



**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательная организация  
высшего образования**

**«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-  
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «ЮУрГГПУ»)**

**Профессионально-педагогический институт**

**Кафедра автомобильного транспорта, информационных технологий  
и методики обучения техническим дисциплинам**

**Разработка и внедрение рекомендаций по повышению эффективности  
защиты информации в образовательной организации СПО**

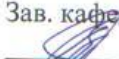
**Выпускная квалификационная работа  
по направлению 44.04.04 Профессиональное обучение**

**Направленность программы магистратуры**

**«Управление информационной безопасности в профессиональном  
образовании»**

Проверка на объём  
заимствований:

92,3% % авторского текста  
Работа рекомендована к защите  
« 25 » мая 2018 г.

Зав. кафедрой АТ, ИТ и МОТД  
 В.В. Руднев

Выполнил:

студент гр. ОФ-309/210-2-1

Суслов Владислав Сергеевич

Научный руководитель:

к.т.н., доцент, заведующий кафедры

АТ, ИТ и МОТД

Руднев Валерий Валентинович

Челябинск, 2018

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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»  
Программа подготовки магистров «Управление информационной  
безопасностью в профессиональном образовании»

**ЗАДАНИЕ**

на выпускную квалификационную работу  
(магистерскую диссертацию)

Магистранту Суслову Владиславу Сергеевичу, обучающемуся в группе  
ОФ-309/210-2-1 по направлению подготовки 44.04.04. «Профессиональное  
обучение (Управление информационной безопасностью в профессиональном  
образовании)»

Научный руководитель квалификационной работы: Руднев В.В., к.т.н.,  
доцент кафедры АТ, ИТ и МОТД.

1. Тема квалификационной работы: «Разработка и внедрение  
рекомендаций по повышению эффективности защиты информации в  
образовательной организации СПО», утверждена приказом Южно-  
уральского государственного гуманитарно-педагогического университета №  
1238-с от «24» мая 2017 г.

2. Срок сдачи магистрантом законченной работы на кафедру «25» мая  
2018г.

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

– раскрыть сущность и содержание защиты информации в  
образовательной организации СПО;

– раскрыть задачи, функции, организационную структуру ГБПОУ  
«Челябинский педагогический колледж №1»;

– раскрыть методы предпроектного исследования и проектирования  
образовательной организации защиты информации в ГБПОУ «Челябинский  
педагогический колледж №1»

– проанализировать организацию защиты информации в ГБПОУ  
«Челябинский педагогический колледж №1»;

– разработать рекомендации по совершенствованию организации  
защиты информации в ГБПОУ «Челябинский педагогический колледж №1».

4. Материалы для выполнения квалификационной работы:

- Учебная, научно-техническая, педагогическая, методическая, нормативно-правовая литература по теме выпускной квалификационной работы (магистерской диссертации).

- Материалы научно-исследовательской работы, педагогической и преддипломной практики.

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.) Таблица, таблицы и диаграммы результатов экспериментальной проверки внедрения в организации СПО и экспертной проверки действующих педагогов и руководителей СПО и ВО, а также технических специалистов.

6. Консультанты по специальным разделам ВКР:

Раздел	Консультант	Отметка

Дата выдачи задания « 24 » мая 2017 года

Задание выдал, зав. кафедрой АТ, ИТ и МОТД

к.т.н., доцент \_\_\_\_\_

Руднев В.В.

Задание принял \_\_\_\_\_

Суслов В.С.

**КАЛЕНДАРНЫЙ ПЛАН**  
**выполнения выпускной квалификационной работы**  
**(магистерской диссертации)**

№ п/п	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1	Предзащита ВКР	25.05.2018г.	
2	Доработка ВКР после предзащиты	30.05.2018г.	
3	Нормоконтроль	11.06.2018г.	
4	Подписание ВКР научным руководителем	19.06.2018г.	
5	Оформление пояснительной записки и презентации ВКР	20.06.2018г.	
6	Подписание рецензии на ВКР		
7	Защита ВКР на заседании ГАК		

Автор \_\_\_\_\_ Суслов В.С.

Научный руководитель,  
к.т.н., доцент кафедры АТ, ИТ и МОТД \_\_\_\_\_ Руднев В.В.

Заведующий кафедрой АТ, ИТ и МОТД  
к.т.н., доцент \_\_\_\_\_ Руднев В.В.

## Содержание

Введение	6
Глава 1. Теоретические основы организации защиты информации в системе управления образовательной организации СПО	11
1.1. Организация защиты информации: основные понятия	11
1.2. Нормативно-правовые основы работы с информацией в учреждении	19
1.3. Технология защиты информации в образовательной организации СПО	26
Глава 2. Особенности организации защиты информации ГБПОУ «Челябинский педагогический колледж №1»	36
2.1. Общая характеристика ГБПОУ «Челябинский педагогический колледж №1»	36
2.2. Анализ организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1»	47
Глава 3. Разработка рекомендаций по повышению эффективности защиты информации	60
3.1. Пути повышения эффективности системы защиты информации	60
3.2. Разработка рекомендаций по повышению эффективности защиты информации в ГБПОУ «Челябинский педагогический колледж №1»	64
Заключение	71
Список использованных источников	75

## Введение

В настоящее время невозможно представить себе серьезную компанию, не использующую в своей работе современные информационные технологии для ведения бизнеса. Одной из неперенных составляющих данных технологий является объединение вычислительных ресурсов компании в единую распределенную корпоративную сеть.

Проблема информационной безопасности в корпоративных сетях передачи данных сегодня очень остро стоит перед компаниями любого уровня. Утечка критически важной корпоративной информации, рост объемов паразитного трафика, вымогательство, шантаж и заказные атаки на информационные ресурсы стали в последнее время частым явлением.

Непрерывно изменяющаяся ситуация в сфере информационной безопасности постоянно ставит перед организациями новые задачи. Быстрое распространение вирусов и шпионских программ, постоянное усложнение сетевых атак, тревожащий рост организованной киберпреступности и шпионажа с использованием Интернета, хищение персональных данных и конфиденциальной информации, более сложные способы инсайдерских атак, развитие новых форм угроз для мобильных систем — вот лишь несколько примеров многообразия и сложности реальных угроз, формирующих современный ландшафт безопасности.

Поскольку сети являются ключевым механизмом ведения бизнеса, при их проектировании и реализации необходимо учитывать проблемы безопасности, чтобы гарантировать конфиденциальность, целостность и доступность данных и системных ресурсов, поддерживающих основные бизнес-процессы компании.

В наши дни для достижения приемлемого уровня безопасности уже не достаточно развернуть точечные продукты на периметре сети. Сложность и изощренность современных угроз требует внедрения интеллектуальных совместно работающих механизмов безопасности во все элементы

распределенной инфраструктуры. С учетом этих соображений все чаще используется подход глубокой многоуровневой (эшелонированной) защиты, согласно которому множество уровней защиты распределены по стратегически важным элементам по всей сети и действуют в рамках унифицированной стратегии. Информация о событиях и состоянии систем согласованно используется различными элементами системы информационной безопасности, что позволяет обеспечить более надежный контроль состояния ИТ-инфраструктуры, а ответные действия координируются в рамках общей стратегии управления.

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

В повседневной жизни человека сохранность информации «о его жизни» зависит от него самого. Но совсем другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу, а конкретно – работодателю. Работник в данной ситуации передает конфиденциальную информацию о себе на ответственное хранение. Далее за сохранность данных отвечает уже работодатель. Способы их защиты, а также ответственность работодателя за невыполнение обязательств по обеспечению сохранности информации.

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

Проблемы защиты информации рассматривались в трудах российских ученых, таких как: А.В. Меньшиковой [37], где она выделила некоторые проблемы защиты информации работника и определила перспективы и пути

их решения; проблемные вопросы понятия и сущности информации в своих трудах рассмотрел А.В. Минбалеев [38].

В настоящее время в образовательных учреждениях активно внедряются информационные системы, осуществляющие обработку информации в образовательной организации, делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных воспитанников, обучающихся, родителей и работников образовательных учреждений, оперативного управления учреждением. Образовательные организации должны отреагировать на требования законодательства о защите информации участников образовательного процесса в первую очередь, т. к. речь идет о защите сведений, незаконное использование которых может серьезно отразиться на правах граждан.

**Актуальность.** Тема диссертации актуальна, так как лица, ответственные за обработку информации не всегда знают элементарных правил безопасности, доверенной им информации. Поэтому на специалистов по информационной безопасности возлагается не только ответственность за безопасность информационной системы, но система обучения персонала.

**Гипотеза.** Если будет реализован разработанный в диссертации комплекс рекомендаций по защите информации в ГБПОУ «Челябинский педагогический колледж №1», то уровень защищенности информации значительно повысится.

**Объектом** исследования является организация защиты данных в образовательной организации ГБПОУ «Челябинский педагогический колледж №1».

**Предмет** исследования являются особенности организации защиты информации.

**Целью** диссертации является анализ организации защиты информации (на примере управления ГБПОУ «Челябинский педагогический колледж №1»).

В соответствии с поставленной целью были выделены следующие



**задачи:**

- раскрыть сущность и содержание защиты информации в образовательной организации СПО;
- раскрыть задачи, функции, организационную структуру ГБПОУ «Челябинский педагогический колледж №1»;
- раскрыть методы предпроектного исследования и проектирования образовательной организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1»
- проанализировать организацию защиты информации в ГБПОУ «Челябинский педагогический колледж №1»;
- разработать рекомендации по совершенствованию организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1».

В процессе написания выпускной квалификационной работы были использованы законодательные акты и нормативно-методические документы, регламентирующие организацию защиты информации. Использование законодательных актов и нормативно-методических документов было продиктовано темой исследования.

Основополагающие нормы, регулирующие отношения по поводу информации, содержатся в Федеральном законе от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» [6].

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» [6] определяет, процессы функционирования информации и документации в обществе, в системе государственного и хозяйственного управления. Настоящий закон регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации,

прав субъектов, участвующих в информационных процессах и информатизации.

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

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

**Научная новизна** исследуемой проблемы заключается в том, что в диссертации предложен комплексный подход к вопросам организации защиты информации в образовательной организации СПО.

