Министерство образования и науки Российской Федерации

САНКТ–ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

А.С. Исаев, Е.А. Хлюпина

Правовые основы организации защиты персональных данных

Учебное пособие

Санкт–Петербург

2014

УДК 34.069

Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с.

В настоящем учебном пособии изложены и проанализированы основные правовые аспекты защиты персональных данных согласно действующей международной и Российской нормативно - правовой документации. Рассмотрены понятия обработки и защиты персональных данных, ответственность и права операторов и субъектов персональных данных.

Рекомендовано студентам, бакалаврам, специалистам и магистрами по специальностям: 090103 «Организация и технология защиты информации», 090900 – «Информационная безопасность», которые по роду своей деятельности непосредственно сталкиваются с организацией защиты персональных данных в организациях различного рода деятельности.

Рекомендовано к печати Ученым советом Института комплексного военного образования СПб НИУ ИТМО протокол №11 от 31 марта 2014 г. в качестве учебного пособия для студентов кафедры мониторинга и прогнозирования информационных угроз.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт–Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Содержание

Содержание 3

Введение 5

1. Правовое регулирование в области защиты персональных данных 7

1.1 Международная нормативно-правовая документация в области защиты персональных данных 7

1.1.1 Европейская конвенция о защите прав человека и основных свобод..... 7

1.1.2 Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 8

1.1.3 Директива № 2002/58/ЕС Европейского Парламента и Совета ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи 16

1.2 Нормативно-правовая документация Российской Федерации в области защиты персональных данных 23

1.3 Федеральный закон «О персональных данных» 30

2. Права субъекта и обязанности оператора при обработке персональных данных 34

2.1 Субъект персональных данных и его права при обработке персональных данных 34

2.2 Оператор персональных данных 40

2.3 Обязанности оператора при обработке персональных данных 41

2.4 Меры по обеспечению выполнения оператором своих обязанностей 48

2.5 Меры по обеспечению безопасности персональных данных при их обработке 50

3. Нарушители безопасности персональных данных 55

3.1 Классификация нарушителей безопасности информационных систем персональных данных 55

3.2 Внутренний нарушитель 57

4. Государственные регуляторы и их нормативно-правовая документация в области защиты персональных данных 62

4.1 Государственные органы исполнительной власти, осуществляющие надзор за соблюдением требований законодательства в области обработки персональных данных 62

4.2 Нормативно-правовая документация государственных органов исполнительной власти, осуществляющих надзор за соблюдением требований законодательства в области обработки персональных данных 66

4.3 Обеспечение выполнение мер, утвержденных постановлением Правительства Российской Федерации от 21.03.2012 г. N 211 72

5. Осуществление проверки соблюдения правил в области защиты персональных данных и ответственность за их нарушение 75

5.1 Контроль за соблюдением требований законодательства в области защиты персональных данных 76

5.2 Лицензирование деятельности по технической защите конфиденциальной информации 78

5.3 Ответственность за нарушения установленных правил по обработке персональных данных 89

Литература 102

Введение

Современное общество все чаще встречается с информационным обменом в своей повседневной жизни. Каждый из нас регулярно сообщает о себе информацию, позволяющую напрямую или косвенно определить и идентифицировать нас. С учетом положений действующего законодательства Российской Федерации, такая информация является нашими персональными данными.

Согласно действующему Указу Президента Российской Федерации, персональные данные являются конфиденциальной информацией. Основным законом, регламентирующим вопросы в части персональных данных, является Федеральный закон №152-ФЗ от 27 июня 2006 года «О персональных данных». Согласно его положениям, персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Таким образом, все мы, как граждане своего государства, являемся субъектами персональных данных, в связи с чем, для нас становится актуальным вопрос о наших законных правах в части нашей жизни, а также законности использования этих сведений. Согласно закону «О персональных данных», лица, осуществляющие любые действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных являются операторами персональных данных. Исходя из этого, в целях обеспечения выполнения наших законных интересов и защиты нашей личной жизни необходимо знать и контролировать выполнение обязанностей, возложенных на оператора персональных данных. Таким образом, защита персональных данных является одним из наиболее приоритетных направлений в существующей сфере обеспечения информационной безопасности в организациях различных форм и родов деятельности.

