Министерство НАУКИ и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Псковский государственный университет»

**Физико-математический факультет**

**Кафедра Прикладной информатики в образовании**

РЕФЕРАТ

на тему:

Персональные данные

Работу выполнил

студент 1 курса

очного отделения

Бухарев Роман Сергеевич

Работу проверил

Гаврилов Алексей Алексеевич

Псков-2019

**Содержание**

Введение…………………………………………………………………………...3

1 Важность защиты персональных данных……………………………………..4

2 Персональные данные…………………………………………………………..5

3 Категории персональных данных……………………………………………...7

4 Принципы и условия обработки персональных данных……………………..9

5 Защита персональных данных и ответственность……..……………………11

Список литературы 13

**Введение**

Защита персональных данных была и остается одной из наиболее

острых проблем в информационных отношениях между гражданами,

государством и негосударственными организациями. В Конституции (гл.

2. “Права и свободы гражданина и человека”) и законах Российской

Федерации можно найти положения, которые признают важность одного

из фундаментальных прав человека – права на неприкосновенность

частной жизни. Однако целостной системы и эффективного механизма

защиты этого права в России до недавнего времени практически не

было. Между тем, практика вторжения в частную жизнь в настоящее

время приобрела угрожающие масштабы. Повсеместно собираются

избыточные персональные данные, отсутствуют гарантии уничтожения

этих данных; когда цель сбора достигнута, собранные данные

бесконтрольно передаются третьим лицам, мнение владельцев

персональных данных игнорируется.[[1]](#footnote-1)

Несмотря на важность рассматриваемой проблемы, в нашей

стране до недавнего времени не уделялось достаточного внимания

выполнению работ, связанных с обеспечением информационной

безопасности персональных данных граждан. Кроме того, фактически все

граждане, так или иначе, в качестве клиентов и партнеров

взаимодействуют с различными организациями, передавая им свои

персональные данные без надлежащей защиты. Это было связано,

прежде всего, с отсутствием необходимой нормативной базы,

неподготовленностью специалистов и недостаточным практическим

опытом в области защиты персональных данных. Для предотвращения

бесконтрольного оборота персональных сведений граждан и защиты

частной жизни граждан в Российской Федерации 27 июля 2006 года

принят Федеральный закон №152 «О персональных данных», который

выдвигает в области защиты информации самые общие требования, не

опускаясь до конкретных мероприятий, являясь, таким образом, лишь

набором общих рекомендаций. Так, данный закон гласит, что “оператор

персональных данных обязан принимать необходимые организационные

и технические меры … для защиты персональных данных от

неправомерного или случайного доступа к ним”. В 2007 году премьер-министр

России подписал “Положение об обеспечении безопасности

персональных данных при их обработке в информационных системах

персональных данных”, которым обязал уполномоченные органы ФСБ и

ФСТЭК разработать более детальные нормативы к Федеральному закону

№152 «О персональных данных» к 18 февраля 2008 г.

**Важность защиты персональных**

Сегодня вряд ли можно представить деятельность организации без обработки информации о человеке. В любом случае организация хранит и обрабатывает данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных приводит к невосполнимому ущербу, а порой и к полной остановке деятельности организации. Представьте себе работу кредитно-финансовой или телекоммуникационной компании, которая потеряла хотя бы часть информации о своих клиентах. Долго ли просуществует такая компания на рынке?..

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту персональных данных. Законодательство Российской Федерации в этой области основывается на Конституции РФ и международных договорах Российской Федерации и состоит из Федерального закона РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных», других федеральных законов, определяющих случаи и особенности обработки персональных данных, отраслевых нормативных актов, инструкций и требований регуляторов.

В 1981 году Совет Европы принял Конвенцию «О защите личности в связи с автоматической обработкой персональных данных». 25 ноября 2005 г. Государственная Дума ратифицировала данную Конвенцию (ФЗ от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»), возложив на Российскую Федерацию обязательства по приведению в соответствие с нормами европейского законодательства деятельность в области защиты прав субъектов ПДн. Первым шагом в реализации взятых обязательств стало принятие Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных». Закон вступил в силу в январе 2007 года.

