МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Разработка рекомендаций по повышению эффективности защиты конфиденциальной информации в организации

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасности в профессиональном образовании»
Форма обучения очная

Проверка на объем заимствований :
64% авторского текста

Выполнил:
студент группы ОФ-209/210-2-1
Савина Екатерина Сергеевна

Работа рекомендована к защите
« 27 » мая 2020 г.
Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Научный руководитель:
д.т.н., профессор кафедры АТ, ИТ и МОТД
Белевитин Владимир Анатольевич

Челябинск, 2020

Содержание

Введение

В условиях современной экономики важным ресурсом является информация. Информация представляет собой ценный компонент, обеспечивающий оптимальный режим работы организации в целом. Совокупность данных, хранящихся в виде бумажных документов или сведений на цифровых носителях, доступных для передачи заранее определённому узкому кругу лиц называется конфиденциальной информацией(КИ). КИ в зависимости от сферы применения представляет собой коммерческую, государственную или служебную тайну.

Обеспечение безопасности конфиденциальной информации – это важная задача всех операторов конфиденциальной информации в целом, и операторов организаций среднего профессионального образования в частности. Информационные ресурсы и информационные системы относятся к ряду основных защищаемых элементов во всех сферах жизнедеятельности современных организаций среднего профессионального образования.

Незаконное использование, потеря или утечка той или иной конфиденциальной информации может привести к сбоям в работе и нанести серьезный экономический ущерб организации.

Для предотвращения подобных сценариев организации обеспечивают комплексную защиту КИ, путём введения законодательных норм, обеспечения организационных мер и технических средств защиты КИ, а также посредством проведения качественной кадровой работы.

Введение законодательных норм подразумевает применение федеральных законов, доктрин, приказов и локальных нормативных актов для решения вопросов, касающихся защиты КИ.

Организационные меры представляют собой разработку внутренней документации, проведение инструктажей, разграничение зоны ответственности, внедрение программных продуктов, составление планов восстановления системы.

Технические средства, как правило, совмещают аппаратные и программные средства: резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе, установка программного обеспечения, обеспечивающее защиту баз данных и другой информации от несанкционированного доступа, обеспечение от пожара или повреждение компьютера водой. В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.

Кадровая работа состоит в проведении инструктажа, подписании дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе.

Поэтому одним из приоритетных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации, согласно списка, утвержденного Секретарем Совета Безопасности Российской федерации Н.П. Патрушевым 31.08.2017, является «исследование проблем развития системы обеспечения информационной безопасности РФ». В этой связи перед учеными стоит ряд задач направленных на достижение цели – совершенствование имеющихся систем обеспечения информационной безопасности и открытие принципиально новых путей решения данной проблемы.

Колоссальный вклад в совершенствование теории и практики безопасности сложных информационных систем, информационного взаимодействия, защиты технических, программных и информационных ресурсов внесли отечественные ученые. Среди них В.А. Садовничий [56], А.Р. Алавердов [22], А.А. Герасимова [35], А.А. Грушо[36], С.В. Дворянкина [38], В. А. Минаев [48], М.А. Маслеха [44] и другие.

В Челябинском институте путей сообщения, сотрудники, в том числе преподаватели и студенты находятся в тесном контакте между собой,

поскольку происходит постоянный обмен информацией, в том числе персональными данными, например кураторы учебных групп, в силу своих должностных полномочий, обязаны владеть сведениями, относящимся к персональным данным студентов, и их родителей, для поддержания постоянного контакта. В результате чего преподаватели становятся угрозой распространения данной информации.

В этой связи, обеспечение защиты КИ является важной задачей не только специалистов по информационной безопасности данной организации , но и преподавателей в том числе.

Актуальность. Тема диссертации актуальна, так как, несмотря на принятые меры защиты КИ, основной угрозой защиты всегда являются непосредственно сами сотрудники организации, так как не все знают, что является КИ и, соответственно, правила обработки КИ. В этой связи, ответственным за информационную безопасность необходимо заниматься качественным обучением сотрудников и студентов работе с КИ.

Целью исследования является разработка обучающего курса по работе с КИ для сотрудников и преподавателей и рекомендации по его применению в Челябинском институте путей сообщения.

Гипотеза исследования состоит в предположении о повышении эффективности защиты КИ при внедрении и применении обучающего курса по работе с КИ для сотрудников и преподавателей.

Объект исследования – это система защиты конфиденциальной информации в Челябинском институте путей сообщения.

Предмет исследования: внедрение и применение обучающего курса по работе с КИ для сотрудников и преподавателей.

Задачи исследования:

- раскрыть информационную систему КИ ЧИПС УрГУПС;
- выявить возможные уязвимости и риски;

– раскрыть нормативно-правовые требования, предъявляемые к СОБ КИ;

– разработать обучающий курс для обучения сотрудников и преподавателей по работе с конфиденциальной информацией;

– подготовить рекомендации по повышению защиты конфиденциальной информации в ЧИПС УрГУПС.

– дать экономическое обоснование внедрения обучающего курса в систему защиты КИ.

В процессе написания выпускной квалификационной работы были использованы федеральные законы, нормативно-методические документы, положения локальных актов, регулирующие организацию системы защиты КИ.

Научная новизна исследования заключается в том, что показана возможность необходимого обновления существующей системы безопасности конфиденциальной информации в образовательной организации среднего профессионального образования путем внедрения и применения обучающего курса для сотрудников и студентов.

Практическая значимость данной работы заключается в создании и внедрении обучающего курса «Управление информационной безопасностью в образовательной организации» на базе электронной образовательной платформе Black Board learn +, позволяющего повысить уровень осведомленности сотрудников и студентов в области защиты КИ.

Ход исследования и проблема исследования докладывались и обсуждались на конференциях всероссийского уровня:

1. Всероссийская научно-практическая конференция «Национальная безопасность и молодёжная политика. Вместе вне зависимости» Публикация: «Повышение эффективности защиты конфиденциальной информации образовательной организации путём внедрения обучающих курсов»./ [Текст] Савина Е.С., Белевитин

В.А.//Сборник материалов Всероссийской научно-практической конференции, г. Челябинск, 31 марта 2020 г. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера», 2020. – с.161 – 163.

2. II Международная научно-практическая конференция «Инновации в информационных технологиях, машиностроении и автотранспорте». Публикация: «Применение онлайн и офлайн тестов на занятиях дисциплины профессионального цикла./[Текст] Савина Е.С., Гафарова Е.А.// Сборник материалов II Международной научно-практической конференции (03 - 04 октября 2018 года), Кемерово [Электронный ресурс] / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева»; редкол.: Д.М. Дубинкин (отв. ред.) [и др.]. – Кемерово, 2018 – с. 68- 70.

Выпускная квалификационная работа (магистерская диссертация) состоит из введения, трёх глав, заключения, списка использованной литературы и приложения.

Во введении обосновывается выбор темы, приводится анализ степени её изученности, формулируются объект, предмет, цель и задачи исследования, методологические основы и структура работы.

В первой главе рассматривается структура ИС, описывается технологический процесс обработки информации, и приводится анализ рисков и уязвимостей существующей системы защиты КИ.

Во второй главе раскрыты нормативно-правовые требования локальных актов в том числе, предъявляемые к системе обеспечения защиты КИ.

В третьей главе описаны рекомендации по повышению эффективности защиты КИ, в виде внедрения обучающего курса на базе электронной образовательной платформы Black Board learn+, а так же дано экономическое обоснование внедрения.

В заключении подводятся итоги проведенного исследования, формулируются основные выводы по работе.

Список литературы содержит 59 источников.

В приложении представлено методическое пособие обучающего курса на базе электронной образовательной платформы BlackBoard learn +.

Экспериментальная база – Челябинский институт путей сообщения.

ГЛАВА 1. ИНФОРМАЦИОННАЯ СИСТЕМА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ЧИПС УРГУПС: СТРУКТУРА, ФУНКЦИОНИРОВАНИЕ, СИСТЕМА ЗАЩИТЫ

1.1 Функциональная структура ИС, содержание и средства ИС

В составе ИС выделяют следующие структурные компоненты – объекты информатизации:

– ИС «Контур-Экстерн» (расположен в Акционерном обществе «Производственная фирма «СКБ Контур» (далее по тексту – СКБ Контур);

– сегменты ИС «Контур-Экстерн» – подключаемые к системе «Контур-Экстерн» абонентские пункты (рабочие места пользователей в организациях – абонентах, размещающих отчетности в системе «Контур-Экстерн»).

– ИС 1С ЗуП (расположена в Федеральном государственном учреждении высшего образования «Уральский государственный университет путей сообщения» (далее по тексту – ФГБОУ ВО УрГУПС);

– сегмент ИС 1С ЗуП – подключаемые к системе ИС 1С ЗуП абонентские пункты (рабочее место пользователя ИС 1С ЗуП, расположенное в ФГБОУ ВО УрГУПС).

Сетевая структура ИС «Контур-Экстерн», расположенная в СКБ Контур, состоит из двух контуров – внешнего и внутреннего:

1) во внешнем контуре развернута подсистема «Контур-Экстерн» – интернет-портал. На интернет-портале размещаются открытые для общего пользования информационные материалы, связанные описанием возможностей системы и общедоступной информацией о ней. Интернет-портал доступен для всех пользователей сети Интернет.

2) во внутреннем (конфиденциальном) контуре развернуты ключевые подсистемы, обеспечивающие технологические процессы ИС «Контур-Экстерн»:

– внутренний портал;
– загрузка отчетных данных сформированных в 1С ЗуП;
– мониторинг результатов проверки отчетов;
– планирование и контроль деятельности;
– электронное хранилище отчетов;
– поиск и навигация по информационным ресурсам. [14]

Внутренний портал доступен только для авторизованных пользователей ИС «Контур-Экстерн» и обеспечивает их взаимодействие с другими подсистемами внутреннего контура ИС.

Сетевая структура ИС 1С ЗуП расположенная в ФГБОУ ВО УрГУПС, состоит из внутреннего контура. Во внутреннем (конфиденциальном) контуре развернуты ключевые подсистемы, обеспечивающие технологические процессы системы ИС 1С ЗуП:

1) пользовательский интерфейс сервера приложений;
2) формирование сведений бухгалтерской отчетности;
3) выгрузка данных для дальнейшего размещения в ИС «Контур-Экстерн»;
4) планирование и контроль деятельности;
5) электронное хранилище данных бухгалтерской деятельности.

Пользовательский интерфейс доступен только для авторизованных пользователей системы 1С ЗуП и обеспечивает их взаимодействие с другими подсистемами внутреннего контура ИС.

Архитектура ИС Отчетность схематично представлена на рис. 1.

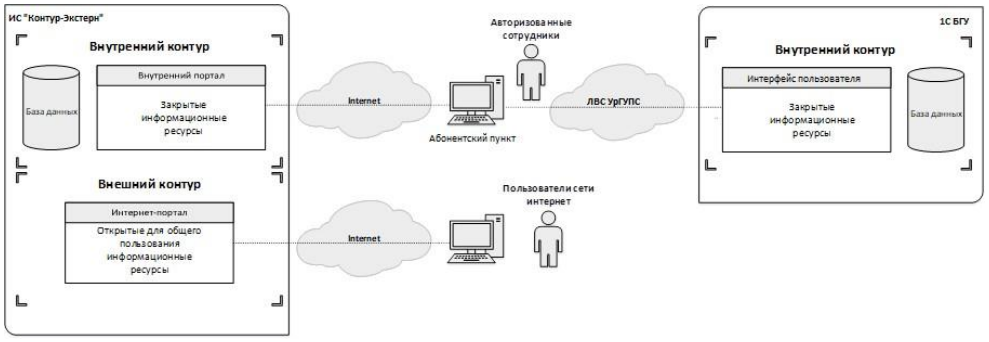

Рисунок 1 – Архитектура ИС Отчетность

В ФГБОУ ВО «Уральский государственный университет путей сообщения» расположены:

1) сегмент информационной системы – абонентский пункт (далее по тексту – АП) ИС «Контур-Экстерн». АП представляет собой удаленный объект информатизации ИС «Контур-Экстерн», подключаемый к сети Интернет с помощью коммуникационного оборудования и предназначенный для взаимодействия с информационными ресурсами во внутреннем (конфиденциальном) контуре ИС «Контур-Экстерн».

2) сегмент информационной системы – абонентский пункт (далее по тексту – АП) ИС 1С ЗУП. АП представляет собой удаленный объект информатизации ИС 1С ЗУП подключаемый к локальной вычислительной сети предприятия с помощью коммуникационного оборудования и предназначенный для взаимодействия с информационными ресурсами во внутреннем (конфиденциальном) контуре ИС 1С ЗУП. [14]

Расположение ИС

Челябинский институт путей сообщения является филиалом ФГБОУ ВО «Уральский государственный университет путей сообщения». Основные технические средства обеспечения защиты КИ расположены в главном вузе: ФГБОУ ВО «Уральский государственный университет путей сообщения» номер помещения: Б2-48. Адрес: 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова. д. 66

Описание программного обеспечения ИС

Весь комплекс программного обеспечения (далее по тексту – ПО) ИС разделяется на две основные группы:

- системное ПО;
- прикладное ПО.

