Федеральное агентство по образованию
Алтайский государственный университет
Исторический факультет
Кафедра архивоведения и исторической информатики

Правовая защита персональных данных в РФ
(Курсовая работа)

Выполнила студентка
1 курса 194 группы
Никифорова К.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Научный руководитель
к.и.н., ст. преп. Сарафанов Д.Е.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Работа защищена
«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2010 г.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Барнаул 2010

**Оглавление**

Введение…………………………………………………………………………………...2

Глава 1 Понятие «персональные данные» в отечественном законодательстве и научной литературе…………………………………………………………...…………..6

* 1. Определение понятия «персональные данные» в законодательстве………………6
	2. Определение понятия «персональные данные» в научной литературе………….13

Глава 2 Защита персональных данных и ответственность за нарушение работы с ними....................................................................................................................................17

* 1. Правовые меры по защите персональных данных...………………………………17
	2. Ответственность за нарушение работы с персональными данными……….…….24

Заключение ……………………………………………………………………………....28

Список источников и литературы ……………………………………………………....30

**Введение**

С течением времени у человечества появляется все больше новых объектов, нуждающихся в защите путем закрепления соответствующих норм в законе. Основной объект на сегодняшний день – 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. Ст.2 Конституции Российской Федерации закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью»[[1]](#footnote-1). Соответственно и информация, непосредственно затрагивающая частные интересы человека должны уважаться и защищаться государством.

Цель работы заключается в исследовании правовой защиты персональных данных в РФ. Для достижения цели, необходимо решить следующие задачи:

1. на основе анализа научных работ и законодательств изучить содержание понятия «персональные данные»;
2. изучить различные аспекты защиты персональных данных

**Историография.** “Персональные данные” рассматриваются как информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие[[2]](#footnote-2). В современном мире к защите этих сведений предъявляют все большие требования, к обеспечению гарантий по их сохранности и неразглашению относятся очень серьезно.

А.Г. Саидов посвятил свой труд вопросам информационной безопасности, правовому регулированию и компонентам системы информационной безопасности государства. Предметом его исследования выступает содержание и значение конституционно-правовых норм, обеспечивающих создание системы информационной безопасности личности, российского общества и государства. Абдулмуталиб Гасанович внес немалый вклад в исследование правовой защиты персональных данных и информационной безопасности в целом. По мнению А.Г.Саидова, главное, чего не хватает российскому законодательству (и что можно почерпнуть из зарубежного опыта), это позитивной (некарательной) направленности[[3]](#footnote-3). Защита персональных данных – это новая область деятельности, здесь важно научить, разъяснить, помочь, а не запретить и наказать.

Автор считает необходимым принятие Федерального закона «О неприкосновенности частной жизни», в котором бы устанавливался исчерпывающий перечень случаев ограничении прав в соответствии с конституционными основаниями и решениями Европейского суда по правам человека. По мнению Саидова, государство должно создавать условия для обеспечения защиты персональных данных каждого гражданина Российской Федерации.

В работе В.Я. Ярочкина «Информационная безопасность», персональные данные относятся к тому типу информации, которым необходима правовая защита. Он рассматривает необходимость правовой защиты персональных данных человека и гражданина, доказывает важность сохранности личной информации. Автор перечисляет виды правовых актов, ориентированных на правовую защиту информации, и другие средства, направленные на сокрытие персональных данных[[4]](#footnote-4). В его работе можно увидеть и угрозы конфиденциальной информации, а также виды таких угроз, приводящие к неправомерному овладению охраняемыми сведениями. В заключении, Владимир Иванович перечислил рекомендации по обеспечению защиты информации.

В целом, можно сказать, что труд В.И. Ярочкина направлен на характеристику и полное описание охраны безопасности персональных данных и других видов конфиденциальной информации.

В исследовании В.В. Полякова и В.А. Мазурова «Проблемы правовой и технической защиты информации» идет речь о создании и применении эффективных методов и средств для обеспечения информационной безопасности. Отдельной важной задачей, исследуемой в этом сборнике, является подготовка специалистов по защите информации[[5]](#footnote-5).Авторы отмечают, что квалифицированных специалистов по информационной безопасности не хватает. Это связано в значительной степени с большими требованиями, предъявляемыми к ним.

В «Большом справочнике кадровика», автором которого является Н.А.Алимова, рассматриваются проблемы защиты персональных данных работника (на мой взгляд, они относятся к разновидностям персональных данных в целом). Н.А. Алимова, разъясняет, что такое персональные данные работника, для чего они нужны, каким образом они охраняются, какие требования должен выполнять работодатель при обработке данных работника при приеме на работу[[6]](#footnote-6). В данной работе говориться о том, что порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований ТК РФ и иных федеральных законов. Н.А. Алимова исследовала в своей работе сами правила передачи персональных данных работника и необходимые для этого требования. Немаловажным аспектом исследования данной темы в работе является порядок привлечения к дисциплинарной ответственности за невыполнение обязанностей и требований по хранению и обеспечению безопасности персональных данных работника, а также формы такой ответственности.