**Практическая значимость** данной работы заключается в создании эффективно действующей системы защиты информации в образовательной организации СПО.

Диссертация состоит из введения, трех глав, заключения, списка использованных источников и литературы. Во введении обосновывается выбор темы исследования, ее актуальность, анализируется степень ее изученности, формулируются объект, предмет, цели, задачи, методологические основы исследования, структура работы.

В первой главе раскрываются теоретические основы организации защиты информации системе управления организацией

Во второй главе рассматриваются цели, задачи, функции защиты информации в образовательной организации.

В третьей главе разработаны рекомендации по совершенствованию организации защиты информации в организации образования.

В заключении подводятся итоги проведенного исследования, формулируются основные выводы. Список использованной литературы содержит 55 источников по теме.

# Глава 1. Глава 1. Теоретические основы организации защиты информации в системе управления образовательной организацией СПО

## 1.1. Организация защиты информации: основные понятия

Информация (от лат. *informātiō* — «разъяснение, представление, понятие о чём-либо», от лат. *informare* — «придавать вид, форму, обучать; мыслить, воображать») — сведения независимо от формы их представления [1, с. 7].

Несмотря на широкую распространённость, понятие информации остаётся одним из самых дискуссионных в науке, а термин может иметь различные значения в разных отраслях человеческой деятельности.

Информация — это не материя и не энергия, информация — это информация Норберт Винер [1, с. 8].

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 [3, с. 9].

В международных и российских стандартах даются следующие определения:

- знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста (ISO/IEC 10746-2:1996) [4, с. 10];
- знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл (ISO/IEC 2382:2015) [5, с. 15];
- сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации (ГОСТ 7.0-99) [6, с. 16].

Хотя информация должна обрести некоторую *форму представления* (то есть превратиться в данные), чтобы ею можно было обмениваться, информация есть в первую очередь интерпретация (смысл) такого представления (ISO/IEC/IEEE 24765:2010). Поэтому в строгом смысле *информация* отличается от *данных*, хотя в неформальном контексте эти два термина очень часто используют как синонимы [7, с. 17].

Первоначально «информация» — сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т. д.); с середины XX века термин «информация» превратился в 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 (например, генетическая информация); одно из основных понятий кибернетики [8, с. 18].

Слово «информация» происходит от лат. *informatio*, что в переводе обозначает *сведение, разъяснение, ознакомление*. Понятие информации рассматривалось ещё античными философами [9, с. 19].

Латинские слова «*de saxis informibus*» из Вульгаты Иеронима (342—419) переводятся как «из камней цельных» (Втор. 27:6), а слова «*informem adhuc me*», которые переводятся как «Зародыш мой» (Пс. 138:16), можно перевести и как «бесформенного ещё меня», потому что именно как «ещё бесформенная» переводятся слова «*adhuc informem*» из Исповеди Августина (354—430) [10, с. 20].

Итальянским словом «*informa*» в Комедии Данте (1265—1321) обозначается уже не просто бесформенное, а процесс формирования, образования, творения (Ч. XVII 16-18, Ч. XXV 40-42, Р. VII 133—138) [11, с. 11].

В современном мире информация представляет собой один из важнейших ресурсов и, в то же время, одну из движущих сил развития человеческого общества. Информационные процессы, происходящие в

материальном мире, живой природе и человеческом обществе, изучаются (или, по крайней мере, учитываются) всеми научными дисциплинами от философии до маркетинга.

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

Информатика, сформировавшаяся как наука в середине XX века, отделилась от кибернетики и занимается исследованиями в области способов получения, хранения, передачи и обработки семантической информации.

Исследования смыслового содержания информации основываются на комплексе научных теорий под общим названием семиотика [13, с. 17].

В России философская проблематика понятия «информация» разрабатывалась, начиная с 1960-х годов, когда вышла статья А. Д. Урсула «Природа информации». С тех пор, явно или неявно, рассматриваются в основном две концепции защиты информации: *атрибутивная*, по которой информация свойственна всем физическим системам и процессам (А. Д. Урсул, И. Б. Новик, Л. Б. Баженов, Л. А. Петрушенко и другие), и *функциональная* — информация присуща лишь самоорганизующимся системам (П. В. Копнин, А. М. Коршунов, В. С. Тюхтин, Б. С. Украинцев и другие)<sup>[11]</sup>.

Защита информации представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности информации и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании [19, с. 114].

В процессе трудовой деятельности работника работодатель копит и хранит документы, содержащие информацию работника. Исходя из определения информации, которое, такие сведения могут содержаться в следующих документах:

- трудовая книжка или ее копия со сведениями о трудовом стаже,

предыдущих местах работы;

– копии свидетельств о заключении брака, рождении детей. Такие документы содержат сведения о составе семьи, которые могут понадобиться работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством;

– копия документа, удостоверяющего личность работника. Здесь указываются фамилия, имя, отчество, дата рождения, адрес регистрации, семейное положение, состав семьи работника, а также реквизиты этого документа;

– анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу. В этих документах содержатся анкетные и биографические данные работника;

– личная карточка № Т-2. В ней указываются фамилия, имя, отчество работника, место рождения, состав семьи, образование, а также данные документа, удостоверяющего личность, и пр.;

– документы воинского учета с информацией об отношении работника к воинской обязанности и необходимы работодателю для осуществления в организации воинского учета работников;

– справка о доходах с предыдущего места работы. Нужна информация работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством;

– документы об образовании с квалификацией работника;

– документы обязательного пенсионного страхования работника;

– трудовой договор со сведениями о должности работника, заработной плате, месте работы, рабочем месте, а также иные информацию работника;

– подлинники и копии приказов по личному составу. В них содержится информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника;

– при необходимости – иные документы, содержащие информацию

работников.

Кроме того, работодатель в процессе своей деятельности собирает информацию о соискателях, необходимую для принятия решения о вступлении с ними в трудовые отношения. Если эта информация содержит информацию соискателей, к ней в полной мере относятся установленные законом требования о сборе, обработке, хранении, защите информации.

Так же существует такое понятие как обработка информации, что является неотъемлемой частью процесса защиты информации.

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

Можно выделить некоторые принципы обработки информации.

Обработка информации должна осуществляться на законной и справедливой основе.

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

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

Обработке подлежат только информация, которые отвечают целям их обработки.

Содержание и объем обрабатываемой информации должны соответствовать заявленным целям обработки. Обрабатываемые информацию не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке информации должны быть обеспечены точность

информации, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки информации. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

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

Существуют некоторые условия обработки информации, которые перечислены ниже.

Обработка информации осуществляется с согласия субъекта информации на обработку его информации.

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

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

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



такой услуги, для регистрации субъекта информации на едином портале государственных и муниципальных услуг [12].

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

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

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

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

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

Осуществляется обработка информации, доступ неограниченного круга лиц к которым предоставлен субъектом информации либо по его просьбе (далее - информацию, сделанные общедоступными субъектом информации).

Осуществляется обработка информации, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Ниже кратко даны понятия, определяющие основные элементы системы защиты информации:

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

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

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

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

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

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

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

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

Трансграничная передача информации – передача информации на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Таким образом, информация о сотруднике – это, прежде всего, паспортные данные, сведения о семейном положении, сведения об образовании, номера ИНН, страхового свидетельства государственного пенсионного страхования, медицинской страховки, сведения о трудовой деятельности, социальное и имущественное положение, сведения о доходах. Такие данные есть практически в каждой организации.

Проведя теоретическое исследование основных понятий системы информации можно дать следующее определение: «Защита информации представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка конфиденциальности, целостности, доступности, достоверности информации и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности организации.

## 1.2. Нормативно-правовые основы работы с информацией в образовательной организации СПО

Обработка информации должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных заранее определенных и законных целей. Не допускается обработка информации, несовместимая с целями сбора информации. Обрабатывать можно только те персональные, которые отвечают целям их обработки.

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

В соответствии с новыми установленными законом требованиями образовательная организация обязана разместить на своём сайте сведения:

– о персональном составе педагогических работников с указанием

уровня образования и квалификации;

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

В этой связи нужно обратить внимание, что Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации», установлены жёсткие требования к защите и обработке информации. Обработка информации преподавателей и обучающихся в большом объёме осуществляется в каждой образовательной организации, которое, как предусмотрено федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации», обязаны принять меры по защите информации. В свою очередь данные меры предусматривают, прежде всего, создание достаточно большого количества локальных нормативных актов образовательной организации.

Кроме того, статьёй 29 закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» ещё более усилены требования к информационной открытости образовательной организации. А статьёй 98 данного закона установлены требования к информационным системам в сфере образования, которые обязывают образовательные организации осуществлять обработку информации указанных системах в строгом соответствии с законодательством.

Таким образом, обработка информации должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации». Обработка информации допускается в следующих случаях:

– обработка информации осуществляется с согласия субъекта информации на обработку его информации;

– обработка информации необходима для достижения целей,

предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

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

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

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

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

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

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

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

законные интересы субъекта информации;

– обработка информации осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации», при условии обязательного обезличивания информации;

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

– осуществляется обработка информации, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

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

Лицо, осуществляющее обработку информации по поручению оператора, обязано соблюдать принципы и правила обработки информации, предусмотренные Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации». В поручении оператора должны быть определены действия (операции) с информацией, которые будут совершаться лицом, осуществляющим обработку информации, и цели обработки, нужно установить обязанность такого лица соблюдать конфиденциальность информации и обеспечивать безопасность информации при их обработке, а также должны быть указаны требования к защите обрабатываемых информации в соответствии со статьей 19 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации,

информационных технологиях и о защите информации».

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

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

Основополагающие нормы, регулирующие отношения по поводу информации, содержатся в Федеральном законе от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации». В соответствии с п. 1 ст. 3 этого Закона информацией является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту информации), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [7].

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

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

Так же можно выделить еще три группы нормативных документов по защите информации – это: методические материалы ФСТЭК России; Приказ

ФСТЭК России о составе и содержании мер по обеспечению безопасности информации в ИСПДн; Методические материалы ФСБ России [29, с. 89].

