Министерство общего и профессионального образования Ростовской области
государственное бюджетное профессиональное
образовательное учреждение Ростовской области
«Ростовский-на-Дону колледж радиоэлектроники, информационных
и промышленных технологий»
(ГБПОУ РО «РКРИПТ»)

ДОПУЩЕН К ЗАЩИТЕ
Заместитель директора
по учебно-методической работе
_____ С.А. Будасова
«_____» июня 2019 г.

ДИПЛОМНАЯ РАБОТА

по специальности 46.02.01 Документационное обеспечение управления и архивоведение

Тема **Правовое регулирование организации конфиденциального делопроизводства в организации на примере ГБПОУ РО «РКРИПТ»**

РКРИПТ.46.02.0102.3115.000ДР

Работу выполнил _____ Е.С.Петрикеева

Нормоконтроль _____ Е.Н.Круглова

Руководитель _____ М.В.Маркина

Рецензент _____

2019

Содержание

Перечень сокращений.....4
Введение.....5
Глава 1 Правовые и организационные основы конфиденциального делопроизводства.....8
1.1 Понятие и особенности конфиденциальной информации, источники ее правового регулирования.....8
1.2 Порядок организации конфиденциального делопроизводства.....14
Глава 2 Механизм обеспечения сохранения конфиденциальности персональных данных на примере ГБПОУ РО «РКРИПТ».....18
2.1 Общие требования к обработке персональных данных работников, обучающихся и выпускников ГБПОУ РО «РКРИПТ».....18
2.2 Меры по обеспечению конфиденциальности персональных данных.....24
2.3 Обязанности оператора при сборе персональных данных.....31
Глава 3 Охрана и защита конфиденциальной информации.....39
3.1 Юридическая ответственность за нарушения законодательства о конфиденциальной информации.....39
3.2 Надзор за соблюдением законодательства о конфиденциальной информации.....42
Заключение.....48
Список использованных источников.....51
Приложение А (обязательное) Соглашение о неразглашении персональных данных субъекта.....53
Приложение Б (обязательное) Журнал учета передачи персональных данных.....54

Приложение В (обязательное) Согласие на обработку персональных данных работника.....55
Приложение Г (обязательное) Согласие на обработку персональных данных подопечного.....56
Приложение Д (обязательное) Согласие субъекта на получение его персональных данных у третьей стороны.....57
Приложение Е (обязательное) Отзыв согласия на обработку персональных данных.....58

Перечень сокращений

В настоящей работе применяют следующие сокращения:

АИС – автоматизированная информационная система

ГБПОУ РО «РКРИПТ» – государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий».

ДОУ –Документационное обеспечение управления

ИСПД – Информационные системы персональных данных

КоАП РФ – Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ

ПФР –Пенсионный фонд Российской Федерации

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

РФ – Российская Федерация

СЭД – Система электронного документооборота

ТК РФ – Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ

УК РФ – Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ

ФЗ «О коммерческой тайне»– Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ

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

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

ФСС – Фонд социального страхования Российской Федерации

Введение

Современное общество все чаще встречается с информационным обменом в своей повседневной жизни. Каждый из нас регулярно сообщает о себе информацию, позволяющую напрямую или косвенно определить и идентифицировать нас. С учетом положений действующего законодательства Российской Федерации, такая информация является нашими персональными данными. Согласно действующему Указу Президента Российской Федерации от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»,персональные данные являются конфиденциальной информацией. В статье 2 ФЗ «Об информации, информатизации и защите информации» конфиденциальная информация определена как документированная информация, доступ к которой ограничивается в соответствие с законодательством РФ.

В достаточном бурном развитии экономики России и в условиях ужесточения конкурентной борьбы на рынке, все чаще организации подвергаются различным видам коммерческих шпионажей, в том числе и промышленным. Как правило, в большинстве случаев, организации и предприятия используют бумажные носители информации (в том числе и конфиденциальной) из-за их более удобного практичного и долговечного хранения. Однако бумажные носители не имеют никаких специальных степеней безопасности, как электронные и другие виды носителей, поэтому сохранность бумажных документов зависит, в частности, от правильной организации конфиденциального документооборота.

Актуальность выбранной темы обусловлена необходимостью строгого соблюдения организациями норм действующего законодательства, регулирующего конфиденциальное делопроизводство. Несоблюдение установленных правил работы с конфиденциальной информацией может стать причиной её утечки, что влечет за собой причинение имущественного

ущерба организации, а в случаях, установленных действующим законодательством, наступление юридической ответственности.

Система делопроизводства постоянно усложняется, и современное делопроизводство представляет собой организацию документооборота, в котором задействовано множество структурных подразделений и их сотрудников. Обязанности каждого сотрудника четко регламентированы и находятся в рамках подразделения, в котором он задействован. В связи с этим усложняется задача защиты конфиденциальной информации, поскольку конфиденциальное делопроизводство имеет не менее сложную организацию по сравнению с открытым делопроизводством.

Наиболее существеннымявляется многоступенчатый учет всех процедур и операций, выполняемых с документом, что отличает технологию обработки и хранения конфиденциальных документов от документов открытых и что лежит в основе процесса защиты этих документов от любого вида угроз по организационным и техническим каналам.

Объектом исследования данной работы являются общественные отношения, возникающие по поводу организации конфиденциального делопроизводства.

Предметом исследования выступают как федеральные нормативные правовые акты, регулирующие порядок работы со сведениями конфиденциального характера, так и локальные акты ГБПОУ РО «РКРИПТ».

Целью данной работы является комплексное исследование вопросов организации конфиденциального делопроизводства на примере ГБПОУ РО «РКРИПТ».

Для достижения указанной цели в работе поставлены следующие задачи:

1) исследовать понятие и виды конфиденциальной информации, особенности ее правового режима,

2) определить и изучить источники правового регулирования конфиденциальной информации,

3) в связи с особенностью организации, на примере которой раскрывается тема дипломного исследования, особое внимание уделить вопросам обработки и защиты персональных данных,

4) исследовать виды юридической ответственности за нарушение законодательства о конфиденциальной информации.

Структура работы обусловлена предметом, целью и задачами исследования. Работа состоит из введения, трех глав и заключения.

Во введении раскрывается актуальность данного дипломного исследования, определяется теоретическая и практическая значимость работы. Также во введении устанавливаются объект и предмет, ставятся цель и задачи дипломного исследования.

В первой главе рассматриваются правовые и организационные основы конфиденциального делопроизводства.

Во второй главераскрывается механизм обеспечения сохранения конфиденциальности персональных данных работников на примере ГБПОУ РО РКРИПТ.

Третья глава посвящена охране и защите конфиденциальной информации.

В заключении подводятся итоги исследования, формируются окончательные выводы по рассматриваемой теме.

Глава 1 Правовые и организационные основы конфиденциального делопроизводства

1.1 Понятие и особенности конфиденциальной информации, источники ее правового регулирования

Понятие «конфиденциальная информация» стало неотъемлемой частью российской юридической лексики. В настоящий момент оно используется в нескольких сотнях нормативных правовых актов Российской Федерации.

Согласно ст.2 ФЗ «Об информации, информационных технологиях и защите информации»конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (23, ст. 2).[1]

Обладателями информации могут быть гражданин (физическое лицо), юридическое лицо, государственные органы и органы местного самоуправления (далее – государственные и негосударственные структуры) в пределах их полномочий. Обладатель информации вправе:

- разрешать или ограничивать доступ к информации,
- определять порядок и условия такого доступа,
- использовать информацию, в том числе распространять ее по своему усмотрению,

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

- передавать информацию другим лицам по договору или на ином установленном законом основании.

При осуществлении своих прав обладатель информации обязан:

- принимать меры по защите информации,

- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Информация ограниченного доступа, относящаяся к конфиденциальной и составляющая какую-либо тайну, за исключением государственной, не существует сама по себе.