В.А. Мазуров в своем труде «Уголовно-правовые аспекты информационной безопасности» рассматривает понятие и принципы информационной безопасности, основные направления развития законодательства об информации, а также правовое понятие и классификацию охраняемой законом информации. Он выделил различные меры по обеспечению защиты конфиденциальных данных, а также раскрыл определение и классификацию возможных угроз безопасности[[7]](#footnote-7). Особой частью его работы является исследование и описание уголовно-правовой защиты информации ограниченного доступа. В.А. Мазуров изучает и характеризует объект и предмет преступлений, посягающих на тайну частной жизни. Раскрывает объективную сторону составов преступлений, посягающих на неприкосновенность частной жизни, разъясняет в каком случае наступает правонарушение в сфере информационной защиты, и перечисляет формы ответственности за нарушение тайны о персональных данных, в соответствии со статьями УК РФ.

В целом, можно сказать, что тема, касающаяся персональных данных и их защиты, изучена довольно хорошо и тщательно. В большом количестве работ содержится информация о классификации, охраняемой законом информации, о видах правовых актов, направленных на сохранение безопасности персональных данных, о методах и способах защиты, о типах угроз, о видах ответственности за нарушение работы с персональными данными. Обилие такой информации способствует увеличению степени и качества защиты персональных данных.

**Глава 1**

**Понятие «персональные данные» в отечественном законодательстве и научной литературе.**

 **1.1.** **Определение понятия «персональные данные» в законодательстве.**

В современном мире к защите персональных данных относятся очень серьезно. Нормативные акты, регулирующие обеспечение их сохранности предусмотрены не только национальным законодательством, но и международными актами.

 Всеобщая декларация прав человека является одним из важнейших документов в истории человечества. 10 декабря 1948 года Генеральная Ассамблея Организации Объединенных Наций приняла Декларацию.

Статья 12 Всеобщей декларации прав человека 1948 года гласит «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию.Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств»[[8]](#footnote-8).

Право на уважение к личной и семейной жизни содержится так же и в Конвенции о защите прав человека и основных свобод, в которой так же говориться о том, что «Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц» [[9]](#footnote-9). Конвенция была принята Советом Европы 4 ноября 1950 года в Риме. Российская Федерация ратифицировала ее, приняв Федеральный закон № 54-ФЗ от 30 марта 1998 г.

Спустя некоторое время закрепление политических прав человека, право неприкосновенности личной жизни было подтверждено Международным пактом о гражданских и политических правах[[10]](#footnote-10).

Международный пакт о гражданских и политических правах Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года в Нью-Йорке. [СССР](http://ru.wikipedia.org/wiki/%D0%A1%D0%A1%D0%A1%D0%A0) подписал пакт [18 марта](http://ru.wikipedia.org/wiki/18_%D0%BC%D0%B0%D1%80%D1%82%D0%B0) [1968](http://ru.wikipedia.org/wiki/1968) года. Ратифицирован Президиумом Верховного Совета СССР [18 сентября](http://ru.wikipedia.org/wiki/18_%D1%81%D0%B5%D0%BD%D1%82%D1%8F%D0%B1%D1%80%D1%8F) [1973](http://ru.wikipedia.org/wiki/1973) года с заявлением. Ратификационная грамота СССР депонирована Генеральному секретарю ООН [16 октября](http://ru.wikipedia.org/wiki/16_%D0%BE%D0%BA%D1%82%D1%8F%D0%B1%D1%80%D1%8F) 1973 года. Вступил в силу для СССР 3 января 1976 года.

Эти международные правовые акты заложили основу создания национальных правовых систем. В Российской Федерации на ряду с международными правовыми актами сохранность персональных данных обеспечивается отечественными нормативными актами.

Во-первых это Конституция РФ[[11]](#footnote-11). В ее положениях признается не только само право на неприкосновенность личной жизни, личную и семейную тайну (ч.1 ст.23), но и обеспечивающие это право дополнительные гарантии. В соответствии со ст. 2 Конституции «человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства». Таким образом, Российская Федерация не только устанавливает право, но и обязуется защищать его; ставит интересы человека и гражданина на ступень выше, чем интересы государства, общества, либо общественных или коммерческих организаций. Ч.1 ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. И, наконец, согласно ст. 46 каждому гарантируется судебная защита его прав, в том числе в межгосударственных органах.

Конституция Российской Федерации обладает высшей юридической силой, ее прямое действие применяется на территории всей страны, любые законы, применяемые в стране не должны противоречить Конституции. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются основной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора[[12]](#footnote-12).

 8 июля 2006 года Государственной думой был принят Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных». Целью настоящего Федерального закона 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[[13]](#footnote-13). Данный закон дает определение понятию «персональные данные», а так же другим основным понятиям, используемым в Федеральном законе. Также, в законе рассматривается его сфера действия, принципы и условия обработки персональных данных, права субъекта персональных данных, обязанности оператора[[14]](#footnote-14), контроль и надзор за обработкой персональных данных, ответственность за нарушение требований за нарушение настоящего Федерального закона.

Следуя статье 3 Федерального закона, 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.