Методические материалы ФСТЭК России:

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

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

Согласно Приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620) методические материалы ФСБ России включают:

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

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

– состав и содержание организационных и технических мер,



необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для 2 уровня защищенности;

– состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для 1 уровня защищенности;

Требования[18]:

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

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

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

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

Таким образом, требования методических материалов, разработанных ФСБ России и направленных на разъяснение требований по обеспечению

безопасности ПД путем организации криптографической защиты данных, перестали носить обязательный характер [11].

В соответствии со ст. 24 лица ФЗ от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации», виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность Закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации». Неисполнение требований Закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» операторами баз данных может повлечь: гражданские иски со стороны работников; репутационные риски; приостановление или прекращение обработки информации в школе, осуществляемой с нарушением требований Закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации»; направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов информации; привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях. В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту информации работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

1 июля 2017 года вступает в силу Федеральный закон от 07.02.2018 № 13-ФЗ, который вносит поправки в ст. 13.11 КоАП. В частности, он предусматривает расширение перечня оснований для привлечения

к административной ответственности за незаконную обработку информации (ПДн) и существенное увеличение штрафов.

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

### 1.3. Технология защиты информации в образовательной организации СПО

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

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

В общих чертах защита информации сводится к созданию режима обработки информации, включающего:

- разработку внутренней документации по работе с информацией;
- создание организационной структуры системы защиты информации;
- внедрение технических мер защиты информации;
- получение сертификатов регулирующих органов (Федеральной службы безопасности и Федеральной службой по техническому и экспортному контролю) на средства защиты информации;
- при необходимости, получение лицензий регулирующих органов

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

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

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

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

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

Угрозы 3-го типа актуальны для информационной системы, если для нее

актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности информации, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение Федерального закона «О информации», и в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О информации».

При обработке информации в информационных системах устанавливаются 4 уровня защищенности информации.

Необходимость обеспечения 1-го уровня защищенности информации при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории информации, либо биометрические информацию, либо иные категории информации;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории информации более чем 100000 субъектов информации, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности информации при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные информацию;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории информации сотрудников оператора или специальные категории информации менее чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические информацию;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные информацию более чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории информации более чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории информации более чем 100000 субъектов информации, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности информации при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные информацию сотрудников оператора или общедоступные информацию менее чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории информации сотрудников оператора или иные категории информации менее чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории информации сотрудников оператора или специальные категории информации менее чем 100000 субъектов информации, не являющихся сотрудниками оператора;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические информацию;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории информации более чем 100000 субъектов информации, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности информации при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные информацию;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории информации сотрудников оператора или иные категории информации менее чем 100000 субъектов информации, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности информации при их обработке в информационных системах необходимо выполнение следующих требований:

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей информации;

– утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности информации при их

обработке в информационных системах помимо выполнения требований, предусмотренных ФЗ, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности информации в информационной системе.

Для обеспечения 2-го уровня защищенности информации при их обработке в информационных системах помимо выполнения требований, предусмотренных требованиями к защите информации, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для обеспечения 1-го уровня защищенности информации при их обработке в информационных системах помимо требований, предусмотренных правилами, необходимо выполнение следующих требований:

- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

- создание структурного подразделения, ответственного за обеспечение безопасности информации в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Таким образом, при создании системы защиты информации в



организациях, на современном этапе развития в РФ, можно выделить следующие последовательные этапы:

- выяснить и определить все случаи, когда необходимо проводить обработку информации в организации;

- определить бизнес-процессы, в которых обрабатываются информация;

- наметить обязательные (в том числе предварительные) этапы работ по защите информации:

- выделить все возможные ситуации, когда необходимо проводить обработку информации;

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

- определить совокупность обрабатываемых информации и круг информационных систем;

- провести ранжирование информации по категориям и предварительную классификацию информационных систем.

- наметить меры по минимизации категорий обрабатываемых информации;

- подготовить действующую модель угроз для информационной системы обработки информации.

- разработать техническое задание по созданию необходимой системы защиты;

- провести уточнение соответствия классов информационных систем, с дальнейшей подготовкой предложений по использованию технических средств защиты информации;

- подать уведомление о начале обработки информации в уполномоченный орган по защите прав субъектов информации

(Роскомнадзор) для регистрации в качестве оператора информации;

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

- разработать требования для конкретной системы обработки информации, учитывая класс защиты информационной системы .

- для защиты информационной системы обработки информации и помещений подготовить технический проект.

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

- провести внедрение системы защиты информации;

- с субъектов информации взять согласие на обработку информации;

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

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

Применение системы защиты информации является не обязательным для всех типов информационных систем обработки информации. Выбор системы защиты информации необходимо осуществлять учитывая, что конечный набор мер для защиты информации должен отвечать требованиям, предъявляемым к информационной системе обработки информации

соответствующего класса, определение которых приведено в Приказе ФСТЭК России от 18.02.2013 N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации (Зарегистрировано в Минюсте России 14.05.2013 N 28375) (ред. от 23.03.2017). В соответствии с Указом Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» осуществляется подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно телекоммуникационным сетям международного информационного» (ред. от 22.05.2015).

Таким образом, для системы защиты информации информационная система обработки информации выбирается в зависимости от класса информационной системы с учетом: угроз безопасности персональным данным; структуры информационной системы; наличия межсетевого взаимодействия и режимов обработки информации с использованием соответствующих методов и способов защиты информации от несанкционированного доступа (реализуются функции управления доступом, регистрации и учета); обеспечения целостности защиты информации; анализа защищенности информации; обеспечения безопасного межсетевого взаимодействия; обнаружения вторжений. Система защиты информации включает в себя меры организационного и технического характера, которые определяются с учетом актуальных угроз безопасности для информации и информационных технологий, используемых в системе обработки информации организации.

## Глава 2. Особенности организации защиты информации ГБПОУ «Челябинский педагогический колледж №1»

### 2.1. Общая характеристика ГБПОУ «Челябинский педагогический колледж №1»

Организовано 10.10.1910 года (Челябинская педагогическая семинария)

*Сведения о реорганизации:*

- Челябинская педагогическая семинария реорганизована в Челябинский педагогический образовательная организация СПО в 1922 году (Постановление заседания коллегии Губпрофобра от 26.07.1922г.).
- Реорганизована в Челябинское педагогическое училище в 1936 году.
- Реорганизовано в Челябинское педагогическое училище №1 25.05.1965г. (Решение Облисполкома № 227).
- Челябинское педагогическое училище № 1 преобразовано в Челябинский государственный педагогический колледж № 1 (Приказ Министерства образования РФ № 405 от 09.08.96г.).
- Челябинский государственный педагогический колледж № 1 преобразован в Государственное учреждение среднего профессионального образования (среднее специальное учебное заведение) «Челябинский государственный педагогический колледж № 1» (Постановление Главы города Челябинска от 09.04.01г. № 384 - П., регистрационный №180-1).
- Государственное учреждение среднего профессионального образования (среднее специальное учебное заведение) «Челябинский государственный педагогический колледж №1» преобразован в «Государственное образовательная организация среднего профессионального образования (среднее специальное учебное заведение) Челябинский государственный педагогический колледж №1» (далее ЧГПК №1)

(Постановление Главы города Челябинска № 1753 - П от 03.12.01г., регистрационный №180-2)

- Государственное бюджетное профессиональное образовательная организация "Челябинский педагогический колледж № 1"( далее ГБПОУ "ЧПК №1")

*Учредитель:* Министерство образования и науки Челябинской области.  
454113, Россия, Челябинская область, Челябинск, Революции площадь, 4.  
Тел.: 8(351)263-67-62, 263-46-31; E-mail:  
minobr@minobr174.ru; [www.minobr74.ru](http://www.minobr74.ru).

График работы Министерства образования и науки Челябинской области.

ГБПОУ «Челябинский педагогический колледж № 1» — среднее специальное учебное заведение г. Челябинск.

Сегодня ГБПОУ «Челябинский педагогический колледж № 1» – многоуровневое учебное заведение, обеспечивающее среднее профессиональное образование базового и повышенного уровня. Повышенный уровень среднего образования реализуется через 24 программы дополнительной подготовки. В составе колледжа 7 отделений и 8 кафедр. За годы существования в колледже подготовлено более 23 тыс. специалистов в области образования, спорта, культуры. Колледж имеет современную материальную базу и техническое оснащение: четыре учебных корпуса общей площадью 11700 кв. м., общежитие на 400 мест, столовую на 120 мест, библиотеку с читальным залом на 80 мест, с книжным фондом более 74 тыс. экземпляров, музей, четыре спортивных зала, стадион, актовый, выставочный и два концертных зала, 60 учебных кабинетов, мастерских и лабораторий, четыре компьютерных класса, хоровой, оркестровый, хореографический классы, лыжную базу и т.д. Преподавательский состав МПК – 99 человек, из них 8% имеют ученые степени, 70% преподавателей имеют высшую квалификационную категорию, 33% преподавателей имеют почетные звания и награды. В колледже активно работают разнообразные творческие и спортивные студенческие объединения, широкое развитие получила

концертно-исполнительская деятельность. Выпускники колледжа имеют возможность получать высшее образование в ВУЗах-партнерах, функционирующих на базе колледжа – это Челябинский государственный педагогический университет, Уральский государственный университет физической культуры, Челябинский государственный университет. Колледж ведет дополнительную профессиональную подготовку: курсы повышения квалификации преподавателей физической культуры, учителей начальных классов, воспитателей дошкольных образовательных учреждений, курсы переподготовки специалистов для работы в сфере образования, семинары, методические объединения, конференции, консультации и т.д. На базе колледжа открыта экспериментальная площадка

ГБПОУ «Челябинский педагогический колледж № 1» – многоуровневое учебное заведение, обеспечивающее среднее профессиональное образование базового и повышенного уровня по следующим специальностям:

#### ОБРАЗОВАНИЕ ПЕРЕЧЕНЬ СПЕЦИАЛЬНОСТЕЙ ПОДГОТОВКИ

Обучение в колледже осуществляется на русском языке.