С учетом влияния действующих общемировых тенденций по вопросам защиты информации в целом, и персональных данных в частности, возникает вопрос о необходимости применения все более и более совершенных средств и механизмов защиты информации. Зачастую, применение новых технологий влечёт за собой ухудшение информационной безопасности в целом, что может плачевно отразится и на персональных данных. В связи с этим, в Российской Федерации на законодательном уровне происходит регулирование правовых отношений в части персональных данных, формирование отдельных органов исполнительной власти, основной целью которых является проведение работ по

выявлению и последующему устранению существующих нарушений и несоответствий в части обработки и защиты персональных данных. Следует отметить, что наибольшую популярность в Российской Федерации вопрос обеспечения информационной безопасности персональных данных, набрал лишь в последние несколько лет. Данный факт подтверждается тем, что все больше и больше высших учебных заведений, осуществляющих подготовку бакалавров, специалистов и магистров по защите информации, вносят предметы в учебную программу (по данным специальностям), так или иначе связанные с изучением правовых основ защиты информации.

С учетом того, что с точки зрения действующего законодательства Российской Федерации, персональные данные являются отдельным видом конфиденциальной информации, изучение правовых основ организации защиты и обработки персональных данных является одним из приоритетных направлений.

Настоящее учебное пособие содержит в себе систематизированный перечень основных правовых аспектов по вопросам организации защиты персональных данных, их обработки, а также нормативных требований по выполнению положений действующих международных и Российских нормативно-правовых документов, а также дает представление о последствиях нарушения данных требований, включая определение ответственности за их несоблюдение и\или ненадлежащее соблюдение.

1. Правовое регулирование в области защиты персональных данных

1.1 Международная нормативно-правовая документация в области защиты персональных данных

Во многих странах вопрос об обеспечении защиты персональных данных стал актуален намного раньше чем в России, именно поэтому институт защиты персональных данных на международном уровне является более развитым. Одним из первых документов в данном вопросе является Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных, которая была утверждена 28 января 1981 г. в Страсбурге.

1.1.1 Европейская конвенция о защите прав человека и основных свобод

Европейская конвенция «О защите личности в связи с автоматической обработкой персональных данных» рассматривает порядок сбора, хранения, способы физической защиты персональных, а также принципы доступа к таким данным. Данная конвенция была ратифицирована Россией 7 ноября 2001 года и вступила в силу с 1 сентября 2013 года. В ней определен порядок обеспечения реализации прав человека на уважение частной жизни и свободу информации, которые зафиксированы в 8 и 9 статьях Европейской конвенции о защите прав человека и основных свобод, принятой в Риме 4 ноября 1950 г.

В 8-й статье Европейской конвенции «О защите прав человека и основных свобод» рассматриваются права на уважение частной и семейной жизни, согласно её положению, каждый человек имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции и не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, 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.

В 9-й статье Европейской конвенции «О защите прав человека и основных свобод» говорится о свободе мысли, совести и религии, согласно её положениям каждый человек имеет право на свободу мысли, совести и религии. Это право включает свободу менять свою религию или убеждения и свободу исповедовать свою религию или убеждения как индивидуально, так и сообща с другими, публичным или частным порядком, в богослужении, обучении, отправлении религиозных и культовых обрядов.

Одной из ключевых особенностей в данном вопросе, согласно Конвенции, заключается в том, что свобода исповедовать свою религию или убеждения подлежит лишь ограничениям, которые предусмотрены законом и необходимы в демократическом обществе в интересах общественной безопасности, для охраны общественного порядка, здоровья или нравственности или для защиты прав и свобод других лиц.

Также в нынешнее время вопросы защиты персональных данных на международном уровне регламентируются директивами Европарламента и Совета Европейского Союза, а именно:

а) директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных;
б) директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 года относительно обработки персональных данных и защите частной жизни в электронном коммуникационном секторе.

Под директивой следует понимать – тип законодательного акта Европейского союза, которая носит обязательный характер для всех стран-участников и имеет верховенство над национальным правом.

1.1.2 Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995

Данный документ применяется к обработке персональных данных, полностью или частично автоматическими средствами, и обработке средствами, отличными от автоматических, персональных данных, составляющих часть картотеки или предназначенных составлять часть картотеки.

В его первой главе представлены общие положения, и дан основной перечень терминов и определений, используемых в дальнейшем. Стоит отметить, что подавляющее большинство терминов, используемых в данном документе полностью или частично совпадают с установленными терминами Российским законодательством.

Во второй главе документа рассмотрены общие нормы законности обработки персональных данных для государств–участников, в частности:

- принципы, касающиеся качества данных;
- критерии для легитимности обработки данных;
- особые категории обработки;

- информация, передаваемая субъекту данных;
- право субъекта данных на доступ к данным;
- исключения и ограничения;
- право субъекта данных на возражения;
- конфиденциальность и безопасность обработки;
- уведомление.

