Приложение № 1
к приказу № 744-О от 01.09.18

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
**«ПОЖАРНО-СПАСАТЕЛЬНЫЙ КОЛЛЕДЖ
«САНКТ-ПЕТЕРБУРГСКИЙ ЦЕНТР ПОДГОТОВКИ СПАСАТЕЛЕЙ»**

ПРИНЯТО
Общим собранием работников
Санкт-Петербургского Пожарно-
спасательного колледжа
Протокол от «29» 08 2018 № 7

УТВЕРЖДЕНО
приказом директора Санкт-Петербургского
Пожарно-спасательного колледжа
от «01» 09 2018 № 744-О
Директор Санкт-Петербургского Пожарно-
спасательного колледжа
_____ Л.А. Беляев

Локальный акт № 62

Положение об обработке и защите персональных данных работников
в Санкт-Петербургском государственном бюджетном
профессиональном образовательном учреждении
«Пожарно-спасательный колледж
«Санкт-Петербургский центр подготовки спасателей»

Санкт-Петербург
2018 год

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Пожарно-спасательный колледж «Санкт-Петербургский центр подготовки спасателей» (далее – Колледж).

Под работниками подразумеваются лица, заключившие трудовой договор с Колледжем.

1.2. Цель настоящего Положения – защита персональных данных работников предприятия от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной строго охраняемой информацией.

1.3. Основанием для разработки настоящего Положения являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, другие действующие нормативные правовые акты Российской Федерации.

1.4. Настоящее Положение и изменения к нему утверждаются руководителем предприятия и вводятся приказом по Колледжу. Все сотрудники Колледжа должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

1.5. Персональные данные работников являются конфиденциальной информацией.

2. Понятие и состав персональных данных

2.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному
или определяемому физическому лицу.

2.2. Состав персональных данных работника:

- анкета;
- автобиография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- ИНН, СНИЛС;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний и мобильный телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии, данные об изображении лица и иные сведения, относящиеся к персональным данным работника;

- рекомендации, характеристики;
- принадлежность лица к конкретной нации, этнической группе, расе;
- привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
- семейное положение, наличие детей, родственные связи;
- религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);
- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.3. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

3. Обязанности работодателя

3.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.1.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.1.3. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.1.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

3.1.8. Работники и их представители должны быть ознакомлены под роспись с документами предприятия, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.1.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

4. Обязанности работника

Работник обязан:

4.1. Передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации.

4.2. Своевременно в разумный срок, не превышающий 5 дней, сообщать работодателю об изменении своих персональных данных.

5. Права работника

Работник имеет право:

5.1.На полную информацию о своих персональных данных и обработке этих данных.

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.3. На доступ к медицинским данным с помощью медицинского специалиста по своему выбору.

5.4. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.5. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.6. Обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

5.7. Определять своих представителей для защиты своих персональных данных.

6. Сбор, обработка и хранение персональных данных

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

6.2. Все персональные данные работника следует получать у него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

6.3. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

6.4. Работник представляет работодателю достоверные сведения о себе.

Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

6.5. При поступлении на работу работник заполняет анкету.

6.5.1. Анкета представляет собой перечень вопросов о персональных данных работника.

6.5.2. Анкета заполняется работником самостоятельно. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах.

6.5.5. Анкета работника должна храниться в личном деле работника. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным работника.

6.5.6. Личное дело работника оформляется после издания приказа о приеме на работу.

6.5.7. Все документы личного дела подшиваются в обложку образца, установленного на предприятии. На ней указываются фамилия, имя, отчество работника, номер личного дела.

6.5.8. К каждому личному делу прилагаются две фотографии работника.

6.5.9. Все документы, поступающие в личное дело, располагаются в хронологическом порядке.

6.5.10. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

7. Передача персональных данных

7.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

8. Доступ к персональным данным сотрудника

8.1. Внутренний доступ (доступ внутри предприятия).

Право доступа к персональным данным сотрудника имеют:

- директор;
- специалист по кадрам;
- заместители директора, заведующие отделениями (доступ к личным данным только работников своего подразделения) по согласованию с директором;
- сотрудники бухгалтерии – к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

8.2. Внешний доступ.

Персональные данные вне организации могут представляться в государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- общественные организации;
- учредитель.

8.3. Другие организации. Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

8.4. Родственники и члены семей.

Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

9. Защита персональных данных работников

9.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников организации все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

9.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках предприятия.

9.3. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу , электронной почте без письменного согласия работника запрещается.

9.4. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

9.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

10. Ответственность за разглашение информации, связанной с персональными данными работника

10.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение № 2

ЛИСТ СОГЛАСИЯ
работника на обработку персональных данных

Оператор персональных данных: Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Пожарно-спасательный колледж «Санкт-Петербургский центр подготовки спасателей»

Адрес оператора: 193315, г. Санкт-Петербург, пр. Большевиков, д.52 корп.1, лит. К, 193315, г. Санкт-Петербург, пр. Большевиков, д.52 корп.1, лит. Б

Ответственный за обработку персональных данных: специалист по кадрам –
_____

Цели обработки персональных данных

Обработка персональных данных работника осуществляется:

- в целях исполнения трудового договора, одной стороной которого является субъект персональных данных;
- для содействия работнику в осуществлении трудовой деятельности, наиболее полного исполнения им своих обязанностей, обязательств и компетенций, определенных Федеральным законом "Об образовании";
- для содействия работнику в обучении, повышении квалификации и должностном росте;
- для обеспечения личной безопасности, защиты жизни и здоровья работника;
- для учета результатов исполнения работником должностных обязанностей;
- для статистических и иных научных целей, при условии обязательного обезличивания персональных данных;
- в целях ведения финансово-хозяйственной деятельности учреждения;
- для формирования и ведения делопроизводства и документооборота, в том числе и в электронном виде.