Системное ПО включает в себя Операционную систему «Windows 10 Корпоративная (64-bit)».

Прикладное ПО состоит из шести элементов: 1) Интернет браузер GoogleChrome 67.0; 2) Интернет браузер Internet Explorer 11; 3) офисный

пакет Microsoft Office профессиональный + 2010; 4) архиватор 7Zip; 5) крипто-провайдер Крипто Про CSP 4.0; 6) клиент удаленного рабочего стола Microsoft Remote Desktop clients.

Информация, обрабатываемая в ИС

В ИС обрабатывается информация ограниченного доступа (далее по тексту – ИОД), в том числе иные категории персональных данных (далее по тексту – ПДн) сотрудников, учащихся Челябинского института путей сообщения филиал ФГБОУ ВО «Уральский государственный университет путей сообщения».

Описание возможных категорий ПДн в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в таблице 1.[14]

Таблица 1

№ п/п	Категории ПДн	Описание
1	Специальные категории	Данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн.
2	Биометрические ПДн	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.
3	Общедоступные ПДн	Данные субъектов ПДн, полученные только из общедоступных источников ПДн.
4	Иные категории ПДн	Обрабатываются ПДн, не относящиеся к специальной, биометрической или общедоступной категории ПДн.

1.2 Описание технологического процесса обработки КИ

Схема технологического процесса обработки ИОД в ИС приведена на рис. 2.

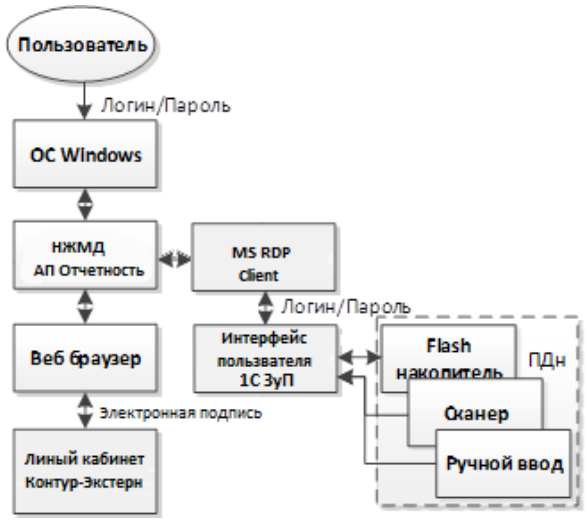

Рисунок 2 – Схема функциональной структуры ИС

В процессе обработки ИОД в ИС участвуют следующие субъекты доступа:

1) Администратор – организует и контролирует работу пользователей.

2) Пользователь – имеет ограниченный доступ к ресурсам ИС, установленный Администратором.

Объектами доступа ИС являются:

– рабочая станция;
– устройства ввода-вывода на съемные носители информации;
– монитор;
– каталоги для файлов с защищаемой ИОД;
– оперативная память;
– операционная система (далее по тексту – ОС);
– физические носители информации;
– электронные документы и таблицы, содержащие ИОД;
– программное обеспечение, предназначенное для обработки ИОД.

Ниже описывается технологический процесс обработки информации с учетом объектов и субъектов доступа.

Обработка ИОД осуществляется в три этапа:

1) Подготовка к обработке ИОД. На данном этапе осуществляется: проверка работоспособности электронной вычислительной машины (далее по тексту – ЭВМ) и вход пользователя в ОС.

2) Обработка ИОД. На данном этапе осуществляется подключение к через MS RDP Client к терминальному серверу интерфейса пользователя 1С ЗуП; выгрузка исходных ИОД в виде xml-файла на локальный компьютер ИС Отчётность; подключение АП ИС «Контур-Экстерн» к внутреннему порталу ИС «Контур-Экстерн»; загрузка xml-файла, содержащего ИОД с помощью прикладного ПО;

3) Сохранение результатов обработки ИОД. На данном этапе осуществляется: сохранение результатов обработки ИОД на жестком диске ЭВМ в своем личном каталоге и на удаленном внутреннем портале ИС «Контур-Экстерн».[15]

Организационно-штатная структура ИС

В ИС предусмотрены следующие функциональные роли:

- эксплуатационный персонал;
- обслуживающий персонал;
- ответственные за защиту информации.

К эксплуатирующему персоналу относятся пользователи ИС Отчетность. Эксплуатирующий персонал обеспечивает выполнение основных процессов деятельности в ИС Отчетность.

К обслуживающему персоналу относится администратор ИС Отчетность. Обслуживающий персонал обеспечивает функционирование информационной системы на протяжении всего ее жизненного цикла.

К ответственным за защиту информации относятся:

- ответственный за организацию обработки персональных данных в ФГБОУ ВО «Уральский государственный университет путей сообщения»;
- ответственный за защиту информации в ИС.

Ответственные за защиту информации обеспечивают информационную безопасность ИС Отчетность и поддерживают в актуальном состоянии нормативно-справочную и организационно-распорядительную документацию. В ФГБОУ ВО УрГУПС должны быть разработаны документы по обеспечению безопасности ИОД при обработке в ИС.

Приказ о создании комиссии по защите информации ограниченного доступа, обрабатываемой в информационных системах создается на основании Пунктов 8 «Требования к защите ПДн» (№1119) и 14.2 «Требования о защите информации (№17)[10],[15].

Также рекомендуется создать перечень информации ограниченного доступа, обрабатываемой в ИС Отчетность.

На основании Статьи 22.1 ФЗ «О персональных данных» (№152-ФЗ) и Пункта 9 «Требования о защите информации» (№17) необходимо создать приказ и инструкций: приказ о назначении ответственных лиц в ИС Отчетность; инструкцию ответственного за организацию обработки персональных данных; инструкцию ответственного за защиту информации в ИС [7],[15].

Основанием для Инструкции администратора является Пункт 16.2 «Требования о защите информации»(№17)[15.]

Ряд статей: статья 18.1, часть 1, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ); статья 19, часть 2, пункт 8 Федерального закона «О персональных данных» (№152-ФЗ); пункт 16.3 «Требований о защите информации ...» (№17);АВЗ.1, АВЗ.2, ЗСВ.9, УПД.15, ОДТ.4, ОДТ.5, ЗСВ.8, ОЦЛ.3, ОПС.3, ЗИС.8, ЗИС.9 «Требований о защите информации ...» (№17); статья 19, часть 2, пункт 7 Федерального закона «О персональных данных» (№152-ФЗ); пункт 18.1 «Требований о защите информации ...»

(№17) являются основополагающими при составлении Инструкции по эксплуатации ИС Отчетность[7],[15].

Одним из важных документов является Инструкция по эксплуатации ИС Отчетность, которая создается на основании статьи 18.1, часть 1, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ); статьи 19, часть 2, пункт 8 Федерального закона «О персональных данных» (№152-ФЗ); пункта 16.3 «Требований о защите информации ...» (№17); АВЗ.1, АВЗ.2, ЗСВ.9, УПД.15, ОДТ.4, ОДТ.5, ЗСВ.8, ОЦЛ.3, ОПС.3, ЗИС.8, ЗИС.9 «Требований о защите информации ...» (№17); статья 19, часть 2, пункт 7 Федерального закона «О персональных данных» (№152-ФЗ); пункта 18.1 «Требований о защите информации ...» (№17)[7],[10],[15].

Пункт 13.б «Требований к защите ПДн ...» (№1119) и пункт 19.2, ЗНИ.1, ЗНИ.2, ЗНИ.8, УПД.15, ЗИС.30 «Требований о защите информации ...» (№17), а также статья 19, часть 2, пункт 5 Федерального закона «О персональных данных» (№152-ФЗ) являются основанием для составления Порядка обращения со съемными машинными носителями информации ограниченного доступа[7],[15].

Инструкция по обращению с криптографическими средствами защиты информации разрабатывается на основании пункта 30, пункта 51, Раздела 2, раздела 3 «Инструкции об организации...» (№152); пункта 13.а «Требований к защите ПДн ...» (№1119); ЗТС.3 «Требований о защите информации ...» (№17)[15],[16].

Рекомендуется для учёта помещений составить Перечень помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним, а также издать Правила доступа в помещения, выделенные для установки средств криптографической защиты информации и хранения ключевых документов к ним.

Положение о разрешительной системе доступа и Матрица субъектов доступа ИС Отчетность составляются на основании статьи 19, часть 2, пункт 8 Федерального закона «О персональных данных» (№152-ФЗ); пункта 16.3,

пункт 18.1, ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.15, УПД.17, РСБ.7, ОЦЛ.6, ЗСВ.1, ЗСВ.2, ЗСВ.6, ЗИС.1, ЗИС.8, ЗИС.9, ЗИС.15, ЗИС.30 «Требований о защите информации ...» (№17); пункта 19 «Инструкции об организации…» (№152) [15].

Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа и регламент реагирования на инциденты информационной безопасности создаются на основе ряда статей: статья 18.1, часть 1, пункт 4 Федерального закона «О персональных данных» (№152-ФЗ); статья 19, часть 2, пункт 6 Федерального закона «О персональных данных» (№152-ФЗ); пункт 17.б «Требований к защите ПДн ...» (№1119); пункт 16.2, пункт 18.1, пункт 18.2, пункт 18.4, УПД.14, УПД.15, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, АНЗ.1, АНЗ.2, АНЗ.3, АНЗ.4, АНЗ.5, ОДТ.3, ОДТ.7, ЗСВ.3, ЗИС.7, ЗИС.8, ЗИС.9, ЗИС.12, ЗИС.13, ЗИС.30, ОПС.2 «Требований о защите информации ...» (№17); пункт 73 «Инструкции об организации…» (№152) [15].

Предписанием для заведения Журнала учета съемных машинных носителей информации ограниченного доступа является Инструкция по порядку обращения с машинными носителями информации ограниченного доступа.

На основании пункта 7 «Инструкции об организации…» (№152) и инструкция по обращению с шифровальными (криптографическими) средствами защиты информации издается Приказ о допуске к работе со средствами криптографической защиты информации [16].

Журнал учета лиц, имеющих доступ к обработке информации ограниченного доступа необходимо создать на основании Положения о разрешительной системе доступа.

Приказ о допуске к работе со средствами криптографической защиты информации является основанием для создания Журнала учета

ознакомления пользователей с правилами работы шифровальных (криптографических) средств.

На основании Пункта 7 «Инструкции об организации…» (№152), а также Инструкции по обращению с шифровальными (криптографическими) средствами защиты информации создается Журнал поэкземплярного учета шифровальных (криптографических) средств защиты информации [16].

Инструкция по обращению с шифровальными (криптографическими) средствами защиты информации является основанием для Заключения о подготовке и допуске к самостоятельное работе со средствами криптографической защиты информации и Журнала учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей от хранилищ, личных печатей от хранилищ.

Приказ о границах контролируемой зоны издается на основании: пункта 13.в «Требований к защите ПДн ...» (№1119); пункта 19 «Инструкции об организации…» (№152); ЗТС.2, ЗИС.3 «Требований о защите информации ...» (№17) и пункта 21 «Инструкции об организации…» (№152) [15],[16].

Так же рекомендательным является Положение об обеспечении безопасности информации ограниченного доступа.

Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации создается на основании регламента реагирования на инциденты информационной безопасности в информационных системах.

На основании пункта 30 «Инструкции об организации…» (№152) создается Приказ о хранилищах.

Обязательным к созданию является также Перечень должностей сотрудников, допущенных к обработке информации ограниченного доступа в ИС Отчетность на основании Пункта 13.в «Требований к защите ПДн ...»

(№1119) и Приказ о проведении испытаний системы защиты информации [10].

1.3. Анализ рисков и уязвимостей системы защиты КИ

К объектам защиты относятся:

- ПДн;
- СКЗИ;
- среда функционирования СКЗИ (далее по тексту – СФ);
- информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИС Отчетность и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые на ИС Отчетность в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые на ИС Отчетность каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы ИС Отчетность, имеющие отношение к криптографической защите ПДн.

Характеристики безопасности ПДн

Возможные характеристики безопасности ПДн:

- конфиденциальность;
- целостность;
- доступность;

- подлинность.

Область применения СКЗИ в информационной системе

СКЗИ на ИС установлены на рабочих местах/рабочем месте, подключенных/подключенного к сети Интернет и используемых для связи с порталом ИС «Контур-Экстерн».

Цели применения СКЗИ в информационной системе

Целью применения СКЗИ на ИС является защита ПДн от раскрытия, модификации при их передаче по каналам связи, имеющим выход за пределы контролируемой зоны (далее по тексту – КЗ).

Объекты, в которых размещены ресурсы информационной системы ИС Отчетность расположен по адресу: 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова. д. 66.

Физические меры защиты объектов, в которых размещены ресурсы информационной системы

Меры технической защиты реализованы следующим образом:

– для хранения СКЗИ используется металлическое хранилище;

– входные двери в помещения оснащены надежными замками;

– обеспечивается постоянное закрытие дверей помещений с СКЗИ на замок и их открытие только для санкционированного прохода;

– помещения с СКЗИ оборудованы соответствующими техническими устройствами, оповещающими о несанкционированном вскрытии данных помещений.