Государственная тайна – самостоятельная правовая категория, и ее правовой режим является предметом регулирования отдельной отрасли законодательства. Если рассмотреть более подробно общедоступную нормативную правовую базу о государственной тайне, то можно отметить следующее:

- сведения, составляющие государственную тайну или отнесенные к государственной тайне, – это информация ограниченного доступа, особенности которой необходимо знать при изучении особенностей конфиденциальной информации, также относящейся к категории ограниченного доступа,

- технологии конфиденциального делопроизводства и документооборота во многом совпадают с технологиями организации работы с документированной информацией, составляющей государственную тайну, и самое главное – по своей сути они не являются секретными и определены в общедоступной нормативной правовой базе о государственной тайне.[2]

Виды конфиденциальной информации установлены Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (в ред. от 13.07.2015).[3] К ней относятся:

---

[2] Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, А.Г. Фабричнов; под общ.ред. Н.Н. Куняева. – М.: Логос, 2016.— 500 с.

[3] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13.07.2015)

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях,

2) сведения, составляющие тайну следствия и судопроизводства,

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна),

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.),

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна),

6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Персональные данные, в соответствии с ФЗ «О персональных данных»,[4]– любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Указанным законом установлен порядок обработки персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не

[4] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017)

входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств.

Служебные сведения ограниченного доступа (служебная тайна). Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (в ред. от 13.07.2015) определяет служебную тайну как служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами [2].

Постановлением Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»[5] установлен порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти относит к служебной информации ограниченного распространения несекретную информацию, касающуюся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. Положением установлено, что на документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования». Положение также определяет порядок изготовления, учета документов ограниченного распространения и организации их документооборота.

[5] Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

Сведения, связанные с профессиональной деятельностью: врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и др. Порядок обращения и порядок доступа к информации, составляющей различные виды профессиональной тайны, регламентируется рядом законодательных актов Российской Федерации.[6] Как правило, это законодательные акты, регулирующие отношения в определенных сферах деятельности. Например, Федеральный закон от 31.05.2002 № 63-ФЗ (в ред. 29.07.2017 г.) «Об адвокатской деятельности и адвокатуре в Российской Федерации»[7]содержит ст. 8 «Адвокатская тайна», в которой установлено, что адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

Основы законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1 (в ред. от 18.10.2018)[8] устанавливают: «Нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий, или увольнения, за исключением случаев, предусмотренных настоящими Основами. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия» (ст. 5).

[6] https://www.profiz.ru/sr/4_2008/normativnaya_baza_raboty/

[7] Федеральный закон от 31.05.2002(в ред. 29.07.2017 г.) № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31.05.2002(в ред. 29.07.2017 г.) № 63-ФЗ

[8] «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 01.02.2019)

Федеральный закон от 17.07.1999 № 176-ФЗ[9] «О почтовой связи» содержит положения, направленные на защиту тайны связи, – тайны переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи. Тайна связи не подлежит разглашению без согласия пользователя услуг почтовой связи. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи[6]. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям (ст. 15).

Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений в соответствии с Уголовным кодексом Российской Федерации (ст. 138) влечет уголовную ответственность.

Сведения, связанные с коммерческой деятельностью, доступ к которым ограничивается (коммерческая тайна). Определение коммерческой тайны приведено в Гражданском кодексе Российской Федерации (ст. 139) и ФЗ «О коммерческой тайне».[10] Закон трактует коммерческую тайну как конфиденциальность информации, позволяющую ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (ст. 3).

ФЗ «О коммерческой тайне» устанавливает виды информации, которая не может составлять коммерческую тайну. Это информация, содержащаяся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об

[9] Федеральный закон «О почтовой связи» от 17.07.1999 № 176-ФЗ

[10] Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ

индивидуальных предпринимателях в соответствующие государственные реестры; содержащаяся в документах, дающих право на осуществление предпринимательской деятельности; о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов; о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом; о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест и др. (ст. 5).

Данный Закон устанавливает меры организационного характера, обеспечивающие защиту документов, содержащих коммерческую тайну, от несанкционированного доступа. В том числе законом установлен гриф ограничения доступа к документам, содержащим коммерческую тайну, – «Коммерческая тайна».

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, в соответствии с Указом Президента РФ 06.03.1997 № 188, также являются конфиденциальной информацией. Меры по защите такого рода информации установлены Гражданским кодексом Российской Федерации (ч.4).

1.2 Порядок организации конфиденциального делопроизводства

Организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации.

Организация конфиденциального делопроизводства должна включать в себя учет, хранение, обработку и использование конфиденциальных документов, установление его статуса, структуры, обеспечение необходимых условий труда, разработку или приобретение нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства, создание постоянно действующей экспертной комиссии, оформление допуска сотрудников к коммерческой тайне и обучение их правилам работы с конфиденциальными документами. [11]

Организации конфиденциального делопроизводства в информационной безопасности уделяется, как правило, наименьшее внимание, хотя получение конфиденциальной информации через пробелы в делопроизводстве является одним из наиболее доступных способов.

Этапы создания отдела конфиденциального делопроизводства:[12]

1 этап — создание специального подразделения, отвечающего за делопроизводство в организации или введение в штат должности, в чьи функциональные обязанности будет входить обеспечение делопроизводства организации,

2 этап — приобретение необходимого оборудования, принадлежностей для работы отдела конфиденциального делопроизводства, установка сейфов, шкафов, технического оборудования,

3 этап — создание и принятие необходимых локальных документов (инструкций, положений, договоров, должностных обязанностей и т.д.),

---

[11] Конфиденциальное делопроизводство и защита коммерческой тайны. Курс лекций: МАБИВ; Орел; 2014

[12] Конфиденциальное делопроизводство: Учебное пособие: / Сост. Е.А.Давыденко. — Нижневартовск: Изд-во Нижневарт. гос. ун-та, 2015. — 83 с.

4 этап — ознакомление с нормативными документами сотрудников в рамках их должностных обязанностей,

5 этап — создание особых механизмов административного контроля за соблюдением конфиденциального делопроизводства,

6 этап — создание и регламентация механизма персональной ответственности за нарушение правил конфиденциального делопроизводства.

Порядок создания конфиденциального бумажного делопроизводства:

1 этап — создание делопроизводства на бумагоносителях,

2 этап — определение перечня сведений конфиденциального характера,

3 этап — утверждение перечня сведений, носящих конфиденциальный характер,

4 этап — определение правил ведения конфиденциального делопроизводства на основе общего делопроизводства на бумагоносителях,

5 этап — регламентация порядка допуска сотрудников к секретным сведениям,

6 этап — заключение договоров о нераспространении конфиденциальных сведений между сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации,

7 этап — создание необходимой нормативно-правовой базы, регламентирующей конфиденциальное делопроизводство,

8 этап — доведение нормативных документов до сведения сотрудников,

9 этап — организация механизмов управленческого и технического контроля за сотрудниками, работающими с конфиденциальными документами,

10 этап — разъяснение основных моментов административной, уголовной и гражданско-правовой ответственности сотрудникам - носителям конфиденциальной информации, оформляющих секретные документы.

Порядок изготовления конфиденциальных документов, режим обращения с ними требуют определенных знаний, которые должны быть приобретены до начала работы с документами и постоянно пополняться. С этой целью необходимо организовывать различные формы обучения сотрудников: техническую учебу, семинары, самостоятельную подготовку со сдачей зачетов и др.

Для проведения занятий следует привлекать не только сотрудников подразделения конфиденциального делопроизводства, но и руководителей соответствующих подразделений предприятия, а также специалистов по конфиденциальному делопроизводству, работающих в соответствующих научно-исследовательских и учебных заведениях [12].