Работник:_____
(ФИО полностью)

Дата рождения: _____

Место рождения:_____

Основной документ, удостоверяющий личность:

_____**серия:**_____**номер:**_____

дата выдачи:_____ **кем выдан:**_____

Проживающий: адрес по регистрации:_____

_____

фактический адрес

проживания:_____

В соответствии с требованиями статьи 9 Федерального закона от 27.07.06 «О персональных данных» №152-ФЗ подтверждаю свое согласие на обработку моих персональных данных в указанных целях Оператором персональных данных (далее – Оператор) и его структурными подразделениями в соответствии с действующим законодательством.

К персональным данным на обработку которых дается согласие, относятся: паспортные данные**,** анкетные данные (данные о возрасте и поле, данные о гражданстве, данные налогоплательщика, данные СНИЛСа, информация для связи), квалификационные

характеристики (поощрения и взыскания, награды и достижения), семейное положение (данные о семейном положении и членах семьи), сведения о воинском учете (для военнообязанных) (данные военного билета), должностная информация (данные трудовой книжки), сведения о категории работника (совместитель, молодой специалист, пенсионер), сведения о педагогической деятельности (данные о преподаваемых предметах, данные о дополнительной педагогической нагрузке, данные о классном руководстве), сведения (об образовании и повышении квалификации, о стаже и аттестации, о научно-методической работе, о материальной ответственности, финансовые данные, сведения для расчета оклада сотрудника), дополнительные сведения (копии документов, предоставляемых при трудоустройстве и в ходе выполнения должностных обязанностей, и другие дополнительные сведения, фотография сотрудника данные об изображении лица), биометрические данные.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор персональных данных, систематизацию персональных данных, накопление персональных данных, хранение персональных данных, уточнение (обновление, изменение) персональных данных, использование персональных данных, распространение внутреннее, распространение внешнее, размещение в Интернет, ознакомление, обнародование, предоставление доступа к персональным данным иным способом, обезличивание персональных данных, блокирование персональных данных, уничтожение персональных данных.

Срок хранения персональных данных составляет семьдесят пять лет. Настоящее согласие действует бессрочно.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

Дата_____ Подпись_____/_____/
Субъекта персональных данных

Дата_____Подпись_____/_____ /
Ответственного за обработку персональных данных

Приложение 3

ИНСТРУКЦИЯ
по работе Колледжа с персональными данными

РАЗДЕЛ I
«Организация работы администрации по защите персональных данных»

1. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕДСТАВЛЯЕТ СОБОЙ

комплекс мер технического, организационного, организационно-технического и правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (работнику).

2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ ВКЛЮЧАЮТ В СЕБЯ:

- ✓ фамилия, имя, отчество;
- ✓ год, месяц, дата и место рождения;
- ✓ адрес;
- ✓ семейное, социальное, имущественное положение;
- ✓ образование;
- ✓ профессия;
- ✓ доходы
- ✓ и другая информация

Работодатель, получающий доступ к персональным данным, должен обеспечить их конфиденциальность

Перечень сведений конфиденциального характера, утвержденный указом Президента Российской Федерации от 6 марта 1997 года № 188 (ред. от 13.07.2015 № 357), относит персональные данные к категории конфиденциальной информации.

- **Биометрические данные** - это всё то, что характеризует биологические или физиологические особенности человека, на основании которых можно установить его личность.

- ✓ Оператор выдаёт сотрудникам электронные пропуска для входа на свою территорию
- ✓ Оператор оказывает какие-либо услуги и фотографирует клиента при получении банковской карты, пропуска, при заполнении анкеты и т.д.

- **Использование фотографии** без разрешения фотографируемого человека разрешено, если человек сам выложил в Интернет свои фотографии.

3. ВИДЕОНАБЛЮДЕНИЕ

- ✓ для организации видеонаблюдения нужно разработать локальный нормативный акт;
- ✓ работа видеокамер не должна нарушать право работников на частную жизнь

- **Для организации видеонаблюдения без нарушений необходимо:**
- ✓ в правила внутреннего трудового распорядка следует включить пункт о наличии в организации системы видеонаблюдения;
- ✓ издание приказа об установке системы видеонаблюдения;
- ✓ разработать положение об организации видеонаблюдения;
- ✓ установка системы видеонаблюдения;
- ✓ принятие видеооборудования на баланс в оперативное управление;
- ✓ периодический осмотр системы видеонаблюдения с заполнением акта проверки;
- ✓ размещение оповещающих знаков «Ведется видеонаблюдение».