20.02.1995 г. был утвержден Федеральный закон N 24-ФЗ «Об информации, информатизации и защите информации», в котором в ч. 1 ст. 11 было определено, что персональные данные являются конфиденциальной информацией, а ч. 3 этой же статьи предупреждает о наступлении ответственности юридических и физических лиц за нарушение режима защиты, обработки и порядка использования этой информации. Также в этом законе было дано понятие «персональные данные», оно определялось как «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»[[15]](#footnote-15). В настоящее время данный закон не действует, его заменил Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. N149-ФЗ.

 В ст.2 нового закона об информации рассмотрены основные понятия, используемые в данном законе, а в ст. 3 говориться о правовом регулировании отношений, возникающих в сфере информации, информационных технологий и защите информации. В этой статье говориться о том, что ограничения доступа к информации может устанавливаться только федеральным законом. Конкретного понятия персональных данный в этом законе нет, очевидно, потому что был утвержден Федеральный закон «О персональных данных».

 В статье 5, ФЗ «Об информации, информационных технологиях и защите информации», сказано: «информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)».

Общедоступная информация – это та информация, которую нельзя скрывать от общества. Примером может служить информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Информацией ограниченного доступа является информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании. В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную тайну и информацию, соблюдение конфиденциальности которой установлено федеральным законом (конфиденциальная информация).

22 октября 2002 года был принят Федеральный Закон N 125-ФЗ «Об архивном деле в Российской Федерации». Этот закон регулирует отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда нашей страны и других архивных документов независимо от их форм собственности, а также отношения в сфере управления архивным делом в Российской Федерации в интересах граждан, общества и государства. Данный закон в 3 статье рассматривает такие понятия, как документы по личному составу (отражающие трудовые отношения работника с работодателем), особо ценный документ (документ, который имеет непреходящую культурно-историческую и научную ценность, особую важность для общества и государства и в отношении которого установлен особый режим учета, хранения и использования), уникальный документ (особо ценный документ, не имеющий себе подобных по содержащейся в нем информации и (или) его внешним признакам, невосполнимый при утрате с точки зрения его значения и (или) автографичности) и т.д. Также в этом законе выделяются архивные документы, относящиеся к государственной собственности, а так же муниципальной и частной[[16]](#footnote-16). В ст. 10 поясняются особенности положения архивных документов, находящихся в собственности Российской Федерации или муниципальных образований. Глава 6 посвящена сфере доступа к архивным документам и их использованию. Пользователь архивными документами имеет право свободно искать и получать для изучения архивные документы. Но существует и ограничение на доступ к архивным документам, которые рассматриваются в 25 статье. В данной статье сказано, что Доступ к архивным документам может быть ограничен в соответствии с международным договором Российской Федерации, законодательством Российской Федерации, а также в соответствии с распоряжением собственника или владельца архивных документов, находящихся в частной собственности, также в данной статье сказано, что ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов.

ФЗ РФ “Об оперативно - розыскной деятельности” от 12 августа 1995 № 144-ФЗ предусмотрены ограничения конституционных прав граждан на тайну телефонных переговоров, переписки, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи на основании судебного решения и только при наличии информации о подготовке, совершении или совершенном противоправном деянии либо о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

Данный нормативный устанавливает исчерпывающий перечень оперативно - розыскных мероприятий и органов, осуществляющих оперативно - розыскную деятельность. Он разрешает иметь оперативно - технические силы и средства для контроля почтовых отправлений, телеграфных и иных сообщений; прослушивания телефонных переговоров с подключением к стационарной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги связи; снятия информации с технических каналов связи только лишь органам ФСБ и МВД, которые могут предоставлять эти силы и средства на основе специальных соглашений или межведомственных нормативных актов другим органам, осуществляющим оперативно - розыскную деятельность[[17]](#footnote-17). Но органы (должностные лица), осуществляющие оперативно-розыскную деятельность, при проведении оперативно-розыскных мероприятий должны обеспечивать соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции[[18]](#footnote-18).

Сфера отношений, касающаяся персональных данных работника регулируется гл.14 Трудового кодекса Российской Федерации. Где установлено понятие персональных данных работника, установлен порядок работы с ними и закрепляется ответственность работодателя за нарушение соответствующих норм. В Трудовом кодексе говориться, что персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника[[19]](#footnote-19).

В Уголовно-процессуальном кодексе Российской Федерации от 5.12.2001 г. также затрагивается сфера персональных данных. В ст. 13 говорится о тайне переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений. В данной статье сказано о том, что наложение ареста на почтовые и телеграфные отправления и их выемка в учреждениях связи, контроль и запись телефонных и иных переговоров могут производиться только на основании судебного решения[[20]](#footnote-20).

 Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6.03.97 г. N 188 [«Об утверждении перечня сведений конфиденциального характера»](http://dehack.ru/zak_akt/npa_prezidentarf/up188/). К видам конфиденциальной информации можно отнести следующее:

* Персональные данные - сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* Тайна следствия и судопроизводства - сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ и другими нормативными правовыми актами Российской Федерации;
* Служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
* Профессиональная тайна - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);
* Коммерческая тайна - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
* Сведения о сущности изобретения - сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Перечень сведений, отнесенных к государственной тайне опубликован в ст. 5 Закона РФ N 5485 от 21.07.1993 «О государственной тайне». Согласно данному закону к таким сведениям относятся: сведения в военной области; в области экономики, науки и техники; в области внешней политики и экономики; в области разведывательной, контрразведывательной и оперативно-розыскной деятельности. Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с настоящим Законом. В ст. 2 раскрывается понятие государственной тайны – «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». В данном законе также говориться о рассекречивании, защите, распоряжении сведениями, относящихся к государственной тайне.

