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

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Анализ защищенности информационных систем персональных данных в профессиональной образовательной организации

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

Проверка на объем заимствований:
73,07 % авторского текста

Работа рекомендована к защите
«16» декабря 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Лысенко Никита Алексеевич

Научный руководитель:
д.т.н., профессор
Белевитин Владимир Анатольевич

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования.

Повсеместное развитие, разработка и интеграция информационных технологий является основным вектором развития современного научно-технического прогресса. Рассматриваемые технологии находят свое активное использование практически во всех как бытовых, так и профессиональных сферах жизнедеятельности человека. В частности, одной из наиболее важных с точки зрения необходимости использования информационных технологий, сферой является образование. Несмотря на ряд объективных преимуществ, которые несет использование новых технологий в образовании, наблюдается целое множество как потенциальных, так и реальных проблем, связанных с безопасностью студентов. Во многом это связано с обработкой и хранением большого количества персональных данных, владение которыми может привести к серьезным негативным последствиям и нарушить безопасность личности студента. В связи с этим актуализируется задача, связанная с более подробной проработкой и исследованием данного вопроса, а также формированием требований к задаче по обеспечению безопасности хранения персональных данных. [28]

Защита персональных данных граждан России – это вопрос национальной безопасности страны. Стратегической планом государства является модернизация информационной инфраструктуры России, с целью становления России одним из мировых центров хранения, обработки, передачи и надежной защиты информационных массивов, так называемых больших данных. Проблемы защиты персональных данных и поиска баланса интересов личности, государства и общества отмечается в действующих программных документах:

1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Конвенция Совета Европы от 28 января 1981 года № 108 «О защите персональных данных».

3. ГОСТ Р ИСО/МЭК 27001-2013 «Информационная технология. Методы обеспечения информационной безопасности. Системы управления информационной безопасностью. Требования».

4. ГОСТ Р ИСО/МЭК 27799-2012 «Информационная технология. Методы обеспечения информационной безопасности. Руководство по рисканализу в области информационной безопасности».

5. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении Правил обработки персональных данных».

6. Рекомендации различных организаций, таких как Институт информационной безопасности ISO, The International Association of Privacy Professionals (IAPP) и др

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы при рассмотрении вопросов защиты данных и информации указывает на «необходимость соблюдения баланса между своевременным внедрением современных технологий обработки данных с защитой прав граждан, включая право на личную и семейную тайну». [5]

Обучение и социализация обучающихся в условиях гиперинфорамционного общества предопределили утверждение Концепции информационной безопасности, приоритетными задачами которой являются: повышение уровня медиаграмотности студентов, формирование у обучающихся чувства ответственности за свои действия в информационном пространстве; воспитание ответственности за свою жизнь, здоровье и судьбу, изживание социального потребительства и инфантилизма.

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

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

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

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

К основным угрозам безопасности персональных данных возможно отнести следующие:

− получение доступа третьими лицами к информационным сервисам организации;

− перехват третьими лицами аутентифицирующей информации;

− получение доступа во внутренние информационные подсистемы;

− кражи заинтересованными лицами личных персональных данных сотрудников вуза и студентов;

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

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

− нарушение доступа к веб-сайту.

Особое внимание уделяется вопросам защиты персональных данных в автоматизированных информационных системах. Требования к защите персональных данных, в соответствии с рядом документов, учитывают категорию и количество персональных данных, специфику решаемых задач и ряд других показателей. Выполнение этих требований, как правило, связано с существенными материальными и финансовыми затратами, вызванными необходимостью создания системы защиты, обеспечением высокой квалификации персонала, получением разрешительных документов, что не

всегда возможно для большого числа пользователей информации и операторов, представляющих малобюджетные организации. [26]

На современном этапе развития общества и цифровых технологий, становится очевидным тот факт, что образовательным организациям все сложнее обеспечивать соответствие законодательству по обеспечению персональных данных всех субъектов образовательного процесса. [27]

Цель исследования: на основе теоретического анализа разработать рекомендации для реализации защиты персональных данных в профессиональной организации с учетом требований нормативно-правовой базы Российской Федерации.

Объектом исследования является организация системы защиты персональных данных в профессиональной организации.

Предметом исследования является защита персональных данных.

Гипотеза: Следует ожидать, что повышение эффективности системы защиты персональных данных возможно, если оценить существующие средства защиты и обеспечить их оптимальное обновление с учетом соответствия техническим требованиям.

Задачи исследования:

1. Рассмотреть понятие и значение защищенности информационных систем персональных данных в образовательной организации.

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

3. Определить способы организации защиты персональных данных в образовательной организации.

4. Провести оценку информационной безопасности персональных данных в ФГБОУ ВО «Южно-уральский государственный технический колледж».

5. Разработать рекомендации по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный технический колледж» г. Челябинска.

6. Оценить эффективность рекомендаций по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный технический колледж».

Методы исследования. Для написания работы использовались такие методы, как: изучение и анализ теоретико-методической литературы по теме исследования, анализ документации образовательной организации, анализ и сопоставление имеющихся средств для защиты данных, проектирование системы защиты персональных данных.

Теоретико-методологическая база исследования сформирована на официальных материалах и открытых публикациях авторов, таких как: Авдеев М.Ю., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Кузнецова Т.В., Лушников А., Медведева Т.М., Савельев А.И., Серков П.П., Ситникова Е.Г., Сенаторова Н.В., Терещенко Л.К., рассмотревших в своих работах вопрос защищенности персональных данных.

Положения, выносимые на защиту:

Разработанные рекомендации по организации системы защищенности информационной системы персональных данных для ФГБОУ ВО «Южно-Уральский государственный технический колледж» г. Челябинска. Данные рекомендации позволят обеспечить более высокий уровень безопасности хранения персональных данных в образовательной организации.

Научная новизна магистерской диссертации заключается в разработке новой модели обеспечения безопасного хранения персональных данных, включающей в себя три основных блока: обеспечение безопасности в информационном пространстве образовательной организации; освоение компетенций ИБ студентами; пакет нормативно-правовых документов.

Практическая значимость исследования. Практическая значимость работы заключается в разработке рекомендаций по организации системы защиты персональных данных в образовательной организации, разработанной на основе

анализа частной модели угроз ФГБОУ ВО «Южно-Уральский государственный технический колледж», которые могут быть применены в других образовательных организациях

База исследования. ФГБОУ ВО «Южно-Уральский государственный технический колледж».

Этапы исследования. На первом этапе формулировалась тема исследования, проводился сбор информации по теме исследования из различных источников, осуществлялась формулировка гипотезы, постановка цели, задач.

В ходе второго этапа осуществлялся анализ защищенности персональных данных в организации, проводился анализ научной литературы и отбор информации по теме исследования.

Третий этап заключался в предложении рекомендаций по организации системы защищенности информационной системы персональных данных в ФГБПОУ "ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ".

Структура и объем работы.

Работа включает в себя титульный лист, содержание, введение, две главы, заключение, список литературы и приложения. Во введении актуальность темы исследования, сформулированы цель и главные задачи исследования, определен его объект и предмет, сформулирована научная новизна и гипотеза, а также представлен перечень методов, которые были использованы в исследовании.

В первой главе представлены теоретические аспекты защищенности информационных систем персональных данных в профессиональной организации. В частности, параграф один рассматривает специфику понятия защищенности персональных данных; параграф два посвящен нормативно-правовому аспекту защищенности персональных данных в РФ; параграф три рассматривает основные особенности планирования, внедрения и реализации защиты персональных данных в профессиональной организации.