- **При организации видеонаблюдения запрещено:**

✓ Устанавливать видеокамеры в помещениях, где работники не выполняют должностные обязанности (в комнате отдыха, туалетных комнатах для персонала и др.)

Согласие с работников на использование изображений собирать не обязательно!

4. ПРИ ЗАКЛЮЧЕНИИ ДОПОЛНИТЕЛЬНОГО СОГЛАШЕНИЯ С ЧОП, НЕОБХОДИМО ПРОПИСЫВАТЬ:

✓ какие персональные данные необходимо обрабатывать;

✓ порядок обработки и защиты персональных данных;

✓ как и когда должна прекращаться обработка (происходить уничтожение) персональных данных.

5. ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ НЕОБХОДИМО ЗНАТЬ АДМИНИСТРАЦИЯ КОЛЛЕДЖА ДОЛЖНА:

✓ четко осознавать степень ответственности;

✓ особое внимание уделять тем случаям, когда приходится выносить персональные данные из образовательной организации: поездки, олимпиады, диспансеризации;

✓ любая передача персональных данных должна быть запротоколирована;

✓ если Колледж не уверено в правомочности обращения за персональными данными, то вправе потребовать письменного предъявления доказательств;

✓ при публикации на личном сайте, педагогическом портале или Интернет-ресурсе достижений студентов с подписями их имен, фамилий и группы нужно либо не указывать полные ФИО, либо иметь разрешение от родителей на такую публикацию с указанием ФИО студента.

6. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ:

✓ привлечение юристов, специалистов отдела кадров и по информационной работе (компьютерным технологиям);

✓ правовая составляющая (разработка локальных актов, формирование механизма взаимоотношений с органами государственной власти, профсоюзными организациями, органами контроля и надзора и т.д.);

✓ четкая регламентация функций работников;

✓ оценка наличия предусмотренных законодательством оснований для обработки персональных данных, а в случаях, когда они отсутствуют, – получение согласия субъекта персональных данных на их обработку;

✓ учреждение предварительно должно получить согласие граждан на обработку их персональных данных;

✓ внимательно подойти к вопросу размещения информации, содержащей персональные данные, на интернет-сайте Колледжа.

7. ЭТАПЫ РАБОТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ:

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

✓ выделение процессов, в которых обрабатываются персональные данные;

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

✓ определение круга информационных систем и совокупности обрабатываемых персональных данных;

✓ определение уровня защищенности персональных данных;

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

✓ внедрение системы обеспечения безопасности информации.

- **Основной локальный нормативный акт** - Положение о защите персональных данных работников (принимается с учетом мнения педагогического Совета Колледжа), определяющий:
  - ✓ порядок обработки персональных данных работников;
  - ✓ обеспечение защиты прав и свобод работников при обработке их персональных данных;
  - ✓ ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Данный локальный нормативный акт является обязательным (его отсутствие может быть квалифицировано государственным органом контроля и надзора – как нарушение работодателем трудового законодательства).

8. ДОКУМЕНТЫ, РЕГУЛИРУЮЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ НА ЛОКАЛЬНОМ УРОВНЕ:

- ✓ в процессе получения персональных данных – согласие работника на получение работодателем персональных данных от третьих лиц и уведомление работника о получении его персональных данных от третьих лиц;
- ✓ при обработке персональных данных – согласие работника на обработку его персональных данных;
- ✓ при хранении персональных данных – приказ об утверждении списка лиц, имеющих доступ к персональным данным работников, и обязательств о неразглашении;
- ✓ при передаче персональных данных работников – согласие работника на передачу его персональных данных третьим лицам.

1. Журнал учета внутреннего доступа к персональным данным	- обязательное присутствие при проверке возвращенного документа, содержащего персональные данные, на наличие всех имеющихся документов по описи; - лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые
2. Журнал учета выдачи персональных данных работников организациям и государственным органам	В журнале необходимо регистрировать: - поступающие запросы; - сведения о лице, направившем запрос; - дату передачи персональных данных или уведомления об отказе в их предоставлении; - какая именно информация была передана.
3. Журнал проверок наличия документов, содержащих персональные данные работников	
4. Журнал учета применяемых работодателем носителей информации	

- **Работодатель (оператор), при обеспечении защиты персональных данных работников обязан:**
  - ✓ осуществить блокирование персональных данных, относящихся к

соответствующему субъекту персональных данных;

✓ устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления;

✓ незамедлительно прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты достижения цели обработки, и уведомить об этом субъекта персональных данных или его законного представителя;

✓ прекратить обработку персональных данных и уничтожить их, в случае отзыва субъектом персональных данных согласия на их обработку, в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва.

Персональные данные работника могут быть переданы работодателем <u>третьей стороне</u> только в следующих случаях:	**При передаче персональных данных работника работодатель должен соблюдать следующие обязательные требования:**
- выдача работником письменного согласия на передачу персональных данных третьей стороне; - передача персональных данных работника в целях предупреждения угрозы жизни и здоровью самого работника; - другие случаи, установленные федеральным законом.	- не сообщать персональные данные работника третьей стороне без письменного согласия работника; - разрешать доступ к персональным данным работников только специально уполномоченным лицам; - передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами.

