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

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»

Проверка на объем заимствований:
92 % авторского текста
Работа_____к защите
« 27 »____мая___2020 г.
Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Выполнила:
Магистрантка группы ОФ-209/210-2-1
Сальникова Анна Евгеньевна

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

Челябинск, 2020

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Южно-Уральский Государственный Гуманитарно-Педагогический Университет»

(ФГБОУ ВО «ЮУрГГПУ»)

Профессионально-педагогический институт

Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Направление подготовки 44.04.04 – Профессиональное обучение (управление информационной безопасностью в профессиональном образовании)

З А Д А Н И Е

на выпускную квалификационную работу

Магистрантке группы Ф-209/210-2-1 очного отделения Сальниковой Анне Евгеньевне, обучающейся по программе магистратуры Управление информационной безопасностью в профессиональном образовании.

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

1. Тема квалификационной работы: «Защита конфиденциальной информации в образовательной организации» утверждена приказом ректора Южно-Уральского государственного гуманитарно-педагогического университета №_____от «___ »_____20 г.

Срок сдачи магистранткой законченной работы на кафедру 29.06.2020.

2. Материалы для выполнения квалификационной работы:

2.1. Учебная, научно-техническая, теоретико-методическая литература по теме квалификационной работы, основные положения об обработке и защите персональных данных; научные, практические, методические рекомендации

по организации защиты конфиденциальной информации ведущих специалистов в этой области.

2.2. Материалы преддипломной практики по теме квалификационной работы.

3. Основные части магистерской диссертации (перечень подлежащих разработке вопросов) и сроки их выполнения представлены в таблице 1.

Таблица 1 - Основные части магистерской диссертации

№ п/п	Перечень вопросов, подлежащих разработке в диссертации	Сроки выполнения ВКР
1.	Разработка плана работы и примерного перечня, необходимых для анализа нормативно-правовых, научных, статистических, и практических материалов	
2.	Составление предварительной библиографии по теме ВКР	
3.	Сбор информации и ее обработка	
4.	Написание первой и второй (теоретической) части работы	
5.	Написание третьей части работы	
6.	Написание введения и заключения	
7.	Представление первой редакции работы руководителю ВКР	
8.	Подготовка окончательной редакции работы, ее оформление и сдача на отзыв руководителю ВКР	
9.	Получение акта внедрения авторской разработки	
10.	Оформление пояснительной записки и презентации ВКР	
11.	Защита ВКР на заседании Государственной экзаменационной комиссии	

Дата выдачи задания: «25» ноября 2019 г.

Заведующий кафедрой АТ, ИТ и МОТД:

Руднев Валерий Валентинович, к.т.н, доцент _____

Фамилия, Имя, Отчество, ученое звание — Подпись заведующего кафедрой

Задание выдал:

Белевитин В.А., д.т.н., профессор каф. АТ, ИТ и МОТД _____

Фамилия, Имя, Отчество, ученое звание и степень — Подпись научного руководителя

Задание приняла:

Сальникова Анна Евгеньевна _____

Фамилия, Имя, Отчество студента — Подпись магистрантки

АННОТАЦИЯ

Магистрантка Сальникова Анна Евгеньевна _____
(Ф.И.О.) Подпись

Тема магистерской диссертации «Защита конфиденциальной информации в образовательной организации».

Магистерская диссертация содержит 84 страницы, 2 таблицы, 12 рисунков, 76 источников литературы.

Ключевые слова: информация, информационная безопасность, конфиденциальная информация, персональные данные, защита информации, защита конфиденциальной информации, угрозы защиты конфиденциальной информации, методы и инструментарий защиты конфиденциальной информации.

Объект исследования – Методическое обеспечение процесса защиты конфиденциальной информации в образовательной организации.

Предмет исследования – Методическое обеспечение процесса защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность".

Цель магистерской диссертации – рассмотрение особенностей работы с конфиденциальной информацией, а именно персональными данными, и разработка предложений по совершенствованию мер системы защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

В процессе исследования изучены теоретические аспекты - понятия, свойства, аспекты безопасности конфиденциальной информации, а также основные источники правового регулирования конфиденциальной информации.

В результате проведенного исследования разработаны предложения организационных и технических мероприятий по обеспечению защиты конфиденциальной информации (персональных данных) для образовательной организации, проведена оценка эффективности комплекса мер защиты персональных данных.

Степень внедрения – полученные результаты исследования находятся в стадии внедрения в методические материалы образовательной организации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

На сегодняшний день информация является важнейшим продуктом общественного производства, постоянно наращиваемый ресурс человечества.

Деятельность организаций неразрывно связана с получением и использованием различного рода информации. В современных условиях информация представляет собой товар, имеющий определенную ценность. Разглашение такой информации может привести к угрозам безопасности различной степени тяжести. Боязнь лишиться таких активов заставляет организации создавать различные системы защиты, в т. ч. организационную, техническую, а главное - правовую.

В связи с чем, информация разделяется на три группы: информация для открытого пользования любым потребителем в любой форме; информация ограниченного доступа - только для органов, имеющих соответствующие законодательно установленные права (полиция, налоговая инспекция, прокуратура); информация только для сотрудников (либо руководителей) организации.

Информация, относящаяся ко второй и третьей группам, является конфиденциальной и имеет ограничения в распространении. Часть этой информации составляет особый блок и может быть отнесена к коммерческой тайне. Конфиденциальная информация является важнейшей составляющей любых информационных отношений. Вопросы правового регулирования по поводу использования и распространения информации в последнее время занимают одно из значительных мест в юридической литературе. Это обусловлено, прежде всего, тем, что содержание юридически значимой тайны заключается в том, что ее предмет образует информация, не предназначенная для широкого круга лиц, а ее разглашение может повлечь нежелательные последствия для владельцев и обладателей тайны.

Проблема защиты конфиденциальной информации в организациях любой формы в настоящее время стоит наиболее остро, так как угрозы нарушения информационной безопасности носят глобальный характер. Способы ре-

ализации угроз информационной безопасности и формы их проявления постоянно совершенствуются, высокая технологичность этих угроз требует адекватных мер противодействия, предъявляет требования к квалификации специалистов по информационной безопасности, материально-техническому и кадровому обеспечению.

Несмотря на большое количество работ по проблематике информационной безопасности конфиденциальных данных, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма безопасности конфиденциальной информации в образовательных организациях не соответствуют условиям реального времени.

Потребность в проработке вопросов использования все более совершенных методов обеспечения защиты конфиденциальной информации образовательных организаций определили *актуальность* настоящего исследования.

Анализ состояния проблемы позволил выявить *противоречие* между необходимостью обеспечения качественных методов и средств защиты конфиденциальной информации и отсутствием разработанных предложений по улучшению мер защиты конфиденциальной информации в образовательной организации МБУ ДО «ЦВР "Юность" г. Челябинска», для дальнейшего внедрения в систему защиты конфиденциальной информации.

Выявленное противоречие позволило сформулировать *проблему* необходимости разработки предложений по совершенствованию системы защиты конфиденциальной информации в образовательной организации.

Поиск путей решения проблемы определил *тему исследования*: «Защита конфиденциальной информации в образовательной организации».

Решение указанной проблемы определило *цель исследования* - рассмотрение особенностей работы с конфиденциальной информацией, а именно персональными данными, и разработка предложений по совершенствованию

мер системы защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

Объект исследования – Методическое обеспечение процесса защиты конфиденциальной информации в образовательной организации.

Предмет исследования – Методическое обеспечение процесса защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

Рабочее предположение диссертационного исследования заключается в следующем, что можно улучшать уровень защиты конфиденциальной информации, если при разработке комплекса предложений по защите конфиденциальной информации сделать уклон именно на организационные и технические меры.

Задачи исследования:

1. Изучить понятия, свойства, аспекты безопасности информации, исследовать основные источники правового регулирования конфиденциальной информации, рассмотреть организацию доступа и порядок работы персонала с персональными данными в образовательной организации, выявить угрозы и меры по предупреждению утечки конфиденциальной информации
2. Проанализировать меры и средства защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска»
3. Разработать предложения по совершенствованию организационных и технических мер защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска»
4. Оценить эффективность комплекса организационных и технических мер защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод как анализ документации образовательного учреждения; анализ и сопоставление имеющихся средств

для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием политики защиты конфиденциальной информации; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Теоретико-методологическая основа исследования – основные положения об обработке и защите персональных данных; научные, учебные, практические, методические рекомендации по организации защиты конфиденциальной информации ведущих специалистов в этой области, таких как А.И. Алексенцев [22, 23] и Е.А. Степанов [67; 68] и др.

Нормативно-правовая основа - Конституция как основном законе Российской Федерации [1]; статья 23 Конституции РФ гарантирует право на личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщении; ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149 [8]; основными в области безопасности конфиденциальной информации также являются законы РФ: ФЗ «О государственной тайне» от 22 июля 2004 г. [4]; ФЗ №98 «О коммерческой тайне» от 29 июля 2004 [5]; Указ Президента РФ №188 «Об утверждении Перечня сведений конфиденциального характера» [9]; ФЗ №152 «О персональных данных» от 27 июля 2006 № [6]; Постановление Правительства № 731 «Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну» [10]; стандарт, закрепляющий основные термины и определения в области защиты информации - ГОСТ Р 50922-96 [21].

Основные *этапы исследования*:

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

Второй этап – в ходе данного этапа осуществлялся анализ методов и средств, которые задействуются в организации по защите персональных данных, а также проводился анализ научной литературы и отбор информации по

теме исследования, осуществлялось написание и публикация научной статьи по теме исследования.

Третий этап заключался в том, что осуществлялась оценка эффективности разработанной политики по защите конфиденциальной информации, осуществлялся сбор и анализ данных, полученных в результате исследования, а также последующая оценка полученных результатов.

Положения, выносимые на защиту:

1. В ходе исследования обоснована необходимость пересмотра мер и средств защиты конфиденциальной информации, а именно персональных данных, в образовательной организации.

2. Для улучшения уровня защиты персональных данных в образовательной организации следует пересмотреть организационные и технические меры защиты и усовершенствовать их.

3. В ходе исследования выдвинута гипотеза: при отсутствии практически-усовершенствованной политики по защите конфиденциальной информации в образовательной организации, не осуществляется полноценная защита персональных данных. Гипотеза была выдвинута в ходе преддипломной практики и анализа организационно-правовых, технических и физических мер защиты конфиденциальной информации на базе исследования.

4. На основании изложенного, разработан комплекс предложений организационных и технических мер по защите конфиденциальной информации и выявлена эффективность разработанного комплекса.

Сформулированные выше задачи определили структуру дипломной работы, которая состоит из введения, трех глав, заключения, списка литературы (76 наименований). В тексте работы представлено 2 таблицы, 12 рисунков.

Во введении обоснована актуальность темы исследования, представлен научный аппарат исследования темы.

В теоретической главе раскрыты понятия, свойства, аспекты безопасности конфиденциальной информации, а также основные источники правового регулирования конфиденциальной информации.

В практической главе разработан комплекс предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации для образовательной организации, проведена оценка эффективности комплекса предложений.

База исследования: МБУ ДО «ЦВР "Юность" г. Челябинска».

ГЛАВА 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ

1.1. Информация: понятия, свойства, аспекты безопасности

На сегодняшний день информация является важнейшим ресурсом и одной из движущих сил развития человеческого общества. Информационные процессы, происходящие в материальном мире, живой природе и человеческом обществе, изучаются всеми научными дисциплинами от философии до маркетинга.

Исторически сложилось так, что исследованием непосредственно информации занимаются две комплексные отрасли науки — кибернетика и информатика.

Информация как объект правоотношений должна быть конкретизирована, организована должным образом, «привязана» к ситуации и конкретному виду отношений, классифицирована по видам и тому подобным образом «подготовлена» для осуществления по ее поводу действий, регулируемых нормами права.

В практическом смысле определение информации дал С.И. Ожегов: информация — это:

1. сведения об окружающем мире и протекающих в нем процессах;
2. сообщения, осведомляющие о положении дел, о состоянии чего-либо.

До середины 20-х гг. XX в. под информацией (в переводе с латыни — ознакомление, разъяснение, изложение) понимались «сообщения и сведения», передаваемые людьми устным, письменным или другим способом. А уже с середины XX в. информация определяется как общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму как генетическая информация, одно из основных понятий кибернетики [73].

В связи с развитием средств связи и телекоммуникаций, вычислительной техники и их использованием для обработки и передами информации возникла необходимость измерять количественные характеристики информации. Появились разные теории, и понятие «информация» начало наполняться разным содержанием.

В 1949 г. К. Шеннон и У. Уивер опубликовали статью «Математическая теория связи», в которой были предложены вероятностные методы для определения количества передаваемой информации. Однако такие методы описывают лишь знаковую структуру информации и не затрагивают заложенного в ней смысла (в сообщении, сведениях) [39].

В 1948 г. Н. Винер предложил «информационное видение» кибернетики как науки об управлении в живых организмах и технических системах. Под информацией стали понимать не просто сведения, а только сведения новые и полезные для принятия решения, обеспечивающего достижение цели управления [37]. Остальные сведения не считались информацией.

На сегодняшний день определений информации существует множество, причём академик Н. Н. Моисеев даже полагал, что в силу широты этого понятия нет и не может быть строгого и достаточно универсального определения информации [73].

В международных и российских стандартах даются следующие определения:

– знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста;

– знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл;

– сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации [35].

Хотя информация должна обрести некоторую форму представления, то есть превратиться в данные, чтобы ею можно было обмениваться, информа-

ция есть в первую очередь интерпретация такого представления. Поэтому в строгом смысле информация отличается от данных, хотя в неформальном контексте эти два термина очень часто используют как синонимы.

Термин «информация» и связанные с ним термины сегодня широко применяются и законодателем.

Различают основные виды информации, которые *классифицируют* по ее форме представления, способам ее кодирования и хранения:

– графическая

– звуковая (акустическая)

– текстовая – кодирует речь человека с помощью специальных символов – букв (для каждого народа свои)

– числовая – кодирует количественную меру объектов и их свойств в окружающем мире с помощью специальных символов – цифр

– видеоинформация – способ хранения «живых» картин окружающего мира, который появился с изобретением кино.

По степени доступа информация подразделяется на открытую и информацию ограниченного доступа, распространение которой возможно в условиях конфиденциальности или секретности (Рисунок 1).

Информация

Открытая (общедоступная):

– Информация как объект гражданских прав (произведения, патенты и авторские свидетельства, другая информация, создаваемая с целью извлечения прибыли);

– Массовая информация;

– Информация о выборах, референдуме;

– Официальные документы;

– Обязательно представляемая информация;

– Другая открытая информация.

