МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждениевысшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологийи методики обучения техническим дисциплинам

Организация режима защиты конфиденциальной информации в образовательной организации

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасности в профессиональномобразовании»

Проверка на объём заимствований:
84,07 % авторского текста

Работа рекомендована к защите
«1» июня 2022 г.

Зав. кафедрой АТ,ИТиМОТД
_____В.В. Руднев

Выполнил:
студент гр. ОФ-209/210-2-1
Грамотеев Никита Дмитриевич

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

Челябинск, 2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательноеучреждение высшего образования
Южно-Уральский государственный гуманитарно-педагогический
университет(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта,
информационных технологийи методики обучения
техническим дисциплинам

Направление подготовки: 44.04.04. «Профессиональное обучение»
Программа подготовки магистров «Управление информационной
безопасностьюв профессиональном образовании»

ЗАДАНИЕ
на выпускную квалификационную
работу(магистерскую диссертацию)

Магистранту Грамотееву Никите Дмитриевичу, обучающемуся в группе ОФ-209/210-2-1 по направлению подготовки 44.04.04. «Профессиональное обучение (Управление информационной безопасностью в профессиональном образовании)» Научный руководитель квалификационной работы: Дмитриев М.С., д.т.н., доцент кафедры АТ, ИТ и МОТД.

1. Тема квалификационной работы: «Организация режима защиты конфиденциальной информации в образовательной организации», утверждена приказом Южно-Уральского государственного гуманитарно-педагогического университета № 3007-с от «14» 12 2020 г.

2. Срок сдачи магистрантом законченной работы на кафедру « » _____2022 г.

3. Содержание и объем работы (пояснительной расчетной и экспериментальной частей, т.е. перечень подлежащих разработке вопросов):

- раскрыть сущность и содержание защиты персональных данных в образовательных организациях;

– раскрыть задачи, функции, организационную структуру ГБПОУ «Южно-Уральского государственного технического колледжа»
– проанализировать организацию защиты персональных данных в ГБПОУ ЮУрГТК;
– разработать мероприятия по совершенствованию организации защиты персональных данных в ГБПОУ ЮУрГТК.

4. Материалы для выполнения квалификационной работы:
   – Учебная, научно-техническая, педагогическая, методическая, нормативно-правовая литература по теме выпускной квалификационной работы (магистерской диссертации).
   – Материалы научно-исследовательской работы, педагогической и преддипломной практики.

5. Перечень графического материала (с точным указанием обязательныхтаблиц, чертежей или графиков, образцов и др.)

Таблица, таблицы и диаграммы результатов экспериментальной проверки внедрения в организации СПО и экспертной проверки действующих педагогов и руководителей СПО и ВО, а также технических специалистов.

6. Консультанты по специальным разделам ВКР:

Раздел	Консультант	Отметка о

Дата выдачи задания «_____»_____2020 г.

Задание выдал, зав. кафедрой АТ, ИТ и МОТД к.т.н., доцент
_____ Руднев В.В.

Задание принял _____Грамотеев Н.Д.

КАЛЕНДАРНЫЙ ПЛАН
выполнения выпускной квалификационной работы(магистерской диссертации)

№ п/п	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1	Предзащита ВКР	01.06.2022г.	
2	Доработка ВКР после предзащиты		
3	Нормоконтроль		
4	Подписание ВКР научным руководителем		
5	Оформление пояснительной записки и презентации ВКР		
6	Подписание рецензии на ВКР		
7	Защита ВКР на заседании ГАК	29.06.2022г.	

Автор _____Грамотеев Н.Д.

Научный руководитель,
д.т.н., профессор кафедры АТ, ИТ и МОТД_____Дмитриев М.С.

Заведующий кафедрой АТ, ИТ и МОТД
к.т.н., доцент _____Руднев В.В.

Содержание

Введение

Защита персональных данных приобретает все большее значение, так как в нынешнем веке информационные технологии развиваются стремительней, чем когда-либо. В связи с этим появляется нужда в совершенствовании методов и средств для защиты конфиденциальной информации путем введения и закрепления соответствующих правовых актов и законов. Главным объектом на данный момент, как раз и является информация. В настоящее время общество полностью зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине сами данные приобретают высокую ценность. И чем выше цена полезной информации, тем выше ее сохранность.

В первом квартале 2022 года количество утечек конфиденциальной информации из учебных заведений по всему миру увеличилось более чем на 15% по сравнению с аналогичным периодом прошлого года. Хакеры и внутренние злоумышленники крали личные данные и другую конфиденциальную информацию.

Проблема защиты конфиденциальной информации в организациях любой формы стоит в настоящее время наиболее остро, так как угрозы нарушения информационной безопасности носят глобальный характер. Способы реализации угроз информационной безопасности и формы их проявления постоянно совершенствуются, высокая технологичность этих угроз требует адекватного противодействия, предъявляет требования к квалификации специалистов по информационной безопасности и персоналу.

Персональные данные являются важнейшим активом любой современной организации и в то же время её серьезной проблемой. Утечка персональных данных не выгодна ни организации: она испытывает серьезные репутационные потери и получает конфликт с законом, ни владельцам этой информации, так как они испытывают как минимум

беспокойство, а нередко становятся жертвами различных афер.

Ввиду вышесказанного, законодательными актами, как в России, так и зарубежных стран предусматривают немалое количество норм, направленных на регулирование создания, пользования, передачи и защиты информации во всех ее формах.

Особой ценностью обладает информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью». Соответственно и информация, непосредственно затрагивающая частные интересы человека, должны уважаться и защищаться государством.

В повседневной жизни человека сохранность информации «о его жизни» зависит от него самого. Но совсем другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу или какой-либо организации – банку, работодателю, учебному заведению и т.д. Клиент в данной ситуации передает конфиденциальную информацию о себе на ответственное хранение. Далее за сохранность, способы их защиты, а также ответственность за невыполнение обязательств по обеспечению безопасности персональных данных отвечает уже организация, к которой обратился человек.

Проблемы функционирования систем обеспечения информационной безопасности нашли отражение в трудах А.А. Герасимова [27], А.А. Грушо [28], С.В. Дворянкина [31], В. А. Минаева [41], С.В. Скрыля [50], М.П. Сычева [51] и ряда других ученых.

Проблемы защиты персональных данных рассматривались в трудах российских ученых, таких как: А.В Меньшиковой [37], где она выделила некоторые проблемы защиты персональных данных работника и определила перспективы и пути их решения; проблемные вопросы понятия и сущности персональных данных в своих трудах рассмотрел А.В Минбалеев [38].

В настоящее время образовательные учреждения активно внедряют информационные системы, обрабатывающие персональные данные в образовательном учреждении, делопроизводство, бухгалтерские программы и прочее. Эти системы предназначены для ведения базы данных воспитанников, студентов, родителей и сотрудников образовательных учреждений, оперативного управления учреждением. Образовательные учреждения должны в первую очередь соблюдать требования законодательства по защите персональных данных участников образовательного процесса, так как речь идет о защите информации, неправомерное использование которой может серьезно повлиять на права граждан.

Несмотря на большое количество работ по проблеме информационной безопасности конфиденциальных данных, следует отметить, что его теоретические знания явно недостаточны, практические методы формирования оптимального механизма защиты конфиденциальной информации в образовательных организациях не соответствуют условиям реального времени.

Противоречие между необходимостью обеспечения качественных методов и средств защиты конфиденциальной информации и недостаточным уровнем разработанных предложений по улучшению мер защиты конфиденциальной информации в образовательной организации позволило сформулировать **проблему** необходимости разработки предложений по совершенствованию системы защиты конфиденциальной информации в образовательной организации.