Во второй главе проводится анализ уровня защиты персональных данных в ФГБОУ ВО «Южно-Уральский государственный технический колледж» г. Челябинска и разрабатываются рекомендации по организации системы защиты персональных данных в образовательной организации. В частности, параграф один рассматривает основные сведения об образовательной организации; параграф два посвящен анализу условий, необходимых для реализации рекомендаций для защиты персональных данных в профессиональной организации; параграф три посвящен анализу результатов экспериментальной работы.

В заключении подведены основные итоги и рассмотрены результаты проведенного исследования.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРОФЕССИОНАЛЬНОЙ ОРГАНИЗАЦИИ.

1.1. Понятие защищенности персональных данных в профессиональных организациях.

Понятие «персональные данные» считается относительно молодым, его появление связывают с периодом после окончания Второй мировой войны, когда постепенно возникает необходимость в компьютерной безопасности, а в дальнейшем и в сетевой безопасности. В это время правовые системы обращают все больше и больше внимания на регулирование оборота информации о физических лицах и практически разрабатывают новое субъективное право – право индивида на его «персональные данные». Тем не менее, еще задолго до возникновения самого термина «персональные данные», распространение личной информации о других людях в той или иной степени подлежало регулированию как со стороны общества, так и со стороны государства.

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

То есть персональные данные рассматриваются, как различная информация, которая прямо или косвенно относятся к определенному физическому лицу, т.е. субъекту персональных данных. В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Изменения, связанные с регулированием персональных данных (информации о личной жизни человека), происходят сейчас во многих государствах, в том числе и в России, и в первую очередь данная проблема затрагивает образовательную сферу. Под обработкой персональных данных понимается любое действие (операция) или их совокупность, с применением средств автоматизации или без них для их сбора, хранения, использования, предоставления, удаления. [9]

В настоящее время вопрос обработки персональных данных находится в секторе внимания абсолютно любой организации. И на это есть ряд причин. 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. [12]

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 текущих реалиях трудно найти организацию, которая не обрабатывала бы персональные данные своих сотрудников. С момента заключения трудовых отношений хотя бы с одним гражданином, организация становится оператором персональных данных и, соответственно, принимает на себя обязанности по защите указанной информации, становится поднадзорной контролирующим органам, т.н. «регуляторам» (которых на сегодняшний день три).

В свою очередь, любой гражданин в процессе своей жизни вступает во взаимоотношения с различными физическими и юридическими лицами. В результате данного взаимодействия накапливаются данные о конкретном индивиде, начиная с простых (фамилии, имени, отчестве) и заканчивая специфическими (сведения о здоровье, сведения о судимости, биометрические данные). При этом, гражданин может не желать, чтобы эти сведения становились известными широкому кругу лиц. В целях защиты указанной информации используется специальный правовой режим персональных данных. Для обеспечения данного правового режима в 2006 году был принять отдельный Федеральный закон «О персональных данных». Периодически, в него вносятся

поправки, касающиеся обработки персональных данных и принимаются новые подзаконные нормативно-правовые акты, направленные на конкретизацию его норм, так последние поправки вступили в силу в сентябре 2015 года.

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

Термин персональные данные, в свою очередь, тесно связан с понятием обработка. Обработка персональных данных начинается тогда, когда 12 гражданин «свободно, своей волей и в своем интересе» (на что прямо указано в ч. 1 ст. 9 Федерального закона «О персональных данных») передает свои данные оператору для выполнения каких-либо функций (например, заключение трудового договора) или делает их общедоступными (например, регистрируясь в социальных сетях).

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

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 проверки, 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.

Наиболее остро вопрос защиты персональных данных стоит в сферах здравоохранения, образования, финансов, и в государственных органах. Эти обстоятельства предъявляют повышенные требования к системе защиты персональных данных и являются приоритетными для проведения проверок контролирующими органами.

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

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

− передача удаленным пользователем своих идентификационных данных программистам;

− обмен данными пользователя с сервером информационных систем образовательной организации;

− авторизация пользователя;

− шпионские программы, внедренные в информационную систему образовательной организации. Основные инструменты, которыми пользуются злоумышленники для доступа к персональным данным: − слабые пароли, которые создают удаленные пользователи;

− уязвимость каналов передачи персональных данных; − вредоносное программное обеспечение;

− непрофессиональная конфигурация сети передачи персональных данных;

− уязвимости средств и мер защиты.

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

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

− внедрение современных мер защиты персональных данных;

− организация системы всесторонней защиты персональных данных.

В целом защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности любой организации. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение 14 положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности.

1.2. Нормативно-правовой аспект защиты персональных данных в Российской Федерации.

Вопросы по соблюдению конфиденциальности персональных данных в последние годы остаются неизменными и поднимаются как в России, так и за рубежом, потому что они касаются всех граждан, независимо от их национальности и положения.

Основным нормативным актом в области персональных данных является, прежде всего, Конституция Российской Федерации от 12 декабря 1993 года. Этот

документ определяет информацию о лице, которая должна быть защищена законом от наиболее общей формы нарушения. Согласно Конституции Российской Федерации, «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений». А также «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». [8]

Вторым по значимости документом в области персональных данных является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». С момента издания, в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» были внесены изменения, а именно, уточнены основные постулаты о защите персональных данных, а также была запрещена первичная обработка персональных данных за пределами территории Российской Федерации. Это базовый закон, раскрывающий понятие персональных данных, дающий представление о том, как обращаться с персональными данными государственным и муниципальным учреждениям, организациям, используя или не используя средства автоматизации. Он определяет права субъекта персональных данных, обязанности оператора, а именно принципы и условия обработки персональных данных, раскрывает понятие конфиденциальности персональных данных и согласие на обработку, а также концепцию государственного контроля за обработкой персональных данных.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при обработке информации, определяет обязанности оператора, государства при работе с персональными данными и информационными системами, порядок ограничения доступа к информации. Данный документ регулирует порядок работы с различной информацией в России, в том числе, с персональными данными. Документ содержит основные понятия и определения,

используемые во всех правовых актах, связанных с защитой информации, и, среди прочего, вводит понятие информационных категорий и видов информации. В частности, персональные данные классифицируются как информация ограниченного доступа. Согласно Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, поэтому государство устанавливает обязательные стандарты и правила ее обработки. [11]

В целом, регулирование защиты персональных данных в России является довольно важным, сложным и требовательным направлением в правах граждан страны. Особенности правового регулирования можно рассмотреть в виде схемы(рис.1)

Рисунок.1(схема нормативно-правовой базы защиты персональных даннах)

Итак, основными нормативно-правовыми актами, стандартами защиты персональных данных являются:

1.Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных

данных».

2.Конвенция Совета Европы от 28 января 1981 года № 108 «О защите персональных данных».

3.ГОСТ Р ИСО/МЭК 27001-2013 «Информационная технология. Методы обеспечения информационной безопасности. Системы управления информационной безопасностью. Требования».

4.ГОСТ Р ИСО/МЭК 27799-2012 «Информационная технология. Методы обеспечения информационной безопасности. Руководство по риск- анализу в области информационной безопасности».

5.Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении Правил обработки персональных данных».

