Введение

Тема: "Технология защиты персональных данных".

Цель работы: показать уровень владения следующими компетенциями:

* обеспечить защиту персональных данных;
* осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
* использовать информационно-коммуникационные технологии в профессиональной деятельности;
* организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
* понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

Задачи работы:

* подобрать, проанализировать и обобщить источники информации в соответствие с темой работы;
* раскрыть понятие персональные данные;
* изучить технологию защиты персональных данных;
* изучить правила использования персональных данных;
* изучить правовые основы персональных данных;
* научиться составлять ситуационные задачи и вопросы к ним.

Предмет - технология организации защиты конфиденциальных данных в кадровой службе.

Проблема - персональные денные в данное время в том, что персональные данные плохо защищены.

Данная тема является, актуальной в XXI веке у человечества, появляется все больше новых объектов, нуждающихся в защите путем закрепления соответствующих норм в законе. Основной объект в настоящее время – это информация. В наше время общество всецело зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине данные сами по себе приобретают высокую ценность. И тем больше цена полезной информации, чем выше ее сохранность.

В виду вышесказанного, законодательными актами, как в России, так и зарубежных стран предусматривают немалое количество норм, направленных на регулирование создания, пользования, передачи и защиты информации во всех ее формах.

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

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

1. Федеральное законодательство в области защиты конфиденциальной информации

Множество Федеральных законов раскрывают понятие персональных данных, рассмотрим следующие:

Федеральный закон "О персональных данных".

Целью настоящего ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В настоящем ФЗ используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

3) обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

4) распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

5) использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

6) блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

7) уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

8) обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

9) информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

10) конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

11) трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

12) общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

На основании и во исполнение федеральных законов государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных. Нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, не могут содержать положения, ограничивающие права субъектов персональных данных. Указанные нормативные правовые акты подлежат официальному опубликованию, за исключением нормативных правовых актов или отдельных положений таких нормативных правовых актов, содержащих сведения, доступ к которым ограничен федеральными законами.

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Условия обработки персональных данных.

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных.

Согласия субъекта персональных данных, не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

3) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

4) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

7) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Общедоступные источники персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

В случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

Специальные категории персональных данных.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Обработка специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

2.1.) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2) способы обработки персональных данных, применяемые оператором;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных.

Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

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

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Оператор обязан рассмотреть возражение, в течение семи рабочих дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Право на обжалование действий или бездействия оператора.

Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Оператор обязан в порядке, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

В случае предоставления неполных или недостоверных сведений, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

В случае изменения сведений, оператор обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений.

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

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.

Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

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.

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;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, 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 Российской Федерации обязанности.

Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

Ответственность за нарушение требований настоящего Федерального закона.

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ФЗ РФ "Об информации, информационных технологиях и о защите информации"

В настоящем Федеральном законе используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) 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;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

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

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки, содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения целей.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

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. 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.

**Федеральный закон "О коммерческой тайне"**

**Для целей настоящего Федерального закона используются следующие основные понятия:**

**1) коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;**

**2) информация, составляющая коммерческую тайну (секрет производства), сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении, которых обладателем таких сведений введен режим коммерческой тайны;**

**3) обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;**

**4) доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;**

**5) передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;**

**6) контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;**

**7) предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;**

**8) разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.**

**Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.**

**Сведения, которые не могут составлять коммерческую тайну.**

**Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:**

**1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;**

**2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;**

**3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;**

**4) 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;**

**5) 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, и о наличии свободных рабочих мест;**

**6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;**

**7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;**

**8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;**

**9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;**

**10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;**

**11) обязательность раскрытия, которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.**

Предоставление информации, составляющей коммерческую тайну.

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

**Охрана конфиденциальности информации. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:**

**1) определение перечня информации, составляющей коммерческую тайну;**

**2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;**

**3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;**

**4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;**

**5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).**

**В целях охраны конфиденциальности информации работодатель обязан:**

**1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;**

**2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;**

**3) создать работнику необходимые условия для соблюдения, им установленного работодателем режима коммерческой тайны.**

**Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.**

**В целях охраны конфиденциальности информации работник обязан:**

**1) выполнять установленный работодателем режим коммерческой тайны;**

**2) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;**

**3) передать работодателю при прекращении или расторжении трудового договора, имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.**

**Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.**

**Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.**

**Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.**

**Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.**

**По требованию обладателя информации, составляющей коммерческую тайну, лицо, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.**

**2. Персональные данные работников и их защита в кадровых службах**

Персональные данные (или личные данные) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Защита персональных данных** – это комплекс мер, предпринимаемый операторами по противодействию несанкционированному использованию персональных данных, включающих организационно административные и технические методы защиты.