Глава 2 Механизм обеспечения сохранения конфиденциальности персональных данных на примере ГБПОУ РО «РКРИПТ»

2.1 Общие требования к обработке персональных данных работников, обучающихся и выпускников ГБПОУ РО «РКРИПТ»

Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий» (ГБПОУ РО «РКРИПТ», Колледж) является оператором персональных данных, то есть лицом, самостоятельно или совместно с другими лицами, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные работников, то есть та информация, которой обладает работодатель, как в условиях ее ручной обработки, так и в случае использования автоматизированных информационных систем может стать в определенной мере открытой и привести к ущемлению их интересов и прав, причинить моральный вред и материальный ущерб.

В связи с этим в ГБПОУ РО «РКРИПТ» действует локальный нормативный правовой акт Положение «Об обработке и защите персональных данных»[13], утвержденное директором колледжа от 07.08.2017г.

Положение разработано в соответствии с Конституцией РФ,[14] Трудовым кодексом РФ[15], ФЗ «Об информации, информационных технологиях и о защите информации»[1], ФЗ «О персональных данных»[4], Постановлением Правительства РФ от 15.09.2008 г № 687 «Об утверждении Положения об особенностях обработки персональных данных,

[13] Положение «Об обработке и защите персональных данных» в ГБПОУ РО «РКРИПТ», утвержденное директором колледжа от 07.08.2017 г.

[14] «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993)

[15] «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ

осуществляемой без использования средств автоматизации»[16], нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора.

Положение определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, обучающихся и выпускников в соответствии с законодательством Российской Федерации и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю [13].

Как указывалось ранее, персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных – определенному или определяемому физическому лицу (ст. 3ФЗ «О персональных данных»).

К ним относятся:

- фамилия, имя, отчество,

- пол, возраст,

- изображение человека (фотография и видеозапись), которое позволяет установить личность и с этой целью используется оператором - место жительства,

- семейное положение, наличие детей, родственные связи,

- факты биографии и предыдущая трудовая деятельность (место работы, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.),

- финансовое положение. При этом в соответствии с письмомРоскомнадзора от 07.02.2014 № 08КМ-3681, сведения о заработной плате также являются персональными данными,[17]

- деловые и иные личные качества, которые носят оценочный характер,

[16] Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

[17] Письмо Роскомнадзора от 07.02.2014 № 08КМ-3681 «О передаче работодателем третьим лицам сведений о заработной плате работников»

- прочие сведения, которые могут идентифицировать человека.

Персональные данные можно классифицировать на:

1) общие персональные данные — это основная информация о человеке (например, фамилия, имя и отчество; дата рождения; место рождения; гражданство и др.),

2) биометрические персональные данные — это физиологические и биологические характеристики субъекта: дактилоскопические изображения, группа крови, рост, цвет глаз, вес, анализ ДНК и т.д,

3) специальные персональные данные — раса и национальность, вероисповедание, философские убеждения, состояние здоровья, наличие судимостей, интимная жизнь,

4) обезличенные персональные данные — это данные, доступные для любого заинтересованного лица. Источниками информации могут быть: адресные книжки; справочники; реестры; СМИ.

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора. Такие сведения могут содержаться в следующих документах:

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

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

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

- трудовая книжка или ее копия. Содержит сведения 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,

- документы воинского учета. Содержат информацию об отношении работника к воинской обязанности и необходимы работодателю для осуществления в организации воинского учета работников,

- справка о доходах с предыдущего места работы. Такая справка может понадобиться работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством,

- документы об образовании. Подтверждают квалификацию работника, обосновывают занятие определенной должности,

- документы обязательного пенсионного страхования. Нужны работодателю для уплаты за работника соответствующих взносов,

- трудовой договор. В нем содержатся сведения о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные 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 персональные данные 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 персональные данные соискателей, к ней в полной мере относятся установленные законом требования о сборе, обработке, хранении, защите персональных данных.

Следует указать, что обработка персональных данных представляет собой действие с ними, включая сбор, систематизацию, накопление,

хранение, уточнение, использование, распространение,обезличивание, блокирование, и их уничтожение.

ГБПОУ РО «РКРИПТ», как оператор персональных данных, вправе согласно ФЗ «О персональных данных» применять следующие технологии их обработки:

- использование персональных данных – это действия с ними, совершаемые оператором в целях принятия решения, или иные действия, порождающие юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы этого субъекта или других физических лиц,

- распространение персональных данных – это действие, направленное на их передачу определенному кругу лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ним каким-либо иным способом,

- обезличивание персональных данных – действия, в результате которых невозможно определить их принадлежность конкретному физическому лицу,

- блокирование персональных данных – временное прекращение их сбора, систематизации, накопление, использование, распространения, в том числе их передачи,

- уничтожение персональных данных – действие, в результате которых либо невозможно восстановить их содержание в АИС, либо уничтожаются материальные носители персональных данных,

- обработка персональных данных может осуществляться оператором только с согласия субъектов персональных данных. Однако в отдельных случаях согласия субъекта на обработку не требуется, например, при обработке кадровой документации в организации, где работает этот субъект[4].

Работодатель с согласия работника вправе поручить обработку его персональных данных(ведение кадрового, бухгалтерского учета и пр.) другому лицу (ч. 3 ст. 6 ФЗ «О персональных данных», абз. 2 п. 5 Разъяснений Роскомнадзора[18]). При этом ответственность перед работником за действия указанного лица несет работодатель (ч. 5 ст. 6 ФЗ «О персональных данных»).

Хранение персональных данных должно осуществляться в форме, позволяющей определить физическое лицо, не дольше чем этого требуют цели обработки этих данных. По достижению целей обработки или в случае утраты необходимости достижении этих целей последнее подлежит уничтожению [4].

Так, в п. 3.2.9. Положения «Об обработке и защите персональных данных» ГБПОУ РО «РКРИПТ», указано, что в случае увольнения, отчисления субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных вписьменном соглашении, оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональныеданные. В срок, не превышающий трех рабочих дней с даты достижения целиобработки персональных данных, если иное не предусмотрено федеральнымизаконами.

Основные принципы обработки персональных данных в Российской Федерации содержатся в ст. 5 ФЗ «О персональных данных» [3]. К ним относятся: законность целей и способов обработки персональных данных; соответствие целей обработки данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора; соответствие объема и характера обрабатываемых персональных данных и способов их обработки целям обработки персональных данных; достоверность персональных данных, их достаточность для целей обработки,

[18] Разъяснения Роскомнадзора«Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»

недопустимость обработки данных, избыточных по отношению к целям, заявленным при сборе персональных данных; недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

При обработке персональных данных колледж и его работники, а также работники сторонних организаций, обрабатывающие персональные данные, обязаны соблюдать следующие требования:

1) обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения Конституции РФ, законов и иных нормативных правовых актов РФ, содействия субъектам персональных данных в трудоустройстве, продвижении по службе, обучении, контроля количества и качества выполняемой работы, обеспечения личной безопасности субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора,

2) персональные данные не могут быть использованы в целях причинения имущественного и (или) морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации,

3) при принятии решений, затрагивающих интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения,

4) субъекты персональных данных или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области,

5) субъекты персональных данных, не являющиеся работниками, или их законные представители имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области,

6) субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

2.2 Меры по обеспечению конфиденциальности персональных данных

В каждой организации должен быть установлен строгий порядок обмена конфиденциальной документированной информацией, который является составной частью внутри объектного режима и направлен на обеспечение сохранности конфиденциальных документов и предотвращение утечки содержащейся в них информации [2].

Для обеспечения физической сохранности конфиденциальных документов и дел, предотвращения утечки содержащейся в них информации должен быть установлен специальный режим их хранения.

Согласно п. 7 ст. 86 ТК РФ защиту персональных данных работника от неправомерного их использования или утраты работодатель должен обеспечивать за счет своих средств. В соответствии со ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем.