- **Получатели персональных данных работника:**

✓ органы социального страхования, органы пенсионного обеспечения, а также иные органы, организации и граждане;

✓ налоговые органы;

✓ органы прокуратуры и другие правоохранительные органы;

✓ федеральная инспекция труда;

✓ профессиональные союзы;

✓ другие органы и организации в случаях, предусмотренных федеральным законом.

- **Права работников, связанные с обработкой и защитой их персональных данных**

✓ право на полную информацию о своих персональных данных и обработке этих данных;

✓ свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника;

✓ определение своих представителей для защиты персональных данных;

✓ доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

✓ требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона;

✓ требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

✓ обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

<u>Работники обязаны в разумный срок информировать работодателя об изменении персональных данных</u>

9. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СТУДЕНТА

Обработка (получение, сбор, использование, передача, хранение и защита) персональных данных студента может осуществляться исключительно в целях:

- ✓ обеспечения соблюдения законов и иных нормативных правовых актов;
- ✓ содействия студента в получении образования, трудоустройстве;
- ✓ обеспечения их личной безопасности;
- ✓ контроля обучения и воспитания;
- ✓ обеспечения сохранности имущества в минимально необходимом для этих целей объеме.

- **Хранение и использование персональных данных студентов**

Персональные данные студентов хранятся на электронных носителях на сервере Колледжа, а также на бумажных и электронных носителях у оператора (руководителя Колледжа и (или) уполномоченного им лица).

- **При работе с персональными данными в целях обеспечения информационной безопасности необходимо, чтобы:**

- ✓ рабочая станция прошла сертификацию;
- ✓ оператор не оставлял в свое отсутствие компьютер незаблокированным;
- ✓ оператор имел свой персональный идентификатор и пароль;
- ✓ компьютер с базой данных не был подключен к локальной сети и сети Интернет.

- **Доступ к персональным данным студента без получения специального разрешения имеют право:**

- ✓ руководитель Колледжа;
- ✓ заместители руководителя Колледжа;
- ✓ секретарь учебной части;
- ✓ заведующие отделениями (кураторы групп) (только к персональные данные своего отделения (группы).

10. ЭТАПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ЭТАП 1. ***Инвентаризация информационных ресурсов***

Инвентаризация информационных ресурсов – это выявление присутствия и осуществления обработки персональных данных во всех эксплуатируемых в организации информационных системах и традиционных хранилищах данных.

На данном этапе следует: утвердить положение о защите персональных данных, сформировать концепцию, определить политику информационной безопасности, составить перечень персональных данных, подлежащих защите.

ЭТАП 2. ***Ограничение доступа работников к персональным данным***

Ограничение доступа работников организации к персональным данным – неотъемлемая часть мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах.

На данном этапе следует: в необходимой мере ограничить как электронный, так и физический доступ к персональным данным, хранящимся в учреждении.

ЭТАП 3. ***Документальное регламентирование работы с персональными данными***

Субъект персональных данных **самостоятельно решает вопрос их передачи** кому-либо, оформляя свое намерение документально.

На данном этапе следует: собрать согласия на обработку персональных данных, издать приказ о назначении лиц, ответственных за обработку персональных данных, и положение о разграничении прав доступа к обрабатываемым персональным данным, составить инструкции администратора ИСПДн, пользователя ИСПДн и администратора безопасности ИСПДн.

ЭТАП 4. ***Формирование модели угроз безопасности персональных данных***

Формируется на основании следующих **документов, утвержденных Федеральной службой по техническому и экспортному контролю (ФСТЭК)**:

- ✓ базовая модель угроз безопасности персональных данных при их обработке в ИСПДн;
- ✓ методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн.

На данном этапе следует: сформировать модель угроз безопасности персональных данных, обрабатываемых и хранящихся в учреждении.

ЭТАП 5. ***Определение уровня защищенности персональных данных***

На данном этапе следует: составить Акт определения уровня защищенности ПДн при их обработке в ИСПДн.

ЭТАП 6. ***Составление и отправка в уполномоченный орган уведомления***

Уведомление:

- ✓ оформляется на бланке оператора;
- ✓ указываются данные об обработчике, цель обработки, категории данных, категории субъектов, данные которых обрабатываются, правовое основание обработки, дата ее начала, срок (условие) ее прекращения и прочее;
- ✓ направляется в территориальный орган Роскомнадзора Министерства связи и массовых коммуникаций РФ на бумажном носителе или в форме электронного документа с подписью уполномоченного лица.

На данном этапе следует: на сайте Уполномоченного органа по защите прав субъектов персональных данных **http://www.pd.rsoc.ru/operators-registry/notification/form/** заполнить и отправить форму уведомления в электронном виде или распечатать на бумажном носителе.

ЭТАП 7. ***Приведение системы в соответствие с требованиями регуляторов***

Оператор персональных данных **ОБЯЗАН** принимать все необходимые меры по защите безопасности персональных данных.

На данном этапе следует: создать перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним; положение о подразделении по защите информации; методические рекомендации для организации защиты информации при обработке персональных данных; инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций, а также утвердить план мероприятий по защите персональных данных.