Ограниченного доступа:

– Государственная тайна, служебная тайна
– Ноу-хау (секреты производства) и коммерческая тайна
– Персональные данные (в порядке защиты личной тайны)
– Другие виды тайн

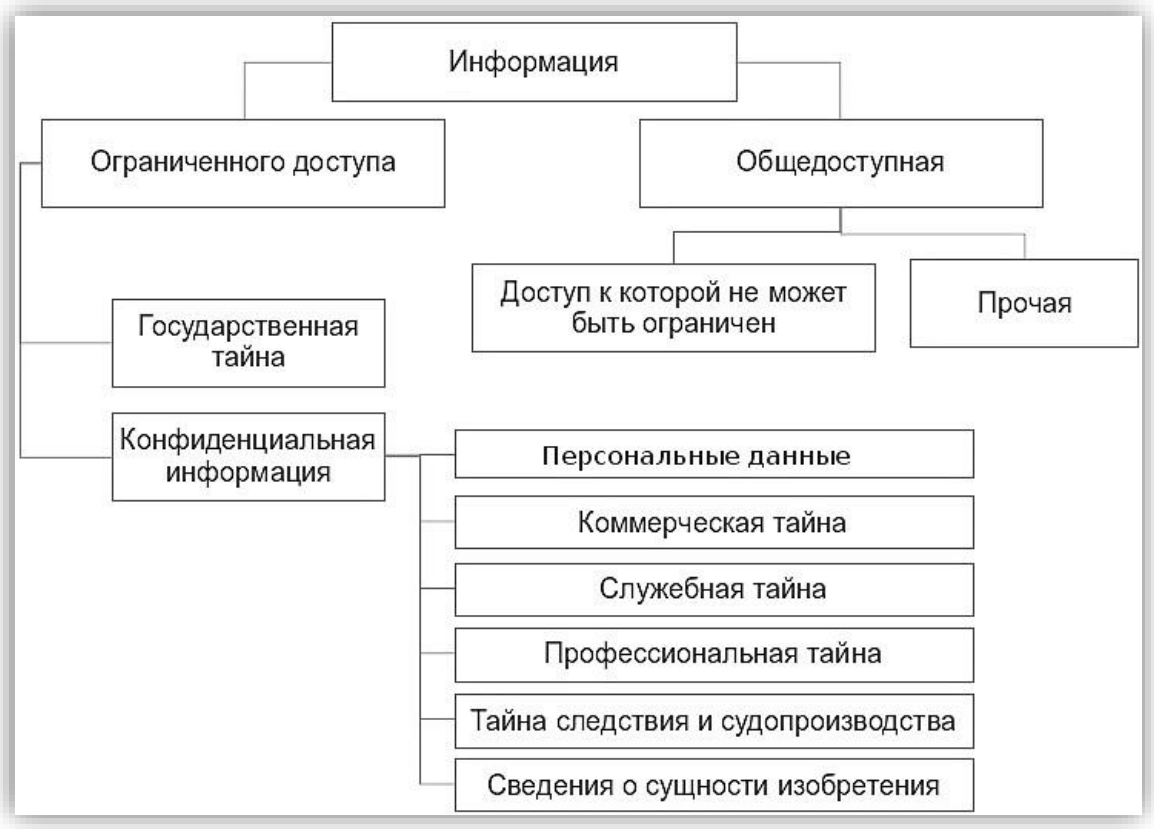


Рисунок 1 – Подразделение информации

Также информация, как и любой объект, обладает свойствами, наиболее важными являются [40]:

– Объективность. Объективная информация – существующая независимо от человеческого сознания, методов ее фиксации, чьего-либо мнения или отношения.

– Достоверность. Информация, отражающая истинное положение дел, является достоверной. Недостоверная информация чаще всего приводит к неправильному пониманию или принятию неправильных решений. Устаревание информации может из достоверной информации сделать недостоверную, т.к. она уже не будет отражением истинного положения дел.

– Полнота. Информация является полной, если она достаточна для понимания и принятия решений. Неполная или избыточная информация может привести к задержке принятия решения или к ошибке.

– Точность информации – степень ее близости к реальному состоянию объекта, процесса, явления и т. п.

– Ценность информации зависит от ее важности для принятия решения, решения задачи и дальнейшей применимости в каких-либо видах деятельности человека.

– Актуальность. Только своевременность получения информации может привести к ожидаемому результату.

– Понятность. Если ценную и своевременную информацию выразить непонятно, то она, скорее всего, станет бесполезной. Информация будет понятной, когда она, как минимум, выражена понятным для получателя языком.

– Доступность. Информация должна соответствовать уровню восприятия получателя. Например, одни и те же вопросы по-разному излагаются в учебниках для школы и вуза.

– Краткость. Информация воспринимается гораздо лучше, если она представлена не подробно и многословно, а с допустимой степенью сжатости, без лишних деталей. Краткость информации незаменима в справочниках, энциклопедиях, инструкциях. Логичность, компактность, удобная форма представления облегчает понимание и усвоение информации.

Рассмотрим аспекты информационной безопасности, можно выделить следующие:

Целостность информации. Целостность информации – это её физическая сохранность, защищённость от разрушения и искажения, а также её актуальность и непротиворечивость.

Целостность информации подразделяется на:

– статическую

– динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и так далее.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Доступность информации

Доступность информации – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Доступность информации подразумевает, что субъект информационных отношений (пользователь) имеет возможность за приемлемое время получить требуемую информационную услугу.

Например, создавая информационную систему с информацией об обучающихся образовательной организации, мы рассчитываем, что с помощью этой системы в любое время в течение нескольких секунд сможем получить требующуюся информацию (список студентов любой группы, полную информацию о конкретном студенте и так далее).

Конфиденциальность информации

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в

обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность информации – это гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Конфиденциальная информация – это информация, на доступ к которой имеет право ограниченный круг лиц.

Если же доступ к конфиденциальной информации получает лицо, не имеющее такого права, то такой доступ называется несанкционированным и рассматривается как нарушение защиты конфиденциальной информации. Лицо, получившее или пытающееся получить несанкционированный доступ к конфиденциальной информации, называется злоумышленником.

Обеспечение конфиденциальности информации является наиболее проработанным разделом информационной безопасности.

Конфиденциальная информация подразделяется на:

– предметную,

– служебную.

Предметная информация - это сведения о какой-то области реального мира, которые, собственно, и нужны злоумышленнику, например, чертежи подводной лодки или сведения о месте нахождения.

Служебная информация не относится к конкретной предметной области, а связана с параметрами работы определенной системы обработки данных. К служебной информации относятся в первую очередь пароли пользователей для работы в системе. Получив служебную информацию (пароль), злоумышленник с ее помощью может затем получить доступ к предметной конфиденциальной информации.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Необходимо представлять, откуда могут исходить и в чем состоять угрозы информационной безопасности, какие меры могут быть предприняты для защиты информации, и уметь грамотно применять эти меры.

1.2. Основные источники правового регулирования конфиденциальной информации

Обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

1. Нормативные правовые акты РФ.
2. Нормативно-методические и методические документы.
3. Стандарты.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

– Акты федерального законодательства

– Международные договоры РФ;

– Конституция РФ;

– Законы федерального уровня (включая федеральные конституционные законы, кодексы);

– Указы Президента РФ;

– Постановления правительства РФ;

– Нормативные правовые акты федеральных министерств и ведомств;

– Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Рассмотрим примеры:

Основные направления правового регулирования информационных отношений - конституционное и гражданско-правовое. Ч. 4 ст. 29 Конституции РФ закрепляет право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом [1]. Перечень сведений, составляющих государственную тайну, определяется соответ-

ствующим федеральным законом. Этому праву корреспондирует общая обязанность органов государственной власти и местного самоуправления, располагающих такого рода информацией, предоставлять ее по соответствующим запросам.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" - назначение закона обеспечение защиты информации, регулирования отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений в области охраны результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации [4].

Пункт 3 ст. 5 Федерального закона № 149 - ФЗ об информации содержит классификацию информации в зависимости от порядка ее предоставления или распространения. Так, по этому основанию информация подразделяется [8]:

1. на информацию, свободно распространяемую, например, посредством средств массовой информации;
2. на информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. на информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4. на информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Конфиденциальная информация определена в п. 7 ст. 2 ФЗ № 149 через требование не передавать такую информацию третьим лицам без согласия ее обладателя [4]. Также данный Федеральный закон напрямую относит к категории конфиденциальной информации персональные данные (информацию о гражданах).

Федеральным законом № 152-ФЗ от 27 июля 2006 "О персональных данных" регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими и физическими лицами с использованием средств автоматизации или без их использования, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации [6].

Федеральные законы "О коммерческой тайне", "Об информации, информационных технологиях и о защите информации" и часть 4 ГК РФ - ввели, как говорилось выше, и новые понятия, и изменили содержание некоторых прежних понятий, относящихся к данному вопросу. Ст. 139 ГК РФ, определявшая коммерческую тайну, отменена.

В ст. 3 Федерального Закона № 98-ФЗ "О коммерческой тайне" коммерческая тайна определяется как режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду[13].

Федеральные законы от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" и от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи" - данные законы призваны обеспечить конфиденциальность информации в электронном виде - подписи, которая рассматривается как личная подпись субъекта.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании" - закон призван обеспечить защиту сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного до-

ступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, продукции (работ, услуг) и объектов, для которых устанавливаются требования, связанные с обеспечением ядерной и радиационной безопасности в области использования атомной энергии, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения указанной продукции и указанных объектов (ст. 5 ФЗ № 184-ФЗ).

Федеральный закон от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности" - закон регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в свете обеспечения защиты конфиденциальной информации при осуществлении лицензирования отдельных видов деятельности [12].

Иные федеральные законы в том или ином аспекте также могут регулировать деятельность, касающуюся информации, информационных технологий и защиты информации. Так, глава 13 Кодекса РФ об административных правонарушениях № 195-ФЗ от 30 декабря 2001 г. устанавливает ответственность за административные правонарушения в области связи и информации.

В числе нормативных правовых актов, частично регулирующих рассматриваемые отношения, следует назвать также Закон "Об архивном деле в Российской Федерации" [3]. Пользователь архивных документов имеет право использовать, передавать, распространять информацию, содержащуюся в них, а также копии архивных документов для любых законных целей и любым законным способом. Кроме того, приняты и иные нормативные правовые акты в данной области.

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах ис-

полнительной власти" - данное постановление регламентирует порядок обращения и работы с конфиденциальной информацией федеральными органами исполнительной власти с целью предотвращения угрозы утечки информации и обеспечения защиты информации [16].

Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных". Положение содержит требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПД) [13].

Постановления: Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 "О лицензировании деятельности по технической защите конфиденциальной информации" [12] и Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 "О лицензировании деятельности но разработке и (или) производству средств защиты конфиденциальной информации" призваны обеспечить защиту конфиденциальной информации путем обязательного лицензирования технических средств защиты [12].

В завершении анализа нормативно правовых норм можно прийти к выводу, что конфиденциальная информация – это информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную, профессиональную или личную тайны, охраняющиеся её владельцем.

Вывод по Главе 1

В первой главе было изучено понятие информации, выявлены её свойства. Стало известно, что выделяют такие аспекты информационной безопасности, как целостность, доступность и конфиденциальность.

В первой главе рассмотрены основные источники правового регулирования конфиденциальной информации.

Отношения по поводу информации в целом и конфиденциальной информации в частности, регулируются правом. При этом информация как таковая и конфиденциальная информация являются предметом регулирования различных отраслей права и нормативных правовых актов РФ, важнейшее место среди которых занимает Конституция РФ.

Также было выявлено, что обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

1. Нормативные правовые акты РФ
2. Нормативно-методические и методические документы
3. Стандарты.

Кроме того в первой главе были проанализированы нормативно-правовые акты Российской Федерации в области информационной безопасности и было выяснено, что Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите и информации" напрямую относит к категории конфиденциальной информации *персональные данные*. Также важным является Федеральный закон № 152-ФЗ от 27 июля 2006 "О персональных данных", в котором регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ.

Рассматривая в главе информацию как объект информационных правоотношений, можно сделать вывод, что *конфиденциальная информация* – это информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

ГЛАВА 2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1. Организация доступа и порядок работы персонала с конфиденциальной информацией в образовательной организации

В каждой образовательной организации (далее – Организация) разрабатывается Положение о конфиденциальной информации, с целью регулирования порядка распространения и защиты конфиденциальной информации.

В основе данного Положения лежит Конституция РФ, федеральный закон № 149-ФЗ от 27.07.2006 года «Об информации, информационных технологиях и защите информации», федеральный закон № 98-ФЗ от 29.07.2004 года «О коммерческой тайне», положение статьи 1464 Гражданского Кодекса РФ, статей 102 и 313 Налогового Кодекса РФ, статьи 7 федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных». Настоящее положение является локальным актом Организации, обязательным для соблюдения всеми работниками, как основными, так и совместителями.

К конфиденциальной информации Организации относятся [47]:

– персональные данные (далее – ПДн) работников, обучающихся и их родителей, в соответствии с нормами 152-ФЗ от 27.07.2006 года и Положением о порядке использования и хранения ПДн, являющимся локальным актом организации;

– сведения о финансово-хозяйственной деятельности организации, за исключением информации о количестве и общей сумме заключенных гражданско-правовых договоров, подлежащих обязательному размещению на официальных сайтах в сети «Интернет» в соответствии с законодательством о контрактной системе и законодательстве в сфере закупок;

– сведения о доходах работников Организации, за исключением, установленных федеральным законодательством для Руководителя Органи-

зации или лиц, предоставление сведений, о доходах которых обязательно в рамках судебного или исполнительного производства;

– сведения бухгалтерского баланса;

– сведения, содержащийся в поступающих по почте (в том числе, в электронной форме) документах от вышестоящих и контролирующих организаций;

– внутренние документы Организации (приказы по основной деятельности, переписка с контрагентами по договорам, жалобы от участников образовательного процесса и др.);

– сведения о поступлении и расходовании бюджетных средств;

– сведения о типе и характеристиках компьютерного оборудования и установлению программного обеспечения;

– коды и пароли доступа;

– сведения о личной жизни сотрудников, а так же сведения о состоянии их здоровья;

– коммерческая, служебная и банковская тайна;

– содержание регистров бухгалтерского учета;

– содержание внутренней бухгалтерской отчетности;

– сведения об открытых в кредитных организациях расчетных и иных счетах, в том числе в иностранной валюте, о движении средств по этим счетам, и об остатке средств на этих счетах, сведения об имеющихся вкладах в банках, в том числе в иностранной валюте;

– сведения о методах управления Организацией.