6.Рекомендации различных организаций, таких как Институт информационной безопасности ISO, The International Association of Privacy Professionals (IAPP) и др.

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

Таким образом, обработка персональных данных обусловлена общими требованиями, которые строятся на базе принципов добровольности, обеспечения равенства возможностей, законности, не допущения дискриминации в трудовых отношениях. Соответственно этим требованиям, содержащихся в нормативно-правовых актах трудового законодательства России, должны соответствовать и не противоречить локальные нормативные акты различных организаций и предприятий, дабы не ущемлять и не нарушать законные интересы гражданина Российской Федерации. [10]

Приказом Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных.

Данное положение устанавливает методы и способы защиты информации в информационных системах, содержащих персональные данные. Оно охватывает процедуры обеспечения конфиденциальности, доступности, целостности и достоверности персональных данных, а также меры по предотвращению несанкционированного доступа к данным.К основным мерам защиты информации относятся следующие стандарты и методы:

– системы управления доступом: для ограничения доступа к персональным данным должны использоваться системы управления доступом, которые позволяют контролировать доступ к данным, определять права пользователя и аудиторскую отчетность;

– криптографические методы: для защиты персональных данных, которые передаются по сети, необходимо использовать криптографические методы, такие как шифрование и дешифрование данных, хэширование и цифровые подписи;

– физический контроль: для защиты персональных данных должен применяться физический контроль, который включает системы контроля доступа к помещениям, меры по уничтожению бумажных копий персональных данных и т.д.;

– программные средства: для защиты персональных данных должны применяться программные средства защиты, такие как антивирусные программы, программы мониторинга, системы обнаружения вторжений и т.д.;

– обучение: для гарантии безопасности персональных данных в информационных системах персонала организации необходимо обучать основам информационной безопасности и требованиям к защите персональных данных.

Данные меры защиты информации должны соответствовать современным требованиям к безопасности персональных данных и регулярно обновляться в соответствии с новыми угрозами и опасностями, которые могут возникнуть.

Необходимо выделить требования, которые данные акты предъявляют к

организациям. Условно их можно разделить на административные и технические. К административным относятся требования организационного характера. Например: создание внутренних нормативных и правовых актов. К техническим требованиям относят внедрение программных и аппаратных средств защиты, а также средства контроля и ограничения доступа. [15]

К основным требованиям по безопасности персональных данных можно отнести:

– конфиденциальность: необходимо обеспечить конфиденциальность информации, чтобы предотвратить несанкционированный доступ к данным;

– целостность: информация должна быть защищена от изменений и вмешательства несанкционированных лиц;

– доступность: необходимо обеспечить доступность информации только тем, кто имеет право ее просматривать;

– авторизация: доступ к информации должен быть предоставлен только с авторизацией;

– аутентификация: система должна проверять подлинность пользователей и предоставлять доступ только тем, кто имеет право на этом;

– шифрование: информация должна быть зашифрована, чтобы предотвратить ее взлом и использование несанкционированными лицами;

– безопасность сети: сеть должна быть защищена от атак внешних лиц, в том числе и вредоносного ПО;

– управление доступом: Пользователям должен быть предоставлен доступ только к необходимой информации в соответствии с их полномочиями;

– аудит: необходимо следить за действиями пользователей и системными событиями для обеспечения безопасности системы;

физическая безопасность: Данные должны быть защищены от утери или кражи, например, размещая их в безопасном месте и/или используя сейфы или шифрование на дисках.

1.3. Организация защиты персональных данных в профессиональной организации.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (далее – Субъекту). 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. [22]

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

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

14. Инструкция администратора ИБ ИСПДн.

15. Инструкция по организации парольной защиты.

16. Инструкция по антивирусной защите.

17. Инструкция по обработке ПДн без использования средств автоматизации.

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

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

20. Приказ о создании комиссии по уничтожению ПДн.

21. Журнал регистрации фактов несанкционированного доступа.

22. Журнал учета обращений субъектов ПДн в ИСПДн.

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

24. Журнал учета мероприятий по контролю ИБ.

25. План проверочных мероприятий по обеспечению безопасности ПДн.

26. АКТ 1 классификации ИСПДн.

27. Приказ о назначении администратора ИБ.

28. Форма согласия работника на обработку его ПДн.

Организация защиты персональных данных должна производиться в несколько этапов:

– инвентаризация информационных ресурсов;

– ограничение доступа работников к персональным данным; – документальное регламентирование работы с персональными данными;

– формирование модели угроз безопасности персональных данных;

– классификация информационных систем персональных данных (ИСПДн) образовательных организаций;

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

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

– создание подсистемы информационной безопасности ИСПДн и ее аттестация (сертификация)

– для ИСПДн классов К1, К2;

– организация эксплуатации и контроля безопасности ИСПДн.

В целях обеспечения прав и свобод человека и гражданина образовательная организация при обработке персональных данных сотрудников и обучающихся обязана соблюдать некие правила. Обработка персональных данных-любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

-сбор, запись, систематизацию, накопление, хранение (до передачи в архив)

-уточнение (изменение, обновление),

-извлечение, использование, передачу (доступ, предоставление),

- обезличивание, блокирование, удаление, уничтожение.

К персональным данным относятся:

-фамилия, имя, отчество;

-адрес места жительства;

-паспортные данные;

-данные свидетельства о рождении;

-контактный телефон;

-результаты успеваемости и тестирования;

-номер группы;

-данные о состоянии здоровья;

-данные страхового свидетельства;

-данные о трудовой деятельности;

-биометрические данные (фотографическая карточка)

-иная необходимая информация, которую Субъект добровольно сообщает о себе для получения услуг, предоставляемых Учреждением, если ее обработка не запрещена законом. [21]

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью учреждения, в частности для:

- предоставления образовательных услуг;
- проведения олимпиад, консультационных семинаров;
- направления на обучение;
- направления работ сотрудников (учащихся) на конкурсы;
- дистанционного обучения;
- ведения электронного дневника и электронного журнала успеваемости;
- ведения сайта ОО;
- автоматизации работы библиотеки;
- проведения мониторинга деятельности образовательной организации.

Образовательная организация должна собирать данные только в объеме, необходимом для достижения выше названных целей.

Правовыми основаниями для обработки персональных данных образовательной организации являются нормативно-правовые акты, регулирующие отношения, связанные с деятельностью организации, в том числе:

- Трудовой кодекс РФ, а также нормативно-правовые акты, содержащие нормы трудового права;

- Бюджетный кодекс РФ;

- Налоговый кодекс РФ;

- Гражданский кодекс РФ;

- Семейный кодекс РФ;

- ФЗ от 29.12.2012 № 273-ФЗ «Об образовании в РФ».

Основанием для обработки персональных данных также являются договоры с физическими лицами, заявления (согласия, доверенности и т.п.) обучающихся и родителей (законных представителей) несовершеннолетних обучающихся, согласия на обработку персональных данных. [14]

Образовательная организация обрабатывает персональные данные:

- работников, в том числе бывших;

- кандидатов на замещение вакантных должностей;

- родственников работников, в том числе бывших;

- обучающихся;

- родителей (законных представителей) обучающихся;

- физических лиц по гражданско-правовым договорам;

- физических лиц, указанных в заявлениях (согласиях, доверенностях и т.п.) обучающихся и родителей (законных представителей) несовершеннолетних обучающихся;

- физических лиц – посетителей образовательной организации.