Меры по обеспечению КЗ

Утверждены документы, определяющие границы КЗ. Организован контроль доступа на охраняемую территорию. В пределах КЗ исключено пребывание посторонних лиц и несанкционированное подключение к сетевому оборудованию. Имеется охранная сигнализация.

ИС Отчетность является единой ИС для всех обрабатываемых ПДн.

Информационное взаимодействие ИС с другими ИС отсутствует.

Каналы (линии) связи и меры по их защите

Используемые на АП каналы (линии) связи, включая кабельные системы, и меры по ограничению несанкционированного доступа к защищаемой информации, передаваемой по этим каналам (линиям) связи, с указанием каналов (линий) связи, в которых невозможен несанкционированный доступ к передаваемой по ним защищаемой информации, и реализуемые для обеспечения этого качества меры: локальная вычислительная сеть построена с использованием 8-и жильной витой пары категории 5. Спуски к местам установки розеток выполнены скрыто в пластиковых в гофротрубах, уложенных в штробы.

Носители защищаемой информации

На ИС Отчетность используются следующие носители защищаемой информации:

- несъемные машинные носители (жесткий диск);
- съемные машинные носители (USB-флеш-накопитель, внешний жесткий диск и т.д.);
- бумажные носители защищаемой информации.

Модель нарушителя безопасности

Целью построения Модели нарушителя безопасности является определение типа возможного нарушителя безопасности ПДн обрабатываемых на ИС Отчетность (далее по тексту – нарушитель).

В качестве нарушителя безопасности информации могут выступать физические лица или организации, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности информации.

Модель нарушителя представляет собой абстрактное описание нарушителей как источников угроз безопасности ПДн, а также предположения об их возможностях, которые могут использоваться для разработки и проведения атак, и ограничениях на эти возможности.

Описание нарушителей безопасности

К потенциальным нарушителям безопасности, ПДн обрабатываемых на ИС Отчетность могут быть отнесены следующие группы нарушителей:

а) разведывательные службы государств;

б) криминальные структуры;

в) конкуренты;

г) работники, зарегистрированные пользователи ИС Отчетность (эксплуатационный персонал);

д) работники, не являющиеся зарегистрированными пользователями ИС Отчетность;

е) уволенные работники;

ж) работники сторонних организаций, которым предоставляется доступ в КЗ в соответствии с договорными обязательствами;

з) внешние субъекты (физические лица);

и) операторы связи, предоставляющие в аренду каналы связи.

Нарушители, перечисленные в пунктах: а), б) и), не имеют мотивации осуществления деятельности.

Таким образом, в качестве нарушителей информационной безопасности имеет смысл рассматривать исключительно субъектов, перечисленных выше в пунктах в), г), д), е), ж), з).

Потенциальные нарушители, перечисленные в пункте в), е), ж), з), и) могут использовать штатные средства только в том случае, если они расположены за пределами КЗ.

Различают высокий, средний и низкий потенциалы нарушителя:

- высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.
- средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей.

- низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Модель нарушителя строится исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации.

Все физические лица, имеющие доступ к техническим и программным средствам ИС Отчетность, разделяются на следующие категории:

- **категория I** – лица, не имеющие права доступа в КЗ;
- **категория II** – лица, имеющие право постоянного или разового доступа в КЗ.

Потенциальные нарушители (источники атаки) подразделяются на:

- **внешних нарушителей**, осуществляющих атаки из-за пределов КЗ;
- **внутренних нарушителей**, осуществляющих атаки, находясь в пределах КЗ.

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа программного обеспечения прикладного программного обеспечения и средств защиты информации, не является целесообразным для нарушителей с учетом высокой стоимости разработки способов и средств

атаки и незначительными негативными последствиям от таких атак для субъектов ПДн;

- являются, в силу специфики информации, одиночками, самостоятельно осуществляющими освоение способов, подготовку и проведение атак.

Описание внешних нарушителей безопасности

Внешними нарушителями могут быть лица как категории I, так и категории II. К данному виду нарушителей относятся:

- оператор связи, предоставляющий в аренду канал связи;
- внешний нарушитель, не имеющий прав доступа в КЗ;
- работник сторонней организации, не являющийся зарегистрированным пользователем ИС Отчетность, но имеющий право доступа в КЗ в соответствии с договорными обязательствами;
- уволенные работники.

Описание внутренних нарушителей безопасности

Внутренними нарушителями могут быть только лица категории II. К данному виду нарушителей относятся:

- работник, не являющийся зарегистрированным пользователем ИС Отчетность;
- работник, зарегистрированный пользователь ИС Отчетность (эксплуатационный персонал).

Возможности нарушителей и вероятность их проявления

СКЗИ класса КС1 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются следующие возможности:

1) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ(внешние субъекты, работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право

доступа в КЗ в соответствии с договорными обязательствами; конкуренты, уволенные работники) – **данная возможность имеется;**

2) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ(конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **данная возможность имеется;**

3) проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (КЗ) (внешние субъекты (физические лица); работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; конкуренты; уволенные работники) – **данная возможность имеется**;

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие СФ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ(конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **данная возможность у нарушителей отсутствует, т.к. не представляется возможным получить доступ к СКЗИ на этапах разработки (модернизации), производства,**

хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы);

5) проведение атак на этапе эксплуатации СКЗИ на: персональные данные; ключевую, аутентифицирующую и парольную информацию СКЗИ; программные компоненты СКЗИ; аппаратные компоненты СКЗИ; программные компоненты СФ, включая программное обеспечение BIOS; аппаратные компоненты СФ; данные, передаваемые по каналам связи; иные объекты, которые установлены при формировании совокупности предложений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО) (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **данная возможность имеется;**

6) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ.

При этом может быть получена следующая информация: общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ; содержание конструкторской документации на СКЗИ; содержание находящейся в

свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ; общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ; сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи); все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами; сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ; сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ; сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ(внешние субъекты (физические лица); работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; конкуренты; уволенные работники) – **данная возможность имеется;**

7) применение находящихся в свободном доступе или используемых за пределами КЗ АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; специально разработанных АС и ПО (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи; внешние субъекты (физические лица); уволенные работники) – **данная возможность имеется**;

8) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: каналов связи, не

защищенных от несанкционированного доступа к информации организационными и техническими мерами; каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **данная возможность имеется;**

9) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети (нарушители, описанные в пункте 8) – **данная возможность имеется;**

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства) (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) - **Данная возможность у нарушителей отсутствует, т.к. эксплуатация СКЗИ осуществляется только в пределах КЗ;**

СКЗИ класса КС2 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности, указанные выше, а также не менее одной из следующих дополнительных возможностей:

1) проведение атаки при нахождении в пределах контролируемой зоны (внешние субъекты (физические лица); работник сторонней организации, не являющийся зарегистрированным пользователем ИС Отчетность, но имеющий право доступа в КЗ в соответствии с договорными обязательствами) – **данная возможность имеется**;

2) проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ. помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **Данная возможность у нарушителей отсутствует, т.к. доступ в КЗ ограничен в соответствии с внутренними документами и пропускным режимом;**

3) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ (возможные нарушители представлены в пункте 2) - **Данная возможность у нарушителей отсутствует, т.к. получение указанных сведений не представляется возможным;**

4) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ - **Данная возможность у нарушителей отсутствует, т.к. получение указанных сведений не представляется возможным;**

5) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий (внешние субъекты (физические лица); работник, не являющийся зарегистрированным пользователем ИС Отчетность) – **Данная возможность у нарушителей отсутствует, т.к. отсутствует доступ к штатным средствам.**

СКЗИ класса КС3 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности, указанные выше, а также не менее одной из следующих дополнительных возможностей:

1) физический доступ к СВТ, на которых реализованы СКЗИ и СФ (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи) – **Данная возможность у нарушителей отсутствует, т.к. доступ в КЗ ограничен в соответствии с внутренними документами и пропускным режимом;**

2) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий **(в**нешние субъекты (физические лица); работник сторонней организации, не являющийся зарегистрированным пользователем ИС Отчетность, но имеющий право доступа в КЗ в соответствии с договорными обязательствами) – **Данная возможность у нарушителей отсутствует, т.к. доступ в КЗ ограничен в соответствии с внутренними документами и пропускным режимом.**

СКЗИ класса КВ применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются

возможности, указанные выше, а также не менее одной из следующих дополнительных возможностей:

1) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи – **Данная возможность у нарушителей отсутствует;**

2) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий (внешние субъекты (физические лица);работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; конкуренты; уволенные работники) – **Данная возможность у нарушителей отсутствует, т.к. эксплуатация СКЗИ осуществляется только в пределах КЗ**;

3) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы связи)

– **Данная возможность у нарушителей отсутствует, т.к. они не обладают исходными текстами входящего в состав СФ прикладного ПО.**

СКЗИ класса КА применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности, указанные выше, а также не менее одной из следующих дополнительных возможностей:

1) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО (конкуренты; работники сторонней организации, не являющиеся зарегистрированными пользователями ИС Отчетность, но имеющие право доступа в КЗ в соответствии с договорными обязательствами; операторы связи, предоставляющие в аренду каналы) – **Данная возможность у нарушителей отсутствует;**

2) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ (нарушители описаны в пункте 1) – **Данная возможность у нарушителей отсутствует, т.к. они не располагают сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;**

3) возможность располагать всеми аппаратными компонентами СКЗИ и СФ(нарушители описаны в пункте 1) – **Данная возможность у нарушителей отсутствует, т.к. они не располагают всеми аппаратными компонентами СКЗИ и СФ [17].**

Описание каналов атак

Основными каналами атак являются:

- каналы связи (как внутри, так и вне КЗ), не защищенные от несанкционированного доступа к ПДн организационно-техническими мерами;

- средства обработки информации;
- машинные носители информации;
- носители информации, выведенные из употребления.

Возможными каналами атак, в частности, могут быть:

- визуальный канал, который может позволить получить ПДн путем просматривания документированной и отображаемой на технических средствах информации;
- физический доступ к документации и в помещения, в которых расположены ресурсы ИС Отчетность.

Обобщенные возможности источников атак

На основании исходных данных об ИС Отчетность, объектах защиты и источниках атак составлена таблица 2.

Таблица 2

№ п/п	Обобщенные возможности источников атак	Да/нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами КЗ.	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования.	Нет
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования.	Нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ).	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных	Нет

	возможностей прикладного программного обеспечения).	
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	Нет

Реализация угроз безопасности ПДн, обрабатываемых в ИС Отчетность определяется возможностями источников атак.

Возможности, актуальность и обоснование актуальности проведения атак описаны ниже.

Проведение атаки при нахождении в пределах КЗ не актуально, так как

– проводятся работы по подбору персонала;

– доступ в КЗ, где располагаются СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;

– - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и работники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии работников, допущенных к самостоятельной работе с СКЗИ;

– работники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;

– пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;

– помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

— утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

— утвержден перечень лиц, имеющих право доступа в помещения где располагаются СКЗИ;

— осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

— осуществляется регистрация и учет действий пользователей с ПДн;

— осуществляется контроль целостности средств защиты;

— на АРМ, на котором установлены СКЗИ: используются сертифицированные средства антивирусной защиты.

Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ не актуально, так как:

— проводятся работы по подбору персонала;

— доступ в КЗ, где располагаются СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;

— документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе;

— помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

— утвержден перечень лиц, имеющих право доступа в помещения.

Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной

системы; сведений о мерах по обеспечению КЗ объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ не актуально так как:

– проводятся работы по подбору персонала;

– доступ в КЗ и помещения, где располагаются ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом;

– сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу работников;

– работники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.

Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий не актуально, так как:

– проводятся работы по подбору персонала;

– помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

– работники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации;

– осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

– осуществляется регистрация и учет действий пользователей;

– в ИСПДн используются: сертифицированные средства антивирусной защиты.

Физический доступ к СВТ, на которых реализованы СКЗИ и СФ не актуально, так как:

— проводятся работы по подбору персонала;

— доступ в КЗ и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

— помещения в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода.

Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий не актуально, так как:

— проводятся работы по подбору персонала;

— доступ в КЗ и помещения, где располагаются СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

— помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

— представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и работники, не являющиеся пользователями СКЗИ находятся в этих помещениях только в присутствии работников, допущенных к самостоятельной работе с СКЗИ.

Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО не актуально, так как:

— не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

— высокая стоимость и сложность подготовки реализации возможности;

— проводятся работы по подбору персонала;

— доступ в контролируемую зону и помещения, где располагаются СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

— помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

— представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и работники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии работников, допущенных к самостоятельной работе с СКЗИ;

— осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

— осуществляется регистрация и учет действий пользователей;

— на АРМ, на котором установлены СКЗИ используются: используются сертифицированные средства антивирусной защиты.

Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий не актуально так как:

– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

– высокая стоимость и сложность подготовки реализации возможности.

Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственного использующего вызовы программных функций СКЗИ не актуально так как:

— не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

— высокая стоимость и сложность подготовки реализации возможности.

Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО не актуально, так как:

— не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

— высокая стоимость и сложность подготовки реализации возможности;

— проводятся работы по подбору персонала;

— доступ в КЗ и помещения, где располагаются СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

— помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

— представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и работники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии работников, допущенных к самостоятельной работе с СКЗИ;

— осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

— осуществляется регистрация и учет действий пользователей;

— на АРМ, на котором установлены СКЗИ:

используются сертифицированные средства антивирусной защиты.

Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ не актуально, так как не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

Возможность воздействовать на любые компоненты СКЗИ и СФ не актуально не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

Определение уровня криптографической защиты информации

На основании вышеизложенного, а также в соответствии с документом «Состав и содержание 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», утв. приказом ФСБ России от 10 июля 2014г. №378 при построении системы

защиты персональных данных для нейтрализации атак необходимо применять СКЗИ класса КС2 или СКЗИ более высокого класса [17].

Выводы по первой главе

В данной главе описана функциональная структура ИС.

В составе ИС выделяют следующие структурные компоненты – объекты информатизации: ИС «Контур-Экстерн»(СКБ –Контур), сегменты ИС «Контур-Экстерн», ИС 1С ЗуП, сегмент ИС 1С.

Весь комплекс программного обеспечения ИС разделяется на две основные группы: системное ПО и прикладное ПО.

В ИС обрабатывается информация ограниченного доступа, в том числе иные категории персональных данных сотрудников, учащихся Челябинского института путей сообщения филиал ФГБОУ ВО «Уральский государственный университет путей сообщения».

В ИС предусмотрены такие функциональные роли как эксплуатационный персонал; обслуживающий персонал; ответственные за защиту информации.

Ответственные за защиту информации обеспечивают информационную безопасность ИС и поддерживают в актуальном состоянии нормативно-справочную и организационно-распорядительную документацию.

На основании проведенного анализа рисков и уязвимостей данной системы защиты КИ 378 при построении системы защиты персональных данных для нейтрализации атак необходимо применять СКЗИ класса КС2 или СКЗИ более высокого класса.

ГЛАВА 2. НОРМАТИВНО-ПРАВОВЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1 Современные нормативно-правовые требования к защите КИ

Законодательством Российской Федерации за надлежащую защиту персональных данных ответственность возлагается на организации, в которых персональные данные обрабатываются. Органом, осуществляющим контроль за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Роскомнадзор проводит плановые (целевые, комплексные) проверки, а также проверки по жалобам и обращениям физических и юридических лиц. Проверки систем защиты персональных данных могут также осуществляться ФСТЭК России или ФСБ России при проведении контроля систем защиты конфиденциальных данных или использования средств криптозащиты. При обнаружении неправомерных действий с персональными данными их обработка должна быть прекращена до устранения выявленных нарушений.

Нарушение законодательства о персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (статья 24) влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, налагаемую в судебном порядке [25]

В целях защиты прав граждан на неприкосновенность частной жизни, личной и семейной тайны в последние годы принят ряд законодательных актов. В настоящее время законодательно-нормативная база по персональным данным включает:

– Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (14 глава, с изменениями и дополнениями);

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

– Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

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

– Постановление Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства РоссийскойФедерации от 15.08.2006 №504 «О лицензировании деятельности по техническо защите конфиденциальной информации»;

– Постановление Правительства Российской Федерации от 16.03.2009 №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

– Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

– Приказ Россвязькомнадзора от 17.07.2008 №08 «Об утверждении образца формы уведомления об обработке персональных данных»;

– Приказ Россвязькомнадзора от 18.02.2009 №42 «О внесении изменений в Приказ Россвязькомнадзора от 17 июля 2008 г. №8 «Об утверждении образца формы уведомления об обработке персональных данных». Обеспечение безопасности персональных данных должно осуществляться в соответствии с методическими документами ФСТЭК России (документыДСП):

– «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года;

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;

– «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года.

– Использование криптосредств для обеспечения безопасности персональных данных должно осуществляться в соответствии с:

– Приказом ФСБ России от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»;

– Постановлением Правительства Российской Федерации от 29.12.2007 №957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

– Методическими рекомендациями по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в

информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 №149/54-144).

Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 №149/6/6-622).

На основании указанных выше документов всеми организациями и физическими лицами на территории Российской Федерации должен обеспечиваться требуемый уровень безопасности персональных данных (в действующих информационных системах). Лица, виновные в нарушении требований, несут предусмотренную законодательством Российской Федерации ответственность [50].

Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

В отношении действующих информационных систем, обрабатывающих персональные данные, операторы обязаны провести их классификацию с оформлением соответствующего акта, комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами в виде системы защиты персональных данных, провести оценку соответствия информационной системы персональных данных требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

Постановление Правительства Российской Федерации от 17.11.2007 №781 возлагает обязанность классификации информационных систем персональных данных и задачу обеспечения их безопасности на оператора персональных данных, а разработку методов и способов защиты

персональных данных в информационных системах - на ФСТЭК России и ФСБ России.

Классификация информационных систем персональных данных осуществляется оператором в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» в зависимости от категории обрабатываемых данных и их количества.

Установлены следующие категории персональных данных (ПД):

– Категория I - ПД, касающиеся расовой, национальной принадлежности политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

– Категория II - ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

– Категория III - персональные данные, позволяющие идентифицировать субъекта ПД;

– Категория IV - обезличенные и (или) общедоступные персональные данные.

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

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

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

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

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

– класс 4 (К4) - информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных. Класс типовой информационной системы определяется оператором в соответствии с таблицей, приведенной в Приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20.

Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных по результатам анализа

регламентируется и осуществляется по решению оператора персональных данных.

Операторы обязаны при обработке персональных данных принимать требуемые организационные и технические меры, в том числе при необходимости использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Система защиты персональных данных должна строиться только на основе сертифицированных ФСТЭК России и ФСБ России средствах защиты (технических, программных, программно-аппаратных и криптографических). Без наличия соответствующих лицензий проведение мероприятий по защите персональных данных возможно только для информационных систем класса К3, а также для информационных систем класса К4.

Для проведения собственными силами мероприятий по обеспечению безопасности персональных данных для специальных информационных систем, систем 1 и 2 класса и распределенных (например, подключенных к Интернет) систем 3 класса операторы обязаны в установленном порядке получить лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Для применения криптографических средств защиты персональных данных (в том числе для изготовления ключей или сертификатов), в зависимости от планируемых действий, потребуются различные лицензии ФСБ России, регламентирующие работы в области криптографической защиты информации.

Исходя из требований законодательства образовательным учреждениям необходимо:

1. Определить (или уточнить) состав и категории обрабатываемых персональных данных;

Осуществить (или уточнить) классификацию действующих информационных систем, обрабатывающих персональные данные;

3. Провести необходимые организационные и технические мероприятия для обеспечения защиты: персональных данных, обрабатываемых без использования средств автоматизации; информационных систем, обрабатывающих персональные данные.

4. Декларировать соответствие или провести аттестационные (сертификационные) испытания информационных систем, обрабатывающих персональные данные.

Мероприятия по обеспечению безопасности персональных данных осуществляются на основе законодательства Российской Федерации, нормативных и методических документов.

В части предварительных организационных мероприятий по защите персональных данных всем подведомственным Министерству науки и образования РФ учреждениям и организациям следует:

– определить перечень, цели и порядок обработки персональных данных;

– назначить ответственных за работу с персональными данными;

– подготовить должностные инструкции сотрудников, обрабатывающих персональные данные;

– обеспечить размещение и охрану средств хранения и обработки персональных данных.

Для информационных систем классов К1 и К2 дополнительно потребуется принять предусмотренные методическими документами ФСТЭК России и ФСБ России меры по защите информации от утечки по техническим каналам.

Аттестационные (сертификационные) испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России. При этом под аттестацией понимают комплекс мер, позволяющих привести информационную систему в соответствие с требованиями по безопасности информации к заявленному классу, изложенными в нормативно-методических документах ФСТЭК России.

Аттестационные (сертификационные) испытания содержат в себе анализ уже имеющихся на объекте информационных систем персональных данных, а также вновь принятых решений по обеспечению безопасности информации и включают проверку:

– организационно-режимных мероприятий по обеспечению защиты информации;

– защищенности информации от утечек по техническим каналам (ПЭМИН); защищенности информации от несанкционированного доступа.

По результатам аттестационных испытаний принимается решение о выдаче «Аттестата соответствия» информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

Декларирование соответствия - это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России.

Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

В случае проведения декларирования на основе собственных доказательств оператор самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3.

Независимо от используемой формы подтверждения соответствия оператор может также предоставить протоколы испытаний, проведенных в исследовательской лаборатории.

Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны имеют одинаковую юридическую силу. Также они имеют действие, аналогичное действию сертификата (аттестата) соответствия, и также действительны на территории всей страны и стран, признающих разрешительные документы системы ГОСТ Р в течение всего срока действия.

Декларация о соответствии оформляется на русском языке и должна содержать:

– наименование и местонахождение заказчика;

– информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект, класс ИС ПД;

– наименование документов, на соответствие требованиям которых подтверждается ИС ПД;

– указание на схему декларирования соответствия;

– заявление заказчика о принятии им мер по обеспечению соответствия продукции необходимым требованиям;

– сведения о документах, послуживших основанием для подтверждения соответствия продукции требованиям;

– срок действия декларации о соответствии.

2.2 Требования локальных актов ЧИПС УрГУПС к системе защиты КИ

В целях выполнения требований ФЗ – 152 «О персональных данных» по приказу ректора утверждено положение ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете».

При осуществлении своей деятельности университет обеспечивает защиту ПДн субъектов ПДн, содержащихся в учетных формах, личных делах, базах данных, ИСПДн и других документах и системах, от неправомерного использования или утраты.

Настоящее положение разработано в соответствии с нормативно-правовыми актами РФ в области ПДн, которыми является:

– Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).

– Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ.

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

– Указ Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

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

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

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

– Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

– Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Приказом ректора университета (ректор университета) определяет перечень должностных лиц, осуществляющих обработку ПДн, либо имеющих доступ к ним в соответствии с требованиями Федерального законодательства, в том числе локальных нормативно-правовых актов Университета, а также ответственность в соответствии с действующих законодательством за нарушение режима защиты этих ПДн.

Обработка ПДн субъектов ПДн осуществляется исключительно в целях обеспечения соблюдения законных интересов сторон, возникающих в процессе осуществления университетом своей уставной деятельности.

Требования настоящего Положения доводятся до сведения работников путем подписания трудового договора и до сведения обучающихся путей подписания договора об обучении.

Состав и субъекты персональных данных

Настоящим положением определяется порядок обработки ПДн следующих категорий субъектов ПДн (далее - субъекты ПДн):

- работники университета;
- поступающие в университет;
- обучающиеся в университете;
- близкие родственники выше указанных лиц;
- лица, ранее состоявшие в трудовых и/или образовательных отношениях с университетом;
- лица, командированные в университет;
- лица, состоящие (состоявшие) в договорных отношениях с университетом;
- лица, проживающие в общежитиях университета, но не являющиеся его работниками и обучающимися;
- иностранные граждане;
- законные представители перечисленных лиц.

На протяжении всех взаимоотношений между субъектом ПДн и Университетом (трудовая деятельность и/или обучение) в личных делах и учетных карточках хранятся следующие документы, содержащие ПДн:

- письменное заявление с просьбой о приеме на работу или на обучение;

– собственноручно (законным представителем) заполненная и подписанная анкета установленной формы с приложением фотографии;

– документы о прохождении конкурса/выборов на замещение вакантной должности (если назначение на должность происходит по результатам конкурса/выборов);

– копия паспорта;

– трудовая книжка;

– копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

– копии решений о награждении государственными наградами, присвоении почетных званий;

– копия акта уполномоченного органа о назначении на должность;

– экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт;

– копии приказов о перемещении по должности или смене места работы внутри Университета, о временном замещении иной должности;

– копии документов воинского учета (для военнообязанных и лиц. подлежащих призыву на военную службу);

– копия акта уполномоченного органа об освобождении от должности, о прекращении служебного контракта или его приостановлении;

– аттестационный лист, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

– копии документов о включении в кадровый резерв, а также об исключении его из кадрового резерва;

– копии решений о поощрении, а также о наложении дисциплинарного взыскания до его снятия или отмены;

– копии документов о начале служебной проверки, ее результатах, об отстранении от занимаемой должности;

– документы, связанные с оформлением допуска к сведениям, составляющим государственную тайну, если исполнение обязанностей по замещаемой должности предполагает использование таких сведений;

– копия страхового свидетельства обязательного пенсионного страхования;

– копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

– копия страхового медицинского полиса обязательного медицинского страхования граждан;

– медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу или ее выполнению;

– справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;

– другие необходимые для выполнения обязанностей Университета документы [18].