Устав Организации, сведения о лицензировании, локальные акты, регулирующие образовательную деятельность (за исключением персональных данных обучающихся), прейскурант на оказание дополнительных платных услуг, являются открытой к доступу информацией и подлежат обязательному размещению на официальном сайте образовательной организации.

Обращение с конфиденциальной информацией

Конфиденциальная информация подлежит обработке, хранению и защите. Каждый сотрудник образовательной организации вправе использовать по своему усмотрению в ходе работы сведения, являющиеся конфиденциальными, самостоятельно определяя способ и степень их использования, в то же время учитывая, что информация с ограниченным доступом не подлежит публичному обнародованию, передаче сторонним физическим и юридическим лицам, включая сотрудников организации, которым данная информация не предназначена и напрямую не затрагивает их интересы.

Иначе говоря, использование конфиденциальной информации образовательной организации, его работников, обучающихся и их родителей (законных представителей) допускается только теми работниками Организации, которым доступ к такой информации необходим в силу выполняемых ими функций.

Сотрудник Организации без разрешения директора не вправе передавать сведения, ставшие ему известными в ходе работы, другим сотрудникам, которым данная информация не предназначена и напрямую не затрагивает их интересы.

При приеме на работу, работники письменно ознакомляются с настоящим положением, обязуясь таким образом хранить конфиденциальность полученных ими в ходе работы сведений и защищать информацию от передачи третьим лицам. Контрагенты по договорам, в процессе подписания договора, уведомляются о необходимости сохранения конфиденциальности, ставшей им известной информации, о чем может быть прописано в договоре.

Предоставление конфиденциальной информации Организации третьим лицам возможно не иначе как с разрешения директора Организации, а конфиденциальной информации работников Организации, обучающихся и их родителей (законных представителей) возможно только с их письменного согласия, также передача конфиденциальной информации допускается только по письменному запросу вышестоящих и контролирующих органов, су-

дов, службы судебных приставов, службы исполнения наказаний, правоохранительных органов, прокуратуры.

Защита конфиденциальной информации

Организация состоит в принятии комплекса мер, направленных на ограничение доступа к конфиденциальной информации третьих лиц, на предотвращение несанкционированного разглашения конфиденциальной информации, выявление нарушений режима конфиденциальной информации, пресечение нарушений режима конфиденциальной информации, привлечение лиц, нарушающих режим конфиденциальной информации к установленной ответственности. Обязательным условием трудовых договоров, заключаемых с сотрудниками Организации, является условие о соблюдении сотрудником служебной и коммерческой тайны.

Каждый сотрудник Организации при принятии на работу предупреждается под расписку об ответственности за нарушение режима служебной и коммерческой тайны. В случае попытки посторонних лиц получить от сотрудника сведения, относящиеся к коммерческой тайне Организации, сотрудник обязуется незамедлительно сообщить об этом Директору Организации в письменной или устной форме. Заключаемые Организацией в лице любых уполномоченных лиц договоры должны содержать условие о сохранении контрагентами конфиденциальности.

За несанкционированное разглашение конфиденциальной информации, неправомерное использование которой может нанести материальный и моральный ущерб Организации либо деловым партнерам и гражданам, на виновное лицо в соответствии с Трудовым кодексом РФ может быть наложено дисциплинарное взыскание (вплоть до увольнения) [17], а также взысканы убытки согласно ст. 139 Гражданского кодекса РФ [2]. Кроме того, виновное лицо может быть привлечено в установленных законом случаях к административной ответственности, а также к уголовной ответственности.

2.2. Угрозы и меры по предупреждению утечки конфиденциальной информации

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Можно сказать, что сотрудники Организации являются главным источником различных угроз в работе с конфиденциальной информацией. Способы осуществления угроз информационной безопасности могут быть различны. Сотрудник, например, может действовать целенаправленно или неосознанно по собственной инициативе, а также под чьим-то влиянием [61].

Основные виды реализации угроз информационной безопасности:

1. завладение конфиденциальными данными, вследствие чего у злоумышленника оказывается их копия. Получение конфиденциальной информации может происходить при помощи разных методов: подслушивание разговоров сотрудников данной Организации, использование технических средств (подслушивающих устройств), копирование секретных данных.

2. кража служебных документов, в результате чего злоумышленник овладевает секретными сведениями, а предприятие в свою очередь их лишается.

3. повреждение или полная ликвидация информации, в результате чего злоумышленник приносит вред предприятию.

4. изменение работником секретной информации, вследствие чего специалисты предприятия могут принять неверные руководящие действия.

Таким образом, вышесказанное ещё раз подтверждает, что самой часто встречающейся причиной осуществления угроз по защите безопасности является безответственность сотрудников организации. Это прослеживается в нарушении сотрудников условий по защите информационной безопасности, что приводит к утечке секретной информации [71].

Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения.

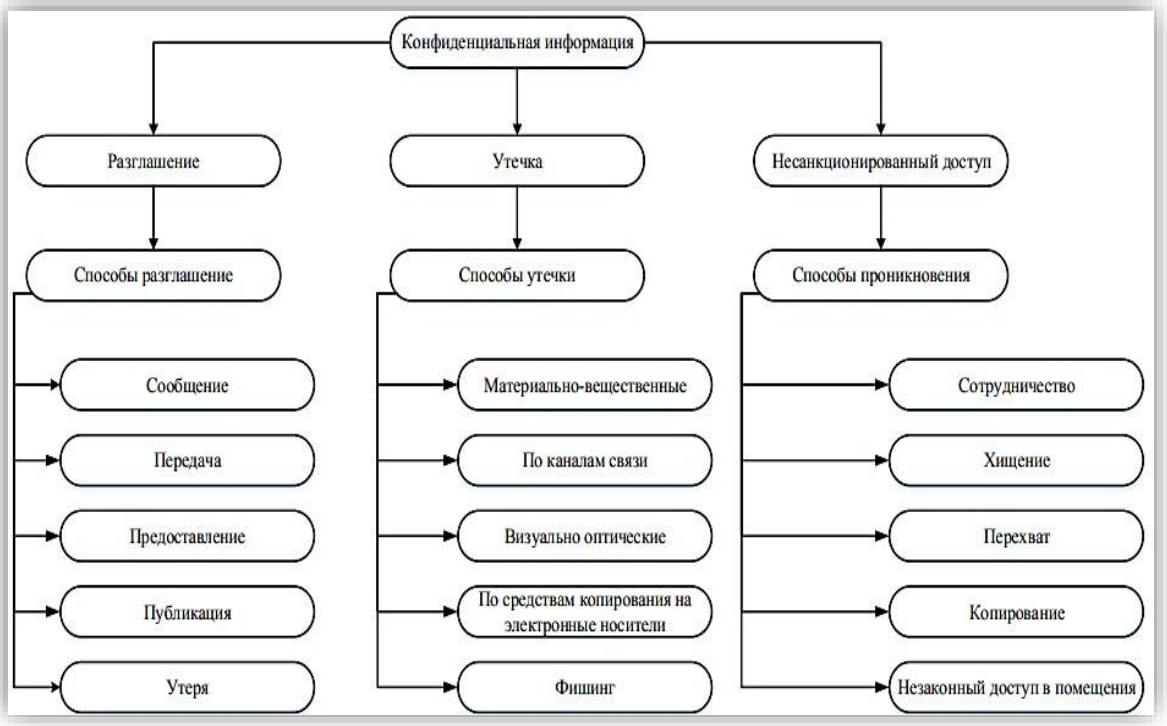


Рисунок 2 – Способы утечки конфиденциальной информации

Главные причины утечки информации:

– нарушение сотрудниками требований в работе с источниками служебной информации и правил использования систем защиты;

– недочёты в конструировании систем защиты;

– проведение злоумышленником технической и агентурной разведок.

Виды утечки информации:

– разглашение;

– несанкционированный доступ к информации;

– получение секретной информацией разведками.

Все каналы утечки конфиденциальной информации делятся на косвенные и прямые. Косвенные каналы не требуют прямого доступа к техническим средствам информации. Прямые каналы – непосредственный доступ к источнику информации.

Примеры косвенных каналов утечки:

– похищение или потеря носителей информации;

– фотографирование, прослушивание на расстоянии;

– перехват электромагнитных излучений.

Примеры прямых каналов утечки [66]:

– утечка информации из-за нарушения сотрудниками служебных требований;

– непосредственное копирование.

Одна из самых сложно решаемых угроз любой информационной системы — присутствие «инсайдера», официального специалиста организации, имеющего доступ к конфиденциальной информации, и, по каким-либо причинам (психологического характера или с целью наживы) осуществляющего кражу такой информации.

Соответственно, для предотвращения этой угрозы ведется планомерное обучение сотрудников и педагогов образовательной организации информационной культуре на заседаниях педагогического совета. Прививаются понятия «корпоративной» этики, ведется мониторинг психологической стабильности работников, в коллективе поддерживается «теплый» психологический климат.

Защита персональных данных представляет собой комплекс мер технического, организационного, организационно-технического, морально-этнического и правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (сотруднику) [71].

Во исполнение Закона в первую очередь должны быть разработаны: приказ об ответственных лицах по сотрудникам, а также положение о защите персональных данных. Такое положение является основным локальным актом, его отсутствие может быть квалифицировано государственным органом контроля и надзора как нарушение работодателем трудового законодательства. Этот документ определяет: порядок обработки персональных дан-

ных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Далее, для предупреждения утечки конфиденциальной информации, может быть создана рабочая группа. Поскольку главным условием защиты персональных данных является четкая регламентация функций сотрудников.

Рабочей группой проводятся следующие мероприятия: уточняются все ситуации, когда требуется проводить обработку ПДн, четко выделяются процессы, в которых обрабатываются ПДн, продумывается разработка пакета организационно-распорядительных документов для обеспечения полноценной защиты.

В общем, защита персональных данных работников образовательной организации сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;

– организацию системы защиты персональных данных;

– внедрение технических мер защиты персональных данных.

Также не стоит забывать, что специфика учебной организации такова, что обработке подвергаются не только данные сотрудников, но и обучающихся и их родителей. Соответственно, должна быть разработана и внедрена система получения согласия родителей на обработку персональных данных их самих и их детей (в случае, если обучающийся совершеннолетний, то он сам дает такое согласие).

С технической стороны защиты персональных данных необходимо использовать единую базу данных с организацией доступа по паролю. Также, необходимо определить возможные каналы утечки информации и возможные угрозы информационной системе, построить модель угроз нарушителя, и уже на их основании строить модель защиты. Проделать эту работу неспеци-

алисту чрезвычайно трудно, соответственно возникает проблема – либо обучаться самостоятельно, либо платить деньги за обучение сотрудника, либо полностью передать вопрос защиты ПДн стороннему интегратору. Не стоит забывать, что еще один необходимый шаг в организации технической стороны защиты персональных данных – обязательная сертификация программного обеспечения для ИСПД [72].

Если осуществляется обработка ПДн, то обязана обеспечиваться и защита. Поскольку потенциальные угрозы безопасности информации весьма многообразны, следовательно, цели защиты информации могут быть достигнуты путем создания комплексной системы защиты информации, под которой понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в образовательной организации.

Итак, исходя из вышесказанного, можно подвести итог и составить перечень методов и средств обеспечения требуемого уровня защищенности персональных данных.

1. Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. *Все меры обеспечения безопасности ИСПДн подразделяются на:*

1.1. Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

1.2. Морально-этические меры защиты. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

1.3. Организационные и административные меры защиты. Организационные и административные меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определе-

нии целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн.

1.4. Физические меры защиты. Физические меры защиты основаны на применении разного рода механических, электро- или электронно- механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

1.5. Аппаратно-программные средства защиты ПДн. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на Рисунке 3.

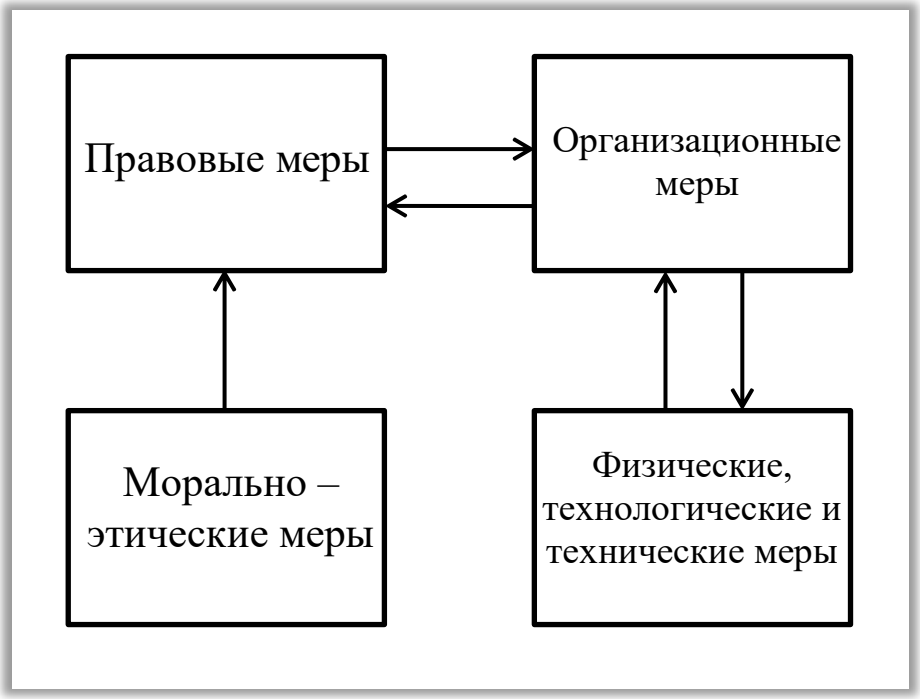


Рисунок 3 - Взаимосвязь мер обеспечения информационной безопасности

2. Контроль эффективности система защите персональных данных (далее – СЗРДн) должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

3. Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

4. Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

5. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

6. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель образовательной организации. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

7. Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

7.1. Планирование и реализация мер по обеспечению безопасности ПДн;

7.2. Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

7.3. Контроль защищенности ИТ инфраструктуры образовательной организации от угроз ИБ путем;

7.4. Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

7.5. Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

7.6. Анализ угроз безопасности ПДн;

Достоинства и недостатки различных видов мер защиты.

Законодательные и морально-этические меры

Эти меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение.

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения.

В некоторых случаях они являются единственно применимыми, как, например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Организационные меры

Очевидно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего, надо решить правовые и организационные вопросы. Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако это вовсе не означает, что систему защиты необходимо строить исключительно на их основе.