Актуальность. Тема диссертации актуальна, так как в современном мире до сих пор являются нередкими случаи утечки информации из-за непонимания важности сохранения данных, знания элементарных правил безопасности, а также недостаточной внимательности, осведомленности лиц, ответственных за обработку персональных данных. Поэтому на специалистов по информационной безопасности возлагается не только

ответственность за безопасность информационной системы, но и за компетентное отношение к своей работе.

Объектом исследования является организация защиты данных в образовательном учреждении ГБПОУ «Южно-Уральский государственный технический колледж».

Предмет – особенности организации защиты персональных данных.

Целью диссертации является рассмотрение особенностей работы с конфиденциальной информацией, а именно персональными данными, а также предложить способы по совершенствованию мер системы защиты конфиденциальной информации.

В соответствии с поставленной целью были выделены следующие **задачи**:

– раскрыть сущность и содержание защиты персональных данных в образовательных организациях;

– раскрыть организационную структуру ГБПОУ «Южно-Уральский государственный технический колледж»;

– проанализировать меры и средства организации защиты персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»;

– предложить мероприятия по совершенствованию организации защиты персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж».

Гипотеза. Если будут реализованы предложенные в диссертации рекомендации по защите персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж», то защищённость конфиденциальной информации станет выше.

В процессе написания выпускной квалификационной работы были использованы законодательные акты и нормативно-методические документы, регламентирующие организацию защиты персональных данных. Использование законодательных актов и нормативно-

методических документов было продиктовано темой исследования.

Основополагающие нормы, регулирующие отношения по поводу персональных данных, содержатся в Федеральном законе «О персональных данных» [6].

Федеральный закон «Об информации, информационных технологиях и защите информации» [5] определяет, процессы функционирования информации и документации в обществе, в системе государственного и хозяйственного управления. Настоящий закон регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В качестве методического материала по защите персональных данных, использованы научные, учебные, практические материалы, подготовленные ведущими специалистами: Е. А. Степановым, Т. В. Кузнецовой[30], В.И. Петренко[42], О. В. Силакова[45]; регламентация работы с персональными данными – С. А. Борисова[25], М. А. Федосова [46] и др.

Для решения задач были использованы следующие методы исследования: анализ публикационного массива по теме, описание, наблюдение, изучение документов.

Практическая значимость данной работы заключается в создании эффективной действующей системы защиты персональных данных в образовательной организации.

Диссертация состоит из введения, двух глав, заключения, списка использованных источников и литературы. Во введении обосновывается выбор темы исследования, ее актуальность, анализируется степень ее

изученности, формулируются объект, предмет, цели, задачи, методологические основы исследования, структура работы.

В первой главе раскрываются теоретические основы организации защиты персональных данных в системе управления организацией, нормативно-правовая база и технологии защиты персональных данных.

Во второй главе рассматриваются цели, задачи, функции защиты персональных данных в образовательной организации, а также предложены мероприятия по совершенствованию организации защиты персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж».

Каждая глава содержит выводы.

В заключении подводятся итоги проведенного исследования, формулируются основные выводы. Список использованной литературы содержит 58 источников по теме.

Глава 1. Основные теоретические элементы организации защиты персональных данных

1.1. Основные терминологические сведения в сфере информационной безопасности

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Под информацией применительно к задаче ее защиты понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В зависимости от формы представления информация может быть устной, телекоммуникационной, документированной.

Информационные процессы - процессы сбора, накопления, обработки, хранения, распространения и поиска информации.

Информационная система - совокупность документов и массивов документов и информационных технологий.

Информационные ресурсы - это документы или массив документов, существующих отдельно или в составе информационной системы.

Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства называется информатизацией.

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и

обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании [19].

Целью защиты информации является предотвращение нанесения ущерба пользователю, владельцу или собственнику. Под эффективностью защиты информации понимается степень соответствия результатов защиты поставленной цели. Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо производить защиту в соответствии с поставленными целями [24].

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Под утечкой информации понимают неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа и получение разведчиками.

Несанкционированный доступ - получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней.

Можно выделить несколько видов несанкционированного доступа:

– Человеческий. Информация может быть скопирована на временные носители и украдена, передана по электронной почте. Кроме того, если есть доступ к серверу, в базы данных могут быть внесены изменения вручную.

– Программный. Для кражи информации используются специальные программы, позволяющие копировать пароли, копировать и прерывать информацию, перенаправлять трафик, расшифровывать и вносить изменения в функционирование других программ.

– Аппаратный. Связан либо с использованием специальных технических средств, либо с перехватом электромагнитного излучения по различным каналам, включая телефон.

Несанкционированное воздействие на защищенную информацию - это воздействие с нарушением правил ее изменения (например, подмена

электронных документов). Под непреднамеренным воздействием на защищенную информацию понимается воздействие на нее из-за ошибок пользователя, сбой техники, или программных средств, природных явлений и других непреднамеренных воздействий (например, уничтожение документа на накопителе на жестком диске).

При принятии на работу в большинстве случаев требуют сообщить исчерпывающую информацию о его семейном положении и ближайших родственниках, о жилищных условиях, состоянии здоровья, о фактах привлечения к уголовной ответственности, о наличии постоянной регистрации по месту жительства и другие моменты, касающиеся жизни человека. Но такого рода информация никаким образом не относится к трудовой деятельности будущего работника. Напротив, тем самым потенциальный работодатель очень тонко балансирует на грани, отделяющую персональные данные от сведений, составляющих тайну частной жизни, личную или семейную тайну гражданина.

В зависимости от ситуации, в которой находится человек, вид персональных данных, требуемых какой-либо организацией, может значительно варьироваться.

Согласно учебному пособию, в котором В.И. Аверченко называет персональные данные «любой информацией, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)», то есть имеется ввиду:

– При поступлении на работу – это данные отдела кадров работодателя, которые работник указывает в личной карточке, автобиографии, других документах, заполняемых при заключении трудового договора.

– При поступлении ребенка в детский сад, школу, институт, другие образовательные учреждения также заполняется множество анкет и форм, в которых указываются данные как ребенка (например, данные свидетельства о рождении), так и его родителей (вплоть до места работы,

занимаемой должности).

– При прохождении лечения в медицинских учреждениях необходимо указывать не только паспортные данные, но и информацию о льготах, медицинской страховке, сведения о предыдущих курсах лечения и результаты анализов. Во многих больницах амбулаторные/стационарные карты дублируются в электронном виде. И все эти данные подлежат защите.

Персональные данные объективно специфичны для любого человека, они подчеркивают правовой статус человека и гражданина – в этом заключена важность конфиденциальности. Персональные данные содержат необходимый объем информации о человеке, участвующем в соответствующих правовых отношениях. Персональные данные принадлежат непосредственно лицу и, как правило, не заинтересованы в его несанкционированном распространении, в связи с чем защита персональных данных различными юридическими средствами не случайна. Исходя из этого, доступ к персональным данным предоставляется очень ограниченному числу лиц, работодателей, сотрудников отдела кадров и так далее. В связи с этим трудно переоценить значимость персональных данных. Правовое регулирование персональных данных в настоящее время привлекает внимание ученых и практиков.

Специалист по информационной безопасности В.И. Петренко в своём учебном пособии «Защита персональных данных в информационных системах» внёс своё определение защиты персональных данных, как комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)[46].

Один из самых часто встречаемых терминов - это обработка персональных данных, что является неотъемлемой частью процесса

защиты персональных данных.

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

Можно выделить некоторые принципы обработки персональных данных.

Обработка персональных данных должна осуществляться на законной и справедливой основе.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо

обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Существуют некоторые условия обработки персональных данных, которые перечислены ниже.

Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

Обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта).

Обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта

персональных данных на едином портале государственных и муниципальных услуг [12].

Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных [30, с. 147].

Обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

Обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных.

Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

Осуществляется обработка персональных данных, подлежащих

опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Далее следуют главные элементы, составляющие основу для систем защиты конфиденциальной информации:

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

– Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

– Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

– Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

– Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

– Обезличивание персональных данных - действия, в

результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

В конечном итоге, нужно отметить, что персональные данные доступны практически в каждой организации, а это довольно внушительный перечень: паспортные данные, сведения о семейном положении, сведения об образовании, номер ИНН, свидетельства государственного пенсионного страхования, медицинской страховки, сведения о трудовой деятельности, социальное и имущественное положение, сведения о доходах.

1.2. Нормативно-правовые аспекты регулирования работы с конфиденциальной информацией в учреждении

Система информационной безопасности образовательного учреждения должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены организации любого несанкционированного проникновения, как случайного характера, так и незаконного, с целью хищения каких-либо данных или внесения изменений в конфигурацию системы.

Три группы могут быть идентифицированы как часть юридически защищенного массива информации, находящегося в распоряжении учебного заведения:

– личная информация о учениках и преподавателях, оцифрованные архивы;

– оригинальные идеи образовательного процесса, носящего

интеллектуальную собственность и защищенного законом;

– структурированная образовательная информация (библиотеки, базы данных, учебные пособия), предоставляющая учебный процесс.

Все эти сведения не только могут стать объектом хищения: умышленное проникновение в них может нарушить безопасность оцифрованных книг, уничтожить хранилища информации, внести изменения в код программ, используемых для обучения.

Обязанностями лиц, ответственных за защиту информации, должна заключаться в защите и обеспечении сохранности и целостности данных:

– доступность в любое время для любого авторизованного пользователя;

– защита от любых потерь или несанкционированных изменений;

– конфиденциальность, недоступность третьим лицам.

Защита информации основывается на действующих законах в этой области, определяющих ее отдельные массивы в качестве объекта защиты. Они подчеркивают информацию, которая не должна быть доступна третьим лицам по разным причинам (конфиденциальная информация, личные данные, коммерческая, коммерческая или профессиональная тайна). Порядок защиты персональных данных определяется, в том числе, Федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методологию обеспечения защиты сведений, составляющих коммерческую тайну. Помимо законов, необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты информации и применяемые для этого методы и аппаратные средства.

Конституция Российской Федерации составляет правовую основу обеспечения информационной безопасности в РФ, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы,

федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Обработка персональных данных должна осуществляться на законной и справедливой основе, ограничиваясь достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Позволяется обрабатывать персональные данные только в том случае, если это соответствует целям их обработки.

Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» установлены конкретные требования по обеспечению создания и ведения официального сайта образовательного учреждения в сети «Интернет», а также требования к информационным системам в сфере образования.

В соответствии с установленными законом требованиями образовательное учреждение обязано разместить на своём сайте сведения:

– о персональном составе педагогических работников с указанием уровня образования и квалификации;

– о доступе к информационным системам и информационно-телекоммуникационным сетям.

В этой связи, нужно обратить внимание, что федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», установлены жёсткие требования к защите и обработке персональных данных. Обработка персональных данных преподавателей и обучающихся в большом объёме осуществляется в каждом образовательном учреждении, которое, как предусмотрено федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», обязаны принять меры по защите персональных данных. В свою очередь данные меры предусматривают, прежде всего, создание достаточно большого количества локальных нормативных актов образовательного учреждения.

Также, статьёй 29 закона от 29.12.2012 г. № 273-ФЗ «Об

образовании в Российской Федерации» требования к информационной открытости образовательного учреждения гораздо серьёзнее. А статья 98, входящая в данный закон, устанавливает требования к информационным системам в сфере образования, которые обязывают образовательные организации осуществлять обработку персональных данных указанных системах в строгом соответствиис законодательством.

Таким образом, обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных» от 27.07.2006 года №152-ФЗ.

Обработка персональных данных допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27.07. 2010 года № 210ФЗ, для обеспечения

– предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

– обработка персональных данных необходима для исполнения договора, стороной которого либо получателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться получателем или поручителем;

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

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных» от 27.07.2006 года №152-ФЗ, при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональныхданных либо по его просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральнымзаконом;

– оператор имеет право поручить обработку персональных данных другому лицу при согласии субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, или путем принятия государственным или муниципальным органом соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных» от 27.07.2006 года №152-ФЗ. В поручении оператора должны быть определены действия (операции) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, нужно установить обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных» от 27.07.2006 года №152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Основополагающие нормы, регулирующие отношения по поводу персональных данных, содержатся в Федеральном законе «О персональных данных». В соответствии с п. 1 ст. 3 этого Закона персональными данными является любая информация, относящаяся к

определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [7].

В соответствии с ч. 1 ст. 85 ГК РФ под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Оценочный характер данного определения отражает лишь общий подход законодателя к категории персональных данных работника. Работодатель может собирать и обрабатывать не любую информацию о лице, являющемся его работником, а лишь ту, которая непосредственно связана с его трудовым правоотношением [3].

В 2012 году было принято новое Постановление Правительства №1119, а в 2013 году введён в действие новый Приказ ФСТЭК №21, а также очередные правки в Федеральном законе №152 от 27.07.2011. Данные документы предъявляют новые требования к оператору персональных данных.

Так же можно выделить еще три группы нормативных документов по защите персональных данных – это: методические материалы ФСТЭК России; Приказ ФСТЭК России о составе и содержании мер по обеспечению безопасности персональных данных в ИСПДн; Методические материалы ФСБ России [29, с.89].

Методические материалы ФСТЭК России:

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (При применении документа следует учитывать, что Постановлением Правительства РФ от 01.11.2012 N 1119 утверждены новые Требования к защите персональных данных при их обработке винформационных системах персональных данных).

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года (При применении документа следует учитывать, что Постановлением Правительства РФ от 01.11.2012 N 1119 утверждены новые Требования к защите персональных данных при их обработке в информационных системах персональных данных).

Согласно Приказа ФСБ России от 10.07.2014 N 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 N 33620) методические материалы ФСБ России включают:

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 4 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 3 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 2 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской

Федерации требований к защите персональных данных для 1 уровня защищенности;

Требования[18]:

– являются обязательными для оператора, осуществляющего обработку персональных данных, а также лица, которому на основании договора оператор поручает обработку персональных данных и (или) лица, которому на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности защиты персональных данных при их обработке в информационной системе с использованием криптосредств. При этом существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе в случаях, предусмотренных действующим;

– распространяются на криптосредства, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, все технические средства которых находятся в пределах Российской Федерации, а также в системах, технические средства которых частично или целиком находятся за пределами Российской Федерации.

– не отменяют требования иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Оператор несёт ответственность за незаконную обработку персональных данных, а именно: оператору нельзя собирать, хранить, использовать и распространять информацию о личной жизни, переписке, телефонных разговорах и т. п., если нет судебного постановления или других законных оснований для этой деятельности.

Оператор не вправе причинять материальный и моральный урон людям, ущемлять их права и свободы, используя персональные данные.

Нарушение закона «О персональных данных» может повлечь за собой дисциплинарную, административную и уголовную ответственность.

Но оператор с учетом особенностей своей деятельности может разрабатывать не противоречащие настоящим Требованиям методические рекомендации по их применению.