Сбор, обработка и хранение персональных данных

Все ПДн субъекта ПДн принимаются Университетом от него самого либо образуются в ходе трудовой деятельности на основании полученных ПДн. Если ПДн субъекта ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

При определении объема и содержания обрабатываемых ПДн Университет руководствуется нормативно-правовыми актами РФ, регулирующих процесс получения, обработки и хранения ПДн.

Субъекты ПДн должны предоставлять Университету достоверные сведения о себе. Университет имеет право проверить достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у него документами. При изменении своих ПДн субъекты ПДн обязаны уведомить об этом соответствующего специалиста Университета в срок, не превышающий 14 календарных дней с момента изменения ПДн [18].

Предоставление субъектом ПДн подложных документов влечет ответственность, предусмотренную действующим законодательством.

При запросе ПДн (поступлении на работу, учебу и в других случаях) субъект ПДн должен быть предупрежден о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и юридических последствиях отказа дать письменное согласие на их получение. Предупреждает субъекта об этом подразделение, на которое возложено получение ПДн.

Обработка ПДн в Университете осуществляется на основе следующих принципов:

– законность целей и способов обработки ПДн и добросовестности;

– соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям лиц, осуществляющих обработку ПДн;

– соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям их обработки;

– обеспечение точности ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн, принятие мер по удалению или уточнению неполных или неточных данных;

– недопустимость объединения созданных несовместимых между собой по целям баз данных информационных систем ПДн

Хранение ПДн должно осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого является субъект ПДн.

Документы, содержащие ПДн, хранятся в личных делах, а также в других делах и в информационных системах ПДн (ИСПДн) [18].

Университет не вправе требовать от субъекта ПДн предоставления информации о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, о частной и интимной жизни, его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

Специалистам Университета, выполняющие свои функциональные обязанности, связанные с обработкой ПДн, запрещается принимать на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Лица, допущенные к обработке ПДн, подписывают Обязательство о неразглашении ПДн субъектов ПДн. Бланк обязательства представлен в приложении В.

Согласие субъекта персональных данных на обработку своих персональных данных

Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн в случаях, предусмотренных действующим законодательством.

Согласие на обработку ПДн субъекта ПДн предоставляется в письменной форме. Содержание согласия разрабатывается в соответствии с федеральным законом.

В Университете устанавливается письменная форма согласия своя для каждой категории субъектов ПДн и для каждой цели. 6.5 ПДн могут быть получены от лица, не являющегося субъектом ПДн, при условии предоставления Университету подтверждения наличия оснований и полномочий, установленных действующим законодательством.

Передача персональных данных субъекта персональных данных

Университет имеет право передавать персональные данные в следующие государственные и негосударственные структуры: налоговые органы; правоохранительные органы; органы лицензирования и сертификации; органы прокуратуры и ФСБ; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения государственных и муниципальных органов управления; банковские организации, имеющие договорные отношения с Университетом.

Университет обязан предупредить лиц, получающих персональные субъектов ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения

того, что это правило соблюдено. Лица, получающие ПДн субъекта ПДн, обязаны соблюдать режим конфиденциальности.

Университет разрешает доступ к ПДн субъектов ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъекта ПДн, которые необходимы для выполнения конкретных функций.

Университет не вправе запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом ПДн трудовой функции или учебной деятельности.

Уничтожение персональных данных

Университет прекращает обработку ПДн и уничтожает собранные ПДн, если иное не установлено законодательством Российской Федерации, в следующих случаях и в сроки, установленные законодательством Российской Федерации:

– по достижении целей обработки или при утрате необходимости в их достижении, а также по окончанию сроков обработки ПДн;

– по требованию субъекта ПДн или Уполномоченного органа по защите прав субъектов ПДн;

– если ПДн являются неполными, устаревшими, недостоверными или не являются необходимыми для заявленной цели обработки;

– при отзыве субъектом ПДн согласия на обработку своих ПДн, если такое согласие требуется в соответствии с законодательством РФ;

– в случае установления факта неправомерной обработки ПДн.

Права и обязанности субъекта персональных данных

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн.

Субъект ПДн вправе требовать от Университета уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с действующим законодательством.

Субъект ПДн имеет право на свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных действующим законодательством.

Университету запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных действующим законодательством.

Субъект ПДн обязан сообщать Университету достоверную информацию о себе и представлять документы, содержащие ПДн, в соответствии с требованиями законодательства Российской Федерации, своевременно сообщать Университету об изменении своих ПДн.

ПДн оценочного характера субъект ПДн имеет право дополнить заявлением, выражающим его собственную точку зрения.

Субъект ПДн вправе требовать извещение Университетом всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Субъект имеет право на обжалование в суде любых неправомерных действий или бездействия работодателя при обработке и защите его ПДн.

Меры по обеспечению выполнения обязанностей, предусмотренных законодательством РФ в области персональных данных.

Университет обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных действующим законодательством РФ в области ПДн и принятыми в соответствии с ним нормативными правовыми актами. Университет самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством РФ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено действующим законодательством РФ.

К таким мерам могут, в частности, относятся:

– назначение Университетом ответственного за организацию обработки ПДн на основании приказа Ректора;

– издание Университетом документов, определяющих политику Университета в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии с действующим законодательством РФ;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных действующему законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Университета в отношении обработки ПДн, локальным актам Университета;

– ознакомление работников Университета, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Университета в отношении

обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

Университет обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

Университет и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено действующим законодательством.

Университет при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Лицо, ответственное за организацию обработки ПДн обязано:

– осуществлять внутренний контроль за соблюдением Университетом и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников Университета положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

В целях обеспечения сохранности и конфиденциальности ПДн субъектов ПД, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только специалистами,

осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

Обработка ПДн, осуществляемая без использования средств автоматизации, осуществляться таким образом, что в отношении каждой категории ПДн определены места хранения ПДн (материальных носителей) и установлены перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Должно быть обеспечено раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Университетом.

Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Университета, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта

ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

– копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

– ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Университета.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн:

– при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными. [18].

Выводы по второй главе

Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по контролю за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

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

Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию

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

Система защиты персональных данных должна строиться только на основе сертифицированных ФСТЭК России и ФСБ России средствах защиты (технических, программных, программно-аппаратных и криптографических).

В целях выполнения требований ФЗ – 152 «О персональных данных» по приказу ректора утверждено положение ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете».

При осуществлении своей деятельности университет обеспечивает защиту ПДн субъектов ПДн, содержащихся в учетных формах, личных делах, базах данных, ИСПДн и других документах и системах, от неправомерного использования или утраты.

Университет при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

ГЛАВА 3. РАЗРАБОТКА РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ ЗАЩИТЫ КИ

3.1 Разработка и апробация обучающего курса по защите КИ

В рамках педагогического исследования по данной проблеме проведен опрос среди сотрудников и студентов Челябинского института путей сообщения, в ходе которого было выявлено количество сотрудников и студентов в процентном соотношении, знакомых с понятием «Конфиденциальная информация».

В опросе участвовали 50студентов и 50 сотрудников. Предлагалось ответить на два вопроса:

- «Что такое конфиденциальная информация?»

-«Перечислите, что является конфиденциальной информацией?».

В результате нами были получены следующие результаты (рис. 3)

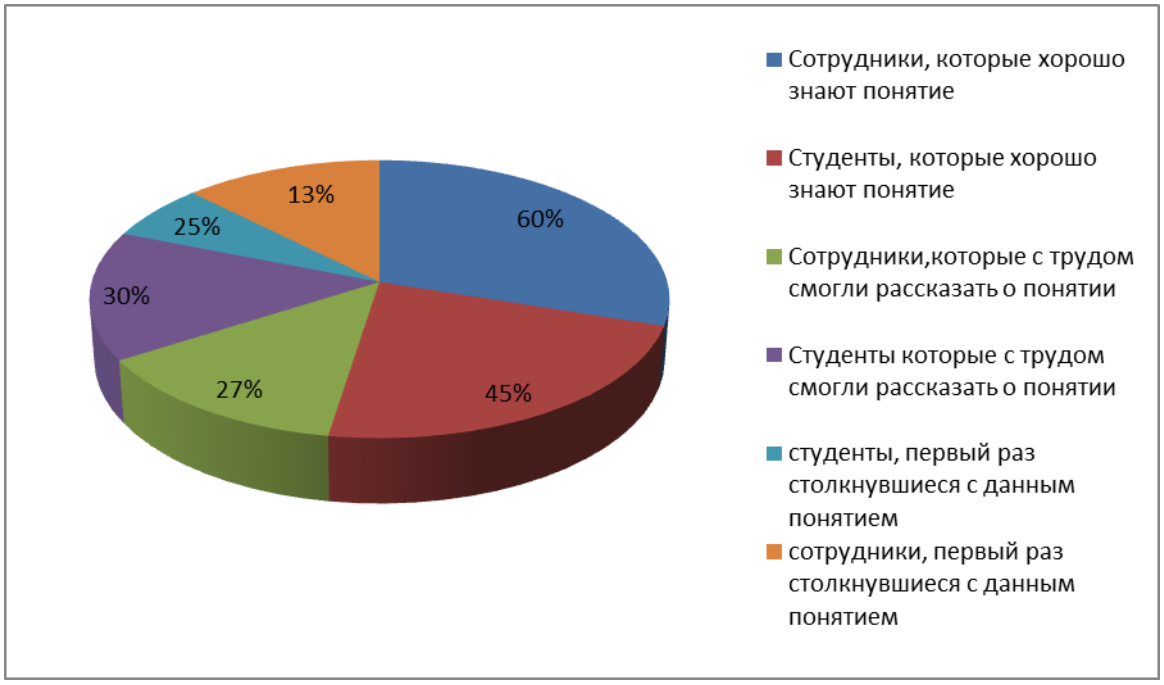

Рисунок 3 – Результаты опроса

Из результатов проведенного опроса видно, что 40% опрошенных сотрудников не достаточно осведомлены с понятием «КИ», тем самым, в

связи с неправильным обращением с КИ могут стать правонарушителями. Это, в свою очередь, снижает степень защиты КИ.

В случае выявления нарушений в области обработки и обеспечения безопасности ПДн, предусмотрена уголовная, административная, дисциплинарная и гражданская ответственность которая может применяться в отношении организации, руководителя организации, подразделения или виновного работника.

К Уголовной ответственности за правонарушения привлекаются по следующим статьям: статья 137 УК РФ Нарушение неприкосновенности частной жизни; статья 140 УК РФ Отказ в предоставлении гражданину информации; статья 272 УК РФ Неправомерный доступ к компьютерной информации и наказываются штрафом, обязательными работами, исправительными работами, принудительными работами, лишением права занимать определенные должности или заниматься определенной деятельностью, арестом, лишением свободы.

Административная ответственность наступает за правонарушения по следующим статьям:

- Статья 5.39 КоАП Отказ в предоставлении информации;
- Статья 13.11 КоАП Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- Статья 13.12 КоАП Нарушение правил защиты информации;
- Статья 13.13 КоАП Незаконная деятельность в области защиты информации;
- Статья 13.14 КоАП Разглашение информации с ограниченным доступом;
- Статья 19.4 КоАП Неповиновение законному распоряжению должностного лица органа, осуществляющего надзор (контроль);

- Статья 19.4.1 КоАП Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора), органа муниципального контроля;
- Статья 19.7 КоАП Непредставление сведений (информации).

Административная ответственность влечет предупреждение, наложение административного штрафа на граждан, должностных лиц, юридических лиц, конфискацию несертифицированных/сертифицированных средств защиты информации, административное приостановление деятельности.

Дисциплинарная ответственность наступает по Статье 90 ТК РФ Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника и Статье 192 ТК РФ.

За совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.

Гражданско-правовая ответственность проявляется по Статье 15 ГК РФ Возмещение убытков и Статье 151 ГКРФ Компенсация морального вреда.

С 1 июля 2017 года вступили в силу поправки в статью 13.11 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ), которые вносят существенные изменения в положения, устанавливающие ответственность за нарушение законодательства в области персональных данных. Данные поправки значительно увеличивают штрафы для операторов персональных данных. Для юридических лиц максимальный штраф составляет 75000 рублей.

В целях повышения эффективности защиты КИ, несмотря на принятые меры её защиты: ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете», в рамках политики защиты КИ, было принято решение о создании обучающего курса «Управление информационной безопасностью в ЧИПС УрГУПС на платформе «BlackBoard».

Прохождение курса будет способствовать формированию понятийного аппарата у сотрудников и студентов, повысит уровень осведомленности в данной теме.

Цель создания обучающего курса – повышение эффективности защиты КИ, путём обучения сотрудников и студентов работе с КИ.

В рамках подготовки курса был подобран материал для проведения лекционных занятий. Подбор материала осуществляли исходя из Положения «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете», чтобы сотрудники и студенты видели точную регламентирующую документацию, на основании которой проводится политика защиты конфиденциальной информации в Университете и его филиалах соответственно. При этом понимали и осознавали те соглашения которые подписываются при трудоустройстве на работу (сотрудники) и поступлении в подразделения университета (обучающиеся).