ЭТАП 8. ***Организация эксплуатации ИСПДн и контроля за безопасностью***

Основные мероприятия:

- ✓ контроль за соблюдением условий использования средств защиты информации;
- ✓ разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных

На данном этапе следует:

1. Разработать проект приказа о положении об электронном журнале обращений пользователей информационных систем персональных данных → создать журнал учета обращений субъектов персональных данных о выполнении их законных прав и журнал учета мероприятий по контролю.
2. Сформировать план внутренних проверок → издать приказ о проведении внутренней проверки → составить отчет о результатах проведения внутренней проверки.

11. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДОСТИГАЕТСЯ:

- ✓ определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- ✓ применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- ✓ применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- ✓ оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- ✓ учетом машинных носителей персональных данных;
- ✓ обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- ✓ восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- ✓ установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- ✓ контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных

12. ВОЗМОЖНЫЕ ПУТИ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ:

- ✓ Электронное письмо с ценной информацией может быть отослано по почтовым протоколам.
- ✓ Информация может быть отправлена посредством клиентов для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber).
- ✓ Голосовые или текстовые сообщения, отправленные через Skype, также могут содержать персональные данные.
- ✓ Информация может быть размещена на форумах, блогах, передана по социальным сетям. Передана по FTP-протоколу.
- ✓ Ценные данные могут быть переписаны на съёмный носитель (USB-флешку или CD/DVD диски).
- ✓ Информация может быть распечатана на принтере.

13. СОЗДАНИЕ И ОТСЛЕЖИВАНИЕ ГРУППЫ РИСКА

Сотрудников, по той или иной причине попавших под подозрение, нужно пристально контролировать. Для этого необходимо анализировать всю информацию, которая уходит во внешний мир под их учетной записью.

В группу риска имеет смысл включать:

- ✓ Сотрудников, которые замечены в нарушении информационной безопасности.
- ✓ Сотрудников, использующих различные трюки (анонимайзеры, TOP-браузер и т.д.).
- ✓ Недовольных сотрудников (негативные отзывы о руководстве, о компании и т.д.).
- ✓ Сотрудников, которые по каким-то причинам начали менее эффективно работать.

РАЗДЕЛ II

«Технические способы защиты информации»

1. ОТВЕТСТВЕННОСТЬ СПЕЦИАЛИСТА В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ:

Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации.

Обеспечение безопасности информации – дело дорогостоящее в связи со сложностью определения границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии

Объекты защиты:

- ✓ технические средства;
- ✓ материальные объекты;
- ✓ программное обеспечение;

- ✓ базы данных

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОЛЖНО БЫТЬ ДОСТИГНУТО ПУТЕМ СОХРАНЕНИЯ СВОЙСТВ ИНФОРМАЦИИ:

Доступность – это свойство информации, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующей их информации.

Целостность информации заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Конфиденциальность – это свойство информации, указывающее на необходимость введения ограничений на доступ к данной информации определенному кругу пользователей

3. ФАКТОРЫ (УГРОЗЫ) ПОТЕРИ ИНФОРМАЦИИ:

Случайные угрозы:

- ✓ ошибки обслуживающего персонала и пользователей:
  - потери информации, связанные с неправильным хранением данных;
  - случайное уничтожение или изменение данных.
- ✓ сбои оборудования и электропитания:
  - сбои кабельной системы;
  - перебои электропитания;
  - сбои дисковых систем;
  - сбои систем архивации данных;
  - сбои работы серверов, рабочих станций, сетевых карт и т.д.;
- ✓ потери информации из-за некорректной работы программного обеспечения:
  - потеря или изменение данных при ошибках в программном обеспечении;
  - потери при заражении системы компьютерными вирусами;
- ✓ потери, связанные с несанкционированным доступом:
  - ознакомление с конфиденциальной информацией посторонних лиц.

Труднопредсказуемые источники угроз:

- ✓ аварии;
- ✓ стихийные бедствия.

Основной способ защиты:

- ✓ хранение архивных копий информации.

4. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- ✓ **Организационные методы** подразумевают рациональное конфигурирование, организацию и администрирование системы.
- ✓ **Технологические методы,** включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации.
- ✓ **Аппаратные методы,** реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т.д.
- ✓ **Программные методы** – это самые распространенные методы защиты информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т.д.).

5. НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ:

- ✓ **Защита от несанкционированного доступа информационных ресурсов** автономно работающих и сетевых компьютеров. Наиболее остро эта проблема стоит для серверов и пользователей сетей Интернета и Интранета. Эта функция реализуется многочисленными программными, программно-аппаратными и аппаратными средствами.

✓ **Защита секретной, конфиденциальной и личной информации** от чтения посторонними лицами и целенаправленного ее искажения. Эта функция обеспечивается как средствами защиты от несанкционированного доступа, так и с помощью криптографических средств, традиционно выделяемых в отдельный класс.

✓ **Защита информационных систем от многочисленных компьютерных вирусов**, способных не только разрушить информацию, но иногда и повредить технические компоненты системы: Flash BIOS, винчестеры и т. д.

6. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Программно-технические средства защиты

Сервис безопасности:

- ✓ идентификация и аутентификация;
- ✓ управление доступом;
- ✓ протоколирование и аудит;
- ✓ контроль целостности;
- ✓ экранирование;
- ✓ анализ защищенности;
- ✓ обеспечение отказоустойчивости;
- ✓ обеспечение безопасного восстановления;
- ✓ туннелирование;
- ✓ управление.

1. От несанкционированного копирования, в том числе:
- средства защиты носителей данных;
- средства предотвращения копирования программного обеспечения, установленного на ПЭВМ

2. Средства криптографической и стенографической защиты информации.

3. Средства прерывание работы программы пользователя при нарушении им правил доступа, в том числе:
- принудительное завершение работы программы;
- блокировка компьютера

4. Средства стирания данных, в том числе:
- стирание остаточной информации, возникающей в процессе обработки данных в оперативной памяти и на магнитных носителях;
- надежное стирание устаревшей информации с магнитных носителей

5. Средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе:
- средства регистрации некорректных обращений пользователей к защищаемой информации;
- средства организации контроля за действиями пользователей ПЭВМ.

6. Средства обнаружения и локализации действия программных и программно-технических закладок.

6.2. Технические средства защиты

- ✓ системы охранной и пожарной сигнализации;
- ✓ системы цифрового видео наблюдения;
- ✓ системы контроля и управления доступом (СКУД). Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- создание контролируемых зон.

6.3. Программные средства защиты

- ✓ средства собственной защиты;
- ✓ средства защиты в составе вычислительной системы;

- ✓ средства защиты с запросом информации;
- ✓ средства активной защиты;
- ✓ средства пассивной защиты.

- **Направления использования программ для обеспечения безопасности конфиденциальной информации:**
  - ✓ защита информации от несанкционированного доступа;
  - ✓ защита информации от копирования;
  - ✓ защита программ от копирования;
  - ✓ защита программ от вирусов;
  - ✓ защита информации от вирусов;
  - ✓ программная защита каналов связи.

- **Программные средства защиты информации имеют следующие разновидности специальных программ:**
  - ✓ идентификация технических средств, задач, массивов и пользователей;
  - ✓ определение прав технических средств, задач и пользователей;
  - ✓ контроль работы технических средств и пользователей;
  - ✓ регистрация работы технических средств и пользователей при обработке закрытой информации;
  - ✓ уничтожение информации в ЗУ после завершения работы;
  - ✓ сигнализация о несанкционированных действиях;
  - ✓ вспомогательные программы различного назначения (контроль работы механизма защиты, автоматическое проставление грифа и т.п.).

6.4. Физические средства защиты

- **ЭТО** разнообразные устройства, приспособления, конструкции, предназначенные для создания препятствий на пути движения злоумышленников.

- **Эти средства применяются для решения следующих задач:**
  - ✓ охрана территории предприятия и наблюдение за ней;
  - ✓ охрана зданий, внутренних помещений и контроль над ними;
  - ✓ охрана оборудования, продукции, финансов и информации;
  - ✓ осуществление контролируемого доступа в здания и помещения

1. Системы ограждения и физической изоляции, обеспечивающие:
   - ✓ защиту объектов по периметру;
   - ✓ защиту элементов зданий и помещений;
   - ✓ защиту объемов зданий и помещений.
2. Системы контроля доступа, реализующие:
   - ✓ контроль доступа на охраняемые объекты;
   - ✓ защиту документов, данных, файлов.
3. Запирающие устройства и хранилища, включающие:
   - ✓ различные системы запирающих устройств (механические, электромеханические, электронные);
   - ✓ различные системы шкафов и хранилищ.

7. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

- **ЭТО** комплекс организационно-технических мероприятий, в результате которых посредством специального документа - «Аттестата соответствия»- подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции.

Обязательной аттестации подлежат следующие информационные системы:

- ✓ информационные системы, в которых обрабатывается информация, составляющая государственную тайну, или информация об управлении экологически опасными объектами;
- ✓ информационные системы, отнесенные к муниципальным или государственным.

- **Порядок проведения аттестации объектов информатизации:**

- ✓ подача заявки на рассмотрение и проведение аттестации;
- ✓ анализ исходных данных по аттестуемому объекту информатизации;
- ✓ проведение предварительного специального обследования аттестуемого объекта информатизации;
- ✓ разработка программы и методики аттестационных испытаний;
- ✓ заключение договоров на аттестацию;
- ✓ испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- ✓ проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;
- ✓ проведение аттестационных испытаний объекта информатизации;
- ✓ оформление, регистрацию и выдачу «Аттестата соответствия».

8. 152-ФЗ И САЙТ КОЛЛЕДЖА:

- ✓ Хостинг и база данных с персональными данными должна располагаться на территории России.
- ✓ Под каждой формой сбора данных, включая сбор email, разместить текст «Нажимая на кнопку, вы даете согласие на обработку своих персональных данных».
- ✓ Указать информацию о том, как физическое лицо может отозвать свое согласие

на обработку персональных данных.

✓ Разместить на сайте в общем доступе ссылку на документ — политику организации в отношении обработки персональных данных на сайте.

✓ Показывать всем новым пользователям сайта предупреждение с текстом о том, что вы собираете метаданные пользователя для функционирования сайта.