Федеральный закон Российской Федерации «О коммерческой тайне» рассматривает и регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну. Согласно данному закону «коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных доходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду»[[21]](#footnote-21). А также рассматриваются понятия режима коммерческой тайны; обладателя такой информации; передачи и предоставления информации, составляющей коммерческую тайну и т.д. В ст. 5 перечислены данные, которые не могут составлять коммерческую тайну. В Федеральном законе «О коммерческой тайне» сказано также и об охране конфиденциальности информации и последствиях невыполнения необходимых мер по охране такой информации.

В Федеральном законе «О кредитных историях» говорится о создании единой системы формирования, хранения и раскрытия информации о добросовестности исполнения заемщиками обязательств перед кредиторами. Нормами закона вводится легальное определение кредитной истории, регламентируется ее состав, порядок формирования, основания хранения и использования кредитных историй, а также круг субъектов данных правоотношений, в состав которых входят: заемщики, бюро кредитных историй, пользователей кредитных историй, Центральный каталог кредитных историй[[22]](#footnote-22).

2.02.2010 года вышел приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) N 58 о**б утверждении положения о методах и способах защиты информации в информационных системах персональных данных.** Это положение было разработано в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001). Данное положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных. В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

 **1.2. Определение понятия «персональные данные» в научной литературе**

В юридической литературе представлена неоднозначная классификация охраняемой законом информации (сведений).

Так, В.А. Копылов по доступу к информации подразделяет ее на открытую и ограниченного доступа.

К открытой информации он относит информацию как объект гражданских прав (произведения, патенты, авторские свидетельства); массовую информацию; информацию о выборах, референдуме (данные о ходже подготовки выборов, референдуме и результатах голосования); официальные документы (документы принятые органами законодательной, исполнительной и судебной власти, носящие обязательный, рекомендательный или информационный характер); обязательно представляемую (контрольные экземпляры документов, представляемые в органы статистики, регистрационная и другая такого рода информация); научно-юридическую и другую информацию.

К информации ограниченного доступа относится информация, составляющая государственную тайну; ноу-хау, коммерческая тайна, персональные данные (в порядке защиты личной тайны), другая информация ограниченного доступа[[23]](#footnote-23).

Информация о гражданах (персональные данные), по мнению В.А.Копылова, создается самими гражданами в их повседневной деятельности, в том числе связанной с реализацией прав и свобод (прав на труд, на жилище, на отдых, медицинское обслуживание, социальное страхование, пенсионное обеспечение, на свободу слова и многое другое) и выполнением обязанностей (например, воинской обязанности) и представляется как сведения о себе (персональные данные) разным субъектам[[24]](#footnote-24).

И.В. Смолькова дает следующую классификацию:

1. Государственная (в том числе военная) тайна.
2. Конфиденциальная информация.
* Личная тайна (в том числе персональные данные)
* Семейная тайна
* Профессиональная тайна
* Коммерческая тайна
* Служебная тайна[[25]](#footnote-25)

На взгляд В.А. Мазурова информацию можно классифицировать следующим образом: информация открытого доступа, ограниченного доступа (конфиденциальная информация (тайна частной жизни, профессиональная тайна, служебная тайна, коммерческая тайна) и государственная тайна)[[26]](#footnote-26).

Наличие нескольких точек зрения поп поводу классификации информации подтверждает то, что в научно-исследовательской литературе нет единого мнения по вопросам о персональных данных. Они изучаются все глубже и тщательней, что обеспечивает более полные знания об информации ограниченного доступа, а принятие множества законодательных актов, направленных на защиту различных видов тайн, обеспечивают более качественную защиту персональных данных. Но все же создание правовой базы защиты различных видов информации, и персональных данных в частности, находится на стадии становления. Несмотря на то, что число нормативных актов, регулирующих те или иные аспекты различных видов информации, насчитывает большое количество. Нельзя сказать, что правовое обеспечение защиты персональных данных удовлетворяет потребностям современного общества.

**Глава 2**

**Защита персональных данных.**

 **2.1. Защита персональных данных.**

Вопрос о необходимости охраны и защиты персональных данных не вызывает сомнений. На данный момент Российское законодательство всеми силами пытается предотвратить нарушение прав граждан государства в сфере персональных данных. Существует масса законов обеспечивающих информационную безопасность, которые обновляются с каждым годом, создавая все большие условия по сохранности конфиденциальности персональных данных. За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности. Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности.

Повышению информационной безопасности способствует международное сотрудничество Российской Федерации со странами мирового сообщества в области обеспечения информационной безопасности. Это неотъемлемая составляющая политического, военного, экономического, культурного и многих других видов взаимодействия стран, входящих в мировое сообщество.

Государственная система защиты информации представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Так же является составной частью системы обеспечения национальной безопасности Российской Федерации и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере.