В соответствии со ст. 24 лица ФЗ «О персональных данных», виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность Закона № 152-ФЗ «О персональных данных». Неисполнение требований Закона № 152-ФЗ «О персональных данных» операторами баз данных может повлечь: гражданские иски со стороны работников; репутационные риски; приостановление или прекращение обработки персональных данных в школе, осуществляемой с нарушением требований Закона № 152-ФЗ «О персональных данных»; направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных; привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях. В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

1 июля 2017 года вступает в силу Федеральный закон от 07.02.2017 № 13-ФЗ, который вносит поправки в ст. 13.11 КоАП. В частности, он предусматривает расширение перечня оснований для привлечения к административной ответственности за незаконную обработку

персональных данных и существенное увеличение штрафов.

Таким образом, нормативной основой защиты персональных данных являются нормы Конституции РФ, Федерального закона «О персональных данных», Указ Президента РФ «О перечне сведений конфиденциального характера», требования и другие нормативно-правовые акты Российской Федерации.

1.3. Технология защиты персональных данных в организации

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. При обработке персональных данных должны быть обеспечены точность достаточность, а в необходимых случаях и актуальность персональных данных по отношению к целям обработки персональных данных.

Хранить персональные данные нужно в форме, которая позволяет определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом, договором, стороной которого получателем или поручителем является субъект персональных данных. После достижения целей обработки, персональные данные необходимо уничтожить либо обезличить, если иное не предусмотрено федеральным законом.

В общих чертах защита персональных данных сводится к созданию режима обработки персональных данных, включающая:

– разработку внутренней документации по работе с персональными данными;

– создание организационной структуры системы защиты персональных данных;

– внедрение технических мер защиты персональных данных;

– получение сертификатов регулирующих органов (Федеральной службы безопасности и Федеральной службой по техническому и

экспортному контролю) на средства защиты информации;

– при необходимости, получение лицензий регулирующих органов (Федеральной службы безопасности и Федеральной службой по техническому и экспортному контролю). Лицензия Федеральной службы по техническому и экспортному контролю России на Техническую защиту конфиденциальной информации, нужна только в случае, если организация оказывает услуги по созданию системы защиты персональных данных для других лиц. При создании системы защиты персональных данных силами организации как техническими средствами, так и организационными – данная лицензия не нужна.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение Федерального закона «О персональных данных».

Для определения уровня защищенности необходимо установить категории обрабатываемых персональных данных субъектов (физических лиц), вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз актуальных для информационной системы.

Категории обрабатываемых персональных данных, подразделяются на 4 группы:

– 1 группа — специальные категории персональных данных, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

– 2 группа — биометрические персональных данных, то есть данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев;

– 3 группа — общедоступные персональных данных, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа — иные категории персональных данных, не представленные в трех предыдущих группах.

По форме отношений между вашей организацией и субъектами обработка подразделяется на 2 вида:

– обработка персональных данных работников (субъектов, с которыми ваша организация связана трудовыми отношениями);

– обработка персональных данных субъектов, не являющихся работниками вашей организации.

По количеству субъектов, персональные данные которых обрабатываются, нормативным актом определены лишь 2 категории:

– менее 100 000 субъектов;

– более 100 000 субъектов;

Также существуют типы актуальных угроз для организации:

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном

программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, точно не регламентировано, в связи с чем, необходимо привлекать компетентных специалистов и производится либо ими, либо оператором с учетом оценки возможного вреда, проведенной во исполнение Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных».

Как правило, выделяют четыре класса методов защиты персональных данных в информационных системах:

– физические методы

– аппаратные

– программные

– организационные.

На организационном уровне защита персональных данных происходит посредством разработки и внедрения соответствующих нормативно-правовых актов, проведения организационно-технических мероприятий.

Физическая защита осуществляется за счет таких средств как служба охраны, система защиты окон и дверей, лазерные и оптические системы, которые реагируют на пересечение злоумышленником световых лучей. То есть физические методы защиты подразумевают под собой физическое

преграждение доступа к персональным данным.

Аппаратные методы защиты возможно реализовать при помощи специальных устройств. К таким средствам можно отнести различные схемы блокировки от несанкционированного использования персональных данных. Аппаратные средства применяются в составе ЭВМ.

Наконец, программная защита осуществляется при помощи программ, к которым можно отнести операционную систему, антивирусы, специальные программы защиты и прочие.

Пожалуй, именно аппаратно-программные средства защиты персональных данных в наибольшей степени позволяют защищать персональные данные от несанкционированного доступа к ним.

Аппаратно-программная защита достигается применением таких способов защиты как:

– Защита от несанкционированного использования персональных данных со стороны пользователей и программ, в том числе и при наличии доступов.

– Защита от некорректного использования имеющихся ресурсов.

– Высокая степень качества используемых аппаратно-программных средств.

Для определения соответствующей защиты информационных систем персональных данных ввели так называемые уровни защищённости, которых существует 4 вида.

– 1 уровень присваивается:

  - если существуют угрозы 1 типа и информационная система работает со специальными, биометрическими или иными категориями ПД;
  - если существуют угрозы 2 типа и информационная система работает со специальными категориями ПД свыше 100 тысяч граждан.

– 2 уровень присваивается при типах угроз:

- 1 и работе с общедоступными личными данными;
- 2 и работе с личными данными служащих оператора или при работе со специальной категорией ниже 100 тысяч человек;
- 2 и работе с использованием биометрических личных данных;
- 2 и обработке общедоступных личных данных при количестве от 100 тысяч человек (без персонала оператора);
- 2 и работе с другими видами ПД с количеством от 100 тысяч человек (без учета работников оператора);
- 3 и работе со специальной категорией более чем 100 тысяч человек (не считая персонала оператора).

– 3 уровень присваивается при типах угроз:

- 2, включая работу с ПД общедоступного характера с количеством людей до 100 тысяч человек;
- 2 с работой с другими категориями до 100 тысяч человек;
- 3 с обработкой специальных категорий до 100 тысяч человек;
- 3 с использованием биометрических ПД;
- 3 с работой с другими категориями, превышающими 100 тысяч человек (кроме персонала оператора).

– 4 уровень присваивается при типах угроз:

- 3 типа и работе с общедоступной информацией;
- 3 типа и обработке других категорий меньше 100 тысяч человек.

Проверку законных оснований для обработки персональных данных проводит Роскомнадзор. Плановая проверка проводится один раз в три года и в точные сроки, подготовленные Роскомнадзором и утвержденные прокуратурой. Плановая проверка оператора проводится в начале его

деятельности и в дальнейшем каждые три года.

Таким образом, при создании системы защиты персональных данных в организациях, на современном этапе развития в РФ, можно выделить следующие последовательные этапы:

– выяснить и определить все случаи, когда необходимо проводить обработку персональных данных в организации;

– определить бизнес-процессы, в которых обрабатываются персональные данные;

– наметить обязательные (в том числе предварительные) этапы работ по защите персональных данных:

– выделить все возможные ситуации, когда необходимо проводить обработку персональных данных;

– отобрать определенное число бизнес-процессов для проведения анализа. (необходимо разработать перечень структурных подразделений и работников организации, принимающих непосредственное участие в обработке персональных данных в рамках своих функциональных обязанностей);

– определить совокупность обрабатываемых персональных данных и круг информационных систем;

– провести ранжирование персональных данных по категориям и предварительную классификацию информационных систем.

– наметить меры по минимизации категорий обрабатываемых персональных данных;

– подготовить действующую модель угроз для информационной системы обработки персональных данных.

– разработать техническое задание по созданию необходимой системы защиты;

– провести уточнение соответствия классов информационных систем, с дальнейшей подготовкой предложений по использованию технических средств защиты персональных данных;

– подать уведомление о начале обработки персональных данных в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) для регистрации в качестве оператора персональных данных;

– подать заявку на получение экземпляров руководящих документов в Федеральную службу по техническому и экспортному контролю России по организации системы защиты персональных данных;

– разработать требования для конкретной системы обработки персональных данных, учитывая класс защиты информационной системы

– для защиты информационной системы обработки персональных данных и помещений подготовить технический проект.