Биометрические персональные данные образовательная организация не обрабатывает.

Образовательная организация обрабатывает специальные категории персональных данных только в соответствии и на основании требований федеральных законов.

Образовательная организация обрабатывает персональные данные в объеме, необходимом:

- для осуществления образовательной деятельности по реализации основных и дополнительных образовательных программ, обеспечения охраны, укрепления здоровья и создания благоприятных условий для разностороннего

развития личности, в том числе обеспечения отдыха и оздоровления обучающихся;

- выполнения функций и полномочий работодателя в трудовых отношениях;

- выполнения функций и полномочий экономического субъекта при осуществлении бухгалтерского и налогового учета, бюджетного учета;

- исполнения сделок и договоров гражданско-правового характера, в которых образовательная организация является стороной, получателем (выгодоприобретателем).

Условия обработки персональных данных:

1. Организация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2. Все персональные данные образовательной организации получает от самого субъекта персональных данных. В случае, когда субъект персональных данных несовершеннолетний – от его родителей (законных представителей) либо с их согласия, если субъект персональных данных достиг возрасти 14 лет. В случае, когда субъект персональных данных – физическое лицо, указанное в заявлениях (согласиях, доверенностях и т.п.) обучающийся и родителей (законных представителей) несовершеннолетних обучающихся, образовательная организация может получить персональные данные такого физического лица обучающихся, родителей (законных представителей) обучающихся.

3. Образовательная организация сообщает субъекту персональных данных о целях, предполагаемых источниках и способах получение персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта

персональных данных дать письменное согласие на их получение.

4. Документы, содержащие персональные данные, создаются путем:

- копирование оригиналов документов;

- внесение сведений в учетные формы;

- получение оригиналов необходимых документов.

5. Образовательная организация обрабатывает персональные данные в случаях:

- согласия субъекта персональных данных на обработку его персональных данных;

- когда обработка персональных данных необходима для осуществления и выполнения образовательной организацией возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

- когда осуществляется обработка общедоступных персональных данных, доступ к которым субъект персональных данных предоставил неограниченному кругу лиц.

6. Образовательная организация обрабатывает персональные данные:

- без использования средств автоматизации;

- с использованием средств автоматизации в программах и информационных системах

7. Образовательная организация обрабатывает персональные данные в сроки:

- которые необходимы для достижения целей обработки персональных данных;

- действия согласия субъекта персональных данных;

- которые определены законодательством для обработки отдельных видов персональных данных.

8. Образовательная организация хранит персональные данные в течение срока, необходимого для достижения целей их обработки, документы, содержащие персональные данные, в течение срока хранения документов,

предусмотренных номенклатурой дел с учетом архивных сроков хранения, сроки в школьной номенклатуре дел учитывают требования региональных и муниципальных правовых актов.

9. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

10. Персональные данные, обрабатываемые с использованием средств автоматизации, в порядке и на условиях, которые определяет политика безопасности данных средств автоматизации.

11. При автоматизированной обработке персональных данных не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) информационных систем.

12. Хранение персональных данных осуществляется не дольше чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

13. Лица, ответственные за обработку персональных данных, прекращают их обрабатывать:

- при достижении целей обработки персональных данных;

- истечении срока действия согласия;

- отзыве субъектом персональных данных своего согласия на обработку персональных данных, при отсутствии правовых оснований для продолжения обработки без согласия;

- выявлении неправомерности обработки персональных данных.

14. Образовательная организация обеспечивает конфиденциальность персональных данных.

15. Образовательная организация передает имеющиеся персональные данные третьим лицам в следующих случаях:

- субъект персональных данных дал свое согласие на такие действия;

- передача персональных данных осуществляется в соответствии с требованиями законодательства Российской Федерации в рамках установленной процедуры.

16. Образовательная организация не осуществляет трансграничной передачи персональных данных.

17. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если иное не предусмотрено договором, стороной, получателем (выгодоприобретателем) по которому является субъект персональных данных.

18. Выделяет документы (носители) с персональными данными к уничтожению комиссия, состав которой утверждается приказом руководителя образовательной организации.

19. Документы (носители), содержание персональные данные, уничтожаются по акту о выделении документов к уничтожению. Факт уничтожения персональных данных подтверждается документальным актом об уничтожении документов (носителей), подписанным членами комиссии.

20. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения. Для уничтожения бумажных документов может быть использован шредер.

21. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

22. Образовательная организация принимает нормативные, организационные и технические меры защиты персональных данных.

23. Нормативные меры защиты персональных данных – комплекс локальных и распорядительных актов, обеспечивающих создание, функционирование, совершенствование механизмов обработки персональных данных.

24. Организационные меры защиты персональных данных предполагают создание в образовательной организации разрешительной системы, защиты информации во время работы с персональными данными работниками, партнерами и сторонними лицами.

25. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

Основными мерами защиты персональных данных в образовательной организации являются:

- Назначение ответственного за организацию обработки персональных данных. Ответственный осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением образовательной организацией и ее работниками требований к защите персональных данных.

- Издание локальных актов по вопросам обработки Образовательная организация. А также локальных актов, определяющих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

- Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, настоящей Политикой, локальными актами по вопросам обработки персональных данных.

-Определение актуальных угроз безопасности персональным данным при их обработке с использованием средств автоматизации и разработка мер и мероприятий по защите персональных данных.

-Установление правил доступа к персональным данным, обрабатываемых с помощью средств автоматизации, а также регистрация и учет действий, совершаемых с персональными данными в информационных системах, и контроль за принимаемыми мерами по обеспечению безопасности персональных

данных и уровня защищенности информационной сети.

-Учет электронных носителей персональных данных.

-Принятие мер по факту обнаружения несанкционированного доступа к персональным данным, обрабатываемым с использование средств автоматизации, в том числе восстановление персональных данных, которые модифицированы или уничтожены вследствие несанкционированного доступа к ним.

-Оценка вреда, который может быть причинен субъектам в случае нарушения законодательства о персональных данных, оценка соотношения указанного вреда и принимаемых мер.

-Внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям законодательства, настоящей Политики, принятых локальных актов.

-Публикация настоящей Политики на официальном сайте образовательной организации.

ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ И СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Образовательная организация:

-Предоставляет субъекту персональных данных информацию о его персональных данных на основании запроса либо отказывает в выполнении повторного запроса субъекта персональных данных при наличии правовых оснований. Запрос в образовательную организацию на обработку подает субъект персональных данных (работник, родитель (законный представитель).

-Разъясняет субъекту персональных данных или его законному представителю юридические последствия отказа предоставлять его персональные данные

-Блокирует или удаляет неправомерно обрабатываемые, неточные персональные данные либо обеспечивает блокирование или удаление таких

данных. В случае подтверждения факта неточности персональных данных образовательная организация на основании сведений, предоставленных субъектом персональных данных или его законным представителем, уточняет персональные данные либо обеспечивает их уточнение и снимает блокирование персональных данных.

-Прекращает обработку и уничтожает персональные данные, либо обеспечивает прекращение обработки и уничтожение персональных данных при достижении цели обработки персональных данных.

-Прекращает обработку персональных данных или обеспечивает прекращение обработки в случае отзыва субъектом персональных данных согласия на обработку персональных данных, если иное на предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между образовательной организацией и субъектом персональных данных либо если образовательная организация не вправе осуществлять обработки персональных данных без согласия субъекта персональных данных на основании, предусмотренных законодательством Российской Федерации.