Руководитель предприятия и сотрудники кадровых служб должны приложить все усилия для защиты персональных данных работника.

В соответствии с ТК РФ персональные данные работника – это информация, необходимая работодателю в связи с трудовыми отношениями и касающихся конкретного работника.

Для обеспечения прав и свобод человека и гражданина работодатель и его представитель при обработке персональных данных работника обязаны соблюдать следующие общие требования:

* + **обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативно правовых актов, содействия работника в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечение сохранности имущества;**
  + **при определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами;**
  + **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 за ранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;**
  + **работодатель не имеет право получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждений и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;**
  + **работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;**
  + **при принятии решений, затрагивающих интересы работников, работодатель не имеет право основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработке;**
  + **работодатель должен обеспечить защиту персональных данных работника от неправомерного их использования или утраты за счет своих средств в порядке, установленном федеральным законом;**
  + **работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а так же об их правах и обязанностях в этой области;**
  + **работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работника, а работники не должны отказываться от своих прав на сохранение и защиту тайны.**

**При передаче персональных данных работника работодатель должен соблюдать следующие правела:**

* + **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 так же в случаях, установленных ФЗ;**
  + **не сообщать персональные данные работников в коммерческих целях без его письменного согласия;**
  + **предупреждать лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых оби сообщены, и требовать от этих лиц подтверждение того, что это правело соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Федеральными законами;**
  + **осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;**
  + **разрешать доступ к персональным данным работников толь специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функции;**
  + **не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу по возможности выполнения работником трудовой функции.**

**Работник наделен правами, обеспечивающими защиту его персональных данных, хранящихся у работодателя. Работник имеет право:**

* + **на полную информацию о своих персональных данных и обработке этих данных;**
  + **свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных ФЗ;**
  + **определение (выбор) своих представителей для защиты своих персональных данных; доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по его выбору;**
  + **требования об исключении или исправлении неверных или не полных персональных данных, а так же данных, обработанных с нарушением требований ТК РФ. При отказе работодателя исключить или исправить персональные данные работника он имеет право в письменной форме заявить работодателю о своем не согласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;**
  + **требование об извещении работодателем всех лиц, которым ранее были, сообщены неверные или не полные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;**
  + **обжалование в суд любых не правомерных действий или бездействия работодателя при обработке и защите его персональных данных.**

**Лица, виновные в нарушении норм, регулирующих получение обработку и защиту персональных данных работника, несут дисциплинарную, административную, и гражданско-правовую или уголовную ответственность в соответствии с федеральными законами (ТК РФ, ст.86 - 90).**

3. Организация работы с конфиденциальными документами

Под безопасностью информационных ресурсов понимается гарантия защиты, информации во времени и пространстве.

Ценная информация и конфиденциальные документы.

Документированные информационные ресурсы, которые используются в бизнесе и в управлении организацией, являются интеллектуальной собственностью организации и нуждаются в защите. Ценность информации определяется размером прибыли от ее использования или размером убытков от ее утраты

Существует два вида информации, ценной для предпринимателя:

1.Техническая, технологическая (методы изготовления продукции, программное обеспечение, производственные показатели, формулы, рецепты, результаты испытания образцов, данные контроля качества и т.д.).

2. Деловая (управленческие решения, результаты исследования рынка, списки клиентов, экономические прогнозы и т.д.).

Наиболее ценными являются сведения о производстве, продукции, рынке, научных разработках, материально-технической базе, переговорах, персонале, службе безопасности.

Под конфиденциальными документами понимается необходимым образом оформленный носитель информации, содержащий сведения об ограничении доступа. Называть конфиденциальные документы секретными или ставить на них гриф секретности не допускается.

Регламентация состава конфиденциальных сведений и документов.

К конфиденциальным не могут быть отнесены следующие сведения и документы:

1. Учредительные документы.

2. Отчетность о финансово-хозяйственной деятельности, необходимая для уплаты налогов.

3. Документы о платежеспособности.

4. Сведения о численности, составе и заработной плате работников, об условиях труда и наличии вакансий.

5. Сведения об уплате налогов.

6. Сведения о причинении ущерба природе, здоровью граждан и государству.

7. Сведения об участии руководящего состава в другой предпринимательской деятельности.