– для документов в информационной системе защиты персональных данных (регламенты, приказы, положения, инструкции) разработать пакет организационно-распорядительные документы;

– провести внедрение системы защиты персональных данных;

– с субъектов персональных данных взять согласие на обработку персональных данных;

– провести контрольные мероприятия по выявлению нарушений защиты персональных данных; физическому или юридическому лицу иностранного государства, при передаче оператором персональных данных через государственную границу Российской Федерации органу власти иностранного государства, проверить находится ли получатель персональных данных в стране, где осуществляется надлежащая защита персональных данных.

В случае необходимости, может привлекаться организация, для выбора и реализации методов и способов защиты информации в информационной системе обработки персональных данных, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации оформленную в установленном законом порядке.

Вывод по главе 1

Таким образом, в данной главе были рассмотрены основная теоретическая база в сфере защиты и обработки персональных данных, касающиеся их нормативно-правовая составляющая в регулировании работы с конфиденциальной информацией, а также элементы, входящие в технологию защиты данных.

Информационная система обработки персональных данных выбирается в качестве системы защиты персональных данных в зависимости от класса информационной системы с учетом: угроз безопасности персональных данных; режимов обработки персональных данных, использование соответствующих методов и средств защиты информации от несанкционированного доступа (реализованы функции контроля доступа, регистрации и учета); обеспечение целостности защиты персональных данных; анализ защищенности персональных данных; обеспечение безопасного соединения; обнаружение проникновения.

Система защиты персональных данных включает меры организационно-технического характера, которые определяются с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в системе обработки информации организации.

Глава 2. Разработка мероприятий по повышению эффективности защиты персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»

2.1. Методы и средства повышения эффективности системы защиты персональных данных

Часто поддержание системы информационной безопасности своими силами кажется трудоемкой задачей. Не каждое учреждение имеет возможность нанять полный штат специалистов в этой области. Во многих случаях проще делегировать эту задачу внешней организации, нанять сторонних специалистов для помощи в подборе и установке соответствующего оборудования, консультирования персонала, оказания поддержки в написании политик конфиденциальности и внутренних регламентов работы с секретной информацией.

Подобное сотрудничество всегда требует большой самоотдачи от высшего руководства организации и всех ее сотрудников. Невнимательность и недостаточное внимание к соблюдению мер защиты может привести к краже данных, крупным штрафам, судебным разбирательствам и потере репутации.

Поэтому необходимо регулярно проводить оценку эффективности выбранных мер защиты, оперативно вносить коррективы, следить за изменениями в законодательстве.

Детальный перечень технических и организационных мер безопасности также законодательно определен. К ним относятся порядок идентификации и аутентификации субъектов и объектов доступа, цепочка контроля доступа, ограничение программной среды, надежная защита машинных носителей, антивирусная защита, предотвращение и обнаружение вторжений, анализ уровня защищенности среды, а также обеспечение доступности данных и выявление событий, которые потенциально могут привести к системным сбоям. Кроме того, закон

обязывает в случае технической невозможности реализации каких-либо мер разработать иные компенсационные меры по нейтрализации угроз.

Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Правовая составляющая должна стать обязательным элементом всей деятельности учреждения в этом направлении, поскольку необходимо: разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных; сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т. д.

При этом согласно Закону № 152-ФЗ «О персональных данных» обязанность доказательства согласия субъекта персональных данных на их обработку возлагается на оператора. Несмотря на то, что в данном комментарии речь идет исключительно о защите персональных данных работников, необходимо учесть, что обрабатываются персональные данные в образовательном учреждении обучающихся и их родителей, поэтому ГБПОУ «Южно-Уральский государственный технологический колледж» предварительно должно получить согласие родителей на обработку персональных данных их самих и их детей.

Следует уделить особое внимание процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие:

– основания для такой передачи, предусмотренного федеральными законами, или согласия на обработку персональных данных в школе субъекта персональных данных, закрепленного, например, в договоре на оказание услуг;

– договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности при обработке персональных данных

в образовательном учреждении.

С учетом вышеизложенного можно выделить следующие обязательные этапы работы по защите персональных данных работников:

– определение всех ситуаций, когда требуется проводить обработку персональных данных;

– выделение процессов, в которых обрабатываются персональные данные;

– выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

– определение круга информационных систем и совокупности обрабатываемых персональных данных;

– проведение категорирования персональных данных и предварительной классификации информационных систем;

– разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

– внедрение системы обеспечения безопасности информации.

Следовательно, защита персональных данных в образовательных учреждениях, по сути, сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;

– организацию системы защиты персональных данных;

– внедрение технических мер защиты персональных данных.

2.2. Рекомендации по профилактике и повышению эффективности защиты конфиденциальной информации в ГБПОУ «Южно-Уральский государственный технический колледж»

В ГБПОУ «Южно-Уральский государственный технический колледж» советом колледжа была создана взаимосвязанная и целостная подструктура по организации и осуществлению защищенного доступа к электронным сетевым сервисам, называемая Информатизационным Центром (ИЦ).

В учреждении было разработано и принято Положение об информатизационном центре (ИЦ), в котором закреплены:

1. Общие положения

1.1. Главной целью деятельности ИЦ является организация и предоставление доступа к электронным сетевым сервисам для повышения эффективности работы подразделений колледжа.

1.2. В своей деятельности руководствуется:

– Конституцией РФ;

– Законом Российской Федерации от 29 декабря 2012 г. № 273-1 «Об образовании в Российской Федерации»;

– Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»;

– Уставом колледжа:

– документацией внутриколледжной системы менеджмента качества;

– документацией внутриколледжной системы менеджмента охраны труда и техники безопасности;

– законодательными и нормативными актами по охране труда, пожарной безопасности и обеспечения защиты персональных данных;

– данным положением.

2. Структура центра и управление

2.1. Информатизационный центр осуществляет свою деятельность

как структурное подразделение колледжа;

2.2. Структура ИЦ состоит из лабораторий, специализирующихся по направлениям:

– лаборатория технического обеспечения;

– лаборатория информационных технологий.

2.3. Руководство лабораторией осуществляет заведующий лабораторией, который подчиняется непосредственно руководителю ИЦ.

2.4. Руководство ИЦ осуществляет руководитель ИЦ, который подчиняется непосредственно заместителю директора по информационным технологиям.

2.5. Руководитель ИЦ и заведующие лабораториями, назначаются на должность и освобождаются от нее приказом директора колледжа.

2.6. Структуру и штатную численность ИЦ утверждает директор колледжа.

2.7. Сотрудники ИЦ являются штатными сотрудниками колледжа.

3. Направления и организация деятельности

Для достижения поставленной цели ИЦ решает следующие задачи:

3.1. Разработка и осуществление единой технической политики и практического использования современных достижений информационных технологий в бизнес-процессах колледжа.

3.2. Выполнение работ по созданию и развитию единой информационной сети колледжа.

3.3. Выполнение работ, ориентированных на создание новых информационных технологий в целях информационного обеспечения учебного процесса и управления в колледже.

3.4. Организация разработки нового программного обеспечения и рекомендаций по использованию готовых программных продуктов, ориентированных на применение компьютерных технологий в учебном и управленческом процессах.

3.5. Участие в планировании повышения квалификации сотрудников колледжа по проблемам использования новых информационных технологий в учебном процессе и управлении.

3.6. Координация организации и проведение научно-методических конференций, школ-семинаров, курсов в области информационных технологий.