Этим мерам присущи серьезные *недостатки*, такие как:

– низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

– дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных

(по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо; перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое ядро безопасности. В этом случае, стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер. Но, даже имея совершенные законы и проводя оптимальную кадровую политику, проблему защиты все равно решить до конца не удастся.

– Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты.

– Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Вывод по Главе 2

Во второй главе был рассмотрен порядок работы персонала с конфиденциальной информацией в образовательной организации и выявлены угрозы утечки конфиденциальной информации, а также предложены меры устранения угроз, выполнение которых позволит повысить эффективность средств защиты, и сократит риск потери и искажения информации в образовательной организации.

Для решения проблемы сохранности конфиденциальной информации необходимо применение законодательных, организационных, морально-этических и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в образовательной организации приобретает все большее значение. Также у каждых из мер защиты бывают свои достоинства и недостатки, которые тоже важно учитывать, при разработке системы защиты.

Технический аспект связан с выбором программного обеспечения, организационный – с проведением мероприятий для реализации закона № 152-ФЗ «О персональных данных», а документационный – с созданием локальных актов образовательной организации.

Таким образом, можно говорить о том, что обеспечение информационной безопасности учебного процесса в современных условиях становится одним из главных видов деятельности образовательной организации. Поэтому на основании этого заключения, в Главе 3 диссертационного исследования описывается процесс разработки рекомендаций по совершенствованию мер защиты конфиденциальной информации, а также их дальнейшая эффективность.

ГЛАВА 3. СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1 Анализ мер и средств защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска»

В первой и второй главе были определены принципы и задачи, которые должны решаться с помощью политики информационной безопасности, а именно мероприятий по защите конфиденциальной информации. Опираясь на эти данные, было принято решение провести анализ мер и средств защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска» и определить задачу на совершенствования мер и средств защиты.

Целью анализа является выявление недостатков, которые могут привести к утечке персональных данных. После анализа текущего положения безопасности персональных данных, в следующем подпункте главы будут даны комментарии и пути совершенствования, которые помогут улучшить качество методов и средств защиты конфиденциальной информации.

Рассмотрим образовательную организацию - МБУ ДО «ЦВР "Юность" г. Челябинска». Управление осуществляется в соответствии с законодательством Российской Федерации, Уставом образовательного учреждения на основе сочетания принципов единоначалия и коллегиальности.

Структура управления образовательной организации представлена на рисунке 4. Единоличным исполнительным органом является директор. К коллегиальным органам управления относятся: Общее собрание работников, Педагогический совет.

Далее, рассмотрим защиту конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска». Как было выяснено ранее, к конфиденциальной информации образовательной организации относятся персональные данные работников, обучающихся и их родителей.

Рисунок 4 – Структура управления МБУ ДО «ЦВР "Юность" г. Челябинска»

Свой анализ начну с рассмотрения организационно – нормативных и технических методов защиты. В образовательной организации разработано Положение о конфиденциальной информации, Положение об обработке и хранение персональных данных, Приказа о наделении полномочиями по обработке персональных данных. Перечисленные Положения являются локальными актами организации.

Право доступа к ПДн обучающихся и их родителей (законных представителей) имеют:

- директор образовательного учреждения
- заместитель директора по УВР
- методист
- социальный педагог
- педагог-психолог
- педагог дополнительного образования

Перечисленные субъекты организации обязаны:

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

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

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

4. Соблюдать требование конфиденциальности персональных данных обучающихся и их родителей (законных представителей);

5. Запрашивать информацию о состоянии здоровья обучающегося только у родителей (законных представителей);

6. Обеспечить обучающемуся или одному из его родителей (законному представителю) свободный доступ к ПДн обучающегося, включая право на получение копий любой записи, содержащей его персональные данные;

7. Предоставить по требованию одного из родителей (законного представителя) обучающегося полную информацию о его ПДн и обработке этих данных.

ПДн обучающихся и родителей (законных представителей) хранятся в отдельных папках, созданных для каждого образовательного объединения. На каждого ребенка, зачисленного в образовательную организацию, заводится личное дело, в котором хранятся все сданные документы. Данные содержатся исключительно на бумажных носителях и размещены в специально отведенном шкафу, без каких-либо физических мер защиты.

Личное дело обучающегося имеет следующую структуру:

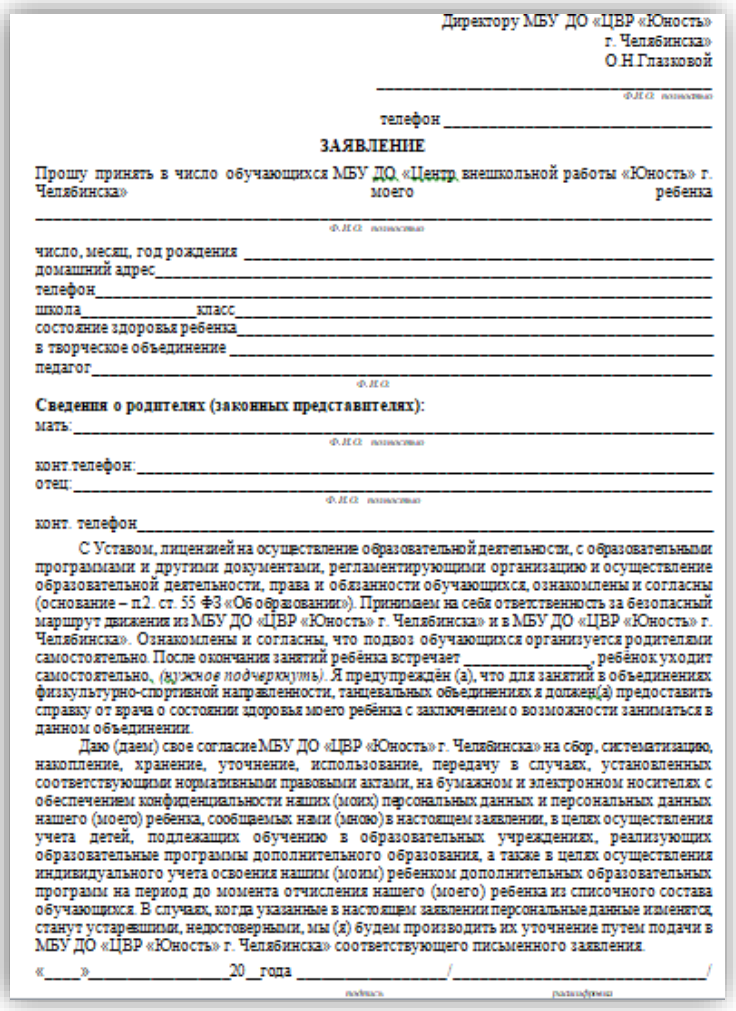
– заявление от родителей на принятие ребенка в число обучающихся, где указывается ФИО ребенка, дата рождения, домашний адрес, телефон,

школа, класс, состояние здоровья ребенка, а также сведения о родителях (законных представителях) (рисунок 5);

– согласие родителей (законных представителей) обучающихся на обработку персональных данных (рисунок 6);

– согласие на фото и видеосъемку несовершеннолетнего (рисунок 7);

– копия свидетельства о рождении, паспорта или иного документа, удостоверяющего личность.



Директору МБУ ДО «ЦВР «Юность»
г. Челябинска»
О.Н.Глазковой

_____
Ф.И.О. полностью

телефон _____

ЗАЯВЛЕНИЕ

Прошу принять в число обучающихся МБУ ДО «Центр внешкольной работы «Юность» г. Челябинска» моего ребенка

_____
Ф.И.О. полностью

число, месяц, год рождения _____
домашний адрес_____
телефон_____
школа_____класс_____
состояние здоровья ребенка_____
в творческое объединение _____
педагог_____
Ф.И.О.

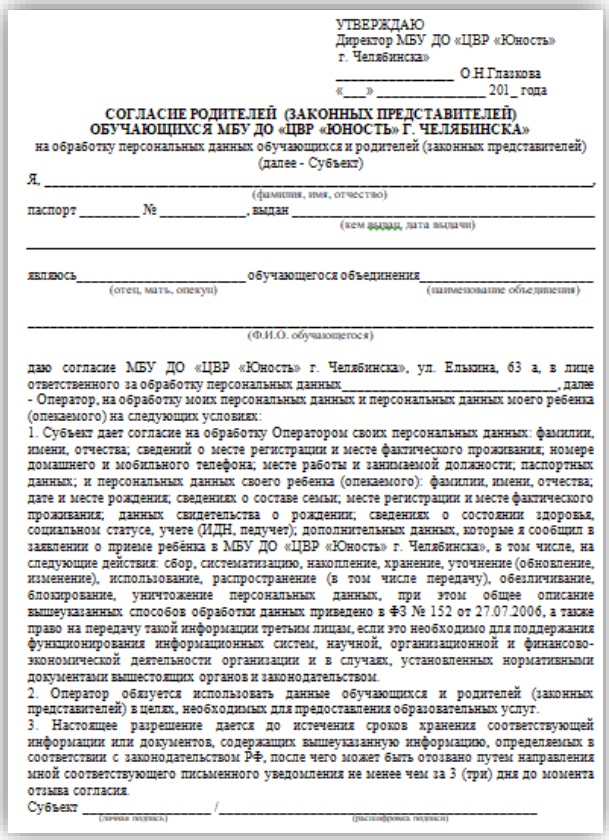
Сведения о родителях (законных представителях):
мать:_____
Ф.И.О. полностью
конт.телефон:_____
отец:_____
Ф.И.О. полностью
конт. телефон_____

С Уставом, лицензией на осуществление образовательной деятельности, с образовательными программами и другими документами, регламентирующими организацию и осуществление образовательной деятельности, права и обязанности обучающихся, ознакомлены и согласны (основание – п2. ст. 55 ФЗ «Об образовании»). Принимаем на себя ответственность за безопасный маршрут движения из МБУ ДО «ЦВР «Юность» г. Челябинска» и в МБУ ДО «ЦВР «Юность» г. Челябинска». Ознакомлены и согласны, что подвоз обучающихся организуется родителями самостоятельно. После окончания занятий ребёнка встречает _____, ребёнок уходит самостоятельно, *(нужное подчеркнуть)*. Я предупреждён (а), что для занятий в объединениях физкультурно-спортивной направленности, танцевальных объединениях я должен(а) предоставить справку от врача о состоянии здоровья моего ребёнка с заключением о возможности заниматься в данном объединении.

Даю (даем) свое согласие МБУ ДО «ЦВР «Юность» г. Челябинска» на сбор, систематизацию, накопление, хранение, уточнение, использование, передачу в случаях, установленных соответствующими нормативными правовыми актами, на бумажном и электронном носителях с обеспечением конфиденциальности наших (моих) персональных данных и персональных данных нашего (моего) ребенка, сообщаемых нами (мною) в настоящем заявлении, в целях осуществления учета детей, подлежащих обучению в образовательных учреждениях, реализующих образовательные программы дополнительного образования, а также в целях осуществления индивидуального учета освоения нашим (моим) ребенком дополнительных образовательных программ на период до момента отчисления нашего (моего) ребенка из списочного состава обучающихся. В случаях, когда указанные в настоящем заявлении персональные данные изменятся, станут устаревшими, недостоверными, мы (я) будем производить их уточнение путем подачи в МБУ ДО «ЦВР «Юность» г. Челябинска» соответствующего письменного заявления.

«____»_____20__года _____/_____/
подпись *расшифровка*

Рисунок 5 – Образец заявления от родителей на принятие ребенка в число обучающихся



УТВЕРЖДАЮ
Директор МБУ ДО «ЦВР «Юность»
г. Челябинска»
_____ О.Н.Глазкова
«___» _____ 201_ года

СОГЛАСИЕ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)
ОБУЧАЮЩИХСЯ МБУ ДО «ЦВР «ЮНОСТЬ» Г. ЧЕЛЯБИНСКА»
на обработку персональных данных обучающихся и родителей (законных представителей)
(далее - Субъект)

Я, _____,
(фамилия, имя, отчество)
паспорт _____ № _____, выдан _____
(кем выдан, дата выдачи)
_____

являюсь_____обучающегося объединения_____
(отец, мать, опекун) (наименование объединения)

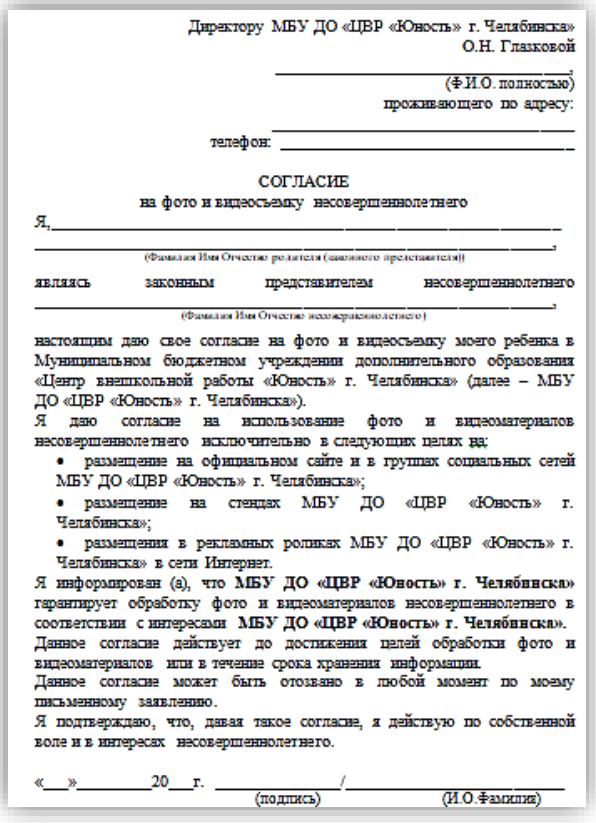
_____
(Ф.И.О. обучающегося)

даю согласие МБУ ДО «ЦВР «Юность» г. Челябинска», ул. Елькина, 63 а, в лице ответственного за обработку персональных данных_____, далее - Оператор, на обработку моих персональных данных и персональных данных моего ребенка (опекаемого) на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных: фамилии, имени, отчества; сведений о месте регистрации и месте фактического проживания; номере домашнего и мобильного телефона; месте работы и занимаемой должности; паспортных данных; и персональных данных своего ребенка (опекаемого): фамилии, имени, отчества; дате и месте рождения; сведениях о составе семьи; месте регистрации и месте фактического проживания; данных свидетельства о рождении; сведениях о состоянии здоровья, социальном статусе, учете (ИДН, педучет); дополнительных данных, которые я сообщил в заявлении о приеме ребёнка в МБУ ДО «ЦВР «Юность» г. Челябинска», в том числе, на следующие действия: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ № 152 от 27.07.2006, а также право на передачу такой информации третьим лицам, если это необходимо для поддержания функционирования информационных систем, научной, организационной и финансово-экономической деятельности организации и в случаях, установленных нормативными документами вышестоящих органов и законодательством.
2. Оператор обязуется использовать данные обучающихся и родителей (законных представителей) в целях, необходимых для предоставления образовательных услуг.
3. Настоящее разрешение дается до истечения сроков хранения соответствующей информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с законодательством РФ, после чего может быть отозвано путем направления мной соответствующего письменного уведомления не менее чем за 3 (три) дня до момента отзыва согласия.