Государственная система защиты информации как система более сложная, включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

Органы, которые регулируют защиту персональных данных:

* Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
* Федеральные органы исполнительной власти, другие органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, Минпромэнерго, Минэкономразвития, Минприроды, ФСО, ФСБ, СВР, ГУСП, РАН, ЦБР)
* Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации
* Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
* Научно-исследовательские организации по проблемам защиты информации
* Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации
* Предприятия, оказывающие услуги в области защиты информации
* Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации
* Органы системы лицензирования деятельности в области защиты информации
* Органы системы сертификации средств защиты информации
* Органы системы аттестации объектов защиты по требованиям безопасности информации[[27]](#footnote-27)

Правовые меры – деятельность законодательных органов по созданию правовой базы, обеспечивающей надлежащее формирование, распространение и использование информации; регулирующей деятельность субъектов, осуществляющих создание, преобразование и потребление информации; предусматривающей ответственность за нарушение в информационной сфере, меры обеспечения безопасности и правовой защиты информации, информационной инфраструктуры[[28]](#footnote-28).

Правовая основа механизма защиты персональных данных сформировалась по двум направлениям: специализированное законодательство и иное законодательство, которое лишь частично содержит правовые нормы, гарантирующие неприкосновенность частной жизни и регулирующие сферу защиты персональных данных. К специализированному законодательствуотносятся такие правовые акты как: Федеральный закон «О персональных данных» от 27 июля 2006 г., Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г., Указ Президента РФ от 6 марта 1997 г. №188, утверждающий «Перечень сведений конфиденциального характера», и другие.

Правовые нормы, регулирующие работу с персональными данными, содержатся также в главе 14 Трудового кодекса РФ «О защите персональных данных работника», в Законе «Об архивном деле в Российской Федерации» от 22 октября 2004 г. (ст.25), в Законе «Об оперативно-розыскной деятельности» (ст. 3, 5, 9, 10, 12, 21), в Законе «О средствах массовой информации» (ст. 41, 43, 46, 51, 57), Закон «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования», в соответствии с которым персональные данные содержатся в индивидуальном лицевом счете застрахованного лица, нормы о защите сведений, полученных в ходе всероссийской переписи населения (персональные данные) содержатся в Законе «О всероссийской переписи населения».

В Европейском Союзе вопросам защиты интересов владельцев персональных данных, которые были подвергнуты электронной обработке, посвящена Конвенция СЕ «О защите физических лиц при автоматизированной обработке персональных данных», подписанная в Страсбурге (Франция) в 1981 году. Федеральный закон о ратификации Конвенции был подписан Президентом РФ 19 декабря 2005 года.

В соответствии со ст. 5 Конвенции, персональные данные, подвергающиеся автоматизированной обработке:

a) собираются и обрабатываются на справедливой и законной основе;

б) хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями;

в) являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;

г) являются точными и, когда это необходимо, обновляются;

д) сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных[[29]](#footnote-29).

 Основным Законом, регулирующим защиту персональных данных в Российской Федерации, является Федеральный Закон «О персональных данных». Основу этого Закона составляют базовые принципы и условия обработки персональных данных, которые были разработаны во исполнение норм Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», а также положений Директивы Европейского Парламента и Совета Европы 95/46/ЕС «О защите личности в отношениях обработки персональных данных и свободном обращении этих данных» и Директивы Европейского Парламента и Совета Европы 2002/58/ЕС от 12 июля 2002 г., касающейся защиты персональных данных и защиты личных данных в электронном коммуникационном секторе, которая заменила Директиву Европейского Парламента и Совета Европы 97/66/ЕС от 15 декабря 1997 г., регламентирующую использование персональных данных и гарантирующую неприкосновенность частной жизни в сфере телекоммуникаций.

Принципы и условия, обработки персональных данных, которые дополняются также обязательными базовым требованиям, предъявляемыми к деятельности по обработке персональных данных, соответствуют принципам и критериям, касающимся персональных данных и легитимизации их обработки, установленные в статьях 6 и 7 Директивы95/46/ЕС. Статья 5 Закона «О персональных данных» устанавливает шесть принципов обработки персональных данных, защищающих персональную информацию человека; данные принципы схожи с принципами, содержащимися во многих европейских правовых актах. Во-первых, персональные данные должны собираться и использоваться законно и добросовестно. Эта норма говорит о том, что персональные данные должны быть собраны и использованы в соответствии с законодательством РФ и только с согласия субъекта персональных данных, но за исключением случаев, четко оговоренных в части 2 статьи 6 Закона, когда такое согласие не требуется. Согласие на обработку своих персональных данных субъект персональных данных должен дать в письменной форме; содержание этого документа четко установлено в п. 4 статьи 9 Закона. К примеру, в письменном согласии субъекта должна быть обязательно указана цель обработки персональных данных и их перечень, а также срок, в течение которого действует согласие и порядок его отзыва.

Во-вторых, заранее четко определенные цели использования персональных данных не должны изменяться. Персональные данные не могут собираться и использоваться для иных целей, о которых субъект, давший письменное согласие на обработку своих данных, не был заранее информирован (п.2 ч. 1 ст. 5).