3.7. Проектирование, создание и развитие автоматизированной системы управления колледжем.

3.8. Анализ потребностей служб и подразделений колледжа в средствах вычислительной и оргтехники, организация работы по их оснащению средствами информатизации.

3.9. Предоставление платных дополнительных услуг для сотрудников и студентов, согласно утвержденному положению.

4. Функции

4.1. Основные функции лаборатории технического обеспечения:

- Текущее обслуживание и организация ремонта (замены) средств вычислительной и офисной техники.
- Организация и проведение комплекса работ по грамотной технической эксплуатации средств вычислительной и офисной техники.
- Оказание помощи преподавателям и студентам по вопросам, связанным с эксплуатацией вычислительной техники и программного обеспечения.

4.2. Основные функции лаборатории информационных технологий:

- Создание, обслуживание и развитие защищенного центрального серверного центра колледжа.
- Проектирование и развитие компьютерной сети с использованием современных достижений в данной области.
- Установка, настройка и сопровождение сетевых программных продуктов.

- Создание надежных условий для доступа всех пользователей к компьютерной сети колледжа.
- Предоставление сетевых сервисов в Целях обеспечения учебных и управленческих работ.
- Организация централизованной антивирусной защиты информационных ресурсов.
- Предоставление сетевых ресурсов для автоматизации управленческой деятельности подразделений.
- Проектирование, разработка, размещение и поддержка внешних и внутренних Web-серверов.
- Подбор, адаптация, разработка нового и внедрение программного обеспечения с целью создания и развития автоматизированной системы управления колледжем.
- Адаптация и внедрение программного обеспечения для организации процесса дистанционного образования и независимой проверки знаний.
- Организация работ по обеспечению защиты информационных систем персональных данных.

5. Взаимоотношения и связи ИЦ

ИЦ осуществляет свою деятельность совместно со структурными подразделениями колледжа в соответствии с нормативными документами колледжа, приказами и распоряжениями директора и заместителя директора по информационным технологиям.

6. Права, обязанности и ответственность

6.1. ИЦ имеет право:

- Требовать от сотрудников колледжа соблюдения правил работы с компьютерным и офисным оборудованием, выполнения инструкций по работе с программным обеспечением, обязательное прохождение обучения на внутренних курсах ИЦ при получении неудовлетворительной

оценки за проверочное тестирование знаний сотрудников колледжа в области ИТ.

- Выполнять работы только по размещенным на внутреннем портале электронным заявкам, за исключением случаев, когда заявки не могут быть размещены в результате недоступности сетевых сервисов.
- Запрашивать и получать от руководства информацию, необходимую для выполнения работ реализующих функции ИЦ.
- Формировать заявки на приобретение необходимой нормативной, технической и справочной документации.
- Участвовать в разработке текущих и перспективных планов работы колледжа.
- Представлять перспективные планы развития единого информационного пространства колледжа, докладывать о текущем состоянии их реализации.
- Вносить предложения руководству колледжа по формированию внутренней структуры и штатного расписания ИЦ.

6.2. ИЦ обязан:

- Осуществлять стратегическое планирование деятельности колледжа в области информационных технологий.
- Обеспечивать бесперебойную работу компьютерной техники, сетевых сервисов и офисного оборудования.
- Своевременно предоставлять отчетную документацию.
- Принимать участие в мероприятиях, предусмотренных планами работ.
- Осуществлять деятельность в соответствии с руководством по качеству и другой документации СМК и СУОТ колледжа.

Как можно заметить, ГБПОУ «Южно-Уральский государственный

технический колледж» имеет довольно сильную подструктуру для контроля обработки и хранения конфиденциальной информации, направленную на точное исполнение своих функций, основывающуюся на чёткой иерархии, а также распределении обязанностей и ответственности.

Также, ГБПОУ «Южно-Уральский государственный технический колледж», согласно законодательству, имеет «Положение об обработке и защите персональных данных», где закреплены соответствующие:

- общие положения;
- понятие и состав персональных данных;
- основные условия проведения обработки персональных данных;
- условия хранения, использования и передача персональных данных;
- обязанности организации по хранению и защите персональных данных;
- ответственность за нарушение норм, регулирующих обработку данных и настоящего Положения.

В связи с тем, что в ГБПОУ «Южно-Уральский государственный технический колледж» уже существует достаточно надёжная система организации защиты персональных данных - ИЦ, то стоит подумать о внедрении профилактических мер, которые помогут избежать случаев несанкционированного доступа к конфиденциальной информации, её потери или незаконного распространения, а также о возможности использования криптографических средств защиты информации и проведения систематических аттестационных мероприятий для определения соответствия применяемого комплекса мер в организации к требуемому уровню защиты данных.

Главными задачей аттестационных испытаний объекта защиты является оценка соответствия системы защиты информации объекта защиты требованиям безопасности информации, выполнение которых

позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носители.

Виды выполняемых, при проведении аттестации, работ:

1. Определение перечня объекта информатизации, подлежащих аттестации, категорирование и классификация.

2. Анализ и оценка исходных данных и документации по защите информации на ОИ, оценка правильности категорирования.

3. Проверка соответствия представленных исходных данных реальным условиям размещения и эксплуатации ОИ.

4. Разработка документации (включая как паспорта ОИ, так и организационно-распорядительную документацию) на ОИ, подготавливаемые к аттестационным испытаниям.

5. Проверка технологического процесса хранения и обработки информации, определение возможных каналов утечки информации и разработка перечня мероприятий по их исключению.

6. Оценка соответствия помещений, в которых установлены ОИ предъявляемым требованиям, включая, при необходимости, специальную проверку на наличие внедренных устройств перехвата информации.

7. Оценка уровня подготовки персонала.

8. При необходимости, проведение мероприятий по защите информации (поставка, установка и настройка средств защиты информации).

9. Подготовка и утверждение программы и методики проведения аттестационных испытаний.

10. Проведение аттестационных испытаний, включая отдельные технические и программные средства, инженерное, ИТ-оборудование и пр.

11. Проведение испытаний объектов информатизации на соответствие требованиям по защите информации от несанкционированного доступа и утечки по техническим каналам.

12. Подготовка отчетной документации (протоколов испытаний, заключения по результатам аттестационных испытаний).

13. Выдача, при условии положительного заключения, «Аттестата соответствия».

14. Анализ результатов аттестационных испытаний, разработка рекомендаций по совершенствованию принятых мер по защите информации от утечки по техническим каналам, закрытию выявленных каналов утечки информации.

Выданный сертификат выдаётся сроком на 3 года, что позволяет периодически проверять надёжность и актуальность систем защиты.

Одним из наиболее действенных способов защиты персональных данных является использование средств криптографии, то есть, шифровании текста с помощью цифрового кода.

К криптографическим средствам относятся аппаратные, программные и комбинированные устройства и комплексы, способные реализовывать алгоритмы криптографического преобразования информации.

Они предназначены одновременно для защиты информации при передаче по каналам связи и защиты ее от неразрешенного доступа при обработке и хранении. Никто не сможет извлечь информацию без соответствующего кода, даже если получит к ним доступ, поскольку не прочтет их.

Регламент использования криптографических средств определяется Федеральной службой безопасности и документирован в соответствующе Приказе Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378.

Криптографический способ ограничения к данным исключает возможность несанкционированного доступа к конфиденциальным данным. Разумеется, для таких средств необходимо установить соответствующую документацию с требованиями и ответственностью,

определить уровни доступа для сотрудников.

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

Со всех лиц, имеющих доступ к персональным данным, рекомендуется под роспись взять обязательство о конфиденциальности и неразглашении персональных данных, проект обязательства.