В связи с этим работодатель должен издать локальный нормативный правовой акт, который будет регулировать порядок хранения и использования персональных данных, и с которым работники должны быть ознакомлены под подпись (п. 8 ст. 86 ТК РФ). Как указывалось выше, в ГБПОУ РО «РКРИПТ» таким актом является Положение «Об обработке и защите персональных данных» [13].

В случае приема на работу нового сотрудника, он должен ознакомиться с положением о персональных данных, как и с остальными локальными нормативными актами работодателя, до подписания трудового договора (ст.68 ТК РФ).

Нужно отметить, что при отсутствии подписи работника работодатель не сможет доказать, что работник был ознакомлен с данным документом.

В случае проверки организации, проверяющие органы могут запросить данный документ и проверить, ознакомлены ли с ним работники. Отсутствие такого документа или неознакомление работников с ним может являться основанием для привлечения работодателя к ответственности согласно части 1 статьи 5.27 КоАП РФ[19], а в случае совершения аналогичного нарушения повторно – по части 2 статьи 5.27 КоАП РФ.

Работодатель должен определить ответственных за работу с персональными данными и ответственных за обеспечение безопасности персональных данных. Таким ответственным может быть как конкретное лицо, так и подразделение. В последнем случае личную ответственность несет руководитель такого подразделения. Этот приказ необходимо довести до сведения всех указанных в нем сотрудников, что должно подтверждаться их подписью.

В ГБПОУ РО «РКРИПТ» существует специфика работы с персональными данными. Поскольку колледж является образовательным учреждением, то он как оператор обработки персональных данных имеет дело не только с персональными данными сотрудников, но и лиц, обучающихся в данном учреждении.

Согласно п. 3.3 должностной инструкции инспектора по кадрам (по личному составу сотрудников) ГБПОУ РО «РКРИПТ», утвержденной 01.09.2014 г., на него возложена ответственность за сохранность конфиденциальности информации о персональных данных сотрудников колледжа, хранящихся в отделе кадров, и осуществлять их обработку в соответствии с Положением об обработке и защите персональных данных колледжа.

[19] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ

А согласно п. 3.5 он обязан контролировать изменения сведений о персональных данных сотрудников колледжа, вносить их в кадровую документацию. Следует отметить, что ФЗ «О персональных данных» не предусмотрена обязанность работника своевременно уведомлять работодателя об изменении своих персональных данных [4]. Однако несвоевременное предоставление работником измененных данных может повлиять на исполнение работодателем своих обязанностей. Поэтому в локальных нормативных правовых актах работодателя целесообразно зафиксировать обязанность работника ставить работодателя в известность о таких изменениях в конкретный срок. Это избавит работодателя от многих проблем, например от неблагоприятных последствий, которые могут возникнуть при подаче в налоговый орган документов, содержащих недостоверные сведения о персональных данных работников.

Так, в п. 4.3.17 Правил внутреннего трудового распорядка ГБПОУ РО «РКРИПТ»[20] зафиксировано, что работники обязаны в течение 2 недель предоставлять в отдел кадров документы, подтверждающие изменения их персональных данных.

Аналогичная ответственность и аналогичные обязанности возложены на инспектора по кадрам (по личному составу студентов) ГБПОУ РО «РКРИПТ» (п.3.2. п. 3.4. должностной инструкции).

Также согласно п.3.4.3 Положения «Об обработке и защите персональных данных» внутренний доступ (доступ внутри организации) [13] к персональным данным субъекта имеют: руководитель организации; бухгалтерия; отдел кадров; непосредственные руководители по направлению деятельности (доступ к персональным данным сотрудников, непосредственно находящихся в его подчинении); заведующие отделениями (доступ к персональным данным субъектов в части, его касающейся); классные руководители (доступ к персональным данным студентов своей

[20] Правила внутреннего трудового распорядка в ГБПОУ РО «РКРИПТ», утвержденные директором колледжа от 26.12.2016 г.

группы в части, его касающейся); преподаватели (доступ к информации, содержащейся в журналах тех групп, в которых они ведут занятия); сам субъект, носитель данных.

Целесообразно с лицами, имеющими доступ к персональным данным, заключать соглашения о неразглашении персональных данных. В ГБПОУ РО «РКРИПТ» разработана форма такого соглашения (Приложение А). В этом соглашении определен перечень сведений, которые субъект обязуется не разглашать, а также дается указание на наступление юридической ответственности в случае их разглашения.

Поскольку на работодателя возложена обязанность соблюдать режим конфиденциальности персональных данных, то целесообразно вести журналы учета персональных данных, их выдачи и передачи другим лицам и представителям различных организаций, государственным органам. В ГБПОУ РО «РКРИПТ» разработана форма журнала учета передачи персональных данных (Приложение Б). Ведение такого журнала поручено специалисту отдела кадров. В журнале учета передачи персональных данных указываются следующие сведения:

1) сведения о запрашиваемом лице,

2) состав запрашиваемых персональных данных,

3) цель получения персональных данных,

4) отметка о передаче или отказе в передаче персональных данных,

5) дата передачи/отказа в передаче персональных данных,

6) подпись запрашивающего лица,

7) подпись ответственного сотрудника.

Система учета персональных данных также может предусматривать проведение регулярных проверок наличия документов и других носителей информации, содержащих персональные данные работников, а также устанавливать порядок работы с ними. В этой связи необходимо ведение журнала проверок наличия документов, содержащих персональные данные работника.

Работодатель обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер. Это следует из п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 ФЗ «О персональных данных».

В частности, работодатель может предусмотреть в локальном нормативном акте требования к помещениям, в которых находятся носители информации (например, компьютеры с базами данных, документы на бумажных носителях), содержащие персональные данные работников.

ФЗ «О персональных данных» и ТК РФ не устанавливают каких-либо требований к упомянутым помещениям. Представляется, что работодатель может определить особый режим доступа в них, требования к оборудованию, установить перечень лиц, имеющих право доступа в данные помещения.

Все документы, содержащие персональные данные работников, такие как личные дела, картотеки, учетные журналы, следует хранить в специально оборудованных шкафах или сейфах, которые запираются и опечатываются. Трудовые книжки работников нужно хранить в сейфе отдельно от личных дел.

Персональные данные при их обработке должны обособляться от иной документированной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков) документов. При фиксации персональных данных на материальных носителях не допускается фиксация на одном носителе данных, цели обработки которых заведомо не совместимы. При обработке различных категорий персональных данных для каждой категории должен использоваться отдельный материальный носитель.

Так в ГБПОУ РО «РКРИПТ» из п. 3.3. Положения «Об обработке и защите персональных данных» следует, что хранение персональных данных субъектов осуществляется кадровой службой, бухгалтерией, учебной частью на бумажных и электронных носителях с ограниченным доступом. Личные

дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденному постановлением Правительства РФ 15.09.2008 г. № 687. 3 [16].

Принимая меры по обеспечению конфиденциальности персональных данных, оператор персональных данных должен помнить о правах работника, предоставленных ему законодательством.

В соответствии с ч. 1 ст. 89 ТК РФ работники имеют право на полную информацию об их персональных данных и обработке этих данных. Соответственно, работодатель обязан ознакомить их с такой информацией.

Также работники, согласно ст. 89 ТК РФ, имеют право на свободный бесплатный доступ к своим персональным данным, в том числе на получение копии любой записи, содержащей такие данные.

Учитывая требования ст. 62 ТК РФ, по письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня получения от работника заявления выдать ему копии документов, связанных с работой (приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы, выписки из трудовой книжки, справок о заработной плате, о начисленных и фактически уплаченных пенсионныхвзносах, о периоде работы у данного работодателя и др.). Данные копии заверяются надлежащим образом и предоставляются работнику безвозмездно.

Также работники имеют право требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями требований ТК РФ или иного федерального закона. В случае отказа работодателя исключить или исправить

персональные данные работника,последний имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения (ст. 89 ТК РФ).