В-третьих, объем, характер и способы обрабатываемых персональных данных должны соответствовать целям обработки персональных данных. Эта норма направлена на исключение ситуаций, когда при сборе персональных данных пытаются получить иную персональную информацию, выходящую за рамки объявленных целей.

В-четвертых, персональные данные должны быть достоверными, а объем собираемой персональной информации должен быть оправдан целями ее сбора. Объем собираемых персональных данных не должен быть избыточным, если это не соответствует определенным и законным целям. При этом, если обнаружено, что были допущены ошибки и персональные данные неточны, субъекту персональных данных принадлежит право внести необходимые изменения (п.3 статья 20).

В-пятых, Закон запрещает объединение персональных данных в единую информационную систему персональных данных, которые были собраны операторами персональных данных для разных целей. Эта норма направлена на то, чтобы избежать ситуации, когда оператор связи содержит базу персональных данных человека, и в случае утечки такой базы, человек будет уязвим перед несанкционированным и недобросовестным использованием этих сведений.

И, наконец, в-шестых, хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Эта норма соответствует п. «е» статьи 5 Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» и также направлена на защиту субъекта персональных данных от несанкционированного использования его персональных данных. Стоит иметь в виду, что данное правило не относится к персональным данным человека, содержащимся в архивных документах, срок хранения которых установлен Законом «Об архивном деле в Российской Федерации» 2004 г.

Доктрина информационной безопасности РФ, утвержденная Президентом РФ 9 сентября 2000г. представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина информационной безопасности определяет 4 основные составляющие национальных интересов РФ в информационной сфере, в том числе соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, а также защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Настоящая доктрина служит основой для:

* Формирования государственной политики в области обеспечения информационной безопасности РФ;
* Подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ;
* Разработки целевых программ обеспечения информационной безопасности Российской Федерации[[30]](#footnote-30).

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

В пункте 2 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных говорится о том, что безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий. В пункте 10 сказано, что безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее - уполномоченное лицо). При обработке персональных данных в информационной системе должно быть обеспечено:

* проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
* своевременное обнаружение фактов несанкционированного доступа к персональным данным;
* недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
* постоянный контроль за обеспечением уровня защищенности персональных данных.
* возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных из-за несанкционированного доступа к ним[[31]](#footnote-31);

 **2.2. Ответственность за нарушение работы с персональными данными**

Закон устанавливает, что лица, виновные в нарушении требований настоящего Закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность[[32]](#footnote-32). В случае нарушения прав субъекта персональных данных, он может обжаловать действия или бездействия в Уполномоченныйорган по защите персональных данных или в судебном порядке. Уполномоченный орган по защите прав субъекта персональных данных является новым для России институтом, деятельность которого направлена на осуществление контроля и надзора за обработкой персональных данных. Уполномоченный орган имеет право обращаться в суд с исковыми заявлениями для защиты персональных данных и представлять интересы субъектов персональных данных в суде.

Дисциплинарная ответственность должна быть установлена внутренними правилами распорядка организации (в данном случае оператора). В виде дисциплинарной ответственности работнику, совершившему какой-либо дисциплинарный проступок в связи с обработкой персональных данных, не повлекший за собой административную, гражданскую или уголовную ответственность, может быть вынесено замечание, выговор, или он может быть уволен по соответствующим основаниям, предусмотренным ст.81 Трудового кодекса РФ. В Трудовом кодексе РФ четко не установлен вид дисциплинарной ответственности за нарушение порядка обработки персональных данных, а лишь указано, за нарушение норм защиты персональных данных работника также устанавливается гражданская, уголовная, административная, дисциплинарная ответственность.

Что касается гражданской ответственности, то субъект персональных данных в порядке гражданского судопроизводства может требовать возмещение убытков и (или) компенсацию морального вреда.

В соответствии со статьей 13.11 Кодекса РФ об административных правонарушениях (КоАП) административная ответственность предусмотрена за нарушение установленного Законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) в виде предупреждения или наложения на граждан административного штрафа в размере от трех до пяти минимальных размеров оплаты труда (МРОТ), от пяти до десяти МРОТ  для должностных лиц и от пятидесяти до ста МРОТ для юридических лиц. Разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет за собой наложение административного штрафа на граждан в размере от пяти до десяти МРОТ, а на должностных лиц — в размере от сорока до пятидесяти МРОТ[[33]](#footnote-33).

Посколькузащита персональных данных человека являются составной частью института гарантий неприкосновенности частной жизни человека, нормы особенной части Уголовного кодекса РФ относительно уголовной ответственности за нарушение неприкосновенности частной жизни человека распространяются, в том числе, и на порядок защиты персональных данных. Так, уголовная ответственность статьей 137 Уголовного кодекса РФ устанавливается за незаконное собирание или распространение сведений о частной жизни лица, составляющих личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Указанные деяния наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до одного года, либо арестом на срок до четырех месяцев. Те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

**Заключение**

Таким образом, проанализировав ситуацию по поводу охраны персональных данных, можно сделать следующие выводы.

