоративные серверы или платежные данные пользователей. Стандартные средства авторизации операционной системы Microsoft Windows недостаточно надежны для эффективного ограничения загрузки и работы в системе. Однако применение электронных USB-ключей и смарт-карт для аутентификации пользователей до загрузки ОС позволяет предоставлять доступ к компьютеру только правомерным пользователям с соответствующими правами.

Secret Disk 5 предлагает наиболее безопасную и надежную процедуру подтверждения прав пользователя - двухфакторную аутентификацию. Для доступа к данным необходимы не только наличие электронного ключа, но и знание пароля к нему. Новый режим шифрования, применяемый в Secret Disk 5, обеспечивает повышенную безопасность пользовательских данных. Зашифрованные файлы и папки с конфиденциальными данными пользователя становятся недоступными даже системному администратору в параллельной сессии Windows. Secret Disk 5 предоставляет ключ шифрования только легитимному владельцу информации.

Создание и восстановление резервной копии файлов в зашифрованных папках может осуществляться системным администратором сети дистанционно. При этом данные остаются зашифрованными и недоступными ни администратору, ни злоумышленникам.

В Secret Disk 5 реализованы две функции безопасного удаления данных. Первая - необратимое удаление данных, что делает невозможным их восстановление стандартными средствами Windows или сторонними приложениями. Вторая - перемещение файла без возможности восстановления по исходному пути, что позволяет перенести файл или папку и одновременно безвозвратно удалить их по исходному пути.

Технические характеристики.

Поддерживаемые платформы:

– Microsoft Windows 10.

– Microsoft Windows 8.1.

– Microsoft Windows 8.

– Microsoft Windows 7.

– Microsoft Windows Vista.

Типы поддерживаемых защищаемых ресурсов:

– Системный раздел жёсткого диска.

– Основные разделы и логические диски в дополнительных разделах базовых жёстких дисков.

– Тома динамических дисков.

– Съемные диски (USB- и Flash-диски и др.).

– Виртуальные диски.

– Файловые папки на системном и логических томах и съёмных дисках (за исключением системных папок операционной системы).

Таким образом, если приобретать данное программное обеспечение у производителя, то лицензия на право использования сертифицированной версии Secret Disk 5 с сетевым управлением, на 1 год будет стоить в 9120 рублей 00 копеек.

В противном случае, если будут выявлены нарушения в области информационной безопасности образовательной организации, то это может повлечь за собой уголовную, административную, дисциплинарную и гражданскую ответсвтенность (таблица 4), которая может быть применена

в отношении олрганизации, руководителя организации, виновного работника и т.д.

Таблица 4 – Нарушения в области информационной безопасности и соответствующие им штрафы

| Уголовная ответственность | | |
|---|---|---|
| Статья 137 УК РФ. Нарушение неприкосновенности частной жизни | Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации | наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев |
| Статья 272 УК РФ. Неправомерный доступ к компьютерной информации | Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации | наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев |
| Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей | Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование | наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев |

| | | |
|---|---|---|
| | компьютерной информации, причинившее крупный ущерб | |

Продолжение таблицы 4

| Административная ответственность | | |
|---|---|---|
| Статья 13.11 КоАП. Нарушение законодательства Российской Федерации в области персональных данных | Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных | влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от шестидесяти тысяч до ста тысяч рублей |
| Статья 13.12 КоАП. Нарушение правил защиты информации | Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации | влечет наложение административного штрафа на граждан в размере от одной тысячи до одной тысячи пятисот рублей; на должностных лиц - от одной тысячи пятисот до двух тысяч пятисот рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей. |
| | Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации | влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой |
| Статья 13.13 КоАП. Незаконная деятельность в области защиты информации | Занятие видами деятельности в области защиты информации (за исключением информации, составляющей | влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; |

| | | |
|---|---|---|
| | государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна) | на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой |

Продолжение таблицы 4

| | | |
|---|---|---|
| Статья 13.14 КоАП. Разглашение информации с ограниченным доступом | Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей | влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц - от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от ста тысяч до двухсот тысяч рублей |
| Дисциплинарная ответственность | | |
| Статья 90 ТК РФ | Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника | |
| Статья 192 ТК РФ | Дисциплинарные взыскания | |
| за совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям. | | |

В соответствии с Федеральным законом «Об образовании в Российской Федерации», каждое образовательное учреждение (учреждение, занимающееся образовательным процессом) является юридическим лицом.