В соответствии со ст. 89 ТК РФ по требованию работника работодатель обязан известить всех лиц, которым ранее были сообщены неверные или неполные персональные данные этого работника, обо всех произведенных в них исключениях, исправлениях или дополнениях. Работники имеют право обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

Конкретный порядок доступа работника к своим персональным данным необходимо устанавливать в локальных нормативных актах, определяющих порядок обработки и защиты персональных данных работника. При этом нужно учитывать, что данный порядок должен гарантировать свободу доступа работника к своим персональным данным[14].

2.3 Обязанности оператора при сборе персональных данных

При сборе персональных данных работников и студентов ГБПОУ РО «РКРИПТ» должен соблюдать требования, установленные законодательством о персональных данных.

Все персональные данные работника следует получать у него самого (п. 3 ст. 86 ТК РФ). Причем это допускается только с его согласия (п. 1 ч. 1 ст. 6 ФЗ «О персональных данных») [4].

Сказанное применимо и к соискателям. Например, согласие на получение персональных данных требуется:

- от претендента на замещение вакантной должности на период принятия работодателем решения о приеме либо отказе в приеме на работу (абз. 11, 12 - 17 п. 5 Разъяснений Роскомнадзора): при поступлении резюме по каналам электронной почты, факсимильной связи; при сборе персональных данных посредством типовой формы анкеты соискателя, утвержденной работодателем,

- для включения соискателя в кадровый резерв работодателя (абз. 22 - 25 п. 5 Разъяснений Роскомнадзора).

Решение работника (соискателя) о предоставлении своих персональных данных должно быть добровольным, какое-либо давление на него недопустимо (п. 1 ст. 9 ФЗ«О персональных данных).

Принимая решение о предоставлении своих данных, работник дает согласие на их обработку (п. 1 ст. 9 ФЗ «О персональных данных»). Согласие должно быть конкретным, информированным и сознательным. Это означает, что содержание указанного согласия должно содержать информацию, позволяющую однозначно сделать вывод о целях, способах обработки с указанием действий, совершаемых с персональными данными, объеме обрабатываемых персональных данных (п. 1 ст. 9ФЗ «О персональных данных», абз. 3 п. 5 Разъяснений Роскомнадзора).

Согласие работника может быть, как закреплено в тексте трудового договора, так и оформлено в виде отдельного документа.

Согласие работника на обработку персональных данных должно включать (ч. 4 ст. 9 ФЗ «О персональных данных»):

1) фамилию, имя, отчество, адрес работника, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе,

2) при получении согласия от представителя работника - его фамилию, имя, отчество, адрес, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия представителя,

3) наименование или фамилию, имя, отчество и адрес работодателя,

4) цель обработки персональных данных,

5) перечень персональных данных, которые подлежат обработке,

6) фамилию, имя, отчество и адрес лица или наименование организации, осуществляющих обработку персональных данных по поручению работодателя, если она поручена такому лицу или организации,

7) перечень действий с персональными данными, на совершение которых работником дано согласие, общее описание способов их обработки,

8) срок, в течение которого действует согласие работника на обработку его персональных данных, и способ отзыва согласия,

9) подпись работника.

Согласно п. 3.2.1. Положения «Об обработке и защите персональных данных» ГБПОУ РО «РКРИПТ», субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку оператором. Форма согласия на обработку персональных данных приводится в приложении № 1 к указанному Положению (Приложение В).

В связи с тем, что в ГБПОУ РО «РКРИПТ» многие обучающие являются несовершеннолетними, указанным выше Положением предусмотрен специальный прядок получения их персональных данных. Вслучае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные субъекта следует получать от его законных

представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку оператором (п. 3.2.2 Положения). Форма согласия на обработку персональных данных несовершеннолетнего приводится в приложении №3 к Положению (Приложение Г)

Не требуется согласие на обработку персональных данных работника (соискателя), получаемых, в частности (п. 2 ч. 1 ст. 6, п. 2.3 ч. 2 ст. 10ФЗ «О персональных данных», абз. 1 Разъяснений Роскомнадзора):

1) из документов (сведений), предъявляемых при заключении трудового договора в соответствии со ст. 65, ч. 4 ст. 275 ТК РФ,

2) по результатам обязательного предварительного медицинского осмотра о состоянии здоровья (ст. 69 ТК РФ, п. 3 Разъяснений Роскомнадзора),

3) в объеме, предусмотренном унифицированной формой № Т-2 (утв. Постановлением Госкомстата России от 05.01.2004 № 1), в том числе персональных данных близких родственников, и в иных случаях, установленных законодательством РФ (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат) (п. 2 Разъяснений Роскомнадзора),

4) от кадрового агентства, действующего от имени соискателя (абз. 12 п. 5 Разъяснений Роскомнадзора),

5) из резюме соискателя, размещенного в сети Интернет и доступного неограниченному кругу лиц (п. 10 ч. 1 ст. 6ФЗ «Оперсональных данных», абз. 12 п. 5 Разъяснений Роскомнадзора).

Согласно п. 3.2.3 Положения «Об обработке и защите персональных данных» ГБПОУ РО «РКРИПТ», письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных[13].

Может возникнуть ситуация при которой персональные данные работника могут быть получены только у третьей стороны. В этом случае действует следующее правило: в случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение.

Согласие оформляется в письменной форме в двух экземплярах, один из которых предоставляется субъекту, второй хранится у оператора. Форма согласия субъекта на получение его персональных данных у третьей стороны представлена в приложении № 5 к Положению «Об обработке персональных данных» (Приложение Д).

Работник в любое время вправе отозвать согласие на обработку персональных данных (ч. 2 ст. 9 ФЗ «О персональных данных») (Приложение Е). В подобной ситуации продолжение обработки персональных данных работника без его согласия возможно при наличии оснований, перечисленных в п. п. 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11 ФЗ «О персональных данных». Это следует из ч. 2 ст. 9 указанного Закона.

Следует отметить, что в Положении воспроизведен установленный законодательством о персональных данных прямой запрет на получение и обработку персональных данных субъекта о его политических, религиозных и иных убеждениях и частной жизни (п. 3.2.6), а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами (п. 3.2.7) [13].

Кроме вопросов получения и сбора персональных данных работников, законодатель регламентирует вопросы передачи этих данных третьим лицам.

Работодатель вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия (абз. 2, 3 ч. 1 ст. 88 ТК РФ).

Перед передачей персональных данных работодатель должен предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено (абз. 4 ч. 1 ст. 88 ТК РФ)[15].

Для защиты персональных данных от неправомерного использования работодатель обязан (абз. 5, 6, 7 ч. 1 ст. 88 ТК РФ):

а) осуществлять их передачу только в пределах одной организации,

б) регламентировать процедуру передачи персональных данных локальными нормативными актами (положение о персональных данных работников, утвержденный приказом список лиц, имеющих доступ к персональным данным, обязательство о неразглашении персональных данных),

в) ознакомить работников, которым открыт доступ к персональным данным других работников организации, с указанными локальными нормативными актами под подпись,

г) передавать персональные данные работников по мотивированному запросу только специально уполномоченным лицам, а также представителям работников, в том объеме, который необходим им для выполнения конкретных функций.

У работников отдела кадров часто возникает вопрос, может ли работодатель передавать персональные данные своих бывших работников новым работодателям по их запросам? Такие действия можно совершать только при наличии письменного согласия работника.