Субъект персональных данных вправе:

-Потребовать уточнения его персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконного полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

-Получать информацию, качающуюся обработки его персональных данных, кроме случаев, когда такой доступ ограничен федеральными законами.

-Обжаловать действия или бездействие образовательной организации в уполномоченном органе по защите прав субъектов персональных данных

ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Образовательная организация ответственна за персональную информацию, которая находится в ее распоряжении и закрепляет персональную ответственность сотрудников за соблюдением, установленных в организации принципов уважения приватности. [16]

Каждый сотрудник, получающий для работы доступ к материальным носителям персональным данных, несет ответственность за сохранность носителя и конфиденциальность информации.

Учреждение должно поддерживать систему приема, регистрации и контроля рассмотрения жалоб Субъектов, доступную с помощью телефонной, или почтовой связи.

Основной задачей при защите персональных данных является снижение влияния и риска возникновения угроз информационной безопасности. Важно отметить, что методы защиты могут быть программными, аппаратными и комбинированными. Конечный результат при использовании таких технологий направлен на поддержание высокого уровня защиты персональных данных образовательной организации и цифровой безопасности студентов [13].

Защита от угроз является основным компонентом снижения рисков утечки информации. На рисунке 2 представлен полный комплекс действий при управления рисками информационной безопасности.

Рисунок 2 – Комплекс действий при управлении рисками ИБ

Вывод по первой главе

По итогам первой главы магистерской диссертации главы можно сделать следующие выводы:

1. Раскрыто понятие персональных данных и значение их защиты в образовательной организации высшего образования.

Персональные данные – это информация, связанная с конкретным человеком, такая как ФИО, дата рождения, адрес проживания, номер телефона, паспортные данные и т.д. Они могут также включать в себя информацию о медицинских проблемах, учебном процессе, результаты тестов, оценках и др.

Защита персональных данных в образовательной организации является основной и важной задачей. Это важно для защиты личной жизни и конфиденциальности обучающихся и сотрудников образовательной организации. Защищая персональные данные, образовательное учреждение гарантирует соблюдение законодательства о защите персональных данных, которое обязывает организации обрабатывать персональные данные только в рамках установленных законом целей и требований.

Защита персональных данных также обеспечивает безопасность предоставления информации о студентах и сотрудниках. Кроме того, защита персональных данных гарантирует, что никакие конфиденциальные данные не будут использованы в несанкционированных целях, таких как мошенничество или кража личности. Руководство образовательной организации должно принимать меры для обеспечения безопасности и конфиденциальности данных студентов и сотрудников.

2. Проанализировано нормативно-правовое обеспечение защиты персональных данных в Российской Федерации. Защита персональных данных в Российской Федерации регулируется несколькими законодательными актами:

– Конституция Российской Федерации: статья 24 обеспечивает право на тайну обмена сообщениями, переписки, связи, телефонных переговоров, почтовых, телеграфных и иных сообщений;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: этот закон определяет правовые основы обработки персональных данных и устанавливает требования к технической защите информации;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: закон определяет правила использования информационных технологий при обработке персональных данных и установлен порядок обработки информации ограниченного доступа;

– Гражданский кодекс Российской Федерации: кодекс определяет правила отношений субъектов при обработке персональных данных и защиту прав потребителей;

– Административный регламент по обеспечению доступа к информации, которое имеется на официальных сайтах органов государственной власти (Федеральной закон от 27 июля 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»).

3. Описаны условия организации защиты персональных данных в образовательной организации. Исходя из этого, можно сказать, что в целом защита персональных данных представляет собой сложный технологический процесс, который включает в себя множество технических, организационных и правовых мероприятий.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО РЕАЛИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРОФЕССИОНАЛЬНОЙ ОРГАНИЦАЗИИ.

2.1. Общие сведения об образовательной организации.

База для проведения исследования – ГБПОУ «Южно-Уральский государственный технический колледж»

Полное наименование Учреждения: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж», аббревиатура – ФГБОУ «ЮУРГТК». Место нахождения Учреждения: 454007, Челябинская область, г. Челябинск, ул. Гагарина, д.7.

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

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

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

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

– профессиональная переподготовка и повышение квалификации специалистов и рабочих;

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

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

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

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

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

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

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

Для осуществления дистанционной образовательной деятельности, размещения информации о предстоящих и прошедших мероприятиях и информирования студентов об актуальных событиях у ГБПОУ «Южно-

Уральский государственный технический колледж» имеется собственный сайт (режим доступа: https://sustec.ru), отвечающий всем требованиям к подобным ресурсам образовательных организаций.

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

ИС ОО состоит из пяти уровней:

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

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

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

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

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

– программные средства управления документооборотом;

– программные средства календарного планирования;

– программные комплексы для ведения конструкторских работ (САПР);

– программные средства электронного офиса (MS Qffice);

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

– информационно-аналитические системы (Deductor).

3. Системный уровень описывает операционные системы и сетевое программное обеспечение, которые составляют рекомендуемое программное окружение для программного комплекса ИС ОО.

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

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

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

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

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

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

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

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

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

2.2. Защита персональных данных в ГБПОУ «Южно-Уральский Государственный технический колледж».

Организация защиты персональных данных в ГБПОУ «Южно-Уральский Государственный технический колледж» включает комплекс мер и правил, направленных на обеспечение защиты данных, обрабатываемых и хранимых в системах и сетях образовательного учреждения. Она охватывает все аспекты информационной безопасности, включая защиту персональных данных сотрудников и студентов от несанкционированного доступа, вредоносного программного обеспечения, утечки данных, манипуляций информацией и других угроз.

Политика безопасности хранения и обработки персональных данных также должна определять цели и задачи в области защиты информации, а также принципы и правила, которые образовательное учреждение будет соблюдать при работе с предоставляемой информацией. Она должна устанавливать также ответственность за информационную безопасность, роли и обязанности сотрудников образовательной организации, связанные с защитой информации.

Политика информационной безопасности должна определять процедуры по обнаружению и реагированию на угрозы, процедуры резервного копирования и восстановления данных, а также процедуры обработки инцидентов и уведомления о них. Более того, политика информационной безопасности должна включать механизмы контроля и мониторинга для обеспечения соблюдения всех установленных правил и мер безопасности.

Все сотрудники образовательной организации должны быть ознакомлены с данной политикой и соблюдать ее требования. Образовательное учреждение должно проводить регулярное обучение и тренинги по вопросам информационной безопасности для своих сотрудников, чтобы повысить их осведомленность и готовность к действиям в случае инцидента с утечкой предоставляемых данных.