9. ЭТАПЫ ПРИВЕДЕНИЯ ПРОЦЕССОВ ОБРАБОТКИ И ЗАЩИТЫ ПДн

✓ Обследование организации на предмет соответствия процессов обработки и защиты персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

✓ Разработка комплекта внутренней организационно-распорядительной документации, регламентирующей процессы обработки и защиты персональных данных.

✓ Определение угроз безопасности и потенциальных нарушителей безопасности персональных данных, обрабатываемых в информационной системе персональных данных.

✓ Определение требуемого уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных.

✓ Разработка технического задания на создание системы защиты персональных данных.

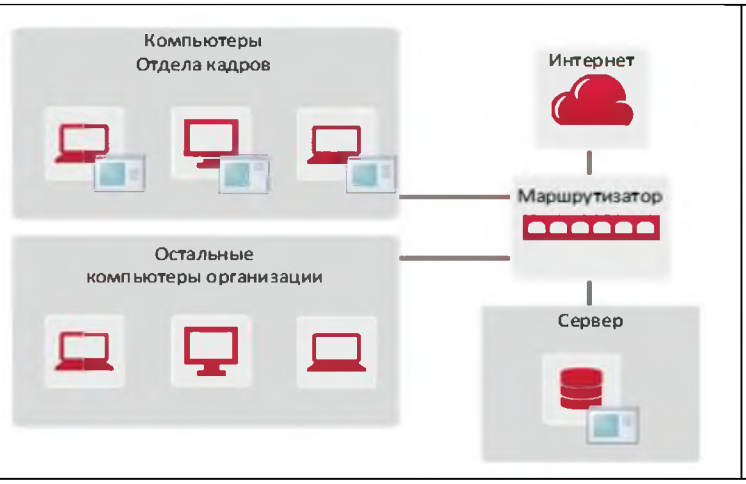
✓ Приобретение средств защиты информации.

✓ Внедрение системы защиты персональных данных.

✓ Организация и проведение аттестации соответствия системы защиты персональных данных требованиям безопасности информации

1. Обследование организации на предмет соответствия процессов обработки и защиты персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Разработка комплекта внутренней организационно-распорядительной документации, регламентирующей процессы обработки и защиты персональных данных.

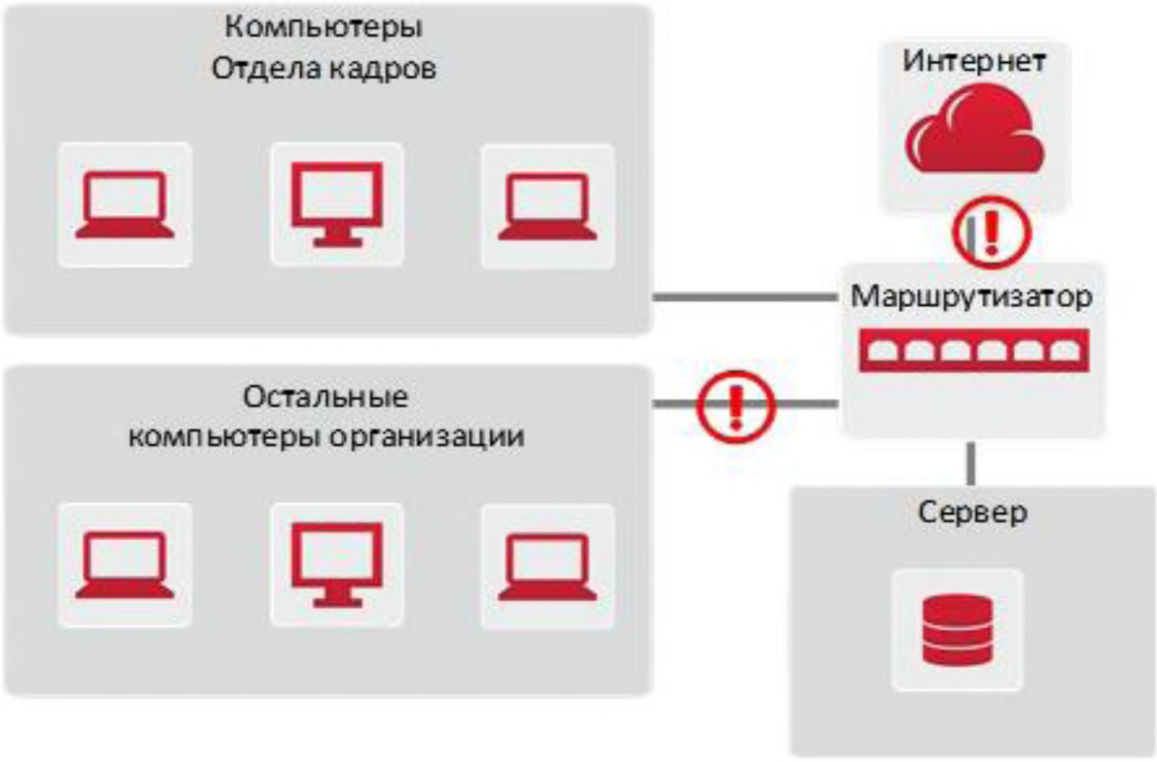


В качестве ПО обработки ПДн используется любое кадровое ПО («Контур-Персонал», «1С: Зарплата и Управление персоналом», сертифицированное ФСТЭК, прочее ПО)
В компании реализованы организационные и физические меры защиты ПДн, однако отсутствуют технические средства защиты информации

3. Определение угроз безопасности и потенциальных нарушителей безопасности персональных данных, обрабатываемых в информационной системе персональных данных.