Так же был разработан Контрольный тест для контроля знаний, проходивших обучение в курсе. Задания для теста создавали разного типа таким образом, чтобы максимально охватить различные аспекты Положения и тем самым, наиболее точно проверить уровень владения информацией у проходивших данное тестирование. Успешное прохождение теста, набрав достаточное количество баллов, гарантирует хороший уровень осведомленности сотрудника и обучающегося, что снижает риск нарушения требований защиты КИ.

Проведя мероприятия по подбору и созданию методических материалов для наполнения курса, совместно с администратором электронной образовательной платформы «Black Board learn+»в Челябинском институте путей сообщения, был создан курс на данной платформе. Обеспечение учебного процесса в электронной образовательной платформе Black Board продиктовано руководством Университета и с 17 марта 2020 ведение курсов, учебных модулей, дисциплин посредством данной технологии является обязательным. Инструктором курса является

преподаватель Челябинского института путей сообщения Савина Е.С. Инструктор курса осуществляет его наполнение методическими разработками, осуществляет контроль знаний зачисленных на данный курс.

В раздел «Методические разработки к лекциям» опубликовали лекционный материал. В раздел «Контроль знаний» опубликовали тест для контроля знаний.

Методическое пособие обучающего курса «Управление информационной безопасностью в образовательной организации» на базе электронной обучающей платформы “Black Board learn+” представлено в (Приложении 1).

Созданный обучающий курс для повышения эффективности защиты КИ одобрен заместителем директора, ответственным за информационную безопасность Челябинского института путей сообщения.

График реализации курса описан в таблице 3.

Таблица 3 График реализации курса

№ п/п	**Дата**	**Планируемые мероприятия**	**Отметка о выполнении**
1	15.04.20–20.04.20	Создание Курса в **“Black Board learn+”**	
2	01.05.20-28.05.20	Создание «Методических разработок к лекциям» и «Контроль знаний»	
3	1.06.20-10.06.20	Наполнение курса методическими разработками, заполнение вкладок курса.	
4	Август 2020	Зачисление студентов 1 курса и сотрудников на курс для обучения	
5	Сентябрь – Октябрь 2020	Проведение On-line обучения	

3.2 Экономическое обоснование внедрения обучающего курса «Управление информационной безопасностью в образовательной организации».

На основании нарушений в области обработки и обеспечения безопасности ПДн произведён расчет стоимости возможных затрат Челябинского института путей сообщения в случае нарушения защиты КИ. Данные расчёта даны в Таблице

Таблица 4 Расчет стоимости затрат

Уголовная ответственность		Размер штрафа
Статья 137 УК РФ	Нарушение неприкосновенности частной жизни	150 -300 т.р.
Статья 140 УК РФ	Отказ в предоставлении гражданину информации	до 200 т.р.
Статья 272 УК РФ	Неправомерный доступ к компьютерной информации	до 200 т.р.
Административная ответственность		
Статья 5.39 КоАП	Отказ в предоставлении информации	5-10 т.р.
Статья 13.11 КоАП	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	5-15 т.р. (для граждан), от 30-50 т.р.(для юридических лиц)
Статья 13.12 КоАП	Нарушение правил защиты информации	1000-1500 р(для граждан и должностных лиц). 15000-20000(для юридических лиц)
Статья 13.13 КоАП	Незаконная деятельность в области защиты информации	4000-5000 р(для должностных лиц), 30000-40000 р. (для юридических лиц)

Статья 13.14 КоАП	Разглашение информации с ограниченным доступом	500-1000 р (для граждан), 4000-5000 р (для должностных лиц)
Статья 19.4 КоАП	Неповиновение законному распоряжению должностного лица органа, осуществляющего надзор (контроль)	5000-10000р. (для должностных лиц) 20000-30000 р. (для юридических лиц)
Статья 19.4.1 КоАП	Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора), органа муниципального контроля	500-1000 р. (для граждан) 2000-4000 р. (для должностных лиц) 5000-10000 р.(для юридических лиц)
Статья 19.7 КоАП	Непредставление сведений (информации)	100-300 р. (для граждан) 300-500 р. (для должностных лиц) 3000-5000 р. (для юридических лиц)
Дисциплинарная ответственность		
Статья 90 ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	
Статья 192 ТК РФ	Дисциплинарные взыскания	
Гражданско-правовая ответственность		
Статья 15 ГК РФ	Возмещение убытков	Полное возмещение убытков или частичное (по решению суда)
Статья 151 ГКРФ	Компенсация морального вреда	

Также произведен расчет затрат на реализацию обучающего курса в Таблице 5.

Таблица 5 Расчет затрат на реализацию обучающего курса «Управление информационной безопасностью»

Создание методического обеспечения курса	Работа в системе Black Board, согласно трудовому договору, рассчитывается исходя из премии раз в полгода в размере 30-40% от установленного оклада: 2400 р.
Наполнение курса методическим обеспечением на платформе «Black Board»	
Дальнейшая работа с курсом	
Затрата на электроэнергию, затраченную во время создания курса и проведения обучения	Исходя из того что 1 компьютер затрачивает около 28 Квт в месяц при условии 8 часового рабочего дня, всего доступно порядка 45 компьютеров для проведения обучения, таким образом затраты на электроэнергию составят: 28*45=1260 р.
Затраты на приобретение пользовательского соглашения патент США BlackBoard	Пользовательское соглашение закупается ФГБО ВО УрГУПС и распространяется на все филиалы Университета, в том числе ЧИПС УргУПС на 2 года. Из расчета стоимости пользовательского соглашения: 3 000 000 / 24=125000. Так как существуют 7 филиалов, то затраты составят: 125000/7= 17857.14 р. в месяц.
ИТОГ	21.517 р.

Таким образом, на основании проведенных расчетов экономической стоимости затрат, рекомендуется внедрить данный обучающий курс в политику защиты КИ ЧИПС УрГПУПС для повышения уровня защиты КИ и снижения рисков распространения КИ.

Перед ответственными за обеспечение информационной безопасности встают ряд задач:

– контролировать работу пользователей информационного пространства института на соблюдение правил хранения и обработки КИ;

– регулярно проводить статистику нарушений защиты КИ;

– обеспечить доступ всем сотрудникам и студентам к электронной образовательной платформе Black Board Learn+;

– обеспечить обучение сотрудников и студентов посредством курса «Управление информационной безопасностью» на базе электронной образовательной платформы Black Board learn+.

Выводы по третьей главе

В данной главе приведены результаты педагогического исследования, в виде опроса, в ходе которого выявлен процент сотрудников и студентов не владеющих понятиями о конфиденциальной информации.

На основании вышеизложенных анализов и исследования было принято решение о внедрении обучающего курса «Управление информационной безопасностью в организации» для обучения сотрудников и студентов работе с КИ.

Также приведено экономическое обоснование внедрения курса в имеющуюся систему защиты КИ.

В соответствии с рекомендациями о внедрении курса для администрации Челябинского института озвучен ряд задач, необходимых для оперативного решения.

Заключение

На основании проведенного исследования в соответствии с целью и поставленными задачами сделаны основные выводы.

Информационная система образовательной организации представляет собой сложную структурированную системы, состоящую из множества различных подсистем, и включающую в себя различные категории КИ, а именно ПДн.

Как и во всех информационных системах, основными нарушителями в области защиты КИ выступают сами сотрудники. Пренебрежение правилами обращения с КИ является одной из причин нарушений.

Несмотря на принятые известные меры по организации защиты КИ (введение законодательных норм, обеспечение организационных мер и технических средств защиты КИ, проведение качественной кадровой работы), случаи возникновения нарушений имеют место быть.

Нарушение законодательства о персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (статья 24) влечет за собой административную, уголовную, гражданскую, дисциплинарную и другие виды ответственности предусмотренные законодательством Российской Федерации.

Образовательные организации, в том числе Челябинский институт путей сообщения являются операторами организации.

Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

В отношении действующих информационных систем, обрабатывающих персональные данные, операторы обязаны провести их классификацию с оформлением соответствующего акта, комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами в виде системы защиты персональных данных, провести оценку соответствия информационной системы персональных

данных требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

Постановление Правительства Российской Федерации от 17.11.2007 №781 возлагает обязанность классификации информационных систем персональных данных и задачу обеспечения их безопасности на оператора персональных данных, а разработку методов и способов защиты персональных данных в информационных системах - на ФСТЭК России и ФСБ России.

Основным документом в политике защиты КИ в Челябинском институте путей сообщения, в целях выполнения требований ФЗ – 152 «О персональных данных» по приказу ректора утверждено положение ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете».

При осуществлении своей деятельности университет обеспечивает защиту ПДн субъектов ПДн, содержащихся в учетных формах, личных делах, базах данных, ИСПДн и других документах и системах, от неправомерного использования или утраты.

При составлении договоров на обучение с полным возмещением затрат, а также поступлении на основе бюджета студенты и при трудоустройстве сотрудники подписывают обязательство рад обязательств и соглашений: Соглашение на обработку ПДн работника, студента, родителей, Обязательство о неразглашении ПДн.

Так же в институте введен пропускной контроль для сотрудников и студентов организации.

На основании детального анализа существующей системы защиты КИ Челябинского института путей сообщения, описанного выше, а также на основании результатов педагогического исследования в качестве рекомендации по повышению эффективности защиты КИ в организации, было принято решение о создании обучающего курса «Управление информационной безопасностью в образовательной организации на базе

электронной образовательной платформы Black Board learn+. Данный курс предназначен для повышения уровня осведомленности сотрудников и студентов в сфере защиты КИ. Продукт был одобрен администрацией Института для внедрения и дальнейшего применения.

Обучающий курс оформлен в виде методического пособия, и представляет собой два вида занятий: лекции и контрольное занятие в виде теста. Лекционный материал, а также контрольный тест, разрабатывались в соответствии с положением «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете». Методическое пособие имеет разрешение администрации и рекомендовано к печати в печатном центре Челябинского института путей сообщения количестве 50 экземпляров на 2020-2021 уч.г.

Курс уже размещен на электронной образовательной платформе Black Board Learn +.

Обучающий курс способствует решению ряда задач по повышению эффективности защиты КИ:

1) повысить уровень осведомлённости сотрудников и студентов в области защиты КИ;

2) снизить риски несанкционированного обращения с КИ;

3) обеспечить исполнения нормативно-правовых документов всеми сотрудниками;

4) обучить правовому обращению с КИ;

Более того, внедрение обучающего курса, с точки зрения экономики позволит избежать затрат на возмещение убытков и устранение последствий правонарушения в области защиты КИ.

Данный программный продукт можно применять в других образовательных учреждениях, и на других образовательных платформах, что отражает его уникальность и универсальность одновременно.

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. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_28399/

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. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_34683/

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. Режим доступа - ttp://www.consultant.ru/document/cons_doc_LAW_140174/27f9ddea0cccf9a6b90bb2cb8b545d436f18157b/

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. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_61798/

6. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – http://www.consultant.ru/document/cons_doc_LAW_61801/

7. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) [Электронный ресурс]//Консультант Плюс: справ.правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_61801/.

8. Приказ ФСБ России от 10.07.2017 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2017 N 33620) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_146520/

9. Указ Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера» [Электронный ресурс]//Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_13532/.

10. Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» [Электронный ресурс]//Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_127610/.

11. Постановление Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]// Консультант Плюс: справ. Правовая

система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_127610/.

12. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».[Электронный ресурс]//Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_127610/.

13. Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». [Электронный ресурс]//Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_151882/.

14. Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».[Электронный ресурс]// Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_151882/.

15. Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608). [Электронный ресурс]//Коснульатнт Плюс6 справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_147084/.

16. Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (Зарегистрировано в Минюсте РФ 06.08.2001 N 2848).[Электронный

ресурс]//Консультант Плюс: справ. Правовая система. Режим доступа - http://www.consultant.ru/document/cons_doc_LAW_32924/.

17. Описание информационной системы Система защиты информации в информационной системе предоставления отчетности в Контур Экстерн Федерального государственного бюджетного учреждения высшего образования «Уральский государственный университет путей сообщения» (СиЗИ ИС Отчетность).

18. Положение ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете» ФГБОУ ВО «УрГУПС».

19. Частная модель угроз безопасности персональных данных Система защиты информации в информационной системе предоставления отчетности в Контур Экстерн Федерального государственного бюджетного учреждения высшего образования «Уральский государственный университет путей сообщения» (СиЗИ ИС Отчетность).

20. Аверченков, В.И. Защита информации в организации : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 3-е изд., стер. - М. : Флинта, 2016. - 124 с.

21. 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

22. Алавердов, А. Р. Организация и управление безопасностью в организациях [Текст]: Учебное пособие/ А. Р. Аведов. – М.: Московский государственный университет статистики и информатики, 2018. – 411с.

23. Абаев, Ф.А. Понятие, правовая природа информации [Текст]/ Ф.А. Абаев // Право и государство: теория и практика. 2017. № 3 (111). С. 126- 131.

24. Аленевская, В.В. Ограничение права на информацию в трудовых отношениях [Текст]/ В.В. Аленевская // Вестник Прикамского социального института. Гуманитарное обозрение. 2017. № 1 (8). С. 42-49.