В следующих разделах устанавливаются обязанности государств-участников по обеспечению процессов законности осуществления обработки персональных данных в пределах своих стран, а также устанавливаются ограничительные рамки на возможность такой обработки, отдельно определяя случаи, при которых обработка персональных данных может быть осуществлена. Согласно положениям директивы, государства–участники обязаны обеспечить условия, при которых бы персональные данные:

- обрабатывались корректно и законно;
- собирались для объявленных, явных и законных целей, и в дальнейшем не обрабатывались каким–либо образом, несовместимым с этими целями;
- были адекватными, относящимися к делу и не избыточными в отношении целей, для которых они собираются и/или в дальнейшем обрабатываются;
- были точными и, если необходимо, актуальными;
- хранились в форме, позволяющей идентификацию субъектов персональных данных не долее, чем это необходимо для целей, с которыми данные собирались или впоследствии обрабатывались.

При этом обработка персональных данных возможна только в случае, если:

- субъект данных недвусмысленно дал свое согласие;
- обработка необходима для исполнения контракта, в котором субъект данных является стороной или для принятия мер до заключения контракта по просьбе субъекта данных;
- обработка необходима для выполнения юридического обязательства, субъектом которого является контролер;
- обработка необходима для защиты жизненных интересов субъекта данных;
- обработка необходима в целях обеспечения законных интересов контролера или третьей стороны (сторон), которым раскрыты данные.

В продолжении данной директивы описан состав и порядок работы с особыми категориями персональных данных. К таким данным будут относится сведения:

- о расовой принадлежности;
- о этническом происхождении;
- о политических взглядах;
- о вероисповедании;
- о философском воззрении;
- о членстве в профсоюзах;
- о здоровье;
- о интимной жизни.

Согласно положениям директивы, государства-участники не допускают обработку таких специальных категорий персональных данных, за исключением если:

- субъект данных дал свое явное согласие на обработку таких данных, кроме случаев, когда законами государства-участника установлено, что указанное выше правило, применяемое государствами-участниками в отношении персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни, не может быть отменено на основании согласия субъекта данных;
- обработка необходима в целях исполнения обязательств и особых прав контролера в сфере законодательства о труде в той мере, в какой это допускается национальным законодательством, предусматривающим адекватные гарантии;
- обработка необходима для защиты жизненных интересов субъекта данных или иного лица, если субъект данных физически или юридически неспособен дать свое согласие;
- обработка осуществляется в ходе законной деятельности с надлежащими гарантиями фондом, ассоциацией или любой иной некоммерческой организацией в политических, философских, религиозных или профсоюзных целях и при условии, что обработка относится исключительно к членам организации или лицам, имеющим регулярный контакт с нею в связи с ее целями, и что данные не раскрываются третьим лицам без согласия субъекта данных;
- обработка относится к данным, которые явно сделаны общедоступными субъектом данных, или являются необходимыми для внесения, поддержания или защиты судебных исков.

Также правило, применяемое государствами-участниками в отношении персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни не применяется в случае, если обработка данных требуется в

целях превентивной медицины, медицинского диагноза, предоставления медицинского обслуживания, лечения или управления услугами здравоохранения, а также если такие данные находятся во владении лица, профессионально занимающегося медицинской деятельностью в соответствии с национальным законодательством или правилами, установленными компетентными национальными органами, устанавливающими обязательства сохранения профессиональной тайны, или иного лица, также имеющего эквивалентные обязательства по сохранению тайны.

Обработка данных, касающихся правонарушений, уголовного наказания или мер безопасности, может осуществляться только под контролем официального органа, или - если в соответствии с национальным законодательством предусмотрены надлежащие особые гарантии - с учетом частичных исключений, установленных государством-участником в соответствии с национальными нормами, предусматривающими надлежащие особые гарантии, однако полный реестр уголовных приговоров может вестись только под контролем официального органа. Государства-участники могут установить, что данные, касающиеся административных санкций или судебных решений по гражданским делам, также могут обрабатываться под контролем официального органа. Также государствами-участниками определяются условия, на которых может обрабатываться национальный идентификационный номер или любой иной идентификатор общего назначения.