Код	Название	Квалификация	Реализуемый уровень образования	Форма обучения	Нормативный срок обучения	Срок действия государственной аккредитации
54.02.01.	Дизайн	Дизайнер, преподаватель	базовый	Очная	3 года 10 месяцев	2016 г
53.02.01.	Музыкальное образование	Педагог музыки, музыкальный руководитель ДОУ	базовый	Очная	3 года 10 месяцев	2017 г
43.01.10.	Туризм	Специалист по туризму	базовый	Очная	3 года 10 месяцев	2016 г
49.02.01.	Физическая культура	Педагог физической культуры	базовый	Очная	3 года 10 месяцев	2016 г
44.02.02.	Преподавание в	Педагог начальных	углубленный	Очная	3 года 10 месяцев	2017 г

	начальных классов	классов			2 года 10 месяцев	
230701	Прикладная информатика	Техник-программист	базовый	Очная	2 года 10 месяцев	2016 г

### ЧИСЛЕННОСТЬ ОБУЧАЮЩИХСЯ ПО РАЗЛИЧНЫМ ОБРАЗОВАТЕЛЬНЫМ ПРОГРАММАМ

Численность обучающихся по реализуемым образовательным программам за счет бюджетных ассигнований федерального бюджета	Численность обучающихся по реализуемым образовательным программам за счет бюджетов субъектов РФ	Численность обучающихся по реализуемым образовательным программам за счет местных бюджетов (область)	Численность обучающихся по реализуемым образовательным программам за счет физических и (или) юридических лиц
734	0	734	78

### УЧЕБНЫЕ ПЛАНЫ

54.02.01. Дизайн (в области культуры и искусства)

53.02.01. Музыкальное образование

43.01.10. Туризм

49.02.01. Физическая культура

44.02.02. Преподавание в начальных классах

230701 Прикладная информатика

За годы существования в колледже подготовлено более 23 тыс. специалистов в области образования, спорта, культуры.

Колледж имеет современную материальную базу и техническое оснащение.

Преподавательский состав МПК – свыше 100 человек, из них 8% имеют ученые степени, 73% преподавателей имеют высшую квалификационную категорию, 33% преподавателей имеют почетные звания и награды.

В колледже активно работают разнообразные творческие и спортивные студенческие объединения, широкое развитие получила концертно-исполнительская деятельность.

Свою жизнедеятельность студенты организуют самостоятельно, для чего в колледже успешно функционирует студенческое самоуправление. Научно-исследовательская работа в организации проводится в соответствии с запросами социальной практики и с учетом задач, стоящих перед коллективом МПК.

Высокая конкурентоспособность выпускников Челябинского педагогического колледжа обусловлена качеством образования, его практической направленностью, высоким уровнем мотивации студентов к обучению.

Кроме этого, колледж, выполняя социальный заказ, ведет дополнительную профессиональную подготовку: курсы повышения квалификации преподавателей физической культуры, учителей начальных классов, воспитателей дошкольных образовательных учреждений, курсы переподготовки специалистов для работы в сфере образования, семинары, методические объединения, конференции, консультации и т.д.

Колледж активно развивает отношения социального партнерства с работодателями, вузами, организациями образования, культуры, спорта, социальной защиты населения. Базами практик являются 27 лучших образовательных организации г. Челябинска.

На базе колледжа открыта экспериментальная площадка Федерального института развития образования (г. Москва) по проблеме «Формирование социальной компетентности студентов педагогического колледжа», осуществляются научные исследования по актуальным вопросам образования и воспитания.

Одно из крупнейших в Челябинской области учреждений среднего профессионального образования, ГБПОУ «Челябинский педагогический колледж № 1» вписал немало ярких страниц в летопись областной образовательной системы и историю Челябинска.

В последние годы колледж заявил о себе не только на уровне города и региона (в 2017 году педколледж признан лучшим организации среднего



профессионального образования Челябинской области). В 2017 и 2018 году колледж вошел в 100 лучших вузов России, он награжден золотыми медалями и дипломами. Достижения учащихся и педагогов отмечены грамотами, дипломами, кубками и медалями.

Численность педагогического коллектива колледжа составляет 74 человека, из них 1 имеет звание кандидата педагогических наук, 2 – звание «Заслуженный педагог РФ», 5 педагогов имеют звание «Отличник народного просвещения», 8 учителей награждены грамотами Министерства образования РФ, 11 человек продолжают учебу в вузах.

Стаж педагогической работы учителей колледжа :

- свыше 20 лет – 25 человек;
- от 10 до 20 лет – 23 человека;
- от 5 до 10 лет – 16 человек;
- от 2 до 5 лет – 6 человек;
- до 2-х лет – 4 человека.

В колледже созданы условия для развития интеллектуального и творческого потенциала учащихся. Развита система дополнительного образования: научное общество учащихся, факультативы, спецкурсы, кружки эстетического, спортивного, прикладного направления, клубы по интересам.

Студенты колледжа ежегодно принимают активное участие и становятся победителями в районных, городских и областных олимпиад и конкурсов.

Важным показателем динамики рабочей силы является текучесть кадров. Текучесть кадров – это процесс незапланированного неорганизованного перемещения рабочей силы, обусловленный неудовлетворенностью работника рабочим местом или неудовлетворенностью предприятия данным работником.

Существует несколько методов расчета текучести, наиболее распространенный – отношение числа покинувших организацию сотрудников к среднему числу занятых в течение года. Высокий уровень текучести кадров

указывает на серьезные недостатки в управлении персоналом и управлении предприятием в целом, это своего рода индикатор неблагополучия.

Уровень текучести кадров определяется коэффициентом текучести по формуле:

$$K_T = \frac{Ч_y}{Ч_c},$$

где  $K_T$  – коэффициент текучести кадров;

$Ч_y$  – численность работников, уволившихся с предприятия;

$Ч_c$  – среднесписочная численность работников предприятия.

Показатель текучести кадров отражает уровень созданных на предприятии условий для наиболее эффективного использования и развития трудового потенциала работников.

Текучесть кадров колледжа .

Среднесписочная численность  
педагогического коллектива  
(январь 2009 года)  
74

Численность педагогов,  
уволившихся из колледжа  
(за 2017 год)  
6

Текучесть кадров по колледже составила за 2017 год 12,3 %.

Анализ показал, что коэффициент текучести значительно превышает норму (5 %), из этого следует, что в колледже большая текучесть кадров. Необходимо выяснить причину этого явления и в будущем стремиться снизить этот показатель.

Попечительский совет ГБПОУ «Челябинский педагогический колледж №1» действует в соответствии с законодательством Российской Федерации и Челябинской области, настоящим Уставом и Положением о Попечительском совете.

В попечительский совет могут входить физические и юридические лица, в том числе представители администрации и работники ГБПОУ «Челябинский педагогический колледж №1», обучающиеся и их родители (законные представители), представители органов государственной власти и местного самоуправления, представители работодателей, социальных партнеров, в количестве 15 человек, сроком на 3 года. Попечительский совет избирает из своего состава председателя и секретаря, определяет руководящие и контрольно-ревизионные органы совета. Права и обязанности участников Попечительского совета указываются в Положении о Попечительском совете. Решения попечительского совета принимаются открытым голосованием и являются правомочными при участии на его заседаниях более половины членов попечительского совета, и если за них проголосовало не менее двух третей присутствовавших. Решения попечительского совета оформляются протоколами.

Попечительский совет:

- участвует в совершенствовании образовательной деятельности в В ГБПОУ «Челябинский педагогический колледж №1»;
- содействует привлечению дополнительных финансовых средств для обеспечения деятельности и развития ГБПОУ «Челябинский педагогический колледж №1»;
- содействует социальной защите и поддержке обучающихся и сотрудников, улучшению условий труда работников ГБПОУ «Челябинский педагогический колледж №1»;
- содействует совершенствованию материально -технической базы В ГБПОУ «Челябинский педагогический колледж №1», благоустройству его помещений и территории;
- определяет порядок расходования денежных средств, полученных за счет добровольных пожертвований физических и (или) юридических лиц;
- осуществляет контроль за использованием указанных средств;

- поддерживает инновационную и научно-исследовательскую деятельность ГБПОУ «Челябинский педагогический колледж №1»;

- содействует установлению связей с работодателями, службами занятости населения, органами государственной власти, органами местного самоуправления, средствами массовой информации, другими организациями, родителями (законными представителями) обучающихся, выпускниками ГБПОУ «Челябинский педагогический колледж №1»;

- рассматривает другие вопросы, отнесенные к компетенции попечительского совета в соответствии с положением о Попечительском совете.

Совет родителей является представительным органом родителей (законных представителей) несовершеннолетних обучающихся. В состав Совета родителей входят по одному представителю родителей от группы, которые избираются на родительских собраниях в группе на срок в соответствии с Положением о Совете родителей.

Совет родителей созывается по мере необходимости по решению председателя Совета родителей, по решению половины членов Совета родителей, по решению директора ГБПОУ «Челябинский педагогический колледж №1». Решения Совета родителей принимаются открытым голосованием большинством голосов и являются правомочными, если за них проголосовало не менее двух третей присутствовавших.

Совет родителей:

- содействует объединению усилий родителей и администрации Учреждения в обучении и воспитании обучающихся;

- оказывает помощь ГБПОУ «Челябинский педагогический колледж №1» в определении и защите социально не защищенных обучающихся, утверждает списки таких обучающихся;

- оказывает ГБПОУ «Челябинский педагогический колледж №1» организационную и консультативную помощь;

– разрабатывает предложения по улучшению условий пребывания обучающихся в ГБПОУ «Челябинский педагогический колледж №1» и другим вопросам деятельности ГБПОУ «Челябинский педагогический колледж №1» и направляет предложения руководителю;

– содействует совершенствованию материально-технической базы в ГБПОУ «Челябинский педагогический колледж №1», благоустройству его помещений и территории;

– контролирует расходование денежных средств, получаемых от добровольных пожертвований, целевых взносов физических и юридических лиц;

– участвует в управлении ГБПОУ «Челябинский педагогический колледж №1» и принятии локальных нормативных актов, по вопросам затрагивающим права и законные интересы обучающихся;

– рассматривает другие вопросы в соответствии с положением о Совете родителей.

Совет родителей действует на основании Положения о Совете родителей.