25. Ануфриева, Н.С. Правовые проблемы обработки информации в трудовых отношениях [Текст]/ Н.С. Ануфриева // Актуальные проблемы современной юридической науки: Сборник научных трудов. Сургут: ИЦ СурГУ, 2017. С. 114-119.

26. Астахова, Л.В., Рублёв Е.Л. Проблемы защиты информации в период смены нормативной базы и пути их решения [Текст]/ Л.В. Астахова, Е.Л. Рублёв // Вестник УрФО. Безопасность в информационной сфере. 2017. № 1 (7). С. 32-41.

27. Барышников, А.Б. Безопасность корпоративных центров обработки информации [Текст]/ Барышников А.Б. // Защита информации. Инсайд. 2017. - № 6 (54). С. 40-41.

28. Бегларян, М.Е. Безопасность информации 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. 2017. С. 24-28.

29. Беденкова, А.А. Правовой статус информации работников [Текст]/ А.А.Беденкова, И.С. Хоменко // Вестник науки Сибири. 2017. - № 4 (14). С. 148-151.

30. Бондарь, А.О. Организация работы по обеспечению защиты государственных информационных систем информации [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», 2017.- С. 174-175.

31. 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.

32. 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.

33. Борисова, С. А. Общие требования при обработке информации работника и гарантии их защиты [Текст]/ С. С. Борисова // Трудовое право. 2017. – N 11. – С. 30-36. 26. Бобылева, М.П. Вопросы использования элементов электронного документооборота внутри организации [Текст]/ М.П. Бобылева// Делопроизводство. 2016. – №2. – С. 15.

34. Герасимов А. А. Задача моделирования процессов защиты информации в информационных системах информации / А.А. Герасимов// Интеллектуальные системы – М. : МГТУ им. Н. Э. Баумана. 2016. – С. 588-589.

35. Грушо, А. А. Теоретические основы компьютерной безопасности: учеб. пособие / А.А. Грушо. : Академия Москва. 2016. 272 с.

36. Гугуева, Т. А. Конфиденциальное делопроизводство [Текст] : учеб. пособие / Т.А. Гугуева. – М. : Альфа-М ; ИНФРА-М. 2016. – 192 с.

37. Дворянкин, С. В. Обеспечение информационной безопасности в распределенных системах обработки данных / С.В. Дворянкин. // Безопасность информационных технологий. 2016. №1. С. 92-93.

38. Ищейнов, В. Я. Информацию в законодательных и нормативных документах Российской Федерации и информационных системах[Текст] / В. Я. Ищейнов // Делопроизводство. 2016. – N 3. – С. 87-90.

39. Кузнецова, Т. В. Организация работы с информацией [Текст] / Т. В. Кузнецова // Делопроизводство. 2016. – № 2. – С. 3–8.

40. Лушников, А. М. Защита информации работника: сравнительно-правовой комментарий гл.14 Трудового кодекса РФ [Текст]/ А.М. Лушников // Трудовое право. 2016 – № 9. – С. 93-101.

41. Маркевич, А. С. Организационно-правовая защита информации в служебных и трудовых отношениях [Текст]: Автореф. дис. на соиск. уч. ст. канд. юрид. наук./ А. С. Маркевич. – Воронеж, 2016. – 28 с.

42. Макаров, А.М. Организация защиты информации : лабораторный практикум / Федеральное государственное автономное образовательная организация 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. 2017. - 92 с.

43. Маслеха, М.А. Теоретические основы защиты информации // Законность и правопорядок в современном обществе. 2017. - № 8.–С. 94- 103.

44. 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.

45. Меликов, У.А. Гражданско-правовая защита информации // Вестник УрФО. Безопасность в информационной сфере. 2017. –№ 4 (18).– С. 49-53.

46. Меньшикова, А.В. Некоторые проблемы защиты информации работника, перспективы и пути их решения // Экономика и менеджмент инновационных технологий. 2017. –№ 11 (38).– С. 156-159.

47. Минаев, В. А. Информационные операции и проблема формирования Современной культуры информационной безопасности / В. А. Минаев // Системы высокой доступности. 2017. №3. – С. 38-46.

48. Минбалеев, А.В. Проблемные вопросы понятия и сущности информации // Вестник УрФО. Безопасность в информационной сфере. 2017.–№ 2 (4).– С. 4-9.

49. Мищенко, Е.Ю., Соколов А.Н. Количественные критерии идентификации физического лица при обезличивании информации // Вестник УрФО. Безопасность в информационной сфере. 2017. - № 1 (11). -С. 27-33.

50. Новичкова, Ю. В. Информацию - без права передачи, или Особенности расторжения трудового договора за разглашение

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

51. . 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 образовательная организация высшего образования «Северо-Кавказский федеральный университет», Министерство образования и науки РФ. - Ставрополь : СКФУ, 2017. - 86 с.

52. Петренко, В.И. Защита информации в информационных системах : учебное пособие / В.И. Петренко ; Федеральное государственное автономное образовательная организация высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации. - Ставрополь : СКФУ, 2016. - 201 с.

53. Савинцева, М. Н. Правовая защита персональной информации граждан в России [Текст]/ М. Н. Савинцева // Законодательство и практика масс-медиа. - 2017. - № 9. – С. 23 48.

54. Садовничий, В.А. Научные проблемы национальной безопасности Российской Федерации [Текст]/ В.А. Савдовничий// Информационная безопасность: приоритетные направления гуманитарных научных исследований. – 2015. - №3. – с.264-271.

55. Силакова О. В. Комплексная безопасность образовательной организации как важнейшее условие обеспечения безопасных условий проведения учебно-воспитательного процесса // Молодой ученый. — 2017. — №18.1. — С. 84-88.

56. Федосова, М. А. Защита информации работника [Текст]/ М.А. Федосова // Финансовые и бухгалтерские консультации. - 2017. - N 11. - С. 71-74.

57. Федосеева, Н.Н. Сущность и проблемы электронного документооборота [Текст] / Н.Н. Федосеева // Юрист. - 2016. - №6. - с.61 – 64

58. Хачатурян, Ю. А. Право работника на защиту информации [Текст]/ Ю. А. Хачатурян // Современное право. - 2016. - N 1. - С. 43-51.

59. Чаннов, С. Е. Правовой режим информации на государственной и муниципальной службе [Текст]/ С. Е. Чаннов // Российская юстиция. - 2017. - N 1. - С. 21-23.

Приложение

Челябинский институт путей сообщения – филиал
Федерального государственного бюджетного
Образовательного учреждения высшего образования
«Уральский государственный университет путей сообщения»
Структурное подразделение среднего профессионального образования

Е.С. Савина

Управление информационной безопасностью в образовательной организации

Учебно-методическое пособие

по обучению и тестированию на базе электронной образовательной платформы Blackboard learn + для студентов и сотрудников ЧИПС УрГУПС

Челябинск

2020

Содержание

1. Материал для проведения лекционных занятий.

1.1 Термины и определения

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Биометрические ПДн – ПДн, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн.

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

Доступ к персональным данным – ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми оператором, при условии сохранения конфиденциальности этих сведений.

Информационная система ПДн (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Обработка ПДн – 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 ПДн.

Общедоступные ПДн: ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Специальные категории ПДн – ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Субъект ПДн — физическое лицо, которое прямо или косвенно определено или определяемо с помощью ПДн.

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

1.2. Нормативно-правовые документы в области управления информационной безопасностью

В целях выполнения требований ФЗ – 152 «О персональных данных» по приказу ректора утверждено положение ПЛ1.2.5-2017 «О порядке обработки и защиты КИ работников и лиц, обучающихся в Университете».

При осуществлении своей деятельности университет обеспечивает защиту ПДн субъектов ПДн, содержащихся в учетных формах, личных делах, базах данных, ИСПДн и других документах и системах, от неправомерного использования или утраты.

Настоящее положение разработано в соответствии с нормативно-правовыми актами РФ в области ПДн, которыми является:

– Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).

– Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ.

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

– Указ Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

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

– Постановление Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных

данных при их обработке в информационных системах персональных данных»

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

– Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

– Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Перечень ПДн субъектов, обрабатываемым в Университете, указан в приложении(…..)

Приказом ректора университета (ректор университета) определяет перечень должностных лиц, осуществляющих обработку ПДн, либо имеющих доступ к ним в соответствии с требованиями Федерального законодательства, в том числе локальных нормативно-правовых актов Университета, а также ответственность в соответствии с действующих законодательством за нарушение режима защиты этих ПДн.

Перечень должностей сотрудников университета, имеющих доступ к персональным данным работников Университета и лиц, обучающихся в Университете (субъектов ПДн) приведен в приложении (….).

Обработка ПДн субъектов ПДн осуществляется исключительно в целях обеспечения соблюдения законных интересов сторон, возникающих в процессе осуществления университетом своей уставной деятельности.

Требования настоящего Положения доводятся до сведения работников путем подписания трудового договора и до сведения обучающихся путей подписания договора об обучении.

1.3.Состав и субъекты персональных данных

Настоящим положением определяется порядок обработки ПДн следующих категорий субъектов ПДн (далее - субъекты ПДн):

– работники университета;

– поступающие в университет;

– обучающиеся в университете;

– близкие родственники выше указанных лиц;

– лица, ранее состоявшие в трудовых и/или образовательных отношениях с университетом;

– лица, командированные в университет;

– лица, состоящие (состоявшие) в договорных отношениях с университетом;

– лица, проживающие в общежитиях университета, но не являющиеся его работниками и обучающимися;

– иностранные граждане;

– законные представители перечисленных лиц.

На протяжении всех взаимоотношений между субъектом ПДн и Университетом (трудовая деятельность и/или обучение) в личных делах и учетных карточках хранятся следующие документы, содержащие ПДн:

– письменное заявление с просьбой о приеме на работу или на обучение;

– собственноручно (законным представителем) заполненная и подписанная анкета установленной формы с приложением фотографии;

– документы о прохождении конкурса/выборов на замещение вакантной должности (если назначение на должность происходит по результатам конкурса/выборов);

– копия паспорта;

– трудовая книжка;

– копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

– копии решений о награждении государственными наградами, присвоении почетных званий;

– копия акта уполномоченного органа о назначении на должность;

– экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт;

– копии приказов о перемещении по должности или смене места работы внутри Университета, о временном замещении иной должности;

– копии документов воинского учета (для военнообязанных и лиц. подлежащих призыву на военную службу);

– копия акта уполномоченного органа об освобождении от должности, о прекращении служебного контракта или его приостановлении;

– аттестационный лист, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

– копии документов о включении в кадровый резерв, а также об исключении его из кадрового резерва;

– копии решений о поощрении, а также о наложении дисциплинарного взыскания до его снятия или отмены;

– копии документов о начале служебной проверки, ее результатах, об отстранении от занимаемой должности;

– документы, связанные с оформлением допуска к сведениям, составляющим государственную тайну, если исполнение обязанностей по замещаемой должности предполагает использование таких сведений;

– копия страхового свидетельства обязательного пенсионного страхования;

– копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

– копия страхового медицинского полиса обязательного медицинского страхования граждан;

– медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу или ее выполнению;

– справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;

– другие необходимые для выполнения обязанностей Университета документы.

1.4Сбор, обработка и хранение персональных данных

Все ПДн субъекта ПДн принимаются Университетом от него самого либо образуются в ходе трудовой деятельности на основании полученных ПДн. Если ПДн субъекта ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

При определении объема и содержания обрабатываемых ПДн Университет руководствуется нормативно-правовыми актами РФ, регулирующих процесс получения, обработки и хранения ПДн.

Субъекты ПДн должны предоставлять Университету достоверные сведения о себе. Университет имеет право проверить достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у него документами. При изменении своих ПДн субъекты ПДн обязаны уведомить об этом соответствующего специалиста Университета в срок, не превышающий 14 календарных дней с момента изменения ПДн.

Предоставление субъектом ПДн подложных документов влечет ответственность, предусмотренную действующим законодательством.

При запросе ПДн (поступлении на работу, учебу и в других случаях) субъект ПДн должен быть предупрежден о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и юридических последствиях отказа дать письменное согласие на их получение. Предупреждает субъекта об этом подразделение, на которое возложено получение ПДн.

Обработка ПДн в Университете осуществляется на основе следующих принципов:

– законность целей и способов обработки ПДн и добросовестности;

– соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям лиц, осуществляющих обработку ПДн;

– соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям их обработки;

– обеспечение точности ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн, принятие мер по удалению или уточнению неполных или неточных данных;

– недопустимость объединения созданных несовместимых между собой по целям баз данных информационных систем ПДн

Хранение ПДн должно осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого является субъект ПДн.

Документы, содержащие ПДн, хранятся в личных делах, а также в других делах и в информационных системах ПДн (ИСПДн).

Университет не вправе требовать от субъекта ПДн предоставления информации о его расовой, национальной принадлежности, политических

взглядах, религиозных и философских убеждениях, о частной и интимной жизни, его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

Специалистам Университета, выполняющие свои функциональные обязанности, связанные с обработкой ПДн, запрещается принимать на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Лица, допущенные к обработке ПДн, подписывают Обязательство о неразглашении ПДн субъектов ПДн. Бланк обязательства представлен в приложении В.