При этом максимальная сумма штрафа, которую может получить образовательная организация за нарушения в области информационной безопасности, составляет 370 000 рублей. Кроме того, также возможны конфискация средств защиты, приостановление или прекращение обработки персональных данных. В случае обнаружения нарушений выдается предписание с указанием сроков и требуемых мер для их устранения. По истечении указанных в предписании сроков на выполнение

требований производится проверка их исполнения. Если результат проверки отрицательный, будут применены санкции и выдано новое предписание.

Таким образом, целесообразно приобрести сертифицированную версию Secret Disk 5 с сетевым управлением, стоимость которого в год будет составлять 9120 рублей 00 копеек. Данное приобретение экономически эффективно, при учете максимальной суммы штрафа за нарушения в области информационной безопасности.

## Вывод по Главе 2

По итогам второй главы магистерской диссертации можно сделать следующие выводы.

В современном информационном обществе, где цифровые технологии проникают во все сферы нашей жизни, защита персональных данных становится все более актуальной и необходимой. Особое внимание следует уделить этому вопросу в образовательных организациях. Зачем же необходимо улучшать защиту персональных данных в таких учреждениях?

Во-первых, образовательные организации работают с большим объемом персональных данных учащихся, преподавателей и персонала. Это могут быть контактные данные, результаты учащихся, медицинские данные и прочая информация, которая требует особой осторожности и конфиденциальности. Отсутствие должной защиты данных может привести к их утечке или злоупотреблению, что может серьезно нарушить приватность и безопасность личной информации.

Во-вторых, с учетом современных требований к образованию, все больше внимания уделяется цифровизации процессов в образовательных учреждениях. В связи с этим значительная часть информации, включая материалы обучения, задания, оценки и коммуникацию, становится доступной в электронном виде. Это открывает новые возможности, но также увеличивает уязвимость к кибератакам и нарушениям

информационной безопасности. Улучшение защиты персональных данных в образовательной организации позволяет оптимизировать процессы цифровизации, обеспечивая конфиденциальность и целостность информации.

В-третьих, улучшение защиты персональных данных в образовательных организациях способствует укреплению доверия учащихся, родителей и других заинтересованных сторон. Когда люди знают, что их личная информация находится под надежной защитой, они чувствуют себя более комфортно и спокойно. Это влияет на качество обучения, стимулирует активное взаимодействие между участниками образовательного процесса, создает благоприятную атмосферу для обмена знаниями и опытом.

Наконец, улучшение защиты персональных данных в образовательных организациях является правовым требованием. Многие страны разрабатывают и внедряют законодательство, которое регулирует сбор, использование и хранение персональных данных. Нарушение этих правил может повлечь за собой серьезные юридические последствия и штрафы. Поэтому образовательным учреждениям в своих интересах создать эффективные и надежные системы защиты данных для соблюдения законодательства и защиты интересов своих пользователей.

В данной главе были рассмотрены рекомендации по улучшение эффективности защиты персональных данных и расписан экономический расчет по усовершенсвованию защиты персональных данных.

Таким образом, улучшение защиты персональных данных в образовательной организации имеет высокую важность. Это обеспечивает конфиденциальность, безопасность и целостность информации, способствует развитию цифровизации в образовании, укрепляет доверие и соответствует правовым требованиям.

Предотвращение утечек и злоупотреблений с персональными данными является гарантией защиты прав участников образовательного

процесса и сохранения доверительных отношений в информационном обществе.

# ЗАКЛЮЧЕНИЕ

Исходя из проведенных исследований, можно сделать вывод о том, что вопрос защищенности информационных систем персональных данных в образовательной организации является актуальным, и вариантов решения данного вопроса может быть большое количество.

Защищенность информационных систем представляет собой целую совокупность различных факторов и условий, которые могут работать только в общем тандеме.

Были сделаны выводы о том, что в современном мире сохранение персональных данных играет важную роль в образовательных учреждениях. Обучающие программы по безопасности данных являются эффективным инструментом в повышении уровня осведомленности и компетенции сотрудников, студентов и родителей. Они помогают минимизировать риски утечки информации, скачковый доступ и злоупотребление персональными данными. Внедрение таких программ является неотъемлемой частью стратегии безопасности данных в обучающих учреждениях, гарантирующей сохранность и конфиденциальность персональной информации всех заинтересованных сторон.

Улучшение защиты персональных данных в образовательных организациях является правовым требованием. Многие страны разрабатывают и внедряют законодательство, которое регулирует сбор, использование и хранение персональных данных. Нарушение этих правил может повлечь за собой серьезные юридические последствия и штрафы. Поэтому образовательным учреждениям в своих интересах создать эффективные и надежные системы защиты данных для соблюдения законодательства и защиты интересов своих пользователей.