В целях учета мнения обучающихся, родителей (законных представителей) несовершеннолетних обучающихся и педагогических работников по вопросам управления ГБПОУ «Челябинский педагогический колледж №1» и при принятии локальных нормативных актов, затрагивающих их права и законные интересы, по инициативе обучающихся, родителей (законных представителей) несовершеннолетних обучающихся и педагогических работников в ГБПОУ «Челябинский педагогический колледж №1» действуют профессиональные союзы обучающихся и (или) работников ГБПОУ «Челябинский педагогический колледж №1», осуществляющие свою деятельность в соответствии с действующим законодательством.

Структуризация ГБПОУ «Челябинский педагогический колледж №1» необходима для децентрализованного управления, к сожалению, в ГБПОУ «Челябинский педагогический колледж №1» сложилась такая

структура управления, которую можно назвать плоской, когда все субъекты управления, начиная с заместителей и заканчивая техперсоналом подчинены только одному человеку – директору. Традиционное учебное заведение является скорее централизованной организацией. Взаимосвязи осуществляются по принципу «команд и контроля». Управление в ГБПОУ «Челябинский педагогический колледж №1» осуществляется в форме законной власти. Стилль управления скорее смешанный: демократичный, т.к. основывается на потребностях высокого уровня: творческая реализация, проявление интеллектуального потенциала, любовь к учащимся; автократичный, т.к. сама система образования предусматривает чёткие рамки программы и централизацию. Анализируя ГБПОУ «Челябинский педагогический колледж №1», можно выявить, что децентрализация приведёт ко многим преимуществам. А именно, развитию навыков руководителей, полномочия и ответственность которых возрастёт; соревнование в организации усилит стимул руководителей к созданию атмосферы конкуренции и большей самостоятельности; а это поможет раскрыть творческие способности руководителей, приведёт к росту и развитию ГБПОУ «Челябинский педагогический колледж №1» в целом, коллектив станет командой единомышленников.

Профессиональная позиция педагогов не однозначная: с одной стороны они готовы обсуждать и решать проблемы с обучающимися, с другой - эти проблемы ограничиваются рамками преподаваемого предмета. Для определённой части педагогов ГБПОУ «Челябинский педагогический колледж №1» характерна повышенная конфликтность в общении с коллегами и учениками. По стилю педагогического общения коллектив неоднороден: демократизм и авторитарные тенденции представлены примерно с одинаковой степенью выраженности. Позиция студентов тоже двойственна: они признают, что могут участвовать в планировании и организации образовательного процесса, но чаще выражают готовность принимать уроки такими, какие они есть.

Таким образом, система управления, сложившаяся в образовательной организации СПО, обеспечена необходимой нормативной и организационно-распорядительной документацией, соответствующей требованиям действующего законодательства и Устава образовательной организации СПО.

## 2.2. Анализ организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1»

Исследование системы защиты информации в ГБПОУ «Челябинский педагогический колледж №1» требует предварительного проведения оргпроектных работ.

Организационное проектирование – это проектирование новых организаций, структурное преобразование или оптимизация деятельности уже существующих организаций, а также формирование их организационных структур. Организационное проектирование позволяет формировать системы с заранее заданными характеристиками, содержащимися в проектной документации.

Целью организационного проектирования является формирование новых организационных структур или развитие уже существующих, а также придание процессу создания новых систем или развитию действующих целенаправленности, научной обоснованности.

Задачами организационного проектирования является:

- выявление условий, влияющих на деятельность организации и методов их изучения;
- определение качественного и количественного состава элементов структур управления, формирование их взаимосвязи;
- определение структуры управления организацией и определение условий, в которых каждая из них будет более эффективна;

- изучение принципов и методов проектирования структур управления и особенностей их применения;
- определение методики расчета необходимой численности персонала;
- разработка рекомендаций по внедрения спроектированных рекомендаций в организацию;
- разработка методов и форм контроля, а также специфики их использования.

Оргпроектирование включает несколько стадий.

Первая стадия называется предпроектным обследованием. Предпроектное обследование организации – один из важнейших этапов успешного внедрения проекта. Этот этап служит фундаментом для всей последующей работы над проектом. Его цель – точное определение состава, объема, стоимости, сроков исполнения предстоящих проектно-исследовательских работ и соответствующее их документирование

Этот этап подразделяется, в свою очередь, на составные элементы:

- предпроектное ориентировочное исследование (экспресс-анализ) – диагностика;
- рабочее, детальное исследование;
- анализ, обобщение и выводы.

Следующий этап, проектирование – это наиболее творческая часть деятельности исследователей и проектантов. Она предполагает применение различных методических и организационно-технических приемов и средств, разработанных наукой и практикой на сегодняшний день в их сочетании.

Предметом организационного проектирования являются новые структуры, системы, управляемые процессы. Организационное проектирование настроено на создание новых объектов, модификацию существующих и коренную реконструкцию объектов и процессов.

План работ проведения оргпроектных работ в ГБПОУ «Челябинский педагогический колледж №1» области представлен в таблице 1



Таблица 1–План работ проведения оргпроектных работ в ГБПОУ «Челябинский педагогический колледж №1»

№ п/п	Наименование этапа	Трудоемкость (дни)	Сроки проведения	Число исполнителей
1.	Обследование	30	01.04.2018г.- 30.04. 2018г.	1
2.	Проектирование	18	02.05. 2018г- 20.05. 2018 г.	1

Организационная работа начинается с разработки программы исследования – это комплекс положений, определяющих цели и задачи исследования, предмет и условия его проведения, а также предполагаемы результат.

Рабочая программа является организационно-методическим документом, содержащим полный перечень вопросов, на которые требуется получить ответы в процессе исследования. Рабочая программа оформляется в виде таблицы 2.

В план работ рекомендуется вносить следующие показатели: номер этапа, наименование этапа, трудоемкость, сроки начала и окончания работ, число исполнителей.

Методы предпроектного исследования необходимы для получения и более полного представления о состоянии объекта исследования на сегодняшний день.

Изучение документов– это метод сбора первичных данных, при котором документы используются в качестве главного источника информации; это также совокупность методических приёмов и процедур, применяемых для извлечения информации из документальных источников при изучении процессов и явлений в целях решения определённых задач[29, с. 139].

Таблица 2–Рабочая программа исследования организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1»

№ п/п	Наименование работ	Методы сбора данных	Источники информации	Форма сбора, обобщения, представления информации	Исполнитель	Сроки
1	2	3	4	5	6	7
1	Изучение направлений деятельности, организационной структуры учреждения	изучение документов	локальные документы организации (историческая справка, приказ о создании, штатное расписание, регламент)	описание	Суслов В.С.	01.04.18-10.04.18
2	Изучение организационных документов, регламентирующих деятельность организации	изучение документов	организационно-правовые акты, приказы, положения	описание	Суслов В.С.	11.04.18-17.04.18
3	Изучение целей, задач, функций по защите информации в организации	изучение документов, наблюдение	Положение, регламент, приказы, должностные инструкции	описание	Суслов В.С.	15.04.18-17.04.18
4	Изучение технологии защиты информации в организации	изучение документов, обследование АРМ и подключение у Интернет	локальные документы организации (положения, штатное расписание, должностные инструкции,)	описание	Суслов В.С.	18.04.18-21.04.18
5	Изучение особенностей и выделение недостатков в функционировании системы защиты информации в организации	изучение документов, обследование АРМ и подключение у Интернет	локальные документы организации (положения, штатное расписание, должностные инструкции,)	описание	Суслов В.С.	22.04.18-29.04.18

Непосредственное наблюдение– регистрация событий, явлений, фактов в соответствии с заранее установленными задачами и порядком их фиксации.

Статистический метод – методы анализа статистических данных, научные методы описания и изучения массовых явлений, допускающих количественное (численное) выражение.

Графический метод – это метод условных изображений статистических данных при помощи геометрических фигур, линий, точек и разнообразных

символических образов [34, с. 128].

Таким образом, в предпроектном обследовании используются следующие методы: изучение документов, непосредственное наблюдение, статистический, графический.

Основной целью создания защиты информации в ГБПОУ «Челябинский педагогический колледж №1» является минимизация ущерба от возможной реализации угроз безопасности информации.

Для достижения основной цели система безопасности информации информационная система информации должна обеспечивать эффективное решение следующих задач:

1. защиту от вмешательства в процесс функционирования информационной системы информации посторонних лиц (возможность использования информационной системой и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

2. разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационной системы информации (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационной системы информации для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

– к информации, циркулирующей в информационной системе информации;

– средствам вычислительной техники информационной системы информации;

– аппаратным, программным и криптографическим средствам защиты, используемым в информационной системе информации;

3. регистрацию действий пользователей при использовании защищаемых ресурсов информационной системы информации в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

4. контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5. защиту от несанкционированной модификации и контроль целостности используемых в информационной системе информации программных средств, а также защиту системы от внедрения несанкционированных программ;

6. защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

7. защиту информации хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

8. обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

9. своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба субъектам информации, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

10. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

Защита информации в ГБПОУ «Челябинский педагогический колледж №1» не регламентирована, т.е. отсутствуют какие-либо документы регулирующие действия по защите информации. В ходе исследования были исследованы все положения (62 положения) регулирующие деятельность образовательной организации СПО.

Объектами защиты ГБПОУ «Челябинский педагогический колледж №1» являются – информация, обрабатываемая в информационной системе информации, и технические средства ее обработки и защиты. Объекты защиты включают:

1. Обрабатываемая информация.
2. Технологическая информация.
3. Программно-технические средства обработки.
4. Средства защиты информации.
5. Каналы информационного обмена и телекоммуникации.
6. Объекты и помещения, в которых размещены компоненты информационной системы информации.

В таблице 3 приведен перечень должностей ГБПОУ «Челябинский педагогический колледж №1», уполномоченных на обработку информации и (или) имеющих доступ к персональным данным.