Из содержания п. 3 ст. 86 ТК РФ следует, что запрашивать информацию у третьей стороны, в том числе и у предыдущего работодателя, нынешний работодатель может только с согласия работника и только если

данную информацию нельзя получить у самого работника. Иными словами, потенциальный работодатель вправе запросить информацию при наличии согласия работника, а прежний работодатель вправе ее передать с тем же условием.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника (абз. 2 ст. 88 ТК РФ, абз. 1 п. 4 Разъяснений Роскомнадзора),

- в ФССРоссии, ПФР в объеме, предусмотренном законом (абз. 15 ч. 2 ст. 22 ТК РФ, абз. 3 п. 4 Разъяснений Роскомнадзора),

- в налоговые органы (пп. 1, 2, 4 п. 3 ст. 24 НК РФ, абз. 5 п. 4 Разъяснений Роскомнадзора),

- в военные комиссариаты (пп. "г" п. 30, пп. "а" - "в", "д", "е" п. 32 Положения о воинском учете, утвержденного Постановлением Правительства РФ от 27.11.2006 № 719, абз. 5 п. 4 Разъяснений Роскомнадзора),

- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем (абз. 5 ч. 6 ст. 370 ТК РФ, п. 1 ст. 17, п. 1 ст. 19 Федерального закона «О профессиональных союзах, их правах и гарантиях деятельности» от 12.01.1996 № 10-ФЗ, абз. 5 п. 4 Разъяснений Роскомнадзора),

- по мотивированному запросу органов прокуратуры (п. 1 ст. 22Федерального закона «О прокуратуре Российской Федерации» от 17.01.1992 № 2202-1, абз. 7 п. 4 Разъяснений Роскомнадзора),

- по мотивированному требованию правоохранительных органов и органов безопасности (ст. 6 ФЗ «О коммерческой тайне», п. "м" ч. 1 ст. 13Федерального закона «О федеральной службе безопасности» от 03.04.1995 № 40-ФЗ, абз. 7 п. 4 Разъяснений Роскомнадзора),

- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности (абз. 3 ч. 1 ст. 357 ТК РФ, абз. 7 п. 4 Разъяснений Роскомнадзора),

- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом (абз. 5 ст. 228 ТК РФ). Перечень оповещаемых органов и сроки направления извещений о несчастном случае установлены ст. 228.1 ТК РФ,

- в случаях, связанных с исполнением работником должностных обязанностей, в том числе при направлении в командировку. Это следует из совокупного анализа ч. 5 - 5.2 ст. 11Федерального закона «О транспортной безопасности» от 09.02.2007 № 16-ФЗ,

- для предоставления сведений в банк, обслуживающий банковские карты работников при условии, что в договоре о выпуске карт (коллективном договоре, локальном нормативном акте организации) содержится пункт о праве работодателя передавать персональные данные работников, либо он действует на основании доверенности на представление интересов работников (абз. 10 п. 4 Разъяснений).

Глава3 Охрана и защита конфиденциальной информации

3.1 Юридическая ответственность за нарушения законодательства о конфиденциальной информации

Нарушение требований по защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации [1].

Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.[21]

Данные мероприятия за правонарушения в области защиты информации устанавливают нормативные правовые акты и предусматривают следующие виды ответственности:

- дисциплинарную (замечание, выговор, увольнение),
- гражданскую (возмещение причинённого ущерба),
- административную (предупреждение, административный штраф),
- уголовную (штраф, лишение свободы).

Рассмотрим подробно каждый вид ответственности:

1) дисциплинарная ответственность работников предприятий предусмотрена ст. 57, 81, 192 и 193 Трудового кодекса РФ. В соответствии со ст. 57 [15] в заключаемом работодателем и работником трудовом договоре

[21] Комплексная система защиты информации на предприятии : учеб.пособие для студ. высш. учеб. заведений / В.Г.Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2015. — 416 с.

могут предусматриваться условия о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной).

В отношении работника, совершившего дисциплинарный проступок, связанный с неисполнением или ненадлежащим исполнением трудовых обязанностей, работодателем могут быть применены следующие дисциплинарные взыскания.[22]

Определенные ст. 192 Трудового кодекса РФ: замечание, выговор, увольнение по соответствующим основаниям. Порядок применения дисциплинарных взысканий определен в ст. 193 кодекса.

Увольнение работника осуществляется в соответствии с положениями ст. 81 Трудового кодекса РФ «Расторжение трудового договора по инициативе работодателя» [15]. В соответствии с подп. 6в указанной статьи трудовой договор с работником может быть расторгнут в случае однократного грубого нарушения работником трудовых обязанностей - разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

2) гражданская ответственность имеет прямую связь с категорией морального вреда, то есть, если гражданину был причинен моральный вред, выраженный в действиях, нарушающих его личные неимущественные права, он вправе выставить правонарушителю требования о выплате денежной компенсации в судебном порядке. Размер компенсации морального вреда определяется судом с учетом всех заслуживающих внимания обстоятельств. Компенсация осуществляется в денежной форме.

В соответствии с п. 7 ст. 243 ТК РФматериальная ответственность работника за разглашение информации, которая напрямую связана с персональными данными других лиц, возлагается на правонарушителя в полном размере причиненного ущерба.

[22] https://pravovedus.ru/practical-law/civil/zashhita-personalnyih-dannyih/

Согласно п. 4.8.3 (е) Правилвнутреннего распорядка в ГБПОУ РО «РКРИПТ», материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами [13].

3) административная ответственность за нарушение порядка сбора, хранения и распространения персональных данных влечет за собой предупреждение или штраф в размере: от 1000 до 3000 рублей - для физических лиц; от 5000 до 10000 рублей - должностных лиц, от 20 тысяч до 50 тысяч рублей – для юридических лиц (ст. 13.11 КоАП РФ). Административная ответственность за распространение информации, охраняемой законом, при исполнении служебных и профессиональных обязанностей, влечет за собой штраф в размере: от 500 до 1000 рублей – для физических лиц, от 4 до 5 тысяч рублей – для должностных лиц (ст. 13.14 КоАП РФ).

4) уголовная ответственность за нарушение неприкосновенности частной жизни, выражающееся в незаконном собирании или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, регулируется ст. 137 УК РФ и наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами насрок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Если же эти действия совершены лицом с использованием своего служебного положения, то наказание предусмотрено более строгое. Такие действия наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.[23]

Отдельно следует указать на юридические последствия передачи персональных данных работника без его согласия в случае, когда такое согласие обязательно.В соответствии со ст. 90 ТК РФ лица, которые виновны в нарушении норм, регулирующих обработку и защиту персональных данных работника, могут быть привлечены к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности. Следовательно, передача персональных данных без согласия работника в случае, когда такое согласие обязательно, расценивается как нарушение законодательства о персональных данных. Работник может обратиться за защитой своих прав в государственные органы, к компетенции которых эти вопросы относятся. Необходимо иметь в виду, что за нарушение законодательства о персональных данных ответственность будут нести лицо, допустившее нарушение (единоличный исполнительный орган), и организация в целом.

3.2 Надзор за соблюдением законодательства о конфиденциальной информации

[23] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных» [4], является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи — Роскомнадзор.

Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.[24]

В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.[25]

Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных,

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений,

3) вести реестр операторов,

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных,

---

[24] Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.02.2019) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"

[25] https://studme.org/78426/pravo/kontrol_nadzor_obrabotkoy_personalnyh_dannyh

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, федерального органа исполнительной власти в области государственной охраны или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных,

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных,

7) выполнять иные предусмотренные законодательством РФ обязанности.

Контроль осуществляется с помощью плановых и внеплановых проверок и в строгом соответствии с установленным порядком проведения данных проверок. Проверки осуществляет Роскомнадзор или его территориальные органы.[26]

Плановые проверки проводятся на основании ежегодного плана проведения проверок:

- в отношении Операторов, включенных в Реестр операторов, осуществляющих обработку персональных данных,

- в отношении Операторов, не включенных в Реестр, но осуществляющих обработку персональных данных.

Внеплановые проверки проводятся по следующим основаниям:

1) истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных,

[26] https://www.intuit.ru/studies/courses/697/553/lecture/12459

2) поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах,

3) возникновение угрозы причинения вреда жизни, здоровью граждан,

4) причинение вреда жизни, здоровью граждан,

5) нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных,

6) нарушение Операторами требований законодательства в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

Обращение гражданина РФ, не позволяющее установить его лицо, либо не содержащее сведения о фактах, указанных выше, не может являться основанием для внеплановой проверки.