Закон № 152-ФЗ определил высокоуровневые требования, которые затем были конкретизированы в подзаконных актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России) и Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор).[[2]](#footnote-2)

**Персональные данные**

В соответствии с Законом №152-ФЗ персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект персональных данных). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту персональные данные.

Состав и содержание персональных данных определяют операторы ПДн1 в зависимости от целей их обработки. Например, перечень персональных данных для популярных в последнее время систем лояльности клиентов компании, как правило, включают контактные данные, необходимые для связи с клиентами, и сведения о предоставленных услугах. Состав этих сведений не должен быть избыточен при этом оставаясь достаточным, чтобы «понимать» предпочтения клиента, его финансовые возможности, «отслеживать» его покупательскую историю и т.п.

Отличие российского и международного законодательства США, Великобритания и Канада, так же как и Россия, разработали технические регламенты, которые транслируют положения законодательства верхнего уровня в конкретные советы и рекомендации по защите персональных данных. Канадский, английский и американский стандарты, в отличие от документов российских регуляторов, дают более общие рекомендации по обеспечению безопасности персональных данных и не предписывают, как конкретно должны защищаться персональные данные. Более того, тот же американский стандарт рекомендует по возможности обезличивать персональные данные, чтобы уйти от различных защитных мер, снижающих удобство пользования информацией.

Существуют случаи, когда цели, состав и содержание персональных данных четко определяются законодательными и нормативно-правовыми актами. Это касается областей, где взаимоотношения между субъектами персональных данных и операторами нуждаются в строгой регламентации. При этом в некоторых случаях субъект персональных данных обязан предоставлять оператору сведения о себе.

Например, функционирование определенных отраслей экономики связано с необходимостью обеспечения безопасности. Так, ФЗ-16 «О транспортной безопасности» определяет необходимость создания единой государственной информационной системы обеспечения транспортной безопасности. Такая система должна состоять из централизованных баз персональных данных о пассажирах, включающих следующие данные:

* фамилия, имя, отчество;
* дата и место рождения;
* вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);
* пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный);
* дата поездки.

Регламентация состава и содержания персональных данных касается отношений, связанных с трудовой деятельностью человека. Если речь идет о кадровой системе, к составу персональных данных относятся сведения, предусмотренные унифицированной формой учета кадров Т-2, утвержденной Постановлением № 1 Госкомстата России от 05.01.2004. К таким сведениям относятся:

* фамилия, имя, отчество;
* дата рождения;
* гражданство;
* номер страхового свидетельства;
* ИНН;
* знание иностранных языков;
* данные об образовании (номер, серия дипломов, год окончания);
* данные о приобретенных специальностях
* семейное положение;
* данные о членах семьи (степень родства, ФИО, год рождения, паспортные данные, включая прописку и место рождения);
* фактическое место проживания;
* контактная информация;
* данные о военной обязанности;
* данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т.п.).

К другим нормативным актам, регулирующим отношения в сфере деятельности человека и определяющим цели обработки, состав и содержание ПДн, относятся ФЗ-179 «Трудовой кодекс РФ», ФЗ-27 «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», ФЗ-129 «О государственной регистрации юридических лиц и индивидуальных предпринимателей» и т.п.

Какие сведения о сотрудниках государственных организаций собирать и как их обрабатывать, определяет Указ Президента РФ от 30 мая 2005 г. N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела». Своя специфика существует и в различных отраслях экономики. [[3]](#footnote-3)

**Категории персональных данных**

Законодательство определяет различные категории персональных данных. К ним могут относиться общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных биометрические персональные данные и другие.

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные.

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

* субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
* персональные данные являются общедоступными;
* персональные данные относятся к состоянию здоровья субъекта персональных данных и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
* обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
* обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности.
* Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет следующие категории персональных данных, которые обрабатываются в информационных системах персональных данных :

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных.