1.5. Согласие субъекта персональных данных на обработку своих персональных данных

Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн в случаях, предусмотренных действующим законодательством.

Согласие на обработку ПДн субъекта ПДн предоставляется в письменной форме. Содержание согласия разрабатывается в соответствии с федеральным законом.

В Университете устанавливается письменная форма согласия своя для каждой категории субъектов ПДн и для каждой цели. 6.5 ПДн могут быть получены от лица, не являющегося субъектом ПДн, при условии предоставления Университету подтверждения наличия оснований и полномочий, установленных действующим законодательством.

1.6. Передача персональных данных субъекта персональных данных

Университет имеет право передавать персональные данные в следующие государственные и негосударственные структуры: налоговые органы; правоохранительные органы; органы лицензирования и сертификации; органы прокуратуры и ФСБ; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения государственных и муниципальных органов управления; банковские организации, имеющие договорные отношения с Университетом.

Университет обязан предупредить лиц, получающих персональные субъектов ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъекта ПДн, обязаны соблюдать режим конфиденциальности.

Университет разрешает доступ к ПДн субъектов ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъекта ПДн, которые необходимы для выполнения конкретных функций.

Университет не вправе запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о

возможности выполнения субъектом ПДн трудовой функции или учебной деятельности.

1.7. Уничтожение персональных данных

Университет прекращает обработку ПДн и уничтожает собранные ПДн, если иное не установлено законодательством Российской Федерации, в следующих случаях и в сроки, установленные законодательством Российской Федерации:

– по достижении целей обработки или при утрате необходимости в их достижении, а также по окончанию сроков обработки ПДн;

– по требованию субъекта ПДн или Уполномоченного органа по защите прав субъектов ПДн;

– если ПДн являются неполными, устаревшими, недостоверными или не являются необходимыми для заявленной цели обработки;

– при отзыве субъектом ПДн согласия на обработку своих ПДн, если такое согласие требуется в соответствии с законодательством РФ;

– в случае установления факта неправомерной обработки ПДн.

1.8.Права и обязанности субъекта персональных данных

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн.

Субъект ПДн вправе требовать от Университета уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с действующим законодательством.

Субъект ПДн имеет право на свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных действующим законодательством.

Университету запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных действующим законодательством.

Субъект ПДн обязан сообщать Университету достоверную информацию о себе и представлять документы, содержащие ПДн, в соответствии с требованиями законодательства Российской Федерации, своевременно сообщать Университету об изменении своих ПДн.

ПДн оценочного характера субъект ПДн имеет право дополнить заявлением, выражающим его собственную точку зрения.

Субъект ПДн вправе требовать извещение Университетом всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Субъект имеет право на обжалование в суде любых неправомерных действий или бездействия работодателя при обработке и защите его ПДн.

1.9. Меры по обеспечению выполнения обязанностей, предусмотренных законодательством РФ в области персональных данных.

Университет обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных действующим законодательством РФ в области ПДн и принятыми в соответствии с ним нормативными правовыми актами. Университет самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим

законодательством РФ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено действующим законодательством РФ.

К таким мерам могут, в частности, относятся:

– назначение Университетом ответственного за организацию обработки ПДн на основании приказа Ректора;

– издание Университетом документов, определяющих политику Университета в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии с действующим законодательством РФ;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных действующему законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Университета в отношении обработки ПДн, локальным актам Университета;

– ознакомление работников Университета, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Университета в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

Университет обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

Университет и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено действующим законодательством.

Университет при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Лицо, ответственное за организацию обработки ПДн обязано:

– осуществлять внутренний контроль за соблюдением Университетом и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников Университета положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

В целях обеспечения сохранности и конфиденциальности ПДн субъектов ПД, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только специалистами, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

Обработка ПДн, осуществляемая без использования средств автоматизации, осуществляться таким образом, что в отношении каждой категории ПДн определены места хранения ПДн (материальных носителей) и установлены перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Должно быть обеспечено раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Университетом.

1.10 Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с персональными данными, которые будут

совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Университета, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

– копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

– ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Университета.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн:

– при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем

изготовления нового материального носителя с уточненными персональными данными.

2. Материал для проведения контроля знаний.

Тест состоит из 25 вопросов, требующих выбора одного правильного ответа или нескольких ответов.

Шкала оценивания результатов:

– 100-92 балла – «отлично»

– 90-78 баллов – «хорошо»

– 76-52 – «удовлетворительно»

– Меньше 50 – не удовлетворительно – тест не пройден.

При выполнении теста на платформе Black Board learn+ подсчет результатов теста производится автоматически. Во время прохождения теста повторно, в случае неудачной первой попытки, порядок вопросов будет изменен системой.

1. Продолжите фразу: Предоставление ПДн - действия, направленные на раскрытие ПДн…

a) определенному лицу или определенному кругу лиц; +

b) неопределенному кругу лиц;

c) лицу, которое прямо определяемо с помощью ПДн.

Эталон ответа: a

2. Уничтожение ПДн – это…

a) любое действие (операция), совершаемых с использованием средств автоматизации с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

b) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

c) действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Эталон ответа: c

3. Сопоставьте понятие с правильным определением:

1. Оператор	a) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
2. Субъект ПДн	b) ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.
3. Общедоступные ПДн	c)совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
4. Информационная	d) физическое лицо,

система ПДн (ИСПДн)	которое прямо или косвенно определено или определяемо с помощью ПДн.
5. ПДн	e) ознакомление определенных лиц (в том числе работников) с персональными данными субъектов, обрабатываемыми оператором, при условии сохранения конфиденциальности этих сведений
6. Специальные категории ПДн	f) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными.
7. Конфиденциальность ПДн	g) ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется

	требование соблюдения конфиденциальности.
8. Доступ к персональным данным	h) обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Эталон ответа:1 – f, 2- d, 3 – g, 4 – c, 5 – a, 6 – b, 7 – h, 8 – e.

4. Обработка ПДн посредством вычислительной техники – это

a) обработка ПДн;

b) автоматизированная обработка ПДн;

c) обезличивание ПДн;

Эталон ответа: b

5. Заполните пропуски:

1. Трудовой кодекс Российской Федерации от_____

(30 декабря 2001 г. № 197-ФЗ)

2. Федеральный закон от_____«Об информации, информационных технологиях и о защите информации». (27 июля 2006 № 149-ФЗ)

3. Федеральный закон от_____ «О персональных данных». (27 июля 2006 г. № 152-ФЗ)

4. Указ Президента Российской Федерации от_____«Об утверждении перечня сведений конфиденциального характера» (06 марта 1997 № 188).

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

6. Что входит в перечень ПДн, обрабатываемых в Университете:

1) фотография

2) фамилия, имя и отчество

3) дата и место рождения

4) номер аудитории

5) информация о гражданстве

6) паспортные данные или иного документа, удостоверяющего личность

7) время работы сотрудника

8) все перечисленное

Эталон ответа:1,2,3,5,6

7. Являются ли сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения) ПДн?

1) да;

2) нет.

Эталон ответа:1

8. Что из перечисленного относится к ПДн , обрабатываемых в Университете?

1) сведения об участии в конференциях, фестивалях, конкурсах, соревнованиях и т.п., о достигнутых в их ходе результатах;

2) сведения о зачислении, переводе и отчислении обучающихся;

3) сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу;

4) сведения о трудовой деятельности и общем стаже;

5) информация об отпусках;

6) сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней

7) все перечисленное.

Эталон ответа: 7

9. Что из перечисленного указывается при трудоустройстве в Университете?

1) сведения о предыдущем (-их) месте (-ах) работы и учебы;

2) сведения о семейном положении и составе семьи;

3) номер расчетного счета;

4) номер банковской карты;

5) сведения о ранее проведенных отпусках

6) сведения о расторжении брака

7) все перечисленное

Эталон ответа:1,2,3,4

10. Право доступа к ПДн (на внутреннем уровне) имеют:

1) ректор;

2) первый проректор;

3) проректоры по направлению деятельности в отношении своих подчиненных и при решении вопросов о приеме на работу новых сотрудников;

4) начальник отдела кадров;

5) работники отдела кадров;

6) работники клининговой компании;

7) персонал охраны;

8) все перечисленное.

Эталон ответа: 1,2,3,4,5.

11. Право доступа к ПДн (на внешнем уровне) меют:

1) налоговые инспекции;

2) правоохранительные органы;

3) военкоматы;

4) органы социального страхования;

5) пенсионные фонды;

6) родственники обучающихся студентов, не имеющие официальных документов об опекунстве, усыновлении;

7) подразделения муниципальных органов управления;

8) правоохранительные органы;

9) суды;

10) сотрудники не обоснования причины обращения к ПДн;

11) исполнительные органы государственной власти ;

12) Государственная инспекция труда;

13) страховые медицинские компании в рамках государственных контрактов;

14) все перечисленное.

Эталон ответа: 1,2,3.4,5,7,8,9,11.12,13.

12. Кто из перечисленных категорий субъектов относится к субъектам ПДн:

1) работники университета;

2) поступающие в университет;

3) обучающиеся в университете;

4) близкие родственники выше указанных лиц;

5) лица, ранее состоявшие в трудовых и/или образовательных отношениях с университетом;

6) лица, командированные в университет;

7) лица, состоящие (состоявшие) в договорных отношениях с университетом;

8) лица, не являющиеся законными представителями обучающихся;

9) лица, проживающие в общежитиях университета, но не являющиеся его работниками и обучающимися;

10) иностранные граждане;

11) законные представители перечисленных лиц.

12) все перечисленное.

Эталон ответа: 1.2,3,4,5,6,7,9,10,11.

13. Документы, содержащие ПДн хрянятся в….

1) личных делах;

2) в сейфе у ректора;

3) других делах и информационных системах ПДн(ИСПДн);

4) открытом доступе.

Эталон ответа: 1,3.

14. Лица, допущенные к обработке ПДн, подписывают…

1) заявление в свободной форме;

2) обязательство о неразглашении ПДн субъектов ПДн

3) согласие на обработку данных абитуриента.

Эталон ответа 2

15. Согласны ли вы с утверждением: Согласие на обработку ПДн субъекта ПДн предоставляется в письменной форме и содержание согласия разрабатывается в соответствии с федеральным законом?

1) да

2) нет

Эталон ответа: 1

16. Университет имеет право передавать персональные данные в следующие государственные и негосударственные структуры:

1) налоговые органы;

2) правоохранительные органы;

3) органы лицензирования и сертификации;

4) органы прокуратуры и ФСБ;

5) органы статистики;

6) страховые агентства;

7) военкоматы;

8) органы социального страхования;

9) пенсионные фонды;

10) подразделения государственных и муниципальных органов управления;

11) банковские организации, имеющие договорные отношения с Университетом

12) все перечисленное

Эталон ответа: 12.

17. Заполните пропуски : Основанием для рассмотрения возможности и целесообразности передачи ПДн третьей стороне является _____на имя ректора, в котором должно быть указано:

1) _____;

2) обоснование необходимости работы с этими сведениями;

3) ссылка на_____, на основании которого запрашиваются ПДн;

4) форма передачи сведений: доступ (ознакомление, выписки или копирование) или предоставление (в каком виде: электронном или бумажном);

5) _____на получение ПДн;

6) обязательство соблюдать _____

(Письменный запрос, состав испрашиваемых данных, федеральный закон (с указанием конкретных статей),представитель, режим конфиденциальности полученных данных)

18. Вход в здание Университета осуществляется….

1) свободно

2) по удостоверениям личности (для сотрудников и посторонних граждан) и студенческим билетам(для студентов).

Эталон ответа:2

19. Конфиденциальность ПДн – это_____

_____

_____.

20. Университет разрешает доступ к ПДн субъектов ПДн :

1) всем сотрудникам;
2) специально уполномоченным лицам;
3) студентам и их законным представителям.

Эталон ответа:2

21. Университет вправе запрашивать информацию:

1) о здоровье, не относящемуся к выполнению должностных обязанностей;
2) о личной жизни;
3) о здоровье, относящемуся к выполнению должностных обязанностей.

Эталон ответа: 3.

22. На основании каких принципов осуществляется обработка ПДн в Университете?_____

_____

_____

_____

_____

_____

_____.

Эталон ответа:

законность целей и способов обработки ПДн и добросовестности; - соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям лиц, осуществляющих обработку ПДн; - соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям их обработки; - обеспечение точности ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн, принятие мер по удалению или уточнению неполных или неточных данных; - недопустимость объединения созданных несовместимых между собой по целям баз данных информационных систем ПДн..

23. Университет не вправе требовать от субъекта ПДн предоставления информации:

1) о его расовой, национальной принадлежности;
2) политических взглядах;
3) о составе семьи;

4) религиозных и философских убеждениях;

5) о частной и интимной жизни;

6) об образовании.

Эталон ответа: 1,2,4,5.

24. Блокирование ПДн – это_____

_____

_____.

25. Информационная система ПДн(ИСПДн) – это_____

_____

_____.