О проведении внеплановой выездной проверки оператор уведомляется не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Если в результате деятельности оператора причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление оператора о начале проведения внеплановой выездной проверки не требуется.

Срок проведения, как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.

В исключительных случаях срок проведения проверки может быть продлен, но не более чем на 20 рабочих дней, в отношении малых предприятий и микропредприятий – на 15 часов.

В ходе проверки осуществляется следующее:

- рассмотрение документов оператора, таких как уведомление об обработке, письменное согласие субъекта, локальных документов, регламентирующих порядок хранения и обработки персональных данных,

- исследование ИСПД в части, касающейся субъектов персональных данных.

Основанием для приостановления проверки является:

- необходимость получения заключений экспертов по вопросам обработки персональных данных, связанным с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований,

- мотивированное решение руководителя контролирующего органа, принятое по причине изъятия документов, являющихся объектами контроля, проведенного ранее сотрудниками прокуратуры, правоохранительных органов, болезни должностных лиц, проводящих проверку. Оператору представляется копия приказа, в котором указываются причины приостановления проверки и период, на который данная проверка приостановлена [25].

Основанием для принятия решения об исключении Оператора из плана проведения плановых проверок является:

- ликвидация или реорганизация Оператора,

- прекращение Оператором деятельности по обработке персональных данных.

Проверка соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных завершается:

- составлением и вручением Оператору акта проверки,

- выдачей Оператору предписания об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных,

- составлением протокола об административном правонарушении в отношении Оператора,

- подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о

возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

В случае выявления в ходе плановых и внеплановых проверок нарушений в области обеспечения безопасности персональных данных, предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность, которая может применяться в отношении руководителя организации, подразделения или виновного в разглашении работника. Наказанием за нарушение требований ФЗ «О персональных данных» [4] могут стать исправительные работы до 1 года или лишение свободы на срок до 2-х лет.

Заключение

В данной дипломной работе были рассмотрены вопросы нормативно-правового регулирования конфиденциальной информации. Дано понятие конфиденциальной информации и конфиденциального делопроизводства, рассмотрены виды конфиденциальной информации.

Нормативно-правовая база в сфере защиты конфиденциальной информации представляет собой широкий свод законов, подзаконных актов и локальных актов, всесторонне регулирующих общественные отношения, возникающие по поводу доступа, хранения, обработки, использования и защиты конфиденциальной информации.

Таким образом, организация и технология конфиденциального делопроизводства регламентированы не только федеральными нормативными правовыми актами. Их должен определять обладатель конфиденциальной информации, учитывая специфику деятельности организации, путем принятия локальных нормативных правовых актов. Однако при этом ему необходимо руководствоваться определенными нормами и правилами работы с конфиденциальными документами, обеспечивающими нужный уровень функционирования предприятия, сохранность документов и конфиденциальность содержащейся в них информации.

Учитывая специфику деятельности ГБПОУ РО «РКРИПТ», особое внимание в дипломной работе было уделено рассмотрению вопросов обработки, хранения и защиты персональных данных. Было изучено Положение «Об обработке и защите персональных данных» ГБПОУ РО «РКРИПТ». Указанное Положение принято в соответствии с ФЗ «О персональных данных» и не противоречит ему.

Следует отметить, что работа отдела кадров ГБПОУ РО «РКРИПТ» с персональными данными работников и обучающихся осуществляется в строгом соответствии с законом. В личных делах имеются согласия на обработку персональных данных, как и требует Положение «Об обработке и защите персональных данных», все личные дела хранятся в сейфе.

Следует отметить, что в настоящее время ГБПОУ РО «РКРИПТ» подключился к системе электронного документооборота «ДЕЛО» (СЭД «ДЕЛО»).

Система «ДЕЛО», разработанная компанией ЭОС, - комплексное решение, обеспечивающее автоматизацию процессов делопроизводства компаний различных масштабов и сфер деятельности, а также ведение полностью электронного документооборота в организации.

Делопроизводители получают автоматизацию знакомых задач, которые обычно ведутся в бумажных журналов с риском потерять документы или пропустить сроки исполнения СЭД «ДЕЛО» предотвращает такие ситуации.

Технология электронной подписи повышает информационную безопасность СЭД «ДЕЛО». Она позволяет удостоверять авторство служебных актов, облегчает процесс согласования между руководителями разных организационных уровней. СЭД «ДЕЛО» зарекомендовало себя с положительной стороны в вопросах работы с конфиденциальной информацией. Шифровка облегчает передачу документов высокого уровня секретности, а также помогает регламентировать доступ к ним с помощью цифровых ключей.

Также в данной дипломной работе рассмотрены вопросы наступления юридической ответственности за нарушение законодательства о конфиденциальной информации. Установлено, что за нарушение законодательства в сфере информации предусматривается дисциплинарная, административная, гражданско-правовая или уголовная ответственность.

Таким образом, подводя итог, можно сделать вывод, что главная задача защиты конфиденциальной информации - это защита доступа (физического или программного) к информации, содержащей сведения ограниченного доступа, таким образом, чтобы максимально обезопасить ее от несанкционированного доступа.

Список использованных источников

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

2. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, А.Г. Фабричнов; под общ.ред. Н.Н. Куняева. – М.: Логос, 2016.— 500 с.

3. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13.07.2015)

4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

5. Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

6.https://www.profiz.ru/sr/4_2008/normativnaya_baza_raboty/

7. Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31.05.2002 № 63-ФЗ

8. «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 01.02.2019)

9.Федеральный закон «О почтовой связи» от 17.07.1999 № 176-ФЗ

10.Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ

11. Конфиденциальное делопроизводство и защита коммерческой тайны. Курс лекций: МАБИВ; Орел; 2014

12. Конфиденциальное делопроизводство: Учебное пособие: / Сост. Е.А.Давыденко. — Нижневартовск: Изд-во Нижневарт. гос. ун-та, 2015. — 83 с.

13. Положение «Об обработке и защите персональных данных» в ГБПОУ РО «РКРИПТ», утвержденное директором колледжа от 07.08.2017 г.

14. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993)

15. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ

16.Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

17. Письмо Роскомнадзора от 07.02.2014 № 08КМ-3681 «О передаче работодателем третьим лицам сведений о заработной плате работников»

18. Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»

19. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ

20. Правила внутреннего трудового распорядка в ГБПОУ РО «РКРИПТ», утвержденные директором колледжа от 26.12.2016 г.

21. Комплексная система защиты информации на предприятии : учеб.пособие для студ. высш. учеб. заведений / В.Г.Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2015. — 416 с.

22. https://pravovedus.ru/practical-law/civil/zashhita-personalnyih-dannyih/

23. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ

24. Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 28.02.2019) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»

25.https://studme.org/78426/pravo/kontrol_nadzor_obrabotkoy_personalnyh_dannyh

26. https://www.intuit.ru/studies/courses/697/553/lecture/12459

ПРИЛОЖЕНИЕ А
(обязательное)

Соглашение о неразглашении персональных данных субъекта

СОГЛАШЕНИЕ
о неразглашении персональных данных субъекта

Я, _____,
паспорт серии _____, номер _____,
выданный
_____
«___»_____ _____ года, понимаю, что получаю доступ к персональным данным работников и/или обучающихся государственного бюджетного профессионального образовательного учреждения Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий» (ГБПОУ РО «РКРИПТ»).

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- адрес места жительства;
- наличие судимостей;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов;
- личные дела и трудовые книжки сотрудников;
- основания к приказам;
- дела, содержащие материалы о повышении квалификации и переподготовке, аттестации;
- копии отчетов, направляемые в органы статистики, пенсионный фонд РФ.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты, я несу ответственность в соответствии со ст. 90 Трудового кодекса Российской Федерации.