В следующем разделе рассматриваются правила работы с информацией, передаваемой субъекту данных. В случаях сбора данных у субъекта персональных данных контролер или его представитель, обязаны предоставить такому субъекту персональных данных по меньшей мере следующую информацию:

- личность контролера или его представителя, если таковой имеется;
- цели обработки, для которых предназначены данные;
- иную информацию, такую, как:
    a. получатели или категории получателей данных;
    b. является ли ответ на вопросы обязательным или добровольным, а также возможные последствия отказа от ответа;
    c. наличие права доступа и права уточнять касающиеся его данные в той мере, в какой требуется дополнительная информация, касающаяся конкретных обстоятельств, при которых собираются данные, чтобы гарантировать корректную обработку применительно к субъекту данных.

В случаях, когда персональные данные получаются не напрямую, а через законного представителя субъекта, контролер или его представитель на момент фиксирования таких персональных данных или в случае если предполагается

передача персональных данных третьей стороне в первый раз, обязан предоставить как минимум следующую информацию:

- личность контролера или его представителя, если таковой имеется;
- цели обработки;
- любую иную информацию, такую, как:
    a. категории используемых данных;
    b. получатели или категории получателей персональных данных;
    c. наличие права доступа и права уточнять касающиеся его данные в той мере, в какой требуется дополнительная информация, касающаяся конкретных обстоятельств, при которых собираются данные,
    d. гарантии корректной обработки применительно к субъекту данных.

Данное правило не применяется при обработке персональных данных в статистических целях или же в целях исторических или научных исследований, а также когда предоставление такой информации оказывается невозможным или может повлечь непропорциональные усилия при их передаче. Отдельно замечено, что к исключениям также относится документирование или разглашение персональных данных в случаях, прямо определяемыми законами государств-участников.

В 5-ой главе директивы рассмотрены права субъекта персональных данных на доступ к своим данным. Согласно им, субъект персональных данных вправе получить от контроллера:

- без принуждения и без чрезмерной отсрочки или затягивания:
    a. подтверждение того, были ли или нет в обработке относящиеся к нему данные, и информацию по меньшей мере о целях обработки, категории используемых данных, получателях или категориях получателей, которым сообщаются персональные данные,
    b. сообщение в доступной форме об обрабатываемых персональных данных и о любой доступной информации, касающейся их источника,
    c. сведения о логике, используемой при автоматической обработке данных, касающихся его, по меньшей мере в случае принятия решений исключительно при автоматизированной обработке.
- по мере необходимости - уточнение, стирание или блокировку данных, в частности, в связи с неполным или неточным характером данных;
- уведомление третьих лиц, которым раскрываются данные, о любых уточнениях, стирании или блокировках данных, произведенных в

соответствии с предыдущим пунктом, если это возможно и не требует непропорциональных усилий.

Также права субъекта персональных данных рассматриваются в других разделах директивы. В них указано, что государствами-участниками должны быть обеспечены:

1. Право в любое время высказывать на законном основании возражение против обработки касающихся его данных, кроме случаев, когда национальным законодательством определено иное. Если возражение является обоснованным, контролер обязан прекратить обработку этих данных.
2. Право бесплатно высказывать возражение против обработки касающихся его персональных данных, которые, по мнению контролера, обрабатываются для целей прямого маркетинга, или получать уведомление прежде, чем персональные данные будут впервые раскрыты третьим сторонам, или использованы по их поручению в целях прямого маркетинга, и в явной форме получать право бесплатно высказывать возражение против такого раскрытия или использования.

Согласно 29-ой статье данной директивы, для защиты индивидуумов в отношении обработки их персональных данных создается Рабочая группа, которая имеет статус консультативного органа и действует в качестве независимой структуры. Рабочая группа состоит из представителя органа или органов надзора, созданного каждым государством-участником, представителя органа или органов, учрежденных для институтов и структур Сообщества, и представителя Комиссии. Каждый член Рабочей группы назначается институтом или органом (органами), которые он представляет. Если государство-участник учредило более одного органа надзора, последние назначают одного общего представителя. Это же правило применяется и в отношении органов, учрежденных для институтов и структур Сообщества.

В качестве обязанностей такой Рабочей группы определено:

- рассматривать любые вопросы, относящиеся к применению национальных положений, принятых во исполнение настоящей директивы с целью обеспечения равного выполнения различными странами указанных положений;
- производить для Комиссии оценку уровня защиты персональных данных внутри Сообщества и в третьих странах;
- консультировать Комиссию по любым проектам поправок к настоящей директиве, любым дополнительным или конкретным мерам по защите прав и свобод физических лиц в отношении обработки их персональных данных и любым иным мерам, предлагаемым к

принятию Сообществом и затрагивающим упомянутые права и свободы;
- давать оценку кодексам поведения, разрабатываемым на уровне Сообщества.