В ходе исследования определено, что в ГБПОУ «Южно-Уральский Государственный технический колледж» действует положение о защите персональных данных, четко определяющее цели и задачи при обеспечении безопасной работы с предоставляемой информацией. С данным положением можно ознакомиться на сайте организации, оно четко определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, студентов, абитуриентов и других физических лиц. Положение о защите персональных данных разработано на основании основании:

– Конституции Российской Федерации;

– Трудового кодекса Российской Федерации;

– Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

– Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»;

– Федерального закона от 27.07.2010г.No210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

– Распоряжения Правительства Российской Федерации от 25 апреля 2011 г. N 729-р г.Москва;

– Части 3,4 ст.б Федерального закона «Об опеке и попечительстве» от 24.04.2008г. N 48-ФЗ (ред. от 23.07.2013г.);

– Постановления Администрации города Челябинска «О предоставлении мер социальной поддержки малообеспеченным студентам высших и средних учебных заведений города Челябинска» от 09.04.2013г. № 87-п;

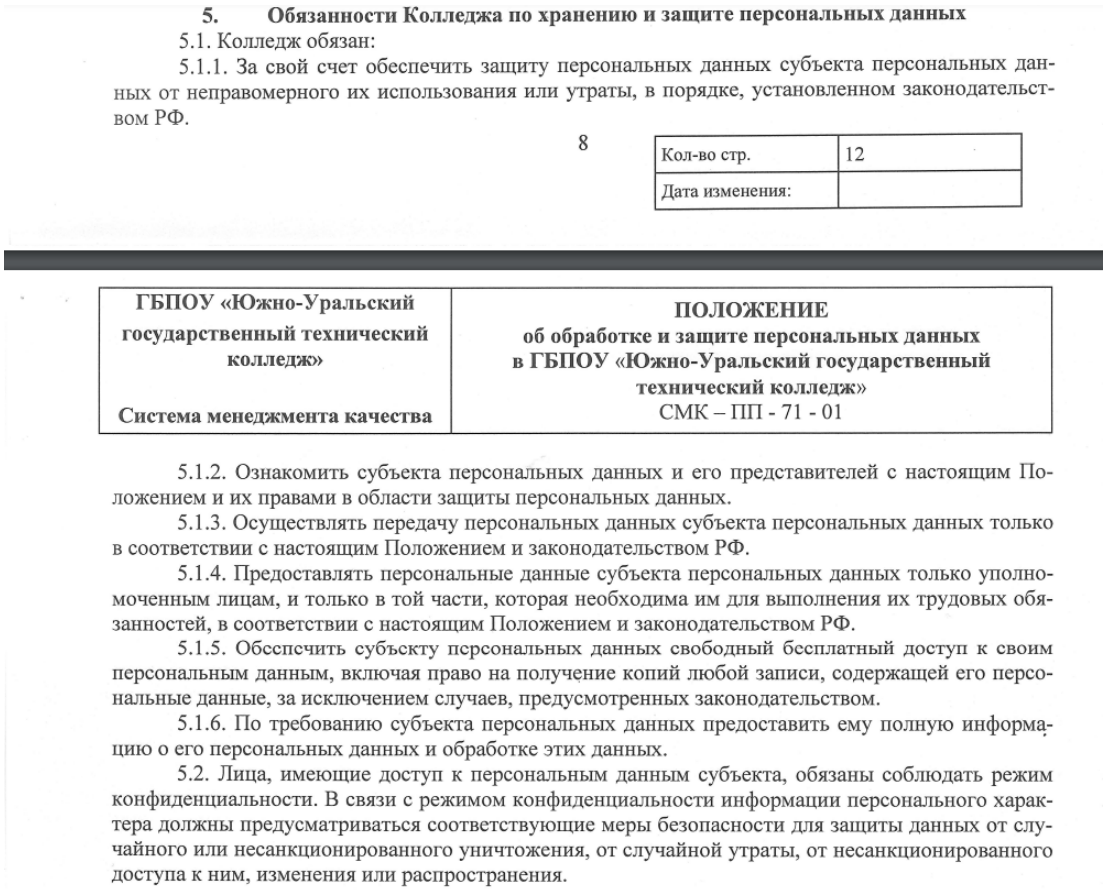
– Постановления Администрации города Челябинска «О внесении изменений в постановление Администрации города Челябинска от 09.04.2013г. N 87-п» от 22.11.2013 № 256-п;

– Совместного приказа Министерства образования и науки Челябинской области и Министерства социальных отношений Челябинской области от 18.04.2013г. № 01/1241/117;

– Устава ГБПОУ «Южно-Уральский государственный технический колледж»;

– другими определяющими случаи и особенности обработки персональных данных нормативно-правовыми актами.

Так, к примеру, в положении четко разъяснены обязанности колледжа по хранению персональных данных. (Рис 2)



5. Обязанности Колледжа по хранению и защите персональных данных

5.1. Колледж обязан:

5.1.1. За свой счет обеспечить защиту персональных данных субъекта персональных данных от неправомерного их использования или утраты, в порядке, установленном законодательством РФ.

8

Кол-во стр.	12
Дата изменения:	

ГБПОУ «Южно-Уральский государственный технический колледж» **Система менеджмента качества**	**ПОЛОЖЕНИЕ** **об обработке и защите персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»** СМК – ПП - 71 - 01

5.1.2. Ознакомить субъекта персональных данных и его представителей с настоящим Положением и их правами в области защиты персональных данных.

5.1.3. Осуществлять передачу персональных данных субъекта персональных данных только в соответствии с настоящим Положением и законодательством РФ.

5.1.4. Предоставлять персональные данные субъекта персональных данных только уполномоченным лицам, и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим Положением и законодательством РФ.

5.1.5. Обеспечить субъекту персональных данных свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством.

5.1.6. По требованию субъекта персональных данных предоставить ему полную информацию о его персональных данных и обработке этих данных.

5.2. Лица, имеющие доступ к персональным данным субъекта, обязаны соблюдать режим конфиденциальности. В связи с режимом конфиденциальности информации персонального характера должны предусматриваться соответствующие меры безопасности для защиты данных от случайного или несанкционированного уничтожения, от случайной утраты, от несанкционированного доступа к ним, изменения или распространения.

Рисунок 3. -обязанности колледжа по хранению персональных данных)

А также дано четкое описание прав и обязанностей субъектов персональных данных на обеспечение защиты их персональных данных. (Рис.3,4)

6. Права субъектов персональных данных на обеспечение защиты их персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся в Колледже, субъекты персональных данных (родители (законные представители) малолетнего несовершеннолетнего обучающегося), имеют право:

6.1.1. Получать полную информацию о своих персональных данных и их обработке.

6.1.2. Свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении субъекта персональных данных (для малолетнего несовершеннолетнего – его родителей, законных представителей) – к соответствующему должностному лицу, ответственному за организацию и осуществление хранения персональных данных субъектов или к директору Колледжа.

6.1.3. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением субъекта на имя директора Колледжа.

При отказе директора Колледжа исключить или исправить персональные данные субъект персональных данных (родитель, законный представитель несовершеннолетнего обучающегося) имеет право заявить в письменном виде директору Колледжа о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект персональных данных (родитель, законный представитель несовершеннолетнего обучающегося) имеет право дополнить заявлением, выражающим его собственную точку зрения.

6.1.4. Требовать об извещении Колледжем всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.5. Обжаловать в суде любые неправомерные действия или бездействия Колледжа при обработке и защите его персональных данных.

Рисунок.4- Описание прав и обязанностей субъектов персональных данных на обеспечение защиты их персональных данных)

7. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

7.1. В целях обеспечения достоверности персональных данных работники обязаны:

7.1.1. При приеме на работу в Колледж представлять уполномоченным работникам Колледжа достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

7.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, семейном положении, сообщать об этом в течение 5 рабочих дней с даты их изменений.

7.1.3. В случае изменения персональных данных работника о состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом незамедлительно в день их изменения.