Категория 4 – обезличенные и (или) общедоступные персональные данные.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, - биометрические персональные данные- могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ст. 11ч.2 ФЗ-№152 «О персональных данных». Биометрические персональные данные могут обрабатываться без согласия субъекта персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, оперативно-розыскной деятельности, государственной службе, уголовно-исполнительным законодательством Российской Федерации, порядке выезда из Российской Федерации и въезда в страну. Идентификаторы персональных данных вызывают беспокойство, непонимание, неприятие и протест части российского общества. Можно ожидать, что активные действия противников идентификаторов лишь верхушка айсберга, а реализация этих проектов грозит масштабным ростом напряжения в обществе. Следовательно, каковы бы ни были экономические и социальные обоснования актуальности введения в действие идентификаторов персональных данных, необходимо прийти к общественному согласию по этим вопросам. Приблизить этот момент можно, выполнив два условия. Во-первых, нужно максимально прозрачно и конкретно определить порядок, в соответствии с которым формируются идентификаторы персональных данных. Во-вторых, необходим реальный и действенный механизм защиты персональных данных.

Для решения данных задач Правительство Российской Федерации утвердило постановление № 512 от 6 июля 2008 года “ Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных”. В документе определены требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных.

Требования этого документа применяются при использовании материальных носителей, на которые записываются биометрические персональные данные, а также при хранении биометрических персональных данных вне информационных систем персональных данных.

**Принципы и условия обработки персональных данных**

Обработка персональных данных должна осуществляться на основе принципов:

* Законности целей и способов обработки персональных данных и добросовестности;
* Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а так же полномочиям оператора;
* Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
* Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
* Недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Принцип законности целей и способов обработки персональных данных и добросовестности означает, что обработка персональных данных должна осуществляться в соответствии с законом и не должна преследовать противоправные цели и осуществляться противозаконными способами.

Принцип соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора означает, что при сборе персональных данных для их последующей обработки заранее должны быть определены и заявлены цели такой обработки, а оператор персональных данных должен обладать соответствующими полномочиями.

Из закреплённого в законе принципа достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных следует, что обрабатываемые персональные данные должны собираться только в таком количестве, которое необходимо для поставленных целей их обработки.

Принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных запрещает осуществление слияния различных баз персональных данных, если они формировались для различных целей.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Согласие субъекта персональных данных, на обработку его 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 осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
3. Обработка персональных данных осуществляется для статических или иных научных целей при условии обязательного обезличивания персональных данных;
4. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
5. 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.
6. Обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
7. Осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, персональных данных кандидатов на выборные государственные или муниципальные должности.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.[[4]](#footnote-4)

**Защита персональных данных и ответственность**

Ответственность за разглашение персональных сведений наступает, в соответствии с частью 1, 2, ст. 13 Федерального закона № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" по отношению к сведениям, которые составляют, например, врачебную тайну, разглашение которых не допускается, в том числе после смерти гражданина. К ним относятся:

* сведения о факте обращения гражданина за оказанием медицинской помощи;
* сведения о состоянии здоровья и диагнозе гражданина;
* иные сведения, полученные при медицинском обследовании и лечении гражданина.

Также в примечании к статье ст. 137 УК РФ говорится, что она предусматривает уголовную ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, либо распространение этих сведений в публичном выступлении, публично демонстрируемом произведении или СМИ, а также за те же деяния, совершенные лицом с использованием своего служебного положения. Из приведенных статей ясно, что к ответственности может быть привлечено любое лицо, нарушающее ФЗ. Выходит, что пока мобильные приложения (соцсети и др.), а также интернет вещей (IoT) не выполняют никаких действий без их подтверждения, то есть требования закона соблюдаются, но стоит отметить, что необходима особенная внимательность пользователя при подтверждении тех или иных прав на доступ к конфиденциальной информации. Это касается и стандартов защиты корпоративных данных.

Хотя имеется возможность настройки пользовательского доступа в соцсетях, это не решает проблему защиты персональных данных. Существуют и другие пути утечки данных, а именно: общедоступные данные, добровольно размещаемые пользователями в социальных сетях, могут быть обработаны сторонними сервисами, но у физического лица всегда есть право на исключение этих данных путем направления соответствующего требования оператору персональных данных (например, оператор связи или хостеру), по которому последний обязан немедленно прекратить обработку персональных данных этого лица.

Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случаях, если это лицо виновно в разглашении информации, составляющей коммерческую тайну, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, если разглашение такой информации последовало в течение срока, установленного в соответствии с п. 3 ч. 3 ст. 11 ФЗ от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне". Кроме того, ответственность предусмотрена ст. 24 ФЗ от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и ст. 17 ФЗ от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

ГК предусматривает также защиту нематериальных благ граждан, включая неприкосновенность частной жизни, личную и семейную тайну, деловую репутацию и другие. Соответственно устанавливаются формы гражданско-правовой ответственности в виде денежной компенсации за причиненный моральный вред, обязанности опровержения сведений, порочащих честь, достоинство или деловую репутацию гражданина (работника) и т.п.

Административная ответственность за нарушение законодательства о труде предусмотрена также в КоАП РФ. Административное взыскание налагается в соответствии со ст. 13.11 КоАП, предусматривающей ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Нарушение данной нормы влечет за собой предупреждение или наложение штрафа в размере на: граждан - от 3 до 5 МРОТ; должностных лиц - от 5 до 10 МРОТ; юридических лиц - от 50 до 100 МРОТ.

Согласно ст. 5.39 КоАП неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, не предоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации - влечет наложение административного штрафа на должностных лиц в размере от 5 до 10 МРОТ. Кроме того, в ст. 13.14 КоАП установлена ответственность за разглашение информации, доступ к которой ограничен (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей. Особое значение приобретает криминализация правонарушений в области работы с персональными данными, в связи с чем Уголовный кодекс Российской Федерации предусматривается уголовная ответственность: за злоупотребления и незаконные действия с информационными данными о частной жизни; за неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, если эти деяния причинили вред правам и законным интересам граждан (в т.ч. работникам);.[[5]](#footnote-5)

**Список литературы:**

1. Аверченков, В. И. Защита персональных данных в организации [Электронный ресурс] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. — Электрон. текстовые данные. — Брянск : Брянский государственный технический университет, 2012. — 124 c.— Режим доступа: http://www.iprbookshop.ru/6993.html

2. Чепурнова, Н. М. Правовые основы информатики [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика» / Н. М. Чепурнова, Л. Л. Ефимова. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 295 c.— Режим доступа: <http://www.iprbookshop.ru/81535.html>

3. Защита персональных данных: [Электронный ресурс] //ИТ-портал компании «Инфосистемы Джет» ,1995-2019. URL: http://www.jetinfo.ru/stati/zaschita-personalnykh. (Дата обращения: 24.03.2019).

4. Персональные данные: [Электронный ресурс] //Википедия ,1995-2019. URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5\_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5. (Дата обращения: 25.03.2019).

1. Аверченков, В. И. Защита персональных данных в организации [Электронный ресурс] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. — Электрон. текстовые данные. — Брянск : Брянский государственный технический университет, 2012. — 124 c.— Режим доступа: http://www.iprbookshop.ru/6993.html [↑](#footnote-ref-1)
2. Защита персональных данных: [Электронный ресурс] //ИТ-портал компании «Инфосистемы Джет» ,1995-2019. URL: http://www.jetinfo.ru/stati/zaschita-personalnykh. (Дата обращения: 24.03.2019). [↑](#footnote-ref-2)
3. Защита персональных данных: [Электронный ресурс] //ИТ-портал компании «Инфосистемы Джет» ,1995-2019. URL: http://www.jetinfo.ru/stati/zaschita-personalnykh. (Дата обращения: 24.03.2019). [↑](#footnote-ref-3)
4. Чепурнова, Н. М. Правовые основы информатики [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика» / Н. М. Чепурнова, Л. Л. Ефимова. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 295 c.— Режим доступа: http://www.iprbookshop.ru/81535.html [↑](#footnote-ref-4)
5. Персональные данные: [Электронный ресурс] //Википедия ,1995-2019. URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5\_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5. (Дата обращения: 25.03.2019). [↑](#footnote-ref-5)