Субъект _____ / _____
(личная подпись) (расшифровка подписи)

Рисунок 6 – Образец согласия родителей обучающихся на обработку ПДн



Директору МБУ ДО «ЦВР «Юность» г. Челябинска»
О.Н. Глазковой
_____,
(Ф.И.О. полностью)
проживающего по адресу:
_____
телефон: _____

СОГЛАСИЕ
на фото и видеосъемку несовершеннолетнего

Я,_____
_____,
(Фамилия Имя Отчество родителя (законного представителя))
являясь законным представителем несовершеннолетнего
_____,
(Фамилия Имя Отчество несовершеннолетнего)

настоящим даю свое согласие на фото и видеосъемку моего ребенка в Муниципальном бюджетном учреждении дополнительного образования «Центр внешкольной работы «Юность» г. Челябинска» (далее – МБУ ДО «ЦВР «Юность» г. Челябинска»).

Я даю согласие на использование фото и видеоматериалов несовершеннолетнего исключительно в следующих целях на:

- размещение на официальном сайте и в группах социальных сетей МБУ ДО «ЦВР «Юность» г. Челябинска»;
- размещение на стендах МБУ ДО «ЦВР «Юность» г. Челябинска»;
- размещения в рекламных роликах МБУ ДО «ЦВР «Юность» г. Челябинска» в сети Интернет.

Я информирован (а), что **МБУ ДО «ЦВР «Юность» г. Челябинска»** гарантирует обработку фото и видеоматериалов несовершеннолетнего в соответствии с интересами **МБУ ДО «ЦВР «Юность» г. Челябинска».**

Данное согласие действует до достижения целей обработки фото и видеоматериалов или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в интересах несовершеннолетнего.

«___»_____20___г. _____/_____
(подпись) (И.О.Фамилия)

Рисунок 7 – Образец согласия на фото и видеосъемку несовершеннолетнего

В процессе обучения личное дело пополняется данными о результатах промежуточной и итоговой аттестаций, документами, подтверждающими достижения в учебе, спорте, иных видах деятельности.

Обработка указанных ПДн допускается в случае, если субъект/родитель (законный представитель) ПДн дал согласие на обработку данных в письменной форме, как представлено на Рисунке 6.

Также в образовательной организации работу с ПДн ведет отдел кадров, на который возложены следующие обязанности:

– документирование трудовых правоотношений организации со штатным и временным персоналом;

– разработка нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации;

– хранение и ведение документации по личному составу, трудовых книжек и личных дел;

– защита персональных данных работников организации.

В состав личного дела входит следующие *документы*:

– личная карточка формы Т-2, которая заводится на каждого работника;

– копии личных документов: паспорта, СНИЛС, ИНН, диплома, военного билета;

– заявление работника о приеме на работу;

– один экземпляр трудового договора и дополнительные соглашения к нему;

– копия приказа о приеме на работу;

– справка о наличии (отсутствии) судимости и (или) факта уголовного преследования;

– медицинская книжка/справки;

Данные работников организации хранятся в личных делах на бумажных носителях в недоступном месте для всеобщего пользования, а именно в

сейфе. Личные дела и трудовые книжки сотрудников хранятся отдельно. Право доступа к личным делам сотрудников имеет лишь ответственное должностное лицо отдела и директор образовательной организации.

С точки зрения технических мер защиты ПДн. Как было выяснено ранее, технические методы защиты персональных данных разделяются на: физические, аппаратные – активные и пассивные, программные. В МБУ ДО «ЦВР "Юность" г. Челябинска» в качестве физических средств защиты используются: замки на дверях, решетки на окнах, сейфы, перед входом в образовательную организацию и кабинеты установлены камеры видеонаблюдения. Также применяются программные меры защиты – антивирусные программы, межсетевой экран Брандмауэр Windows, который фильтрует сетевой трафик между ОС и сетью, к которой подключен компьютер. В данной образовательной организации используется только глобальная сеть Интернет. Локальная вычислительная сеть для обработки персональных данных, сопряженная с Интернет, в образовательной организации - отсутствует.

Из аппаратных средств защиты в образовательной организации ничего не используется.

Рассмотрим применяемое оборудование в работе организации и их количество:

- Персональные компьютеры – 7 шт.;
- Ноутбуки – 2 шт.;
- Маршрутизатор D-Link модель - DIR300 – 2 шт.

3.2 Разработка комплекса предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации для МБУ ДО «ЦВР "Юность" г. Челябинска»

На основе анализа существующих мер защиты, проведенного в пункте 3.1, было выявлено, что присутствуют некоторые уязвимости в обеспечение защиты персональных данных в МБУ ДО «ЦВР "Юность" г. Челябинска»,

поэтому было принято решение по разработке комплекса предложений для совершенствования системы защиты персональных данных.

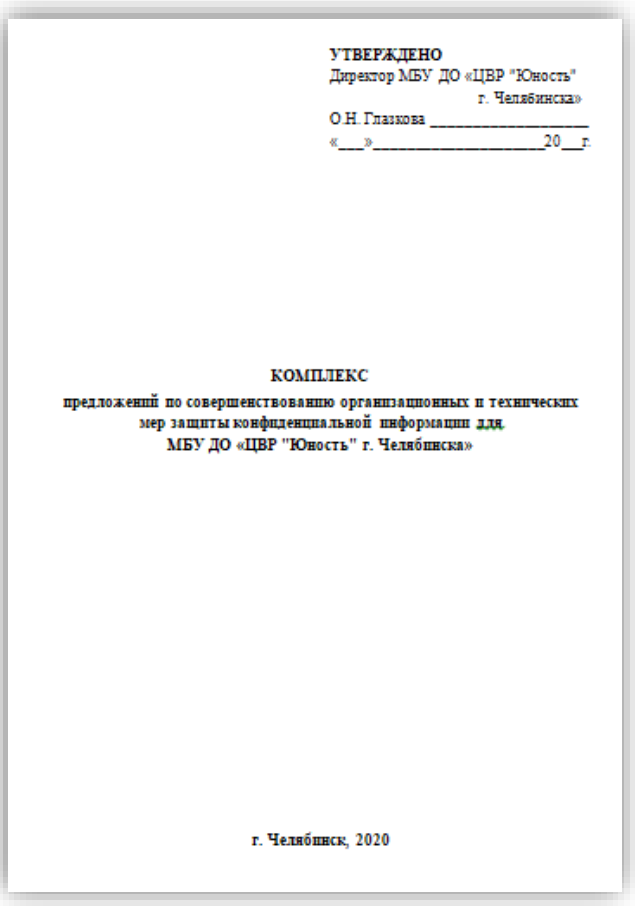
Для устранения недостатков в существующей системе защиты ПДн, необходимо предложить образовательной организации усовершенствовать организационные, технические и физические меры.

Следовательно, в этом подпункте исследовательской работы будет представлено описание разработки, перечислены предложенные меры совершенствования, даны рекомендации по применению разработанных предложений. Комплекс предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации прилагается к исследовательской работе.

Комплекс написан для практического использования в деятельности образовательного учреждения наиболее интересных и эффективных решений по организации системы защиты персональных данный. В Комплексе предложены меры по совершенствованию организационных и технических мер, даны рекомендации по их внедрению, а также представлены разнообразные программные продукты и технологические решения, которые можно использовать в образовательной деятельности.

Материалы Комплекса позволят рассмотреть различные варианты организации СЗПДн в образовательном учреждении. Это использование безбумажного документооборота, организация локальной сети, вопросы информационной защиты, защиты персональных данных.

Рассмотрим структуру разработанного документа. Первым идёт титульный лист, представленный на рисунке 8.



УТВЕРЖДЕНО
Директор МБУ ДО «ЦВР "Юность"
г. Челябинска»
О.Н. Глазкова _____
«___»_____20__г.

КОМПЛЕКС
предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации для МБУ ДО «ЦВР "Юность" г. Челябинска»

г. Челябинск, 2020

Рисунок 8 – Титульный лист Комплекса предложений

Далее:

1. Определения
2. Введение
3. Общие положения
4. Цель и задачи комплекса
5. Объект защиты
6. Субъекты информационных отношений
7. Возможные угрозы и участки вторжения
8. Совершенствование организационных мер защиты ПДн
9. Совершенствование технических мер защиты ПДн
10. ИСПДн
11. Организация локальной сети
12. Приложение №1 - Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
13. Приложение №2 - Инструкция по компьютерной безопасности.

Рассмотрим некоторые структурные элементы подробнее.

Цели и задачи комплекса:

1. Основными целями являются:

– сохранение конфиденциальности критичных информационных ресурсов, а именно персональных данных;

– повышение уровня технических и организационных мер защиты ПДн;

– обеспечение непрерывности доступа к ПДн образовательной организации;

– повышение осведомленности сотрудников в области рисков, связанных с ПДн образовательной организации;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности ПДн.

– повышение уровня эффективности, непрерывности, контролируемости организационных и технических мер по защите от реальных угроз ПДн;

– предотвращение и/или снижение ущерба от инцидентов ИБ.

2. Основными задачами комплекса предложений являются:

– улучшение организационного и технического уровня защиты ПДн;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты ПДн;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

– организация ИСПДн в образовательной организации;

– организация локальной сети;

– организация антивирусной защиты информационных ресурсов школы;

– введение в СЗПДн новые нормативные документы для обеспечения безопасности ПДн;

– защита информации образовательной организации от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи.

Объект защиты

Объектом защиты являются персональные данные работников и обучающихся образовательной организации:

1. информационные ресурсы:

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

– инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

2. технические информационные системы и средства Организации, в которых обрабатывается, хранится и передается информация ПДн;

3. помещения объектов Организации, в которых размещаются информационные ресурсы, и обрабатываются ПДн;

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

Субъекты информационных отношений

1. Субъектами информационных отношений являются:

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

– *Сотрудники* (субъекты персональных данных) - физические лица, состоящие или готовящиеся вступить в трудовые или иные гражданско-правовых отношениях с Организацией-оператором.

2. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;

– достоверности (полноты, точности, адекватности, целостности) информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

– своевременного доступа (за приемлемое для них время) к необходимой им информации;

– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

– защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

Далее, рассмотрим Приложение №2 - Инструкция по компьютерной безопасности:

1. Регулярно, не менее 1 раз в неделю производить обновления операционной системы Windows (http://update.microsoft.com), если это не производится автоматически. Сообщение о наличии обновлений обычно появляется в виде значка на панели задач.

2. Встроенный брандмауэр Windows должен быть активирован.

3. Ежедневно проверять состояние антивирусного программного обеспечения, а именно:

– режим автоматической защиты должен быть включен постоянно;

– дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;

– просматривать журналы ежедневных антивирусных проверок;

– контролировать удаление вирусов при их появлении.

4. При работе с электронной почтой категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц файлы. Контролировать посещение Интернет сайтов пользователями.

5. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними (автозагрузка со сменных носителей информации на компьютере должна быть отключена).

6. Не запускать файлы, попавшие на ваш компьютер независимо из какого источника (Интернет; P2P сети; почта), предварительно не проверив их антивирусом (это же касается и архивов).

7. Регулярно проводить сохранение рабочих документов на внешние носители (не реже 1 раз в неделю). Либо настроить автоматическое сохранение важных папок на компьютере с помощью специальной программы (указываем имя программы).

8. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от локальной сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера.

9. При появлении аналогичных признаков после проделанной процедуры пригласить специалиста в области компьютерной безопасности для дальнейших действий.

Для устранения существующих недостатков в разработанном комплексе *предложены следующие меры* защиты ПДн для образовательной организации:

1. Организационные

1.1. Создать рабочую группу. Поскольку главным условием защиты персональных данных является четкая регламентация функций сотрудников. Рабочей группой проводятся следующие мероприятия: уточняются все ситу-

ации, когда требуется проводить обработку ПДн, четко выделяются процессы, в которых обрабатываются ПДн, продумывается разработка, принятие пакета организационно-распорядительных документов для обеспечения полноценной защиты. Также следует разработать положение о подразделении (рабочей группе), должностные инструкции работников подразделения;

1.2. Разработать новую инструкцию о конфиденциальном делопроизводстве, устанавливающую порядок составления, оформления конфиденциальных документов, конфиденциального документооборота, контроль исполнения конфиденциальных документов, согласования документов, ведения делопроизводства. Ознакомить всех сотрудников организации;

1.3. Разработать единые правила работы с документами, которые содержат персональные данные;

1.4. Обучить сотрудников правилам работы с документами, которые содержать персональные данные;

1.5. Проводить ежегодное тестирование по правилам обращения с персональными данными;

1.6. Особое внимание следует обратить на обучение педагогов, которые работают с персональными данными, собирают их у обучающихся и их родителей (законных представителей), именно эти люди часто находятся в ситуациях, благоприятных для утечки информации. Они должны быть четко проинструктированы;

1.7. Обучить лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

1.8. Исходя из предыдущего пункта, разработать инструкцию по работе пользователей в ИСПДн;

1.9. Разработать Требования по обеспечению безопасности ПДн при их обработке в ИСПДн;

1.10. Разработать для каждого АРМ инструкцию по вопросам безопасности. На каждом рабочем месте в образовательном учреждении должна находиться на видном месте инструкция, с помощью которой пользователь

всегда будет оповещен о правилах безопасной работы с информацией и средствами вычислительной техники и Интернет (пример данной инструкции был представлен ранее, в структурных элементах Комплекса);

1.11. Вести только электронный вариант трудовой книжки. В данном случае бумажный документ будет выдан на руки работнику с соответствующей записью. А работодатель больше не будет нести ответственность за бумажный документ;

1.12. Разработать Положение о локальной информационной сети МБУ ДО «ЦВР "Юность" г. Челябинска»;

1.13. Разработать акт классификации информационной системы персональных данных.