7.2. В целях обеспечения достоверности персональных данных обучающиеся (родители, законные представители несовершеннолетних обучающихся) обязаны:

7.2.1. При поступлении в Колледж представлять уполномоченным работникам Колледжа достоверные сведения о себе (своих несовершеннолетних детях).

7.2.2. В случае изменения сведений, составляющих персональные данные несовершеннолетнего обучающегося старше 14 лет, он обязан в течение 10 дней сообщить об этом уполномоченному работнику Колледжа.

7.2.3. В случае изменения сведений, составляющих персональные данные обучающегося, родители (законные представители) несовершеннолетнего обучающегося в возрасте до 14 лет обязаны в течение месяца сообщить об этом уполномоченному работнику Колледжа.

Рисунок.5-Описание прав и обязанностей субъектов персональных данных на обеспечение защиты их персональных данных)

Данное Положение отлично регулирует отношения, связанные с обработкой персональных данных, включающие в себя производимые колледжем действия по получению, хранению, комбинированию, передаче персональных данных физических лиц или иному их использованию, с целью защиты персональных данных субъектов от несанкционированного доступа, а также неправомерного их использования и утраты.

Защита персональных данных остается одной из наиболее важных задач в современном информационном обществе. Особенно актуальной она является в сфере образования, где обрабатывается огромное количество личной информации учащихся, педагогов и других сотрудников образовательных организаций. В ФГБОУ «ЮУРГТК» используются несколько приемов защиты персональных данных.

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. [17]

В ФГБОУ «ЮУРГТК» 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.

2.3. Рекомендации по организации системы защищенности информационной системы персональных данных для ГБОУ «Южно-Уральский государственный технический колледж.

Для обоснования рекомендаций по организации системы защищенности информационной системы персональных данных был проведен анализ защищенности персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж» В ходе анализа выяснилось, что в данном учебном заведении происходит достаточно активное использование различных методов для защиты персональных данных, но тем не менее возникают некоторые трудности в организации надежной защиты персональных данных.

Одной из таких проблем является то, что эффективность защиты персональных данных определяется не только техническими средствами защиты, но и компетентностью сотрудников, которые имеют 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. Необходимо проводить регулярное обучение и тренировки для сотрудников по вопросам безопасности хранения и обработки персональных данных. Это должно способствовать освению основных правил и процедур по обработке и хранению персональных данных, а также осведомлению сотрудников о последних угрозах безопасности и методах их предотвращения. Такое обучение должно проводиться как при приеме на работу новых сотрудников, так и периодически для существующего персонала.

Еще одной проблемой является то, что постоянно меняются технологии и методы, которые используют злоумышленники для получения доступа к чужим данным. К сожалению, 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.

В современном цифровом мире безопасность и защита данных стали первостепенной задачей для всех пользователей. Одним из самых важных аспектов обеспечения безопасности является регулярное обновление программного обеспечения. Программное обеспечение, особенно операционные системы и приложения, подвержено постоянным угрозам безопасности со стороны хакеров и злоумышленников. Когда в открытом доступе появляется новая уязвимость, разработчики выпускают обновления, которые закрывают эти слабые места и укрепляют систему. Использование устаревших версий программного обеспечения может привести к катастрофическим последствиям, таким как взлом вашей системы или утечка данных. [19]

Обновления программного обеспечения также вносят исправления ошибок, которые могут негативно сказываться на безопасности данных. Баги в программном обеспечении, особенно связанные с безопасностью, могут быть использованы злоумышленниками для получения несанкционированного

доступа к вашим данным или компьютерной системе. Регулярное обновление помогает устранить эти ошибки и обеспечить более надежную защиту. [18]

В отличии от закрытия уже обнаруженных уязвимостей, разработчики программного обеспечения постоянно работают над улучшением безопасности продуктов. Обновления могут включать новые функции, которые расширяют возможности защиты данных. Это решение, направленное на реагирование на постоянно меняющуюся тему угроз. Например, это может быть повышение уровня шифрования или внедрение механизмов двухфакторной аутентификации. Использование устаревших версий программного обеспечения может лишить вас доступа к новым и более современным функциям безопасности.

Третьей проблемой в организаци надежной защиты персональных данных 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.

На основании рисков и уязвимостей системы защиты персональных данных, и анализируя нормативные требования действующего законодательства нами были разработаны рекомендации по организации системы защиты персональных данных в ФГБОУ «ЮУРГТК».

Для устранения недостатков в существующей системе защиты персональных данных, необходимо предложить образовательной организации усовершенствовать организационные, технические и физические меры. Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты персональных данных;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты персональных данных;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

– введение новых нормативных документов для обеспечения безопасности использования 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.

Следующим шагом 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 усовершенствовать физические меры по защите персональных данных:

1. Разработать инструкцию по физической охране и правилам доступа в специальные помещения.

2. Разработать журнал лиц, имеющих право доступа в определенные помещения, для выполнения своих обязанностей.

3. Оборудовать двери специальных помещений и хранилищ приспособлениями для опечатывания.

4. Оборудовать сейфы, предназначенные для хранения документации.

Также, 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.

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 контроль эффективности системы защиты персональных данных. Данная проверка позволяет выявить потенциальные слабые места в системе и своевременно принять меры по их устранению. Рекомендуется проводить данный контроль не реже одного раза в год, а также после любых существенных изменений в системе.

Критерии проверки:

1. Документация по объекту.

2. Анализ структуры информационной системы персональных данных и технический процесс обработки информации.

3. Уровень защиты.

4. Проверка структуры нформационной системы персональных данных по заявленной документации.

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

6. Вопросы охраны проверяемого объекта.

7. Настроены ли штатные средства защиты.

8. Оценка уровня компетентности для ответственных за защиту персональных данных.

9. Проверка знаний и умений персонала нформационной системы персональных данных по информационной безопасности.

10. Проверка прав доступа.

11. Учет и регистрация.

12. Целостности.

13. Все,что связано с антивирусом.

14. Полный анализ уровня защиты.

15. Обнаружение посторонних вторжений.

16. Анализ защиты каналов связи.

17. Проверка защиты информационной системы персональных данных с помощью сканера безопасности.

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

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.

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

Вывод по 2 главе.

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.

В соответствии с анализом рисков и уязвимости системы защиты персональных данных нами были разработаны рекомендации по улучшению защиты персональных данных в ФГБОУ «Южно-Уральский государственный технический колледж», в результате выполнения которых будет повышена эффективность средств защиты и сократится риск потери и искажения информации. Рекомендации по организации системы защиты персональных данных реализуются в несколько этапов:

1. Разработка политики конфиденциальности.

2. Осуществление регулярного обучения и тренировок сотрудников по вопросам безопасности данных.

3. Усовершенствование физических мер по защите персональных данных:

-Разработать инструкцию по физической охране и правилам доступа в специальные помещения.

-Разработать журнал лиц, имеющих право доступа в определенные помещения, для выполнения своих обязанностей.

-Оборудовать двери специальных помещений и хранилищ приспособлениями для опечатывания.

-Оборудовать сейфы, предназначенные для хранения документации.

4. Обеспечить безопасность хранения данных.

5. Осуществить регулярный контроль эффективности системы защиты персональных данных.

6. Установить процедуры реагирования на нарушения безопасности.

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.

В ходе данной работы рассмотрены основные нормативные документы, регулирующие правовые отношения в области защиты персональных данных, приведены сведения о возможных угрозах безопасности информационной системе персональных данных, в том числе подробно приведена и рассмотрена характеристика угроз несанкционированного доступа.