Перечень конфиденциальных сведений организации представляет собой список ценной информации, срок конфиденциальности (1-2года), гриф конфиденциальности (уровень), список сотрудников, которым дано право, использовать, эти сведения в работе. В нем предусматривается дробление ценной информации на отдельные элементы, известные разным людям. Перечень создается в рамках одного структурного подразделения.

Документирование конфиденциальных сведений. Технологическая процедура документирования конфиденциальных сведений включает в себя следующие этапы:

1. Получение разрешения на издание конфиденциального документа.

2. Установление уровня конфиденциальности.

3. Оформление и учет носителей информации.

4. Составление черновика документа.

5. Получение разрешения на изготовление документа.

6. Учет черновика.

7. Издание документа.

8. Уничтожение чернового издания документа.

Гриф ограничения доступа ставится на всех экземплярах документа, черновиках, вариантах и копиях. Можно выделить следующие уровни ограничения доступа:

1. Конфиденциально.

2. Конфиденциальная информация.

3. Строго конфиденциально.

4. Строго конфиденциальная информация.

5. Особый контроль. (Этот гриф присваивается лично первым руководителем предприятия).

6. Для служебного пользования.

7. Служебная информация.

8. Не для печати.

В служебной переписке ниже реквизита адресата может быть пометка "Лично", "Только в руки", "Лично в руки" и т.п.

При регистрации конфиденциальных документов к регистрационному номеру добавляется сокращенное обозначение грифа №37к, №89ск, №97дсп.

На ценных, но не конфиденциальных документах может ставиться отметка об особом внимании к сохранности документа: "Собственная информация фирмы", "Информация особого внимания", "Копии не снимать", "Хранить в сейфе" и т.п.

Носители конфиденциальной информации регистрируются и учитываются. Ими могут быть:

* специальный блокнот с отрывными пронумерованными листами или чистые пронумерованные листы для текстовых документов;
* пронумерованные листы ватмана для чертежей;
* маркированные и пронумерованные машинные носители для машинописных документов;
* маркированные и пронумерованные фотопленки, фотобумага для фотодокументов.

Факт перемещения носителя документируется и учитывается. Учитываются и все черновики конфиденциальных документов с ежедневной проверкой их наличия на этапе подготовки документа.

Конфиденциальные документы нельзя диктовать и записывать на диктофон.

Порядок работы исполнителя с конфиденциальным документом.

Ответственность за сохранность конфиденциального документа несут руководители структурных подразделений.

Сотрудники организации при работе с конфиденциальными документами обязаны:

1. Знакомится только с теми документами, к которым они получили доступ по письменному разрешению руководителя.

2. При проверке немедленно предъявлять все числящиеся за ними конфиденциальные документы.

3. Вести строгий учет конфиденциальных документов.

4. Ежедневно в конце рабочего дня проверять наличие конфиденциальных документов и сдавать их на хранение в службу защиты информации.

5. Сдавать по описи все материалы по окончании работы с конфиденциальным документом.

6. Сдавать по описи все материалы, связанные с работой с конфиденциальной информацией, при увольнении, отпуске или командировке.

7. Немедленно сообщать первому руководителю и в службу безопасности об утрате или недостаче конфиденциальных документов.

Для работы с конфиденциальными документами сотрудник должен быть обеспечен рабочим местом, личным сейфом, кейсом для переноса документов, номерной личной металлической печатью. Рабочее место должно быть организовано таким образом, чтобы исключить возможность ознакомления с конфиденциальными документами другими работниками или посторонними лицами. Экран ПК не должен быть виден другим сотрудникам, из окна или двери. На рабочем столе должен быть только тот конфиденциальный документ, с которым идет работа. Остальные должны быть в сейфе. Прочитанные листы документа должны лежать текстом вниз. Покидая помещение, сотрудник убирает документы в сейф и блокирует компьютер.

Документы должны храниться в рабочих папках без подшивки. Наименование папок: "Ознакомление", "Согласование", "Срочно", "Задание на число", "Возврат", "На подшивку в дело" и т.д.

Дела, закрепленные за одним сотрудником, подшиваются в папки с цветовым отличием.

В конце рабочего дня конфиденциальная информация на ПК переписывается на гибкие носители и стирается с жесткого диска.

Право постоянного хранения конфиденциальных документов на рабочем месте имеют:

* первый руководитель;
* его заместители;
* кадровая служба;

Все остальные сотрудники сдают документы в службу безопасности или в службу защиты информации и утром нового рабочего дня получают их в обмен на пропуск.