Существует несколько точек зрения по поводу классификации информации, но в целом, ее можно разделить на информацию открытого и ограниченного доступа. Ограничение доступа к информации может устанавливаться только федеральными законами. Перечень информации ограниченного доступа, установлен в Указе Президента «Об утверждении перечня сведений конфиденциального характера». К таким сведениям относятся и персональные данные.

Следуя статье 3 Федерального закона «О персональных данных», можно сформировать следующее определение понятия «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 и другая информация.

Также, благодаря нормативно-правовым актам и научно-исследовательским работам становиться ясно, что персональные данные являются конфиденциальной информацией и что за нарушение работы с ними наступает юридическая ответственность.

Что касается защиты персональных данных, то нужно заметить, что безопасность персональных сведений находится на высоком уровне. Этому способствуют как правовая база, так и многочисленные средства технического контроля. Законодательствами стран Европы и Российской Федерации предусмотрены практически все необходимые нормы для защиты этой категории правоотношений. Основным Законом, регулирующим работу с персональными данными, является Федеральный закон «О персональных данных». В нем описаны основные принципы и условия обработки и защиты таких сведений

Закон устанавливает, что лица, виновные в нарушении требований настоящего закона, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерацией, ответственность.

Обилие нормативно-правовых актов, регулирующих отношения в сфере персональных данных, обеспечивает надежную защиту безопасности информации ограниченного доступа, но следует заметить, что необходимо дальнейшее совершенствование механизмов защиты персональных данных, находящихся в распоряжении федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и др.

**Список источников и литературы**

**Источники**

1. Конституция Российской Федерации принята на всенародном голосовании 12 декабря 1993 г.– М., 2002.
2. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) //СПС Консультант плюс, 2009 г.
3. Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изменениями от 21 сентября 1970 г., 20 декабря 1971 г., 1 января, 6 ноября 1990 г., 11 мая 1994 г.) //СПС Консультант плюс, 2009 г.
4. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) //СПС Консультант плюс, 2009 г.
5. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года (ратифицирована РФ 19 декабря 2005 года) // СПС Консультант плюс, 2009 г.
6. Федеральный закон РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных»//СПС Консультант плюс, 2009 г.
7. Федеральный закон РФ от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и защите информации" //СПС Консультант плюс, 2009 г.
8. Федеральный Закон РФ от 12 августа 1995 № 144-ФЗ “Об оперативно - розыскной деятельности” // СПС Консультант плюс, 2009 г.
9. Доктрина информационной безопасности от 9 сентября 2009 г.//СПС Консультант плюс, 2009г.
10. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 г. N 188) //СПС Консультант плюс, 2009 г.
11. Гражданский кодекс Российской Федерации от 30 ноября 1994 г. N 51-ФЗ (с изменениями и дополнениями, вступившими в силу 11 января 2009г.) //СПС Консультант плюс, 2009 г.
12. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изменениями от 30 декабря 2008г.) //СПС Консультант плюс, 2009 г.
13. Кодекс Российской Федерации об административных правонарушениях от 20 декабря 2001 г. N 195-ФЗ (с изменениями от 30 декабря 2008 г.) //СПС Консультант плюс, 2009 г.
14. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с изменениями от 24, 25 июля 2002 г., 30 июня 2003 г.) //СПС Консультант плюс, 2009 г.
15. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных от 17 ноября 2007г. N-781(утв. Постановлением Правительства РФ)//СПС Консультант плюс, 2009г.