2. Технические

– *программные:*

2.1 Перейти с бумажного ведения ПДн на автоматизированные информационные системы ПДн или электронные базы данных, с организацией доступа по паролю;

2.2 Организовать локальную сеть, которая поможет в формирование файлообменной сети, автоматизации управления образовательным учреждением и организации безбумажного документооборота;

2.3 Исходя из предыдущего пункта, в целях обеспечения информационной безопасности, внутренняя сеть и глобальная сеть Интернет должны быть разделены;

2.4 Для локальной сети использовать программу SkyDNS, которая работает как веб-сервис, блокируя доступ к опасным сайтам еще до реального обращения к их ресурсам;

2.5 Своевременно обновлять средства антивирусной защиты;

2.6 Использовать вспомогательные программы для обеспечения защиты своего компьютера. Одна из наиболее популярных программ Spybot - Search & Destroy (Спайбот - найти и уничтожить) поможет обнаруживать и

удалять с компьютера различного рода шпионское программное обеспечение;

2.7 Отключить возможность автозапуска и автозагрузки на компьютере, эти функции используют вирусы, которые приходят с помощью носителей информации. Это легко можно сделать, воспользовавшись программой Autorun Guard. Это бесплатная программа для управления автозапуском на внешних носителях в ОС Windows;

2.8 Архивировать персональные данные. Особенно важно работая с базами данных, с целью сохранения информации необходимо регулярно сохранять копию этой информации на отдельном жестком диске или удаленном компьютере;

2.9 Оптимизировать операционную систему и наиболее часто используемые программы. Например, программа Xp-AntiSpy поможет изменить некоторые настройки операционной системы Windows и пакета программ Microsoft Office с целью отключения не нужных в работе сервисов, в частности: автозагрузки, ограничение количества ПК в локальной сети, отчетов об ошибках, работы с мультимедиа и другое;

– *физические*

2.10 Обеспечить помещения, где хранятся ПДн, сейфом или металлическими шкафами для хранения документов;

2.11 На окнах необходимо повесить жалюзи или светонепроницаемые шторы.

Далее, в разработанном комплексе даны рекомендации по выбору ИСПДн и созданию локальной сети.

При выборе ИСПДн рекомендую обратить внимание на следующие варианты:

1. Автоматизированная информационная система управления «Параграф» - это основа информационного пространства образовательного учреждения. В состав АИСУ «Параграф» входит серверная часть базах данных которой хранится и обрабатывается информация об обучающихся, сотрудни-

ках, образовательной программе, зданиях и помещениях и другие данные, и клиентские части, составляющие автоматизированные рабочие места (АРМ) сотрудников ОУ.

Регламент работы пользователей, организационно-технические условия для установки и эксплуатации программного комплекса «Параграф», требования, связанные с достоверностью, актуальностью и защитой данных, основываются на нормативно-правовой базе и общих требованиях для работы с программным комплексом АИСУ «Параграф».

АИСУ «Параграф» может иметь следующие исходные данные классификации ИСПДн:

- Структура ИСПДн - Локальная информационная система;
- Наличие подключений к ССОП и сетям МИО (Интернет) - Отсутствует;
- Режим обработки ПДн - Однопользовательский;
- Разграничение доступа пользователей - С разграничением прав пользования;
- Нахождение ИСПДн (ее составных частей) в пределах России - Все технические средства находятся на территории Российской Федерации.

2. 1С: ХроноГраф - информационная система администрирования деятельности образовательного учреждения. Программа предоставляет широкие возможности для:

- создания базовой информации, включая информацию общего доступа и периодизированных компонентов;
- автоматизации кадровой работы;
- систематизации данных об обучающихся;
- администрирования учебно-воспитательного процесса;
- поддержки содержания образования;
- автоматизации финансовой и хозяйственной деятельности образовательного учреждения.

В целях обеспечения защиты персональной информации в программе предусмотрены возможности:

- выгрузки базы данных только с паролем;
- заполнения, хранения и ведения листов согласия сотрудников и обучающихся.

Преимущество данное ИС, это наличие лицензия на программное обеспечение «1С: ХроноГраф». Владелец: Закрытое акционерное общество «1С Акционерное общество». Данная лицензия разрешает, безвозмездно, представителям общеобразовательных учреждений Российской Федерации, получившим копию данного программного обеспечения и сопутствующей документации (в дальнейшем именуемыми "Программное Обеспечение"), использовать Программное Обеспечение без ограничений.

3. Также можно создать собственную Базу данных в СУБД Access, задать свои параметры, без лишних затрат на ПО, программа MS ACCESS входит в стандартный пакет Microsoft Office.

Также преимущество данной программы в том, что СУБД Access входит в состав пакета Microsoft Office и имеет лицензию.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;
- ввод в эксплуатацию;
- закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;

– угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

Для разработки акта классификации ИСПДн, необходимо рассмотреть исходные данные о созданной информационной системе ПДн и определить:

– категорию и объем персональных данных;

– структуру информационной системы (автономная, локальная информационная система, распределенная информационная система);

– наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена (да или нет);

– режим обработки персональных данных (многопользовательский или однопользовательский);

– режим разграничения прав доступа пользователей информационной системы (без разграничения прав доступа или с разграничением прав доступа);

– местонахождение технических средств (в пределах российской федерации).

На основе этих данных и в соответствии с пунктами 14 и 15 «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК России, ФСБ России, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 комиссией будет установлен класс для ИСПДн.

При организации локальной сети даны следующие предложения.

При выборе сети должны учитываться такие факторы:

– финансы, выделенные на прокладывание сети и сетевое оборудование;

– предположительная загруженность сети;

– необходимость общего хранилища данных;

– количество компьютеров работающих в сети;

– компактное расположение пользователей;

– глобальное расширение сети в будущем (требуется/нет);

– вопрос защиты данных.

Исходя из вышеперечисленных факторов и анализа применяемого оборудования в образовательной организации в пункте 3.1, был предложен тип локальной сети - одноранговая сеть смешанного типа с использованием беспроводных модулей (часть клиентов подключены через кабель, а остальные подключены к сети через Wi-fi), так как в организации есть, помимо стационарных компьютеров, и ноутбуки.

Одноранговой сеть исключает присутствие сервера. Поскольку каждый компьютер является одновременно и клиентом, и сервером, нет необходимости в мощном центральном сервере или в других компонентах, обязательных для более сложных сетей, значит нет необходимости включать его в сеть и тратить финансы и время.

Для объединения компьютеров в одноранговую сеть достаточно только создать структуру сети (провести кабели или купить беспроводные точки доступа, поставить коммутаторы и другое оборудование). Компьютер необходимо подключить к сети и настроить на использование ресурсов других систем. В свою очередь администратор каждого компьютера определяет, какие ресурсы локальной системы предоставляются в общее пользование, а какие нет, и с какими правами.

При установке одноранговой сети, дополнительного программного обеспечения не требуется. Удобность одноранговой сети характеризуется рядом стандартных решений:

– компьютеры расположены на рабочих столах пользователей;

– пользователи сами выступают в роли администраторов и обеспечивают защиту данных.

Рекомендуемые этапы настройки локальной сети:

1. Установку и настройку необходимо начинать с настройки главного маршрутизатора, он же DHCP сервер. DHCP (Dynamic Host Configuration Protocol) - это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети;

2. Для настройки необходимо подключить кабель интернета в порт WAN - порт, а кабель, идущий к компьютеру, в порт “LAN”. После этого необходимо зайти в любой интернет браузер на компьютере подключенному к маршрутизатору и в строке адреса прописать “192.168.0.1” или “192.168.1.1”, после чего появится запрос авторизации, логин и пароль можно посмотреть на роутере, либо в документации роутера идущей в комплекте (в основном на всех роутерах логин - “admin”, пароль - “admin”). Далее в зависимости от вашего провайдера выставляется тип подключения WAN;

3. В данном случае провайдер осуществляет статическое подключение, значит необходимо заполнить соответствующие поля. После того как прописаны IP адреса, маска, шлюз и DNS сервера, необходимо настроить DHCP. Для этого в одноименном разделе включаем функцию DHCP и прописываем диапазон IP адресов, которые будут раздаваться клиентам задействованных в сети. Например: 192.168.1.50 - 192.168.1.150. После этих настроек главный маршрутизатор (DHCP сервер) готов к работе;

4. После настройки главного маршрутизатора, для удобности, необходимо настроить остальные маршрутизаторы (они будут работать как точки доступа, а именно будут передавать информацию с главного маршрутизатора на компьютеры по сети wifi или по кабелю), они будут сразу после всех необходимых настроек подключены к коммутаторам и компьютерам;

5. Настраиваем маршрутизаторы D-Link модель DIR-300. Для того чтобы зайти в меню настроек данных маршрутизаторов, необходимо прове-

сти такие же действия, какие были необходимы для входа в меню настроек главного маршрутизатора. После этого настраивается тип интернет соединения. Так как у нас уже настроен выход в интернет на главном маршрутизаторе, то выбираем тип подключения - статический IP. Это значит, что маршрутизатор будет принимать все адреса и передавать дальше полученные от главного маршрутизатора;

6. Функцию DHCP необходимо отключить, так как в роли DHCP сервера выступает главный маршрутизатор. В пункте “IP маршрутизатора” для удобности дальнейшего управления выставляем IP адрес по номеру кабинета, в котором будет находится сам роутер. Если в дальнейшем нам будет их необходимо перенастроить, то мы сможем зайти в меню настроек с любого компьютера введя их IP адрес в адресную строку браузера и пройти после этого соответствующую авторизацию;

7. Так как данная сеть смешанного типа (проводная и беспроводная), то на маршрутизаторах обязательно настраивается wifi, а именно устанавливается парольная защита и изменяется имя сети на номер кабинета, в котором находится сам маршрутизатор;

8. В разделе “Настройка беспроводной сети” прописываем имя сети wifi одноименное номеру кабинета, далее выбираем режим безопасности “wpa/wpa2psk” и вводим пароль на саму сеть wifi.

9. После всех проведенных настроек на роутерах, они готовы к работе в сети;

10. Когда все элементы сети настроены, необходимо начать подключение сети. Подключение устройств желательно начинать с самого первого элемента сети ввиду удобства. Первым устройством является главный маршрутизатор, как описывалось ранее кабель интернета подключается в порт WAN порт, а кабель идущий подключается в порт LAN.

11. Следующий элемент сети - это концентратор, который отвечает за объединение нескольких устройств сегмента сети. Подключение кабеля идущего от главного маршрутизатора и подключение кабелей идущих к следу-

ющим элементам сети безразлично. Это связано с тем, что концентратор не программируемый. Аналогично и со следующими концентраторами.

12. Так как маршрутизаторы настроены как точки доступа, а именно как описано ранее отключен DHCP, а тип подключения стоит динамический IP, то кабель идущий от концентраторов и главного маршрутизатора подключается так же как и кабель идущий на следующие элементы сети (либо следующий маршрутизатор, либо компьютер) в LAN порт.

13. После всех действий сеть готова к работе, остается подключение компьютеров (по кабелю от точек доступа) и ноутбуков (по беспроводной сети).

Исходя из ситуации, и в целях совершенствования системы защита персональных данных в локальной сети, необходимо применение, например, такой программы как SkyDNS, которая является настоящим "облачным" решение. Программа работает как веб-сервис, блокируя доступ к опасным сайтам еще до реального обращения к их ресурсам.

В большинстве случаев не приходится ставить какое-либо ПО на компьютеры пользователей. Все, что потребуется - настроить параметры сети интернет-шлюза, и указать категории для блокировки на сайте. Кроме того, SkyDNS имеет небольшую себестоимость. Стоимость годовой подписки на услуги фильтрации составляет ≈ 300 рублей за компьютер.

Для того чтобы начать использовать сервис DNS-фильтрации SkyDNS необходимо:

– определить какие настройки фильтрации требуются - одинаковые или различные для каждого компьютера (группы компьютеров). В данном случае подойдут одинаковые настройки фильтрации;

– выяснить какой внешний IP адрес предоставил провайдер - статический или динамический. Как было выяснено ранее, провайдер образовательной организации предоставляет статический IP адрес;

– определить каким образом получают сетевые настройки компьютеры (по DHCP или прописаны вручную). В сеть включен DHCP сервер, значит, прописывать адреса вручную не приходится;

– привязать внешний статический IP адрес к профилю в аккаунте SkyDNS;

– использовать для разрешения внешних DNS-имен DNS-сервер SkyDNS 193.58.251.251.

Предлагаемый фильтр SkyDNS получил высшую награду Gold Parental Control лаборатории AntiMalware.ru. Интернет-фильтр продемонстрировал результаты, сравнимые с показателями лидера - разработками Лаборатории Касперского.

3.3 Оценка эффективности комплекса организационных и технических мер защиты конфиденциальной информации для МБУ ДО «ЦВР "Юность" г. Челябинска»

На сегодняшний день документы по защите конфиденциальной информации содержат требования, предъявляемые к тому или иному ее виду, но при этом не дают конкретных методик проверки выполнения этих требований (методик оценки эффективности защиты информации). В соответствии с современной теорией оценки эффективности систем качество любого объекта (в том числе и систем защиты информации – СЗИ) проявляется лишь в процессе использования по назначению, поэтому наиболее объективно оценивание по эффективности применения. При этом всегда имеются элементы неопределенности, поэтому эффективность СЗИ невозможно достоверно оценить с помощью одного критерия (показателя). Соответственно, введение множества критериев (показателей) будет характеризовать эффективность защиты наиболее полно.

Процесс определения эффективности СЗИ начинают с выбора и обоснования критериев, а затем переходят к подбору или разработке методик рас-

чета показателей эффективности. На практике используются следующие виды критериев [45]:

– типа «эффект–затраты», характеризуемые соотношением затрат на реализацию механизма защиты и полученного эффекта (экономическая эффективность);

– позволяющие оценивать качество СЗИ;

– позволяющие определить достаточность применяемых мер защиты.

В настоящий момент методики расчета показателей эффективности в нормативных документах не описаны. Соответственно решение данной задачи может производиться с помощью различных методов:

– методы моделирования процессов защиты информации;

– экспертные оценки;

– статистический анализ;

– метод минимизации рисков и т. д.

Ни один из методов не лишен недостатков, поэтому на практике можно их комбинировать.

Для своей исследовательской работы я выбрала метод экспертной оценки. Метод экспертной оценки является таким методом, в котором респондентами являются эксперты — специалисты в определенной области деятельности. Основное назначение метода экспертной оценки — выявление сложных аспектов исследуемой проблемы, повышение надежности информации, выводов.

Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения.

Экспертная оценка эффективности комплекса предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации проводилась на базе МБУ ДО «ЦВР "Юность" г. Челябинска».

В процессе проведения экспертизы, комплекс предложений оценивался по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанного комплекса требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных;

2. Методическая составляющая комплекса предложений: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн;

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений;

4. Системная составляющая: при создании комплекса предложений учитывались все слабые и наиболее уязвимые места существующей системы обработки ПДн.