4. Режим хранения конфиденциальных документов

Хранение конфиденциальных документов требует особого режима, так как информация, содержащаяся в данных документах, является объектом защиты. Специальный режим хранения конфиденциальных документов предусматривает обязательное соблюдение следующих правил:

1.Помещение, где хранятся конфиденциальные документы, не должно находиться на первом или последнем этажах здания, потому что данные этажи потенциально наиболее доступны для проникновения.

2.Вход в помещение разрешается только лицам, имеющим доступ к работе с документами.

3.Уборка помещений, ремонт находящегося в них оборудования и технических средств, связанных с привлечением лиц, не имеющих доступа к хранящимся в помещении документам, должны проходить только в присутствии сотрудников службы защиты информации.

4.Входные двери помещений должны быть обиты металлом и оборудованы надежными замками.

5.По окончании рабочего дня двери не только закрываются, но и опечатываются печатью службы защиты информации. Печать проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск не возможно было снять и восстановить.

6.Перед открытием двери в начале рабочего дня проверяется сохранность оттиска печати и целостность запоров. При обнаружении попыток проникновения в помещение необходимо немедленно поставить в известность службу безопасности и доложить первому руководителю. До принятия решения первым руководителем помещение не открываются и обеспечиваются физической охраной.

7.Для предотвращения несанкционированного входа в помещение в течении рабочего дня на двери устанавливаются электромеханические или электронные замки.

8.Входные двери, окна, сейфы, шкафы, стеллажи следует оснастить охранной сигнализацией.

9.Ключи от сейфов, шкафов, стеллажей, решеток, дверей в не рабочее время должны храниться в опечатанном пенале (конверте) в службе безопасности или в бюро контроля защиты информации. Факт передачи ключа регистрируется в специальном журнале приема-передачи помещений и ключей под охрану. Журнал имеет следующую форму:

Таблица №1: "Журнал приема – передачи помещений и ключей под охрану"

|  |  |  |  |
| --- | --- | --- | --- |
| № помещения, передаваемого под охрану | № печатей, которыми опечатаны помещения и пеналы с ключами | Дата и время передачи под охрану | Подпись и фамилия лица, передавшего помещения и ключи под охрану |
| 1 | 2 | 3 | 4 |

Таблица №2: "Журнал приема – передачи помещений и ключей под охрану"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отметка о включении организации | Подпись и фамилия лица, принявшего объекты под охрану | Дата и время получения пеналов | Подпись и фамилия лица, получившего пеналы | Отметка о выключении сигнализации |
| 1 | 2 | 3 | 4 | 5 |

5. Формулировка и анализ профессиональных задач для использования задач по специальным дисциплинам специальности 032002 "Документационное обеспечение управления и архивоведение с углубленной подготовкой в области кадровой службы"

Ситуационная задача№1

Тема: "Права работника"

Для студентов специальности 032002

"Документационное обеспечение управления

и архивоведение с углубленной подготовкой в области

кадровой службы".

Женщина указала, малолетних детей, а в последующем было установлено, что эта информация не соответствует действительности.

Вопросы:

1. Что будет действительным основанием для увольнения в данном случае?
2. Скрытие информации или наличие у работницы малолетних детей?

Ситуационная задача№2

Тема: "Недостоверные документы, предоставленные работником работодателю"

Для студентов специальности 032002

"Документационное обеспечение управления

и архивоведение с углубленной подготовкой

в области кадровой службы".

Работник предоставил подложную санитарную книжку работодателю.

Вопросы:

1. Возможно ли увольнение в данной ситуации?
2. Каков перечень документов работник должен предоставить работодателю?
3. Понесет ли работник наказание? Если да то, какое?

Ситуационная задача№3

Тема: "Система управления персоналом предприятия"

Для студентов специальности 032002

"Документационное обеспечение управления

и архивоведение с углубленной подготовкой

в области кадровой службы".

Лица, поступающие на работу на вредные и опасные производства; на работу, связанную с управлением источником повышенной опасности (водители, машинисты); на предприятия пищевой промышленности и общественного питания, бытового обслуживания и торговли, а также, независимо от профиля предстоящей работы, лица, не достигшие восемнадцати лет, обязаны при поступлении на работу за счет средств работодателя проходить предварительные медицинские осмотры.

Вопросы:

1. Возможно ли увольнение в данной ситуации?
2. Какие документы работодатель вправе требовать от работника?
3. Может ли быть голословное утверждение о подложности предоставленного документа быть основанием для расторжения трудового договора с работником?

Ситуационная задача№4

Тема: "Права работника"

Для студентов специальности 032002

"Документационное обеспечение управления

и архивоведение с углубленной подготовкой

в области кадровой службы".

Врач рассказал работодателю о болезни работника. Раскрыл врачебную тайну.