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.

Улучшение защиты персональных данных в образовательных организациях является правовым требованием. 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.

Представленная работа содержит две основных главы, каждая из которых решает отдельные задачи, необходимые для формирования рекомендаций по организации системы защищенности информационной системы персональных данных для ФГБОУ «Южно-Уральский государственный технический колледж» г. Челябинска. В результате работы проведен полный анализ основных вопросов относительно угроз и проблем Информационной безопасности информационной безопасности персональных данных в ФГБОУ «Южно-уральский государственный технический колледж».. Определены основные угрозы, степень их влияния и текущая ситуация по решению данной проблемы. Выяснено, что руководство колледжа активно проводит мероприятия, направленные на решение данной задачи. Несмотря на это, возникают некоторые трудности в организации надежной защиты персональных данных. Проблема заключается в нехватке финансовых ресурсов, недостатке информированности

руководителей организаций о необходимых мерах, сложности реализации и поддержки проектов.

Основной целью представленного исследования являлось на основе теоретического анализа разработать рекомендации для реализации защиты персональных данных в профессиональной организации с учетом требований нормативно-правовой базы Российской Федерации.

Для достижения изначально-поставленной цели были решены следующие задачи:

- Рассмотрено понятие и значение защищенности информационных систем персональных данных в образовательной организации.

- Изучено нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.

- Определены этапы организации защищенности информационных систем персональных данных в образовательной организации.

- Проведена оценка информационной безопасности персональных данных в ФГБОУ «Южно-уральский государственный технический колледж».

5. Разработаны рекомендации по организации системы защищенности информационной системы персональных данных для ФГБОУ «Южно-Уральский государственный технический колледж» г. Челябинска.

6. Проведена оценка эффективности рекомендаций по организации системы защищенности информационной системы персональных данных для ФГБОУ «Южно-Уральский государственный технический колледж».

Предлагаемые нами мероприятия по защите персональных данных в профессиональной образовательной организации позволят повысить защиту личных данных сотрудников. Таким образом, поставленные задачи были выполнены и цель достигнута.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022) (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 3

2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3451

3. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448

4. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Собрание законодательства РФ, 22.09.2008, № 38, ст. 4320

5. Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ, 02.04.2012, № 14, ст. 1626

6. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375) // Российская газета, № 107, 22.05.2013

7. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 № 33620) // Российская газета, № 211, 17.09.2014

8. Абдулова, Э. Д. Правовое регулирование в сфере защиты персональных данных / Э. Д. Абдулова // Молодой ученый. – 2022. – № 5(400). – С. 151-154.

9. Алимбаев, В. В. Организация защиты персональных данных и ответственность за несоблюдение требований законодательства в области защиты персональных данных / В. В. Алимбаев, Е. В. Листопадова // Природа. Человек. Культура : Материалы Третьего Международного научнопросветительского форума, Кисловодск, 04–08 октября 2022 года / Под общей редакцией С.Е. Туркулец, Е.В. Листопадовой. – Хабаровск: Дальневосточный государственный университет путей сообщения, 2022. – С. 176-182.

10. Антонова, В. В. Проблемы и решения правового регулирования защиты персональных данных / В. В. Антонова // Учет и контроль. – 2022. – № 3. – С. 15-17.

11. Бакланова, Н. А. Конституционно-правовое регулирование права на защиту персональных данных в РФ и странах Восточной Европы / Н. А. Бакланова, Д. В. Кононенко // Международный журнал гуманитарных и естественных наук. – 2022. – № 6-2(69). – С. 26-28. 72

12. Васильев, И. Д. Организация защиты персональных данных в будущем / И. Д. Васильев // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 34. – С. 1100-1105.

13. Воронина, И. А. Приватность в сети Интернет как способ защиты персональных данных / И. А. Воронина, А. В. Кирпичникова // Право и государство: теория и практика. – 2022. – № 12(216). – С. 95-96.

14. Газизов, А. Р. Аппаратно-программные методы защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем "сниффинг-атак / А. Р. Газизов // . – 2022. – Т. 49, № 3. – С. 52-60.

15. Гармаш, С. В. Правовые аспекты защиты персональных данных несовершеннолетних / С. В. Гармаш // Информатизация образования и науки. – 2022. – № 4(56). – С. 12-18. Шумакова, Н.В. Инновационные технологии в системе профессиональной подготовки студентов [Текст] / Н.В. Шумакова // Молодой ученый. – 2021. – №5. – С. 787–789.

16. Ажмухамедов И.М., Кузнецова В.Ю. Информационная безопасность в цифровой образовательной среде: анализ информационных рисков и выработка стратегий защиты школьников от негативных последствий цифровизации образования // Прикаспийский журнал: управление и высокие технологии. 2020. №3 (51). С. 74-83.

17. Казинец В.А., Редько Е.А.Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022. №5. С. 22-25.

18. Красовская Л. В., Исабекова Т. И. Использование информационных технологий в образовании // Научный результат. Педагогика и психология образования. 2017. №4 (14). С. 29-36.

19. Евстигнеева И.А., Евстигнеев М.Н., Клочихин В.В. Обеспечение информационной безопасности студентов в процессе использования проектной методики в обучении иностранному языку в университете // Вестник ТГУ. 2022. №4. С. 1009-1019.

20. Адольф В.А., Адольф К.В. Угрозы цифровизации образования и их решение // Научный компонент. 2022. №1 (13). С. 88-95.

21. Степанова Т.Ю. Обеспечение информационной безопасности в образовательной организации // Электронный научно-методический журнал Омского ГАУ. 2020. №4 (23). С. 25-29.

22. Ажмухамедов И.М., Кузнецова В.Ю.Информационная безопасность в цифровой образовательной среде: анализ информационных рисков и выработка стратегий защиты школьников от негативных последствий цифровизации образования // Прикаспийский журнал: управление и высокие технологии. 2020. №3 (51). С. 74-83.

23. Казинец В.А., Редько Е.А.Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022. №5. С. 22-25.

24. Красовская Л. В., Исабекова Т. И. Использование информационных технологий в образовании // Научный результат. Педагогика и психология образования. 2017. №4 (14). С. 29-36.

25. Евстигнеева И.А., Евстигнеев М.Н., Клочихин В.В. Обеспечение информационной безопасности студентов в процессе использования проектной методики в обучении иностранному языку в университете // Вестник ТГУ. 2022. №4. С. 1009-1019.

26. Адольф В.А., Адольф К.В. Угрозы цифровизации образования и их решение // Научный компонент. 2022. №1 (13). С. 88-95.

27. Степанова Т.Ю. Обеспечение информационной безопасности в образовательной организации // Электронный научно-методический журнал Омского ГАУ. 2020. №4 (23). С. 25-29.

28. Яриков В.Г. Информационная безопасность обучающихся в образовательной организации // NBI-technologies. 2021. №4. С. 19-24.

29. Какорин И.А. Основные принципы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2023. №2-2 (77). С. 25-27.

30. Мельников П.В., Ешенко Р.А. Проблемы формирования модели угроз информационной безопасности в информационных системах // Вестник науки. 2020. №6 (27). С. 185-189.

31. Сайгушев Н.Я., Веденеева О.А., Гарипов М.А. Актуализация информационной грамотности студентов в процессе профессиональной подготовки // МНКО. 2021. №4 (89). С. 77-80.