5. Комплексная составляющая: согласованное применение разнородных средств, при построении целостной системы защиты, не содержащей слабых мест на стыках отдельных ее компонентов.

Данные критерии были преобразованы в инструментарий в виде информационно-оценочной карты комплекса предложений, которая представлена в Таблице 1.

Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Таблица 1 – Показатели оценки эффективности комплекса предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации

Показатели оценки эффективности	**Эксперты**		
	Эксперт 1	*Эксперт 2*	*Эксперт 3*
	Критерии качества эффективности: – высокий уровень (полностью соответствует показателю) – средний уровень (в основном соответствует показателю) – низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанного комплекса требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных			
2. Методическая составляющая комплекса предложений: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн			
3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений			
4. Системная составляющая: при создании комплекса предложений учитывались все слабые и наиболее уязвимые места существующей системы обработки ПДн			

5. Комплексная составляющая: согласованное применение разнородных средств, при построении целостной системы защиты, не содержащей слабых мест на стыках отдельных ее компонентов			
Итоговая оценка экспертов:			

В нашем случае было решено использовать следующую шкалу: высокий, средний, низкий уровни выраженности показателей эффективности комплекса предложений.

Каждому эксперту предлагался комплекс предложений по совершенствованию мер защиты конфиденциальной информации и информационно-оценочный лист с одинаковыми показателями оценки, по которому и производилась оценка эффективности.

По итогам оценки эксперт представляет отчет, который содержит следующие сведения:

– заполненную информационно-оценочную карту;

– общие выводы.

В состав экспертной комиссии вошли: руководитель образовательной организации, заместитель директора по УВР, системный администратор МБУ ДО «ЦВР "Юность" г. Челябинска».

Таблица – 2 Результаты экспертной оценки эффективности комплекса предложений

Показатели оценки эффективности	**Эксперты**		
	Эксперт В.А.	*Эксперт М.В.*	*Эксперт А.Н.*
	Критерии эффективности: – высокий уровень (полностью соответствует показателю) – средний уровень (в основном соответствует показателю) – низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанного комплекса требованиям	Высокий уровень	Высокий уровень	Высокий уровень

действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных			
2. Методическая составляющая комплекса предложений: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн	Высокий уровень	Высокий уровень	Высокий уровень
3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений	Средний уровень	Высокий уровень	Высокий уровень
4. Системная составляющая: при создании комплекса предложений учитывались все слабые и наиболее уязвимые места существующей системы обработки ПДн	Высокий уровень	Высокий уровень	Высокий уровень
5. Комплексная составляющая: согласованное применение разнородных средств, при построении целостной системы защиты, не содержащей слабых мест на стыках отдельных ее компонентов	Высокий уровень	Высокий уровень	Высокий уровень
Итоговая оценка экспертов:	Высокий уровень эффективности комплекса предложений		

Результаты обработки оценок эффективности каждого эксперта представлены на рисунках 9 - 11.

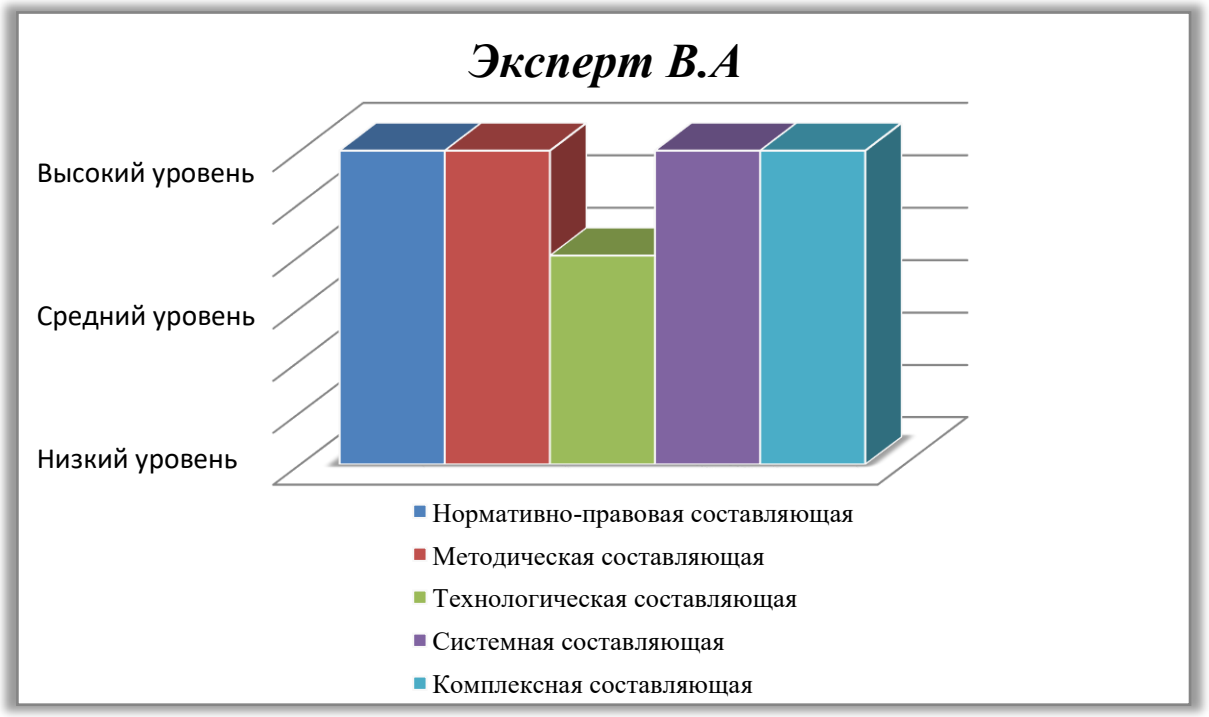


Рисунок 9 – Результаты обработки данных информационно-оценочной карты эксперта В.А.

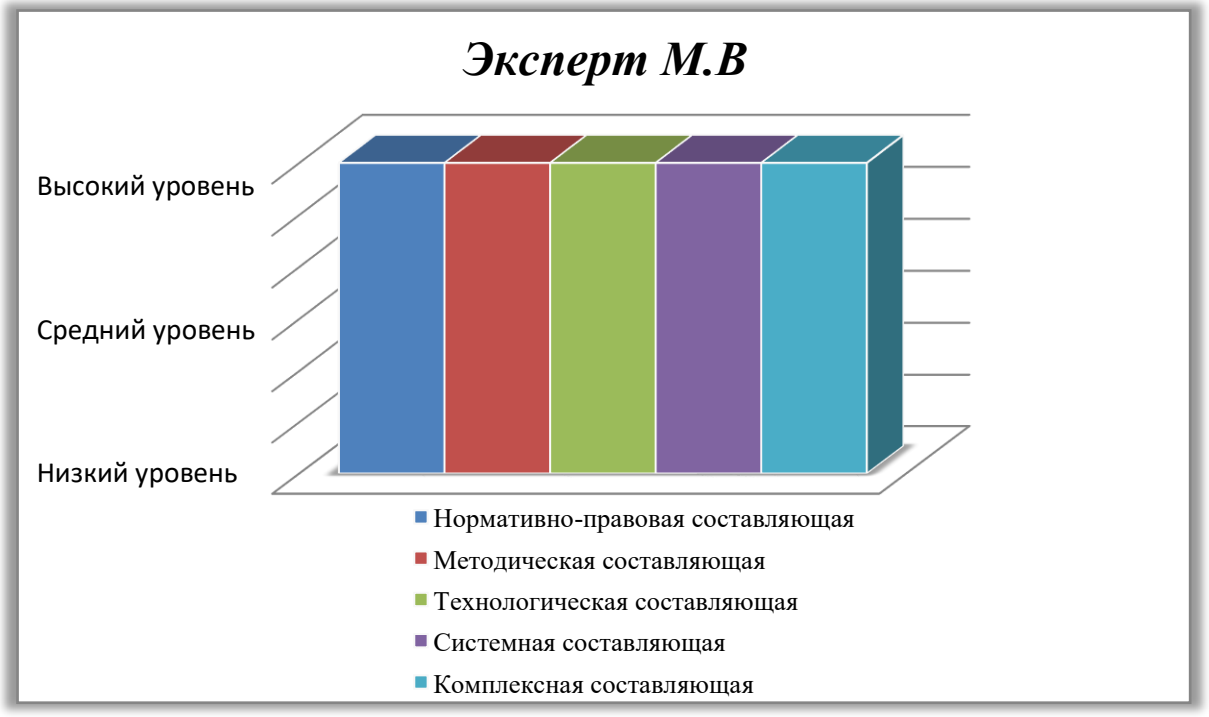


Рисунок 10 – Результаты обработки данных информационно-оценочной карты эксперта М.В.

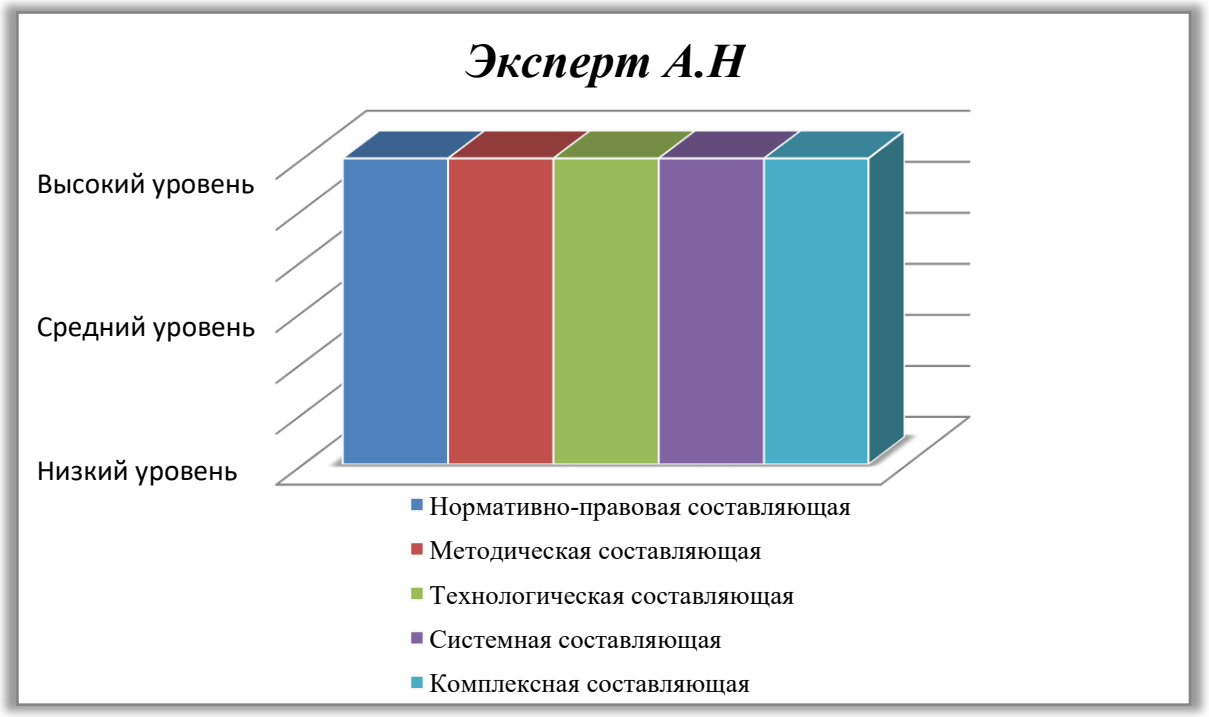


Рисунок 11 – Результаты обработки данных информационно-оценочной карты эксперта А.Н.

Результаты экспертной оценки эффективности чётко видны на результирующей диаграмме, представленной на Рисунке 12.

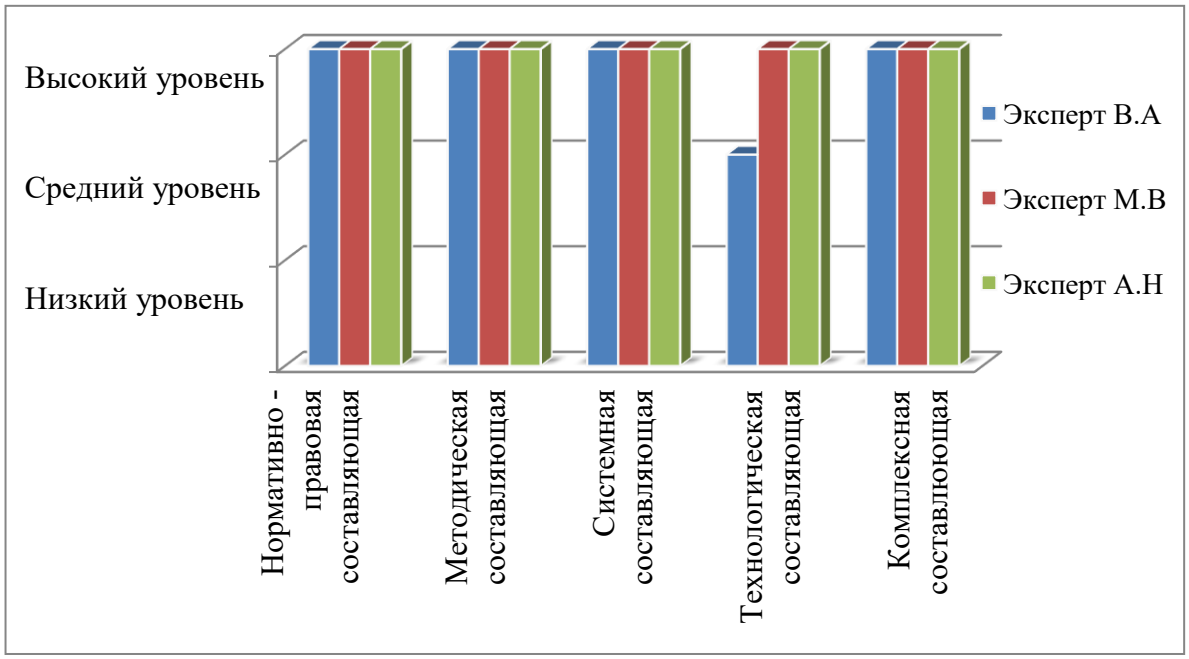


Рисунок 12 – Сводные результаты экспертной оценки эффективности комплекса предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации

Проведенный анализ позволяет сделать вывод, что мнения экспертов относительно совпадают. В то же время, стоит отметить расхождение мнений по технологической составляющей. Расхождение мнений у некоторых экспертов достигает максимум 1балла.

Исходя из результатов экспертизы, можно судить о высоком качестве разработанного комплекса предложений по совершенствованию системы защиты ПДн.