Таблица 3 – Перечень должностей сотрудников образовательной организации, уполномоченных на обработку информации

№ п/п	Наименование должности	К какой информации (сведениям, документам, носителям) допускаются
1.	Директор	в полном объеме
2.	Заместители директора	в объеме, необходимом для выполнения должностных обязанностей
3.	Специалист кадровой службы	к сведениям и документам, регулирующим взаимоотношения (трудовые, обучение) субъектов ПДн и образовательной организации (сторонних организаций)
4.	Специалисты бухгалтерии	к биографическим данным и данным, формируемым в процессе взаимоотношений (трудовые, обучение) с субъектами ПДн
5.	Специалисты ИТ (Администратор информационной системы обработки информации, оператор информационной системы обработки информации)	в объеме, необходимом для выполнения должностных обязанностей
6.	Преподаватели	в объеме, необходимом для выполнения должностных обязанностей

Пользователи информационной системы информации ГБПОУ «Челябинский педагогический колледж №1» делятся на три основные категории:

Администратор информационной системы обработки информации. Сотрудники ГБПОУ «Челябинский педагогический колледж №1», которые занимаются настройкой, внедрением и сопровождением системы. Администратор информационной системы информации обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении информационной системы обработки информации;

- обладает полной информацией о технических средствах и конфигурации информационной системы обработки информации;

- имеет доступ ко всем техническим средствам обработки информации и данным информационной системы обработки информации;

- обладает правами конфигурирования и административной настройки технических средств информационной системы обработки информации.

Программист-разработчик информационной системы обработки информации. Сотрудники ГБПОУ «Челябинский педагогический колледж №1» или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик информационной системы обработки информации обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на информационной системе обработки информации;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы обработки информации на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии информационной системы обработки информации и технических средствах

обработки и защиты информации, обрабатываемых в информационной системе обработки информации.

Оператор информационной системы обработки информации – сотрудники подразделений ГБПОУ «Челябинский педагогический колледж №1», участвующие в процессе эксплуатации информационной системы обработки информации. Оператор информационной системы обработки информации – сотрудник обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству информации;
- располагает конфиденциальными данными, к которым имеет доступ.

Подсистемы – носители информации в информационной системе ГБПОУ «Челябинский педагогический колледж №1» взаимодействующие так кадровый и бухгалтерский учет персонала. Подсистема обеспечения учебного процесса функционирует отдельно.

В ходе исследования было выявлено, что в информационной и системе автоматизированные рабочие места имеющие доступ и обрабатывающие информацию не подключены к сети интернет.

При обработке информации в пределах ГБПОУ «Челябинский педагогический колледж №1» система соответствует нераспределенным информационным системам информации класса КЗ. При этом лицензий ФСТЭК России от оператора информации не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Загрузку обновленных антивирусных баз данных, а также программ и форм персонифицированного учета и отчетности осуществляют на других компьютерах, подключенных к сети Интернет. Осуществляется безопасный перенос загруженных файлов в изолированные от Интернета локальные информационные системы информации с использованием маркированных съемных носителей, в обязательном порядке проверяемых антивирусными средствами перед загрузкой в информационную систему информации.

Официально распространяемые территориальными органами ФНС России и Пенсионного фонда России программы используются при подготовке данных персонифицированного учета. При этом сформированные данные персонализированного учета выгружаются из информационной системы информации на съемные маркированные носители.

Информационная система в ГБПОУ «Челябинский педагогический колледж №1» защищена антивирусной лицензионной программой «Kaspersky».

В ней реализованы следующие функции безопасности:

- разграничение доступа к управлению антивирусной защитой;
- управление работой антивирусной защитой;
- управление параметрами антивирусной защитой;
- управление установкой обновлений (актуализации) базы данных
- признаков вредоносных компьютерных программ (вирусов)

антивирусной защиты;

- аудит безопасности антивирусной защиты;
- сигнализация антивирусной защиты.

В среде, в которой антивирусная защита функционирует, реализованы

- следующие функции безопасности среды:
- обеспечение доверенной связи (маршрута) между антивирусной

защиты и

- пользователями;
- обеспечение доверенного канала получения обновлений

антивирусной защиты;

- обеспечение условий безопасного функционирования;
- управление атрибутами безопасности.

Перечень информации обрабатываемых в ГБПОУ «Челябинский педагогический колледж №1».



Категории субъектов информации в ГБПОУ «Челябинский педагогический колледж №1»:

а) Субъекты, учащиеся в ГБПОУ «Челябинский педагогический колледж №1».

б) Другие категории:

- сотрудники ГБПОУ «Челябинский педагогический колледж №1»;
- лица, обратившиеся в ГБПОУ «Челябинский педагогический колледж №1» с целью трудоустройства;
- лица, уволенные из ГБПОУ «Челябинский педагогический колледж №1».

В таблице 4 приведены статистические данные по учащимся в ГБПОУ «Челябинский педагогический колледж №1».

Таблица 4–Статистические данные по субъектам, учащимся в ГБПОУ «Челябинский педагогический колледж №1»

Субъекты	2016	2017	Изменение 2016- 2017	2018	Изменение 2017-2018
Обучающиеся	994	987	-7	1003	16
Отчисленные	17	11	-3	15	4

Структура категорий субъектов информации учащихся в ГБПОУ «Челябинский педагогический колледж №1» в 2016 году представлена на рисунке 1.

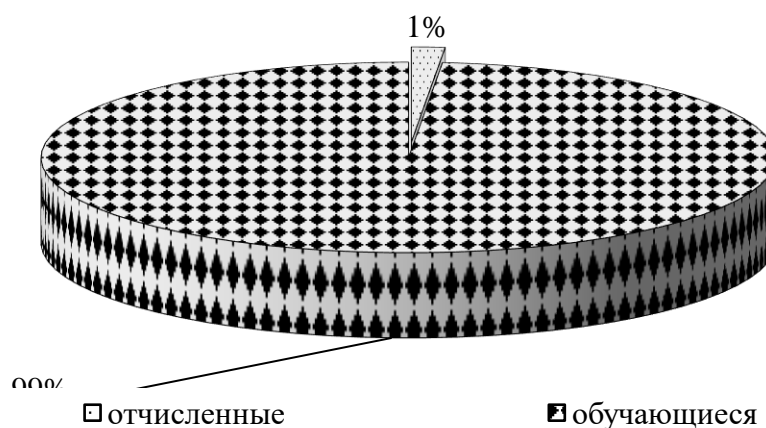


Рисунок 1–Структура категорий субъектов информации учащихся в ГБПОУ «Челябинский педагогический колледж №1»

Таким образом, основным источником носителей информации являются студенты проходящие обучение в образовательной организации. Наблюдается тенденция роста объема информации в ГБПОУ «Челябинский педагогический колледж №1», что обуславливает актуальность защиты информации в организации.

Так же, в архивах и в кадровой службе организации находиться более двухсот дел сотрудников уволенных и работающих на данный момент. В таблице 5 приведены статистические данные движение кадров в ГБПОУ «Челябинский педагогический колледж №1».

Таблица 5–Информацию сотрудников ГБПОУ «Челябинский педагогический колледж №1»

Субъекты	2016	2017	Изменение 2016- 2017	2018	Изменение 2017-2018
сотрудники	184	188	-1	187	-3
лица, обратившиеся с целью трудоустройства	13	11	-2	18	+7
лица, уволенные	2	1	-1	2	+1

ГБПОУ «Челябинский педагогический колледж №1» в целях реализации обучения и других возложенных функций использует следующие виды информационных ресурсов информации:

- автоматизированные информационные ресурсы информации, а именно информационные ресурсы, объединенные системами управления (обновляемые, справочные);
- автоматизированные информационные ресурсы, координатором которых является ГБПОУ«Челябинский педагогический колледж №1», используемые совместно с иными органами государственной власти (Министерство образования и пр);
- автоматизированные информационные ресурсы информации, оператором которых ГБПОУ«Челябинский педагогический колледж №1» не является, но в соответствии с законодательством РФ имеет доступ к хранящимся в них данным;

– локальные информационные ресурсы, используемые для обработки информации сотрудников ГБПОУ «Челябинский педагогический колледж №1».

ГБПОУ «Челябинский педагогический колледж №1» осуществляет обработку информации с использованием средств автоматизации, используя следующие информационные системы:

- «1С-Бюджет»;
- «1С-Зарплата-Кадры»;
- Автоматизированная информационная библиотечная система;
- информационная система «Налогоплательщик»

Места обработки информации:

- бухгалтерия;
- библиотека;
- учительская;
- отдел кадров;
- медпункт.

Исследование организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1» выявило ряд недостатков в функционировании системы защиты информации: нет документов регламентирующих функционирование системы защиты информации, так же, обращает на себя внимание отсутствие рекомендаций обеспечивающих создание единой, целостной и скоординированной информационной системы безопасности информации и создание условий для ее дальнейшего совершенствования.

## Глава 3. Разработка рекомендаций по повышению эффективности защиты информации

### 3.1. Пути повышения эффективности системы защиты информации

Ситуация с выполнением в ГБПОУ «Челябинский педагогический колледж №1» требований ФЗ-149 существенно усложняется особенностями его функционирования. К таковым можно отнести следующие:

- отсутствие финансовых средств на реализацию мер по организационной и технической защите информации;
- отсутствие штатных квалифицированных специалистов по информационной безопасности;
- сложность детерминации отношений между образовательным учреждением, обучаемыми, их представителями и иными лицами (родителями, опекунами, работодателями, организациями, выделяющими гранты, и т. п.).

В ГБПОУ «Челябинский педагогический колледж №1» необходимо осуществить планирование организации защиты информации, а так же разработать документы, регламентирующие ее функционирование.

Отсутствие элементарного положения о защите информации является нарушением закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации». На первый взгляд, штрафы за нарушение правил работы с информацией не так уж и высоки. Согласно статье 13.11 КоАП РФ штрафы составляют 5-10 тысяч рублей для организации и 500-1000 рублей для ее должностного лица.

Однако надо учитывать, что этот штраф может налагаться за каждое допущенное нарушение. А правил для тех, кто работает с информацией, законодатели установили очень много. Так что 10 тысяч рублей штрафа легко могут превратиться в 50 или 100 тысяч рублей даже в рамках одной проверки. А за год эти суммы могут оказаться еще внушительнее.

Главным документом, который должен иметь любой работодатель,

является положение о информации. Принять этот локальный акт, регулирующий порядок хранения и использования информации работодателя обязывает статья 87 Трудового кодекса. В положении обычно прописывают все требования к получению, хранению, комбинированию, передаче и любому другому использованию информации, а также гарантии по их защите.