«___»_____ 20_____ г _____
(подпись)

ПРИЛОЖЕНИЕ Б
(обязательное)

Журнал учета передачи персональных данных

№	Сведения о запрашиваемом лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/ отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника

ПРИЛОЖЕНИЕ В
(обязательное)

Согласие на обработку персональных данных работника

СОГЛАСИЕ

на обработку персональных данных работника

Я, _____, паспорт серия _____ № _____, выданный _____ _____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» НАСТОЯЩИМ даю согласие государственному бюджетному профессиональному образовательному учреждению Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий» (ГБПОУ РО «РКРИПТ»), расположенному по адресу: 344011 г. Ростов-на-Дону, ул. Красноармейская, 11, на обработку моих персональных данных любым законодательно разрешенным способом.Согласие относится к обработке следующих персональных данных: - фамилия, имя, отчество; - пол; - дата и место рождения; - данные паспорта; - адреса регистрации по месту жительства и фактического проживания; - номера телефонов: домашнего и мобильного; - сведения об образовании, профессиональной переподготовке, повышении квалификации; - данные о семейном положении, составе семьи; - отношение к воинской обязанности; - сведения о трудовом стаже, предыдущих местах работы, доходах на предыдущих местах работы; - сведения о номере и серии страхового свидетельства государственного пенсионного страхования; - сведения об идентификационном номере налогоплательщика; - сведения об отсутствии (наличии) судимости (уголовного преследования); - сведения о состоянии здоровья, необходимые работодателю для определения пригодности для выполнения поручаемой работы в пансионе; - сведения о событиях, связанных с моей трудовой деятельностью в пансионе; - сведения об использованных отпусках в пансионе; - данные о моих доходах в пансионе; - информация о моих деловых качествах. Обработка данных должна осуществляться с целью: - Обеспечения соблюдения требований законодательства РФ; - Оформления и регулирования трудовых отношений; - Отражения информации в кадровых документах; - Начисления заработной платы; - Исчисления и уплаты налоговых платежей, предусмотренных законодательством РФ; - Представления законодательно установленной отчетности по физическим лицам в ИФНС и внебюджетные фонды; - Подачи сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы; - Предоставления налоговых вычетов. - Обеспечения безопасных условий труда. - Обеспечения сохранности имущества, принадлежащего работодателю. - Контроля требований к количеству и качеству выполняемой мной работы. Настоящее согласие действительно со дня его подписания до дня отзыва в письменной форме. Мне разъяснено, что в случае отказа от предоставления согласия на обработки персональных данных возможно наступление следующих правовых последствий: - в соответствии с п. 1, ст. 21 Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 г. № 152-ФЗ, осуществляется блокировка персональных данных на период рассмотрения отказа; - в соответствии с п. 5 ст. 21 Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ, прекращается обработка персональных данных и производится их уничтожение в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения договорных отношений. Настоящее согласие вступает в силу со дня его подписания и действует в течение срока хранения личного дела субъекта персональных данных.

_____ _____

Дата Расшифровка подписи

ПРИЛОЖЕНИЕ Г
(обязательное)

Согласие на обработку персональных данных подопечного

СОГЛАСИЕ
на обработку персональных данных подопечного

Я, _____,
паспорт серия _____ № _____, выдан _____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», на основании ст. 64 п.1 Семейного кодекса РФ1. Настоящим даю согласие на обработку государственному бюджетному профессиональному образовательному учреждению Ростовской области «Ростовский-на-Дону колледж радиоэлектроники, информационных и промышленных технологий» (ГБПОУ РО «РКРИПТ»), расположенному по адресу: 344011 г. Ростов-на-Дону, ул. Красноармейская, 11, персональных данных моего несовершеннолетнего ребенка:

_____

(Ф.И.О. сына, дочери, подопечного)

относящихся кперечисленным ниже категориям персональных данных:

- адрес регистрации и проживания ребенка, данные свидетельства о рождении, паспортные данные; ИНН, номер медицинского страхового полиса, данные медицинской карты, сведения о состоянии здоровья ребенка, данные медицинских осмотров, заключения и рекомендации врачей; учебные работы ребенка; данные о составе семьи; персональные данные ребенка: ФИО, адрес электронной почты, фото, номер мобильного телефона, сведения об оценках, успеваемости и достижениях (учет результатов освоения образовательных программ, оценки, результаты участия в спортивно-массовых и культурных мероприятиях, конкурсах);
- персональные данные родителей (законных представителей) включающие ФИО, адрес регистрации и проживания, телефоны (домашний и служебный), место работы, должность (используются для оперативного взаимодействия с Оператором);
- другие данные, используемые в рамках организации работы Оператора.

Я согласен (на), что его(ее) персональные данные будут использованы в целях, связанных с учебной деятельностью и иными гражданско-правовыми отношениями с ГБПОУ РО «РКРИПТ».

Настоящее согласие представляется на осуществление Оператором следующих действий в отношении персональных данных ребенка: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (только в указанных выше целях), обезличивание, блокирование (не включает возможность ограничения моего доступа к персональным данным ребенка), архивирование, копирование, изменение, редактирование, размещение на официальном сайте, уничтожение. Я даю согласие на распространение персональных данных ребенка, в том числе на передачу персональных данных ребенка каким-либо третьим лицам, включая физические и юридические лица, в том числе внешние организации и лица, привлекаемые Оператором для осуществления обработки персональных данных, государственные органы и органы местного самоуправления. Я даю согласие на обработку персональных данных ребенка неавтоматизированным и автоматизированным способом.

В рамках настоящего Соглашения обработка персональных данных на обучение осуществляется с соблюдением Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» и иных нормативно-правовых актов.

Данное Согласие действует до достижения целей обработки персональных данных Оператора или до отзыва данного Согласия. Данное согласие может быть отозвано в любой момент по моему письменному заявлению. Мне разъяснено, что в случае отказа от предоставления согласия на обработки персональных данных возможно наступление следующих правовых последствий: - в соответствии с п. 1, ст. 21 Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 г. № 152-ФЗ, осуществляется блокировка персональных данных на период рассмотрения отказа; - в соответствии с п. 5 ст. 21 Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ, прекращается обработка персональных данных и производится их уничтожение в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в интересах ребенка, законным представителем которого являюсь. Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения договорных отношений. Настоящее согласие вступает в силу со дня его подписания и действует в течение срока хранения личного дела субъекта персональных данных.

_____ _____

Дата Расшифровка подписи

ПРИЛОЖЕНИЕ Д
(обязательное)

Согласие субъекта на получение его персональных данных у третьей стороны

Директору ГБПОУ РО «РКРИПТ»
Горбунову С.В.

СОГЛАСИЕ
субъекта на получение его персональных данных у третьей стороны

Я, _____, паспорт серии _____, номер _____, выданный _____ "___"_____ ____ года, в соответствии со ст. 86 Трудового кодекса Российской Федерации _____
(согласен/не согласен)
на получение моих (сына, дочери, подопечного) персональных данных, а именно:
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес ...))

Для обработки в целях
_____
_____
_____
(указать цели обработки)
У следующих лиц
_____
_____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

"___"_____ 201__ г. _____
(подпись)

ПРИЛОЖЕНИЕ Е
(обязательное)

Отзыв согласия на обработку персональных данных

Отзыв согласия на обработку персональных данных

Директору ГБПОУ РО «РКРИПТ»
Горбунову С.В.

344011 г.Ростов-на-Дону, ул. Красноармейская,11
адрес субъекта

_____
Ф.И.О. субъекта персональных данных

_____
адрес, где зарегистрирован субъект персональных данных

_____
номер основного документа, удостоверяющего его личность

_____
дата выдачи указанного документа

_____
наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих (моего сына, дочери, подопечного) персональных данных в связи с

_____
(указать причину)

«___»_____ 20__ г. _____ _____
(подпись) (расшифровка подписи)