В ГБПОУ «Южно-Уральский государственный технический колледж» рекомендуется разработать инструкцию по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

В Инструкции рекомендуется отразить следующее:

- Общие положения.
- Виды мониторинга информационной безопасности.
- Порядок проведения системного аудита.
- Порядок антивирусного контроля.
- Порядок анализа инцидентов.

Необходимо ввести ведение журнала обращений по ознакомлению с персональными данными.

Журнал рекомендуется вести в каждом структурном подразделении в произвольной форме. В журнале необходимо фиксировать все обращения субъектов персональных данных (дата, ФИО, адрес) по ознакомлению с их персональными данными, дату направления запрашиваемых данных почтовой связью или предоставления лично заявителю. В случае отзыва данных субъектом персональных данных или выявления их несоответствия, в журнале должны быть сделаны соответствующие записи. По каждому обращению необходимо указывать, когда и каким образом на

него было отреагировало.

Хранение журналов должно исключать несанкционированный доступ к ним.

Так же необходимо вести электронный журнал обращений пользователей к персональным данным.

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

С 2021 года законодательно работа с персональными данными была ужесточена снова, в следствие чего, ГБПОУ «Южно-Уральский государственный технический колледж» необходимо ввести в рекомендуемые рекомендации.

Предложенные мероприятия помогут существенно снизить угрозу разглашения персональных данных и избежать неблагоприятных последствий. Организовать систему защиты персональных данных организации, соответствующую современным требованиям и законодательству РФ.

Вывод по главе 2

Таким образом, задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Правовая составляющая должна стать обязательным элементом всей деятельности учреждения в этом направлении, так как это позволит разработать локальные акты (нормативно-правовые), касающиеся не

только организационно-правовой, но и технической защиты личные данные. данные и формировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзами, органами контроля и надзора и др.

Профилактические методы и рекомендации к защите данных необходимо соблюдать, постоянно следить за мировыми тенденциями развития в области информационной безопасности, чтобы в соответствии с актуальными и современными нормами обеспечивать необходимую защиту конфиденциальной информации, не допустить её утечек, потери, уничтожения или разглашения внутри и за пределами образовательной организации.

Заключение

На основе изученных информационных источников по теме исследования в рамках поставленной цели и выдвинутых задач можно делать следующие выводы.

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании.

В соответствии изучены понятия, свойства, аспекты безопасности информации, исследованы основные источники правового регулирования конфиденциальной информации

Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите и информации" напрямую имеет отношение к конфиденциальной информации. Также важным является Федеральный закон № 152-ФЗ от 27 июля 2006 "О персональных данных", в котором регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ и др.

Образовательные организации являются операторами персональных данных, поскольку занимаются обработкой персональных данных учащихся и педагогов. Следовательно, ответственными сотрудниками этих организаций должно обеспечиваться соблюдение законодательства.

Необходимо помнить и понимать, что для решения проблемы сохранности конфиденциальной информации необходимо применение законодательных, организационных и программно-технических мер. Игнорирование хотя бы одного из аспектов этой проблемы может привести

к утечке. Обеспечение информационной безопасности - комплексная задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как сотрудники, электронное оборудование, программное обеспечение и другое.

Исследование проводилось на базе ГБПОУ «Южно-Уральский государственный технологический колледж».

Основной целью создания защиты персональных данных в ГБПОУ «Южно-Уральский государственный технологический колледж» области является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

В целях создания надёжной и защищённой системы информационной безопасности персональных данных и создание условий для ее дальнейшего совершенствования, предлагается ряд рекомендации для ГБПОУ «Южно-Уральский государственный технологический колледж», таких как: журнал учета персональных данных, проведение систематических аттестационных проверок, криптографических средств защиты и др.

Необходимость предложенных выше мер и документов обусловлена стремительным расширением сферы применения информационных технологий и процессов на ГБПОУ «Южно-Уральский государственный колледж», при обработке информации вообще, и персональных данных в частности.

Реализация предложенных мероприятий, рекомендаций в информационных системах персональных данных, позволит:

– провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в информационных системах персональных данных;

– обеспечить необходимый уровень безопасности объектов защиты.

В заключение хотелось бы подчеркнуть, что свести риск потери информации к минимуму возможно лишь при комплексном подходе к вопросам обеспечения информационной безопасности образовательной организации.

Важно уделить внимание предложениям по совершенствованию мер защиты конфиденциальной информации, чтобы не вернуться к прежним методам работы системы защиты персональных данных.

Значимость заключается в принятие руководством анализируемой образовательной организации решения о необходимости совершенствования конфиденциального делопроизводства с учетом всех описанных рекомендаций и факторов по внедрению в комплексе предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации.

Список использованных источников

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Электронный ресурс]// Консультант Плюс : справ. правовая система.
2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.10.2017)// Консультант Плюс: справ. правовая система.
3. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 29.07.2017) «Об образовании в Российской Федерации» [Электронный ресурс]// Консультант Плюс: справ. Правовая система.
4. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 28.12.2016) «Об организации предоставления государственных и муниципальных услуг» [Электронный ресурс]// Консультант Плюс: справ. правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_103023/
5. Федеральный закон от 27.07.2006 N 179-ФЗ (ред. от 29.07.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2017) [Электронный ресурс]// Консультант Плюс:справ. правовая система.
6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных» [Электронный ресурс]// Консультант Плюс: справ. правовая система.
7. Приказ ФСБ России от 10.07.2017 N 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 18.08.2017 N 33620) [Электронный ресурс]// Консультант Плюс : справ. правовая система.

8. Аверченков, В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 3-е изд., стер. - М.: Флинта, 2016. - 124 с.
9. Амелин, Р.В. Информационное право в схемах: учебное пособие / Р.В. Амелин, С.А. Куликова, С.Е. Чаннов; отв. ред. С.Е. Чаннов. - М.: Проспект, 2016. - 125 с
10. Алавердов, А. Р. Организация и управление безопасностью в организациях [Текст]: Учебное пособие/ А. Р. Аведов. – М.: Московский государственный университет статистики и информатики, 2014. – 411с.
11. Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве [Текст]/ Ф.А. Абаев // Пробелы в российском законодательстве. 2013. № 5. С. 136-139.
12. Абаев, Ф.А. Понятие, правовая природа персональных данных [Текст]/ Ф.А. Абаев // Право и государство: теория и практика. 2014. № 3 (111). С. 126- 131.
13. Аленевская, В.В. Ограничение права на информацию в трудовых отношениях [Текст]/ В.В. Аленевская // Вестник Прикамского социального института. Гуманитарное обозрение. 2014. № 1 (8). С. 42-49.
14. Ануфриева, Н.С. Правовые проблемы обработки персональных

данных в трудовых отношениях [Текст]/ Н.С. Ануфриева // Актуальные проблемы современной юридической науки: Сборник научных трудов. Сургут: ИЦ СурГУ, 2012. С. 114-119.