Предлагается разработать основной документ регламентирующий безопасность информации – это положение о защите информации.

Необходимость разработки положения обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в ГБПОУ «Челябинский педагогический колледж №1», при обработке информации вообще, и информации в частности.

Положение будет определять основные цели и задачи, а также общую стратегию построения системы защиты информации. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Положение должно быть разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса рекомендаций, включающих исследование угроз информационной безопасности и разработку системы защиты информации, с позиции комплексного применения технических и организационных мер и средств защиты.

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

Положение будет служить основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ГБПОУ «Челябинский педагогический колледж №1», а также нормативных и методических документов, обеспечивающих ее реализацию, положение не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности

информационных технологий и защиту информации.

При планировании в ГБПОУ «Челябинский педагогический колледж №1» рекомендаций, связанных с защитой информации, рекомендуется привлекать юристов, специалистов отдела кадров и по информационной работе (компьютерным технологиям).

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

Главным условием защиты информации является четкая регламентация функций работников, а также принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных. Далее ключевым вопросом становится оценка наличия предусмотренных законодательством оснований для обработки информации, а в случаях, когда они отсутствуют, получение согласия субъекта информации на их обработку.

При этом согласно Закону от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» обязанность доказательства согласия субъекта информации на их обработку возлагается на оператора, т. е. на работодателя. Несмотря на то, что в данном комментарии речь идет исключительно о защите информации работников, хотелось бы в контексте обратить внимание на то, что обрабатываются информацию в образовательной организации обучающихся и их родителей, поэтому ГБПОУ «Челябинский педагогический колледж №1» предварительно должно получить согласие родителей на обработку информации их самих и их детей. Следует уделить особое внимание процедуре передачи информации третьим лицам. Для этого необходимо наличие: основания для такой передачи, предусмотренного федеральными законами, или согласия на обработку информации в школе субъекта

информации, закрепленного, например, в договоре на оказание услуг; договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности при обработке информации в образовательной организации. Необходимо очень внимательно подойти к вопросу размещения информации, содержащей информацию, на интернет-сайте ГБПОУ «Челябинский педагогический колледж №1».

С учетом выше изложенного можно выделить следующие обязательные этапы работы по защите информации работников:

- определение всех ситуаций, когда требуется проводить обработку информации;

- выделение процессов, в которых обрабатываются информацию;

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

- определение круга информационных систем и совокупности обрабатываемых информации;

- проведение категорирования информации и предварительной классификации информационных систем;

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

- внедрение системы обеспечения безопасности информации.

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

- создание внутренней документации по работе с информацией;

- организацию системы защиты информации;

- внедрение технических мер защиты информации.

Предлагается следующий пакет документов для ГБПОУ «Челябинский

педагогический колледж №1»:

- Положение о защите информации.
- Согласие работника образовательной организации на обработку своих информации.
- Согласие обучающегося (18лет и старше) в образовательной организации на обработку своих информации.
- Согласие законного представителя обучающегося (до18лет) в образовательной организации на обработку информации обучающегося.
- Положение об ответственном лице информационной безопасности образовательной организации.
- Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке информации.
- Журнал учета информации.
- Обязательство работника о неразглашении информации.
- Приказ «О ведении Электронного журнала обращений пользователей информации в ГБПОУ «Челябинский педагогический колледж №1».

Так же более эффективно осуществлять сегментирование до отдельных рабочих мест в сочетании с обезличиванием действующей информационной системы информации. При этом затраты на эксплуатацию единой обезличенной действующей информационной системы информации не увеличиваются, а хранить кодификаторы ФИО (или их части) можно непосредственно на тех рабочих станциях, на которых информацию визуализируются. Если действующей информационной система информации не является распределенной и не подключена к Интернету, то рекомендации по защите отдельных рабочих мест не потребуют больших затрат.

### 3.2. Разработка рекомендаций по повышению эффективности защиты информации в ГБПОУ «Челябинский педагогический колледж №1»



Представим проект организации системы защиты информации в ГБПОУ «Челябинский педагогический колледж №1» в виде таблицы 6.

Таблица 6 – Проект организации системы защиты информации в ГБПОУ «Челябинский педагогический колледж №1»

Рекомендации	Ответственное	Сроки
Издание приказа о назначении ответственных лиц за обработку информации и приказа о создании положения о информации	Директор	24.12. 2017
определение всех ситуаций, когда требуется проводить обработку информации	Ответственное лицо, администратор автоматизированных информационных систем, специалист отдела кадров, секретариат	24.12. 2017-11.01 2018г.
выделение процессов, в которых обрабатываются информацию	администратор автоматизированных информационных систем, администратор автоматизированных информационных систем,	12.01.2018-17.01.2018
формирование перечня подразделений и работников, участвующих в обработке информации в рамках своей служебной деятельности	Ответственное лицо, специалист отдела кадров, администратор автоматизированных информационных систем	12.01.2018-17.01.2018
определение круга информационных систем и совокупности обрабатываемых информации	Ответственное лицо за обработку информации, администратор автоматизированных информационных систем	17.01.2018-18.01.2018
проведение категорирования информации и предварительной классификации информационных систем	Ответственное лицо за обработку информации, администратор автоматизированных информационных систем	19.01.2018-22.01.2018
разработка пакета организационно-распорядительных документов для обеспечения защиты информации (положение, согласия, журнал и пр.)	Ответственное лицо за обработку информации, секретариат, специалист отдела кадров.	24.12. 2017-19.01 2018г.
Ознакомление под роспись всех лиц, имеющих доступ к персональным данным с положением о защите информации	Специалист отдела кадров, ответственное лицо	19.01 – 20.01 2018
разработку технических решений по построению системы защиты информации информационных систем информации, осуществить выбор средств защиты информации для использования в составе системе защиты информации.	администратор автоматизированных информационных систем	24.12. 2017-22.01 2018г.

На первом этапе издается приказ о назначении ответственного лица за

безопасность информации.

Основные задачи ответственного лица за безопасность информации заключаются в следующем.

– Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе информации.

– Обеспечение постоянного контроля в подразделениях за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе информации.

– Разработка и внесение предложений по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе информации.

Проект положения об ответственном лице за информационную безопасность ГБПОУ «Челябинский педагогический колледж №1».

Рекомендуемая структура положения:

- Общие положения.
- Задачи.
- Функции.
- Взаимодействие.
- Ответственность.

Предлагается к работе проект положения о информации обучающихся в ГБПОУ «Челябинский педагогический колледж №1».

Начать положение рекомендуется с раздела с основных понятия и обозначений. Далее выделить понятия и состав информации . Третьим пунктом рекомендуется включить «Создание и обработка информации». В нем обязательно нужно зафиксировать, что информацию в организации можно получить и обрабатывать исключительно на основании письменного согласия работника. А значит, сразу разрабатывается и утверждается форма такого заявления. На подпись такое заявление работнику надо давать сразу

при приеме на работу. А по действующим сотрудникам такую работу придется провести сразу же после утверждения Положения.

В обязательном порядке необходимо взять письменное заявление на обработку информации о обучающихся и родителей.

Далее может следовать раздел «Доступ к персональным данным». В нем последовательно описывается порядок доступа к таким данным работников организации и третьих лиц (отдельно родственников, государственных органов, представителей других организаций). При необходимости тут можно ввести уровни доступа в зависимости от должности сотрудника. Например, директор и аппарат дирекции имеют доступ ко всем персональным данным; сотрудники бухгалтерии - только к тем сведениям, которые необходимы для расчета заработной платы и налогов; представители кадровой службы – к сведениям, необходимым для оформления кадровой документации и т.п.

Продолжит Положение раздел «Порядок обработки и передачи данных». Здесь надо зафиксировать правила для передачи данных о сотрудниках определенным органам или лицам. В случаях, когда передача данных регулируется законодательно (налоговые органы, органы статистики, Пенсионный фонд и т.п.) достаточно сделать ссылки на порядок передачи сведений, установленный законодательством. Но, при этом следует обязательно зафиксировать, кто и в каком порядке вправе готовить данные сведения для передачи в госорганы. В положение обязательно включить раздел ответственность.

Предлагается следующая структура положения о информации работников и обучающихся в ГБПОУ «Челябинский педагогический колледж №1»:

- Общие положения.
- Основные понятия, обозначения.
- Цели и задачи .

- Понятие и состав информации.
- Создание и обработка информации.
- Доступ к персональным данным.
- Порядок хранения, использования и передачи информации.
- Обязанности работодателя по хранению и защите информации работника.

- Обязанности работника администрации, имеющих доступ к персональным данным обучающегося.

- Ответственность работодателя и лиц, осуществляющих работу с информацией

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

Со всех лиц, имеющих доступ к персональным данным рекомендуется под роспись взять обязательство о конфиденциальности и неразглашении информации.

В ГБПОУ «Челябинский педагогический колледж №1» рекомендуется разработать инструкцию по проведению мониторинга информационной безопасности и антивирусного контроля при обработке информации.

В Инструкции рекомендуется отразить следующее:

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

Проект журнала обращений по ознакомлению с информацией.

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

Хранение журналов должно исключать несанкционированный доступ к ним.

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

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

Так же, в нашем случае целесообразно сегментировать слабо взаимодействующие подсистемы информационной системы информации, так необходимо разделить кадровый и бухгалтерский учета персонала и организовать обмен данными между ними с помощью съемных носителей.

Учитывая, что с июля 2017 года ужесточилось законодательство по работе с информацией ГБПОУ «Челябинский педагогический колледж №1» необходимо ввести в практику разработанные нами рекомендации. В таблице 7 приведена эффективность разработанных рекомендаций.

Таблица 7 – Эффективность рекомендаций для ГБПОУ «Челябинский педагогический колледж №1» в целях организации защиты информации

Затраты	Эффективность
---------	---------------

<p>На расходные материалы:  бумага (А4) 4000 листов - 1600руб  картридж в принтер (1) – 2100руб.  Затраты на персонал равны 0, так как работа по совершенствованию деятельности образовательной организации входит в функциональные обязанности управленческого персонала</p>	<p>Избежание штрафов:  – за обработку данных без согласия – штраф до 75 тыс. руб.;</p> <p>– оператор информации (например, работодатель или интернет-сайт) обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки информации – штраф до 30 тыс. руб.</p>
---	---

Предложенные нами рекомендации помогут существенно снизить угрозу разглашением информации и избежать неблагоприятных последствий. Организовать систему защиты информации образовательной организации СПО, соответствующую современным требованиям и законодательству РФ.