4. Определение требуемого уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных.

№ п/п	Угроза безопасности ПДн	Тип угрозы	Вероятность реализации угрозы	Возможность реализации	Опасность угрозы	Актуальность
1	Угрозы, реализуемые за счет непосредственного доступа	3	маловероятно	низкая	средняя	неактуальная
2	Угрозы, реализуемые за счет действия вредоносных программ	3	средняя	средняя	высокая	актуальная
3	Угрозы, реализуемые за счет недостатков сетевого программного обеспечения	3	низкая	средняя	средняя	актуальная
4	Угрозы, реализуемые за счет преднамеренных действий пользователей	3	маловероятно	низкая	средняя	неактуальная

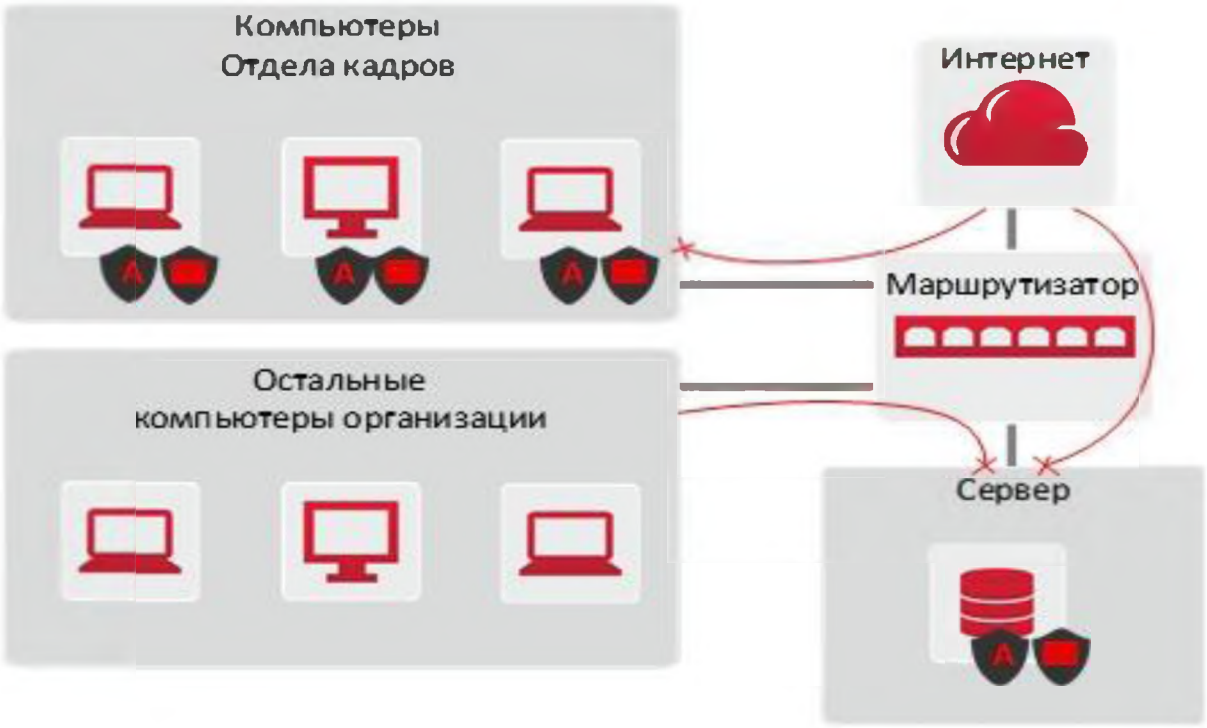


Основные источники угроз:

- ✓ внешние нарушители;
- ✓ внутренние нарушители.

5. Построение системы защиты персональных данных

№ п/п	Содержание мер по обеспечению безопасности ПДн	Нейтрализуемая угроза безопасности ПДн	Способ реализации
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора		Средствами ПО обработки ПДн
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		Средствами ПО обработки ПДн
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		Средствами ПО обработки ПДн
ИАФ.5	Защита обратной связи при вводе аутентификационной информации		Средствами ПО обработки ПДн
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей		Средствами ПО обработки ПДн
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		Средствами ПО обработки ПДн
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Угрозы, реализуемые за счет недостатков сетевого программного обеспечения	Персональный межсетевой экран
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		Средствами ПО обработки ПДн
V. Регистрация событий безопасности (РСБ)			
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		Средствами ПО обработки ПДн
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Угрозы, реализуемые за счет действия вредоносных программ	Антивирусное средство защиты информации
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Угрозы, реализуемые за счет действия вредоносных программ	Антивирусное средство защиты информации


Компьютеры
Отдела кадров
Интернет
Маршрутизатор
Остальные
компьютеры организации
Сервер