15. Астахова, Л.В., Рублёв Е.Л. Проблемы защиты персональных данных в период смены нормативной базы и пути их решения [Текст]/ Л.В. Астахова, Е.Л. Рублёв // Вестник УрФО. Безопасность в информационной сфере. 2013. № 1 (7). С. 32-41.
16. Барышников, А.Б. Безопасность корпоративных центров обработки персональных данных [Текст]/ Барышников А.Б. // Защита информации. Инсайд. 2013. - № 6 (54). С. 40-41.
17. Бегларян, М.Е. Безопасность персональных данных в современной России [Текст]/ М.Е. Бегларян, Е.А. Пичкуренко // Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов материалы 4-ой Международной научно- практической конференции. 2015. С. 24-28.
18. Беденкова, А.А. Правовой статус персональных данных работников [Текст]/ А.А.Беденкова, И.С. Хоменко // Вестник науки Сибири. 2014. - № 4 (14). С. 148-151.
19. Бобров, И.В. Проблема защиты персональных данных работника [Текст]/ И.Вю Бобров, Ю.В. Комарецев // Проблемы российского законодательства и международного права Сборник статей Международной научно-практической конференции. Ответственный редактор: Сукиасян Асатур Альбертович. 2015. - С. 26-28.
20. Бойкова, О.Ф. Обрабатываем персональные данные работников [Текст]/ О.Ф. Бойкова // Независимый библиотечный адвокат. 2012. - № 2. С. 21-32.
21. Болотин, В.С. Механизм защиты права на неприкосновенность частной жизни при обработке персональных данных в

информационных системах [Текст]/ В.С.Болотин, М.А. Маслёха // Вестник государственного и муниципального управления. 2012. - № 3. С. 99-103.

22. Бондарь, А.О. Организация работы по обеспечению защиты государственных информационных систем персональных данных [Текст]/ А.О. Бондарь, В.П. Железняк, В.А. Мещеряков // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно- практической конференции. Воронеж: ИПЦ «Научная книга», 2013.- С. 174-175.
23. Балашкина, И. В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации [Текст]/ И. В. Балашкина. // Право и политика. 2017. – №7. – С. 92-105.
24. Блоцкий, В.Н. Конституционное обеспечение права человека на неприкосновенность частной жизни в Российской Федерации [Текст]/ В.Н. Блоцкий. // Автореф. дис. канд. юрид. Наук – М. 2017. – с. 31.
25. Борисова, С. А. Общие требования при обработке персональных данных работника и гарантии их защиты [Текст]/ С. С. Борисова // Трудовое право. 2013. – N 11. – С. 30-36.
26. Бобылева, М.П. Вопросы использования элементов электронного документооборота внутри организации [Текст]/ М.П. Бобылева// Делопроизводство. 2013. – №2. – С. 15.
27. Герасимов А. А. Задача моделирования процессов защиты информации в информационных системах персональных данных / А.А. Герасимов// Интеллектуальные системы – М.: МГТУ им. Н. Э. Баумана. 2012. – С. 588-589.
28. Грушо, А. А. Теоретические основы компьютерной безопасности: учеб. пособие / А.А. Грушо.: Академия Москва. 2013. 272 с.
29. Гугуева, Т. А. Конфиденциальное делопроизводство [Текст]:

учеб. пособие / Т.А. Гугуева. – М.: Альфа-М; ИНФРА-М. 2016. – 192 с.

30. Бугров А. Международные стандарты для построения системы ин-формационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.
31. Дворянкин, С. В. Обеспечение информационной безопасности в распределенных системах обработки данных / С.В. Дворянкин. // Безопасность информационных технологий. 2012. №1. С. 92-93.
32. Ищейнов, В. Я. Персональные данные в законодательных и нормативных документах Российской Федерации и информационных системах [Текст] / В. Я. Ищейнов // Делопроизводство. 2015. – N 3. – С. 87-90.
33. Кузнецова, Т. В. Организация работы с персональными данными [Текст] / Т. В. Кузнецова // Делопроизводство. 2014. – № 2. – С. 38.
34. Лушников, А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового кодекса РФ [Текст]/ А.М. Лушников // Трудовое право. 2016 – № 9. – С. 93-101.
35. Маркевич, А. С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях [Текст]: Автореф. дис. на соиск. уч. ст. канд. юрид. наук./ А. С. Маркевич. – Воронеж, 2015. – 28 с.
36. Башлыков М. Актуальные вопросы информационной безопасности / М. Башлыков // Финансовая газета. Региональный выпуск. - 2016. - № 11.
37. Макаров, А.М. Организация защиты персональных данных : лабораторный практикум / Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский

федеральный университет», Министерство образования и науки Российской Федерации ; авт.-сост. А.М. Макаров, И.В. Калиберда и др. - Ставрополь : СКФУ. 2015. – 92 с.

38. Маслеха, М.А. Теоретические основы защиты персональных данных // Законность и правопорядок в современном обществе. 2012. - № 8. – С. 94-103.
39. Международные трудовые стандарты и российское трудовое право: перспективы координации: монография / Э.Н. Бондаренко, Е.С. Герасимова, С.Ю. Головина и др.; под ред. С.Ю. Головиной, Н.Л. Лютова. М.: НОРМА, ИНФРА-М, 2016.
40. Меликов, У.А. Гражданско-правовая защита персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2015. – № 4 (18). – С. 49-53.
41. Меньшикова, А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения // Экономика и менеджмент инновационных технологий. 2014. – № 11 (38). – С. 156-159.
42. Минаев, В. А. Информационные операции и проблема формирования Современной культуры информационной безопасности / В. А. Минаев // Системы высокой доступности. 2017. №3. – С. 38-46.
43. Минбалеев, А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. – № 2 (4). – С. 4-9.
44. Мищенко, Е.Ю., Соколов А.Н. Количественные критерии идентификации физического лица при обезличивании персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2014. - № 1 (11). -С. 27- 33.
45. Новичкова, Ю. В. Персональные данные - без права передачи, или Особенности расторжения трудового договора за разглашение

персональных данных[Текст]/ Ю. в. Новикова // Справочник кадровика. – 2016. – N 1. – С. 14- 23.

46. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина; Федеральное государственное автономное образовательное учреждение высшего образования
47. «Северо-Кавказский федеральный университет», Министерство образования и науки РФ. - Ставрополь: СКФУ, 2017. - 86 с.
48. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации. - Ставрополь: СКФУ, 2016. - 201 с.
49. Савинцева, М. Н. Правовая защита персональной информации граждан в России [Текст]/ М. Н. Савинцева // Законодательство и практика масс-медиа. - 2013. - № 9. – С. 23
50. Соколова, О. С. Проблемы реализации Федерального закона «О персональных данных» [Текст]/ О. С. Соколова// Современное право. - 2011. - N 9. - С. 37-41.
51. Силакова О. В. Комплексная безопасность образовательного учреждения как важнейшее условие обеспечения безопасных условий проведения учебно-воспитательного процесса // Молодой ученый. — 2014. — №18.1. — С. 84-88.
52. Скрыль, С. В. Показатели эффективности информационных процессов и их защищенности в системах реального времени / С. В. Скрыль // Безопасность информационных технологий. – М. : МИФИ, 2012. - № 3. –С. 104-106.
53. Сычев М. П. Моделирование угроз информационной

безопасности с использованием принципов системной динамики / М. П. Сычев // Вопросы радиоэлектроники. 2017. - № 6. – С. 75-82.

54. Федосова, М. А. Защита персональных данных работника [Текст]/ М.А. Федосова // Финансовые и бухгалтерские консультации. - 2017. - N 11. - С. 71-74.
55. Федосеева, Н.Н. Сущность и проблемы электронного документооборота [Текст] / Н.Н. Федосеева // Юрист. - 2016. - №6. - с.61 – 64
56. Хачатурян, Ю. А. Право работника на защиту персональных данных[Текст]/ Ю. А. Хачатурян // Современное право. - 2016. - N 1. - С. 43-51.
57. Чаннов, С. Е. Правовой режим персональных данных на государственной и муниципальной службе [Текст]/ С. Е. Чаннов // Российская юстиция. - 2017. - N 1. - С. 21-23.
58. Куликов С. Г. Правовые основы обеспечения информационной безопасности Российской Федерации и Соединённого Королевства Великобритания и Северная Ирландия // Актуальные исследования. 2020. №19 (22). С. 52-55.