## Заключение

Проведенное исследование в рамках поставленной цели и выдвинутых задач позволило делать следующие выводы.

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

Нормативной основой защиты информации являются нормы Конституции РФ, Федерального закона «О информации», Указ Президента РФ «О перечне сведений конфиденциального характера» и другие акты.

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

В Российской Федерации защита информации сводится к созданию режима обработки информации, которые включают ряд последовательных этапов.

В системе защиты информации информационная система обработки информации выбирается в зависимости от класса информационной системы и исходя из угроз безопасности персональным данным, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки информации с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Исследование проводилось на базе ГБПОУ «Челябинский педагогический колледж №1». Деятельность ГБПОУ «Челябинский

педагогический колледж №1»целиком направлена на четкое исполнение образовательных функций.

Для исследования организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1»были проведены оргпроектные работы. План работы включал этап обследования и этап проектирования.

Организационно-методический документ – рабочая программа предпроектного обследования предполагала применения методов исследования: изучение документов, непосредственное наблюдение, статистический, графический.

Основной целью создания защиты информации в ГБПОУ «Челябинский педагогический колледж №1»области является минимизация ущерба от возможной реализации угроз безопасности информации.

**В** ГБПОУ «Челябинский педагогический колледж №1»в целях реализации государственных услуг и других возложенных функций использует следующие виды информационных ресурсов информации:

- «1С-Бюджет»;
- «1С-Зарплата-Кадры»;
- Автоматизированная информационная библиотечная система;
- информационная система «Налогоплательщик»

При обработке информации в пределах ГБПОУ «Челябинский педагогический колледж №1» система соответствует нераспределенным информационным системам информации класса КЗ. При этом лицензий ФСТЭК России от оператора информации не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Исследование организации защиты информации в ГБПОУ «Челябинский педагогический колледж №1» выявило ряд недостатков в функционировании системы защиты информации: нет документов регламентирующих функционирование системы защиты информации, так же, обращает на себя внимание отсутствие рекомендаций обеспечивающих создание единой, целостной и скоординированной информационной системы безопасности информации и создание условий для ее дальнейшего



совершенствования.

В целях создания единой, целостной и скоординированной системы информационной безопасности информации и создание условий для ее дальнейшего совершенствования, предлагается комплексный подход для которого необходимо разработать следующий пакет документов для ГБПОУ «Челябинский педагогический колледж №1»:

- Положение о защите информации.
- Согласие работника образовательной организации на обработку своих информации.
- Согласие обучающегося (18 лет и старше) в образовательной организации на обработку своих информации.
- Согласие законного представителя обучающегося (до 18 лет) в образовательной организации на обработку информации обучающегося.
- Положение об ответственном лице информационной безопасности образовательной организации.
- Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке информации.
- Журнал учета информации.
- Обязательство работника о неразглашении информации.
- Приказ «О ведении Электронного журнала обращений пользователей информации в ГБПОУ «Челябинский педагогический колледж №1».

Целесообразно сегментировать слабо взаимодействующие подсистемы информационной системы информации, так необходимо разделить кадровый и бухгалтерский учета персонала и организовать обмен данными между ними с помощью съемных носителей.

Необходимость разработки предложенных выше положений и документов обусловлена стремительным расширением сферы применения информационных технологий и процессов на ГБПОУ «Челябинский

педагогический колледж №1», при обработке информации вообще, и информации в частности.

Реализация предложенных рекомендаций регламентированных разработанными документами в информационных системах информации позволит:

- оценить состояние безопасности информации в информационных системах информации, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к информационным системам информации;

- провести классификацию, аттестацию информационных систем информации;

- провести организационно-режимные и технические рекомендации по обеспечению безопасности информации в информационных системах информации;

- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих рекомендаций обеспечит создание единой, целостной и скоординированной системы информационной безопасности информационных систем информации и создаст условия для ее дальнейшего совершенствования.

Кроме того, подложенные нами рекомендации помогут существенно снизить угрозу разглашением информации и избежать неблагоприятных последствий. Организовать систему защиты информации образовательной организации СПО, соответствующую современным требованиям и законодательству РФ.

## Список использованных источников

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_28399/](http://www.consultant.ru/document/cons_doc_LAW_28399/)
2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.10.2017)// Консультант Плюс : справ. правовая система. Режим доступа – [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_34683/](http://www.consultant.ru/document/cons_doc_LAW_34683/)
3. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 29.07.2017) «Об образовании в Российской Федерации» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_140174/27f9ddea0cccf9a6b90bb2cb8b545d436f18157b/](http://www.consultant.ru/document/cons_doc_LAW_140174/27f9ddea0cccf9a6b90bb2cb8b545d436f18157b/)
4. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 28.12.2016) «Об организации предоставления государственных и муниципальных услуг» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_103023/](http://www.consultant.ru/document/cons_doc_LAW_103023/)
5. Федеральный закон от 27.07.2006 N 179-ФЗ (ред. от 29.07.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2017) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)
6. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа – [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/)

7. Приказ ФСБ России от 10.07.2017 N 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2017 N 33620) [Электронный ресурс]// Консультант Плюс : справ. правовая система. Режим доступа - [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_146520/](http://www.consultant.ru/document/cons_doc_LAW_146520/)

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

9. Амелин, Р.В. Информационное право в схемах : учебное пособие / Р.В. Амелин, С.А. Куликова, С.Е. Чаннов ; отв. ред. С.Е. Чаннов. - М. : Проспект, 2016. - 125 с

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

11. Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института информации в трудовом праве [Текст]/ Ф.А. Абаев // Пробелы в российском законодательстве. 2018. –№ 5. – С. 136-139.

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

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

14. Ануфриева, Н.С. Правовые проблемы обработки информации в трудовых отношениях [Текст]/ Н.С. Ануфриева // Актуальные проблемы

современной юридической науки: Сборник научных трудов. Сургут: ИЦ СурГУ, 2017. –С. 114-119.

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

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

17. Бегларян, М.Е. Безопасность информации в современной России [Текст]/ М.Е.Бегларян, Е.А. Пичкуненко // Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов материалы 4-ой Международной научно-практической конференции. 2017. С. 24-28.

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

19. Бобров, И.В. Проблема защиты информации работника [Текст]/ И.В.ю Бобров, Ю.В. Комарецев // Проблемы российского законодательства и международного права Сборник статей Международной научно-практической конференции. Ответственный редактор: Сукиасян Асатур Альбертович . 2017. - С. 26-28.

20. Бойкова, О.Ф. Обработка информации работников [Текст]/ О.Ф. Бойкова // Независимый библиотечный адвокат. 2017. - № 2. С. 21-32.

21. Болотин, В.С. Механизм защиты права на неприкосновенность частной жизни при обработке информации в информационных системах [Текст]/ В.С.Болотин, М.А. Маслѐха // Вестник государственного и муниципального управления. 2017. - № 3. С. 99-103.

22. Бондарь, А.О. Организация работы по обеспечению защиты государственных информационных систем информации [Текст]/

А.О.Бондарь, В.П. Железняк, В.А. Мещеряков // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции. Воронеж: ИПЦ «Научная книга», 2017.- С. 174-175.

23. Балашкина, И. В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации [Текст]/ И. В. Балашкина. // Право и политика. 2017. – №7. – С. 92-105.

24. Блоцкий, В.Н. Конституционное обеспечение права человека на неприкосновенность частной жизни в Российской Федерации [Текст]/ В.Н. Блоцкий. // Автореф. дис. канд. юрид. Наук – М. 2017. – с. 31.

25. Борисова, С. А. Общие требования при обработке информации работника и гарантии их защиты [Текст]/ С. С. Борисова // Трудовое право. 2017. – N 11. – С. 30-36.

26. Бобылева, М.П. Вопросы использования элементов электронного документооборота внутри организации [Текст]/ М.П. Бобылева// Делопроизводство. 2016. – №2. – С. 15.

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

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

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

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

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

32. Ищейнов, В. Я. Информацию в законодательных и нормативных

документах Российской Федерации и информационных системах [Текст] / В. Я. Ищейнов // Делопроизводство. 2016. – N 3. – С. 87-90.

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

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

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

36. Макаров, А.М. Организация защиты информации : лабораторный практикум / Федеральное государственное автономное образовательная организация высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации ; авт.-сост. А.М. Макаров, И.В. Калиберда и др. - Ставрополь : СКФУ. 2017. - 92 с.

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

38. Международные трудовые стандарты и российское трудовое право: перспективы координации: монография / Э.Н. Бондаренко, Е.С. Герасимова, С.Ю. Головина и др.; под ред. С.Ю. Головиной, Н.Л. Лютова. М.: НОРМА, ИНФРА-М, 2016.

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

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

41. Минаев, В. А. Информационные операции и проблема формирования Современной культуры информационной безопасности / В. А.

Минаев // Системы высокой доступности. 2017. №3. – С. 38-46.

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

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

44. Новичкова, Ю. В. Информацию - без права передачи, или Особенности расторжения трудового договора за разглашение информации[Текст]/ Ю. в. Новикова // Справочник кадровика. – 2016. – N 1. – С. 14-23.

45. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Федеральное государственное автономное образовательная организация высшего образования «Северо-Кавказский федеральный университет», Министерство образования и науки РФ. - Ставрополь : СКФУ, 2017. - 86 с.

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

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

48. Соколова, О. С. Проблемы реализации Федерального закона «О информации» [Текст]/ О. С. Соколова// Современное право. - 2017. - N 9. - С. 37-41.

49. Силакова О. В. Комплексная безопасность образовательной организации как важнейшее условие обеспечения безопасных условий



проведения учебно-воспитательного процесса // Молодой ученый. — 2017. — №18.1. — С. 84-88.

50. Скрыль, С. В. Показатели эффективности информационных процессов и их защищенности в системах реального времени / С. В. Скрыль // Безопасность информационных технологий. – М. : МИФИ, 2017. - № 3. –С. 104-106.

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

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

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

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

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