Вопросы:

1. Возможно ли увольнение в данной ситуации?
2. Нужно ли согласие гражданина на оглашение данной информации которому принадлежит данная информация?
3. Какое наказание понесет врач за разглашение врачебной тайны?

Ситуационная задача№5

Тема: "Документы, предоставляемые работником работодателю"

Для студентов специальности 032002

"Документационное обеспечение управления

и архивоведение с углубленной подготовкой

в области кадровой службы".

Сотрудник принес поддельный паспорт при устройстве на работу.

Вопросы:

1. Что может делать работодатель с данным документом?
2. Какие наказания понесет работник за подделку документов?

**Заключение**

Целью работы было показать уровень владения следующими компетенциями:

* обеспечить защиту персональных данных;
* осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
* использовать информационно-коммуникационные технологии в профессиональной деятельности;
* организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
* понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

Для достижения данной цели были выполнены следующие задачи:

* подобрать, проанализировать и обобщить источники информации в соответствие с темой работы;
* раскрыть понятие персональные данные;
* изучить технологию защиты персональных данных;
* изучить правела использования персональных данных;
* изучить правовые основы персональных данных;
* научиться составлять ситуационные задачи и вопросы к ним.

В ходе исследования все поставленные цели и задачи были достигнуты.

**Таким образом, персональные данные это очень важные документы потому, что они представляют собой** любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, другую информацию. **Персональные данные должны бать, очень хорошо защищены,** з**ащитой персональных данных** называется комплекс мер, предпринимаемых операторами по противодействию несанкционированному использованию персональных данных, включающих организационно административные и технические методы защиты.

Под безопасностью информационных ресурсов понимается гарантия защиты, информации во времени и пространстве.

**Не смотря на осознанное понимание поднятой проблемы как законодательными, так и государственными и коммерческими организациями, персональные данные все же подвержены утечкам информации, ущерб от которых подчас оценивается весьма впечатляющими цифрами.**

**Отсутствие систематизированного законодательства в сфере персональных данных и специального закона создает состояние правовой незащищенности от несанкционированного доступа к такой информации. На сегодняшний день в российском законодательстве отсутствует и классификация персональных данных, хотя попытка их различия имеет место быть – например, в Трудовом кодексе РФ, где речь идет о так называемых оценочных персональных данных. Между тем зарубежный опыт свидетельствует о целесообразности разделения соответствующей информации на две группы: данные общего характера и особая категория персональных данных, которая определяется как "данные чувствительного свойства" и которой относится информация о расовом происхождении, политических убеждениях, состоянии здоровья, личных пристрастиях и т.д. Персональные данные второй группы должны иметь особый режим защиты и большой уровень конфиденциальности. Сбор, обработка и использование этих данных должны осуществляться только в силу необходимости. Что касается субъектов правоотношений по поводу персональных данных, то, возможно, в число их можно включить и корпоративные объединения, не имеющие статус юридического лица, как это сделано в ряде западных стран.**

**Многократно возрастающий объем информации ограниченного доступа, в том числе и персональных данных, требуют особой ответственности при решении вопросов регулирование соответствующих правоотношений. Исходным принципом при этом должно стать обеспечение информационной безопасности гражданина, защита его личных прав в условиях информатизации общества. Использование персональных данных должно служить основной задачей – повышению эффективности функционирования основных институтов государственной власти, поскольку высшая цель государства, закрепленная в Конституции РФ, - признание, соблюдение и защита прав и свобод человека и гражданина.**

Список использованных источников

1. Федеральный закон "О персональных данных" 26 января 2007г., № 152-ФЗ.
2. ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. № 149-ФЗ.
3. **ФЗ "О коммерческой тайне" от 29июля 2004года №98-ФЗ.**
4. Документационное обеспечение деятельности кадровой службы: Учебное пособие для средне профессионального образования/ Лариса Михайловна Вялова. – М.: Издательский центр "Академия", 2003г.
5. Трудовой кодекс РФ.
6. Конституция РФ.
7. Постановление Правительства РФ "О перечне сведений, которые не могут составлять коммерческую тайну" от 05 декабря 1991 года.
8. Журнал "Управление персонала" 2004 год, № 19.
9. Журнал "современное право" 2004 год, № 2.
10. Журнал "Сетевые решения" 2008 год, №12.
11. http://www.upiter.su/node/36
12. ГОСТ Р6.30-2003. Унифицированные системы документации. Унифицированная система организационно – распорядительной документации. Требования к оформлению документов. – М.: Изд-во стандартов, 2003.