По результатам экспертной оценки эффективности, Комплекс предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации находится в стадии внедрения в инструктивные материалы МБУ ДО «ЦВР "Юность" г. Челябинска».

Выводы по главе 3

В третьей главе исследовательской работы проведет анализ существующих мер и средств защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска», в ходе которого был сделать вывод о необходимости совершенствования конфиденциального делопроизводства с учетом всех рекомендаций и факторов по их внедрению.

Далее, в третьей главе представлена структура разработанного комплекса предложений по совершенствованию системы защиты ПДн, перечислены предложенные меры совершенствования, даны рекомендации по применению разработанных предложений.

В ходе оценки эффективности, при помощи метода экспертной оценки, были рассмотрены такие показатели качества как:

1. Нормативно-правовая составляющая: соответствие разработанного комплекса требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных;
2. Методическая составляющая комплекса предложений: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПДн;
3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений;
4. Системная составляющая: при создании комплекса предложений учитывались все слабые и наиболее уязвимые места существующей системы обработки ПДн.
5. Комплексная составляющая: согласованное применение разнородных средств, при построении целостной системы защиты, не содержащей слабых мест на стыках отдельных ее компонентов;

С помощью этих показателей было проверено качество разработанного комплекса предложений. Экспертная оценка показала, что эффективность комплекса предложений по совершенствованию мер защиты конфиденциальной информации соответствует высокому уровню.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации по теме «Защита конфиденциальной информации в образовательной организации» в соответствии с целью были поставлены и решены ряд задач. Во-первых, были изучены понятия, свойства, аспекты безопасности информации, исследованы основные источники правового регулирования конфиденциальной информации, было выяснено, что Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите и информации" напрямую относит к категории конфиденциальной информации *персональные данные*. Также важным является Федеральный закон № 152-ФЗ от 27 июля 2006 "О персональных данных", в котором регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ.

Во-вторых, рассмотрены организация доступа и порядок работы персонала с конфиденциальной информацией в образовательной организации; выявлены угрозы и меры по предупреждению утечки конфиденциальной информации. Было выявлено, что для решения проблемы сохранности конфиденциальной информации необходимо применение законодательных, организационных и программно-технических мер. Игнорирование хотя бы одного из аспектов этой проблемы может привести к утечке. Обеспечение информационной безопасности - комплексная задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как сотрудники, электронное оборудование, программное обеспечение и другое.

В-третьих, проведет анализ мер и средств защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска», разработан комплекс предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации. При разработке руководствовались результатами анализа существующей системы защиты конфиденциаль-

ной информации в образовательной организации и требованиями обеспечения качественного уровня безопасности ПДн.

И наконец, провели экспертную оценку эффективности комплекса организационных и технических мер защиты конфиденциальной информации для МБУ ДО «ЦВР "Юность" г. Челябинска».

Согласно результатам проведения экспертизы эффективности комплекса предложений, можно сделать вывод, что выставленные оценки по всем показателя, говорят о высоком качестве разработанных предложений по совершенствованию мер защите конфиденциальной информации для МБУ ДО «ЦВР "Юность" г. Челябинска».

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

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

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

Цель, заявленную в магистерской диссертации, можно считать достигнутой, а задачи – выполненными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно – правовые акты

1. Конституция Российской Федерации: офиц. текст. - М.: Право, 2002. - 39 с.

2. Гражданский кодекс Российской Федерации: ФЗ от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. - 2006. - №52. Ч. 1. Ст. 5496

3. Доктрина информационной безопасности Российской Федерации от 09.09.2000: утверждена Президентом РФ В. Путиным // Известия. - 10 декабря 2002. - С.2

4. О государственной тайне: ФЗ по состоянию на 22.08.2004. / Федер. Собр. Рос. Федерации. - М.: ГД РФ, 2004. - 12 с.

5. О коммерческой тайне: ФЗ от 29 июля 2004 № 98 // Собрание актов Президента и Правительства РФ. - № 7. - С.5.

6. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. - № 7. - 2006. - С.15.

7. Об архивном деле в Российской Федерации: ФЗ от 01 октября 2004 № 125 - ФЗ // Собрание актов Президента и Правительства РФ. - № 11. - С.12.

8. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. - №31

9. Об утверждении Перечня сведений конфиденциального характера от 06.03.97 № 188: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 23. С.12 - 14.

10. Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну: постановление правительства РФ от 03.10.2002 № 731 // Собрание актов Президента и Правительства РФ. - 2003. - № 11. - 140 с.

11. Об утверждении положения о государственной системе защиты информации от иностранной технической разведки и от ее утечки по техническим каналам от 15.09.93 № 912 - 51: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 15. - 125 с.

12. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 2002. - № 8. - С.102.

13. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. URL - https://base.garant.ru/192223/. Дата обращения: 21.03.2020

14. Об утверждении правил оказания услуг телеграфной связи: постановление Правительства РФ от 15 апреля 2005г. № 222 // Собрание актов Президента и Правительства РФ. - 2005. - № 5. - С.45.

15. Об утверждений Перечня сведений, отнесенных к государственной тайне от 30.11.95 № 1203: с измен. и доп. от 24.01.98 № 61, от 06.06.2001 № 659, от 10.09.2001 № 1114, от 29.05.2002 № 518, от 11 февраля 2006: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 2006. - № 11.

16. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства РФ от 3 ноября 1994 г. № 1233. // Собрание актов Президента и Правительства РФ. - 1995. - № 10. - С.56.

17. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). URL - https://clck.ru/B8yGj. Дата обращения: 14.04.2020

18. ГОСТ Р 51141. - 98. Делопроизводство и архивное дело. Термины и определения. - М.: Изд-во стандартов, 2003.

19. ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения. - М.: Изд-во стандартов, 1993.

20. ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения. - М.: Изд-во стандартов, 2004.

21. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. - М.: Изд-во стандартов, 1996.

Литература

22. Алексенцев А.И. Конфиденциальное делопроизводство / А.И. Алексенцев. - М.: ООО "Журнал "Управление персоналом", 2013. - 200 с.

23. Алексенцев А.И. Организация и технология размножения конфиденциальных документов / А.И. Алексенцев. - 2013. - № 4. - С.12 - 14.

24. Андреева В.И. Делопроизводство: практ. пособие / В.И. Андреева. - изд.10-е, перераб. и доп. - М.: ООО "Управление персоналом", 2015. - 196 с.

25. Антопольский А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореферат дис. канд. юрид. наук. - М. - 2014.

26. Аутентификация как средство защиты информации в корпоративных информационных системах / Л.А. Сысоева // Секретарское дело. - 2015. - № 1. - С.58 - 64.

27. Бабкин В.В. Модель нарушителя информационной безопасности - превенция появления самого нарушителя // В.В. Бабкин // Управление в кредитной организации. - 2016. - № 5.

28. Бачило И.Л. Концептуальные основы правового обеспечения информатизации России / И.Л. Бачило, Г.В. Белов, В.А. Копылов // Проблемы информатизации. - М. - 2015. - Вып.26. - 22 с.

29. Бачило И.Л. Развитие законодательства РФ в сфере информации / И.Л. Бачило, А.А. Антопольский, Г.В. Белова и др. // Информация и связь / Ин - т госуд. и права РАН. - 2015. - № 7. - 45 с.

30. Башлыков М. Актуальные вопросы информационной безопасности / М. Башлыков // Финансовая газета. Региональный выпуск. - 2016. - № 11.

31. Беззубцев О.А. Законодательство Российской Федерации и криптография. Политика ФАПСИ в области распространения и использования криптосредств // О.А. Беззубцев, В.Н. Мартынов, В.М. Мартынов // Защита информации. Конфидент. - 2013. - № 1. - С.14 - 18.

32. Богатыренко З. Новейшие тенденции защиты персональных данных работника в российском трудовом праве / З. Богатыренко // Секретарское дело. - 2016. - № 11. - С.12 - 23.

33. Борисова С.А. Общие требования при обработке персональных данных работника и гарантия их защиты / С.А. Борисова. - 2015. - № 11. - С.82 - 88.

34. Бройдо Д.М. Информационные ресурсы развития Российской Федерации. Правовые проблемы / Д.М. Бройдо // Информация и связь. - 2013. - № 9.

35. Бугров А. Международные стандарты для построения системы информационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.

36. Васильев Г. Российский рынок информационной безопасности: новые тенденции / Г. Васильев // Финансовая газета. - 2017. - № 5.

37. Винер Н. Кибернетика, или управление и связь в животном и машине; или Кибернетика и общество/ Н. Винер. — М.: Наука; Главная редакция изданий для зарубежных стран, 1983. — 344 с.

38. Волков П. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации / П. Волков // Финансовая газета. - 2006. - № 34.

39. Вус, М.А. Информатика: введение в информационную безопасность / М.А. Вус, В.С. Гусев, Д.В. Долгирев и др. - СПб. - 2014. - 156 с.

40. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. URL - https://www.intuit.ru/studies/courses/10/10/info. Дата обращения: 20.03.2020

41. Гениевский, П. Политика информационной безопасности против "человеческого фактора" / П. Гениевский // Банковское дело в Москве. - ноябрь 2015. - № 11.

42. Горшкова, Л.А. Анализ организации управления / Л.А. Горшкова. - М.: Финансы и статистика, 2013. - 206 с.

43. Громов А. Роль информационной безопасности в обеспечении эффективного управления современной компанией / А. Громов, А. Коптелов // Финансовая газета. - 2014. - № 24.

44. Губенков А.А. Информационная безопасность / А.А. Губенков, В.П. Байбурин. - М.: Новый изд. дом, 2005. - 126 с.

45. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ДиаСофт, 2012.

46. Защита информации и экономической безопасности предпринимательской деятельности: материалы межд. научно-практ. конф. / Под ред. В.М. Кравцова и др. - Челябинск, 2015. - 63 с.

47. Зотова Г. Конфиденциальность, надежность, управляемость / Г. Зотова // Сетевой журнал. - 2013. - № 7. - С.18 - 27.

48. Ильин К. Вопросы информационной безопасности при электронном документообороте / К. Ильин // Защита информации. INSIDE. - 2016. - № 4. - С.18 - 25.

49. Информационная безопасность региона: материалы Всерос. науч. - практ. конф. (Челябинск: Челяб. гос. ун-т., 7 октября 2014 г.). - Челябинск, 2015. - 335 с.

50. Информационные технологии управления / Под ред. Г.А. Титоренко. - 2-е изд., доп. - М. - 2013. - 439 с.

51. Концептуальные основы подготовки специалистов по информационной безопасности / Г.А. Бузов, А.К. Лобанов // Информационное общество. - 2015. - № 6. - С.62 - 65.

52. Королькова Т.А. Лицензирование деятельности по защите информации в России: история и современность / Т.А. Королькова, А.В. Печерский // Делопроизводство. - 2013. - № 3. - С.57 - 65.

53. Кузнецова Т.В. Проектирование рациональной организации делопроизводства / Т.В. Кузнецова // Делопроизводство. - 2015. - № 1. - С.58 - 67.

54. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации // А.А. Малюк и др. - М.: Горячая линия – Телеком. - 2014. - 280 с.

55. Маляревский, А. "Тонкие клиенты" - информационная безопасность и экономия / А. Маляревский // Финансовая газета. - 2015. - № 49.

56. Мельников В.П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М. - 2015. - 331 с.

57. Мецатунян М.В. Некоторые аспекты информационной безопасности / М.В. Мецатунян, В.Я. Ищейнов // Делопроизводство. - 2014. - № 1. - с.57 - 59.

58. Организация работы с документами / Под ред. В.А. Кудряева. - 2-е изд., перераб. и доп. - М.: ИНФРА-М, 2013. - 593 с.

59. Охотников, А.В. Документоведение и делопроизводство / А.В. Охотников. - М.: Дело, 2015. - С.356.

60. Панкратов, Ф.Г. Коммерческая деятельность: учеб. / Ф.Г. Панкратов. - М.: Маркетинг, 2014. - 210 с.

61. Партыка Т.А. Информационная безопасность / Т.А. Партыка, И.И. Попов //Форум, ИНФРА. – М. - 2014. - 367 с.

62. Плотников, Н.И. Конфиденциальность: мифы и реальность о тайнах и секретах / Н.И. Плотников // Управление персоналом. - 2016. - № 20. - С.45 - 50.

63. Пугачев В.П. Руководство персоналом организации: учеб. пособие / В.П. Пугачев. - М.: Аспект-Пресс, 2015. - 279 с.

64. Пшенко А.В. Технология работы с конфиденциальными документами / А.В. Пшенко // Секретарское дело. - 2013. - № 2. - С.7 - 11.

65. Садердинов А.А. Информационная безопасность / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. - М.: Дашков и К', 2014. - 335 с.

66. Снытников, А.А. Обеспечение и защита права на информацию / А.А. Снытиков, Л.В. Туманова. - М.: "Городец-издат", 2013. - 195 с.

67. Соловьев И.Н. Информационная и правовая составляющие безопасности предпринимательской деятельности / И.Н. Соловьев // Налоговый вестник. - 2012. - № 54.

68. Степанов Е.А. Информационная безопасность и защита информации: учеб. пособие / Е.А. Степанов, И.К. Корнеев. - М.: Инфра-М, 2003.

69. Степанов Е.А. Основополагающие принципы защиты и обработки конфиденциальных документов / Е.А. Степанов // Делопроизводство. - 2010. - № 2. - С.31 - 34.

70. Сысоева Л.А. Защита информации на уровне баз данных как компонент системы безопасности корпоративных информационных систем / Л.А. Сысоева // Секретарское дело. - 2015. - № 3. - С.29 - 34.

71. Фионова Л.Р Положение о защите персональных данных работников / Л.Р. Фионова, О.В. Касперская // Секретарское дело. - 2015. - № 10. - С.40 - 49.

72. Храмцовская Н.А. Закон о персональных данных: последствия для делопроизводства / Н.А. Храмцовская // Делопроизводство и документооборот на предприятии. - 2017. - № 2. - С.12 - 30.

73. Хургин В. Об определении понятия «информация»/ В. Хургин // Информационные Ресурсы России. — 2017. — № 3. (15)

74. Чикалев И. Во что обходится информационная безопасность / И. Чикалев, С. Леденко // Банковское дело в Москве. - 2016. - № 7.

75. Шиверский А. А. Защита информации проблемы теории и практики / А.А. Шиверский. - М.: Юрист, 2013. - 112 с.

76. Ярочкин В.Н. Информационная безопасность / В.Н. Ярочкин. - М.: Трикста, Академ. проект, 2015. - 542 с.