Отсюда, было выявлено наличие множества документов по защите персональных данных, которые регулируют разработку собственных нормативных документов в организациях, а именно:

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

—Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

—Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

—ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утверждено постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469 и т.д.

Были рассмотрены основные категории персональных данных, а также классы нарушений безопасности персональных данных, выделены основные приемы защиты персональных данных в образовательном учреждении,

Был проведен анализ состояния информационной системы персональных данных в ГБПОУ «КГСТ» на примере АИС «Сетевой город. Образование».

Были рассмотрены варианты улучшения защиты персональных данных в образовательных организациях, которые должны способствовать укреплению доверия учащихся, родителей и других заинтересованных сторон. Это влияет на качество обучения, стимулирует активное взаимодействие между участниками образовательного процесса, создает благоприятную атмосферу для обмена знаниями и опытом.

Были рассмотрены рекомендации по улучшение эффективности защиты персональных данных и рассмотрена возможность внедрения двухфакторной аутентификации на рабочих компьютерах сотрудников, работающих с персональными данными в ГБПОУ «КГСТ».

Таким образом, улучшение защиты персональных данных в образовательной организации имеет высокую важность. Это обеспечивает конфиденциальность, безопасность и целостность информации, способствует развитию цифровизации в образовании, укрепляет доверие и соответствует правовым требованиям.

Предотвращение утечек и злоупотреблений с персональными данными является гарантией защиты прав участников образовательного процесса и сохранения доверительных отношений в информационном обществе.

## Список литературы


1. Виртуальный клуб юристов//Как выполнить требования Федерального Закона № 152-ФЗ «О персональных данных» - Режим доступа: http://www.yurclub.ru/docs/administrative/article19.html (дата обращения: 20.10.2023)
2. Гатиятуллина Э.М. «Защита персональных данных в условиях цифровизации: эволюция и современное состояние» // Журнал «Закон и власть» [2023] – URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-usloviyah-tsifrovizatsii-evolyutsiya-i-sovremennoe-sostoyanie
3. Кадомец К.С. «Защита персональных данных с помощью шифрования» // Журнал «E-Scio» [2023] – URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-s-pomoschyu-shifrovaniya(дата обращения: 23.10.2023)
4. Китана А.Н. «Защита персональных данных по законодательству российской федерации» // Журнал « Восточно-европейский научный журнал» [2021] – URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-po-zakonodatelstvu-rossiyskoy-federatsii (дата обращения: 23.10.2023)
5. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (дата обращения: 01.12.2023)
6. Комплексное обеспечение безопасности персональных данных при их обработке в информационной системе персональных данных ООО "Арсенал+"- URL: https://revolution.allbest.ru/programming/00264509_2.html#1 (дата обращения: 23.10.2023)
7. Криволапова Л.В. «Защита персональных данных» //Журнал «Право и государство: теория и практика» [2020] – URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-2 (дата обращения: 10.11.2023)

8. Куликова С.В. «Первые шаги в науку» // - URL: http://rushkolnik.ru/docs/index-34551452.html(дата обращения: 23.10.2023)

9. Михайлов А.А., Мороз А.Р.,Уманский С.А.,Шустрова А.Н. «Двухфакторная аутентификация» // Журнал «Инновационные аспекты развития науки и техники» [2021] – URL: https://cyberleninka.ru/article/n/dvuhfaktornaya-autentifikatsiya (дата обращения: 15.11.2023)

10. Николаева К.А., Шабурова А.В. «Совершенствование политики информационной безопасности в организации» // Журнал «Интерэкспо Гео-Сибирь» [2022] – URL: https://cyberleninka.ru/article/n/sovershenstvovanie-politiki-informatsionnoy-bezopasnosti-v-organizatsii (дата обращения: 23.11.2023)

11. Новиков А.Л. «Организация многофакторной аутентификации пользователей в корпоративной сети»» // Журнал «Вестник науки» [2023] – URL: https://cyberleninka.ru/article/n/organizatsiya-mnogofaktornoy-autentifikatsii-polzovateley-v-korporativnoy-seti (дата обращения: 01.12.2023)

12. Серикулы Орынбек «Двухфакторная аутентификация как метод обеспечения информационной безопасности» // Журнал «Вестник магистратуры» [2019] – URL: https://cyberleninka.ru/article/n/dvuhfaktornaya-autentifikatsiya-kak-metod-obespecheniya-informatsionnoy-bezopasnosti

13. Сетевой Город. Образование/URL: http://schoolroo.ru/Help/index.html?personaldata.htm (дата обращения: 01.12.2023)