**Список литературы**

|  |
| --- |
|  |

1. Алимова Н.А. Большой справочник кадровика. – М.: Издательско-торговая корпорация «Дашков и Кْ», 2007. – 536 с.
2. Копылов В.А. Информационное право. М.: Юристъ, 2005. – 512 с.
3. Магнитская Е.В. Правоведение: учебник, Е.В. Магнитская, Е.П. Евстигнеев: Питер, 2003. - 512с.
4. Мазуров В.А. Уголовно-правовые аспекты информационной безопасности: учебное пособие – Барнаул: Изд-во Алт. Ун-та, 2004. – 288с.
5. Поляков В.В., Мазуров В.А. Проблемы правовой и технической защиты: сб. науч. ст./ АлтГУ, 2008. – 179 с.
6. Саидов А.Г. Конституционно-правовые основы обеспечения информационной безопасности Российской Федерации: автореферат: Махачкала, 2004. – 26 с.
7. Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе. – М.: 1999. – 346 с.
8. Теория оперативно-розыскной деятельности: учебник. Ред. – сост. К.К. Горяинов, В.С. Овчинский, Г.К. Синилов – М.: Лист Нью, 2008. - 842 с.
9. Ярочкин В.И. Информационная безопасность: учебник для ВУЗов. - М.: Гаудеамус, 2004. - 544с.
1. Конституция Российской Федерации, принятая на всенародном референдуме 12 декабря 1993 года//СПС Консультант плюс, 2009 г. [↑](#footnote-ref-1)
2. Магнитская Е.В. Правоведение: учебник, Е.В. Магнитская, Е.П. Евстигнеев: Питер, 2003. – С. 346. [↑](#footnote-ref-2)
3. Саидов А.Г. Конституционно-правовые основы обеспечения информационной безопасности РФ: Махачкала, 2004. – С. 24. [↑](#footnote-ref-3)
4. Ярочкин В.И. Информационная безопасность. – М.: Гаудеамус, 2004. – С.31-49, 99-117. [↑](#footnote-ref-4)
5. Поляков В.В., Мазуров В.А. Проблемы правовой и технической защиты: сб. науч. ст./ АлтГУ, 2008. – С. 73-76. [↑](#footnote-ref-5)
6. Алимова Н.А. Большой справочник кадровика. – М.: Издательско-торговая корпорация «Дашков и Кْ», 2007. – С. 126-129, 192-196. [↑](#footnote-ref-6)
7. Мазуров В.А. Уголовно-правовые аспекты информационной безопасности: Издательство Алтайского университета, 2004. – С. 12-16. [↑](#footnote-ref-7)
8. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.)//СПС Консультант плюс, 2009г. [↑](#footnote-ref-8)
9. Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изменениями от 21 сентября 1970 г., 20 декабря 1971 г., 1 января, 6 ноября 1990 г., 11 мая 1994 г.) //СПС Консультант плюс, 2009г. ст. 8. [↑](#footnote-ref-9)
10. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.)//СПС Консультант плюс, 2009г. ст. 17. [↑](#footnote-ref-10)
11. Конституция Российской Федерации от 12 декабря 1993 года//СПС Консультант плюс, 2009 г. [↑](#footnote-ref-11)
12. Конституция Российской Федерации от 12 декабря 1993 г.//СПС Консультант плюс, 2009 г. ст.15 [↑](#footnote-ref-12)
13. Федеральный закон № 152-ФЗ о «персональных данных» //СПС Консультант плюс, 2009г. гл.1 ст.2 [↑](#footnote-ref-13)
14. Федеральный закон № 152-ФЗ о «персональных данных» гл.1 ст.3: 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; [↑](#footnote-ref-14)
15. Федеральный закон N 24-ФЗ «Об информации, информатизации и защите информации» от 20.02.1995 г.//СПС Консультант плюс, 2009г. ст. [↑](#footnote-ref-15)
16. Федеральный закон N 125-ФЗ «Об Архивном деле в Российской Федерации» от 22.10.2004 г.//СПС Консультант плюс, 2009г. ст. 7,8,9. [↑](#footnote-ref-16)
17. Федеральный Закон РФ от 12 августа 1995 № 144-ФЗ “Об оперативно - розыскной деятельности” //СПС Консультант полюс, 2009 г., ст. 6 [↑](#footnote-ref-17)
18. Федеральный Закон РФ от 12 августа 1995 № 144-ФЗ “Об оперативно - розыскной деятельности” //СПС Консультант полюс, 2009 г., ст. 5. [↑](#footnote-ref-18)
19. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ.//СПС Консультант плюс, 2009г. гл.14 ст.85. [↑](#footnote-ref-19)
20. Уголовно-процессуальный кодекс Российской Федерации от 5.12.2001 г.//СПС Консультант плюс, 2009г. ст.13. [↑](#footnote-ref-20)
21. Федеральный закон Российской Федерации N 98-ФЗ «О коммерческой тайне» от 29.07.2007 г. //СПС Консультант плюс, 2009 г., ст. 3. [↑](#footnote-ref-21)
22. Федеральный закон Российской Федерации N 218-ФЗ «О кредитных историях» от 30.12.2004 г// СПС Консультант плюс, 2009 г., ст.2. [↑](#footnote-ref-22)
23. Копылов В.А. Информационное право. М.:Юристъ, 2005. – С.213 [↑](#footnote-ref-23)
24. Копылов В.А. Информационное право. М.:Юристъ, 2005. – С. 226. [↑](#footnote-ref-24)
25. Смолькова И.В. Проблемы охраняемой законом тацны в уголовном процессе. – М.: 1999. – С. 22. [↑](#footnote-ref-25)
26. Мазуров В.А. Уголовно-правовые аспекты информационной безопасности: учебное пособие – Барнаул: Изд-во Алт. Ун-та, 2004. – С. 26. [↑](#footnote-ref-26)
27. Ярочкин В.И. Информационная безопасность: учебник для ВУЗов. - М.: Гаудеамус, 2004. – С. 378. [↑](#footnote-ref-27)
28. Мазуров В.А Уголовно-правовые аспекты информационной безопасности: Издательство Алтайского университета, 2004 г. – С. 12. [↑](#footnote-ref-28)
29. ###  Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года (ратифицирована РФ 19 декабря 2005 года) //СПС Консультант плюс, 2009 г., ст. 5.

 [↑](#footnote-ref-29)
30. Мазуров В.А. Уголовно-правовые аспекты информационной безопасности: учебное пособие – Барнаул: Изд-во Алт. Ун-та, 2004. – С. 244. [↑](#footnote-ref-30)
31. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных от 17 ноября 2007г. N-781//СПС Консультант плюс, 2009г., п. 11. [↑](#footnote-ref-31)
32. Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных»// СПС Консультант плюс, 2009 г., ст. 24. [↑](#footnote-ref-32)
33. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с изменениями от 24, 25 июля 2002 г., 30 июня 2003 г.) //СПС Консультант плюс, 2009 г., ст. 13.14. [↑](#footnote-ref-33)