Если Рабочая группа приходит к заключению о том, что различия между законами или практическими действиями различных государств-участников могут стать для Сообщества источником неравенства в том, что касается защиты индивидуумов в отношении обработки их персональных данных, она обязана должным образом проинформировать Комиссию.

Рабочая группа составляет ежегодный отчет о ситуации в сфере защиты физических лиц в отношении обработки их персональных данных внутри Сообщества и в третьих странах, который она представляет Комиссии, Европейскому парламенту и Совету, данный отчет подлежит опубликованию.

Отдельными разделами в данной директиве отмечен, тот факт, что во время процесса обработки персональных данных должны обеспечиваться конфиденциальность и безопасность данного процесса. Обеспечение конфиденциальности заключается в том, что любое лицо, действующее с санкции контролера или обработчика, включая самого обработчика, имеющее доступ к персональным данным, не должно вести их обработку кроме как по указанию контролера, если это не требуется от него по закону. Обеспечение безопасности включает:

- обязанность контролера реализовывать надлежащие технические и организационные меры для защиты персональных данных от случайного и\или незаконного уничтожения и\или случайной утраты, изменения, неправомерного раскрытия или доступа, в частности, когда обработка влечет передачу данных по сети, а также от всех иных незаконных форм обработки;
- обязанность контролера избирать обработчика, предоставляющего достаточные гарантии в отношении мер технической безопасности и организационных мер, регулирующих осуществляемую обработку, и обеспечить соблюдение таких мер в случае, если обработка осуществляется по его поручению;
- обязанность обработчика осуществлять свою деятельность на основе соглашения или нормативного акта, содержащего обязательства обработчика перед контролером;
- оформление в письменной или иной эквивалентной форме частей контракта или нормативного акта, касающиеся защиты данных, и требований в отношении установленных мер в целях поддержания корректности.

Для соблюдения положений, принятых государствами-участниками во исполнение данной директивы, каждое государство-участник назначает один или несколько государственных органов для надзора на своей территории. При выполнении возложенных на них обязанностей указанные органы действуют в условиях полной независимости. Также каждое государство-участник создает условия для проведения консультаций с органами надзора при разработке административных мер или правил, касающихся защиты прав и свобод индивидуумов в отношении обработки их персональных данных. Каждый такой орган надзора наделяется следующими полномочиями:

- полномочиями для проведения расследований, в том числе правом доступа к данным, являющимся предметом операций по обработке данных, а также правом получения любой информации, необходимой для исполнения его обязанностей по надзору;
- реальными полномочиями для вмешательства в процесс обработки, в том числе правом вынесения суждений до начала операций по обработке данных, а также обеспечения надлежащего уровня гласности в отношении таких суждений;
- правом отдавать распоряжения относительно блокирования, стирания или уничтожения данных, налагать временный или постоянный запрет на обработку данных, выносить предупреждения и налагать взыскания на контрольный орган, а также передавать такого рода дела на рассмотрение национальных парламентов или иных политических структур;
- полномочиями для возбуждения юридических дел в случаях нарушения национальных положений, принятых во исполнение настоящей директивы, а также для привлечения внимания судебных органов к упомянутым нарушениям. При этом решения органа надзора, повлекшие за собой подачу жалоб, могут быть опротестованы в судебном порядке.

К обязанностям органов надзора относят:

- обязанность рассматривать жалобы, поданные любым лицом или представляющей это лицо ассоциацией касательно защиты его прав и свобод в отношении обработки персональных данных. Заинтересованное лицо должно быть проинформировано о результатах рассмотрения жалобы;
- обязанность рассматривать иски любого лица о проверке законности обработки данных в случаях, когда действуют национальные положения, принятые во исполнение статьи 13 данной директивы;
- обязанность составлять регулярные отчеты о своей деятельности, а также их публикации.

Государства-участники обеспечивают соблюдение членами и сотрудниками органов надзора профессиональной тайны в отношении конфиденциальной информации, к которой они имеют доступ, даже после окончания срока их службы в указанных органах. Выше упоминалось, что государства-участники могут принимать законодательные меры для ограничения сферы обязательств и прав, если такое ограничение является необходимой мерой для обеспечения:

a. национальной безопасности;
b. обороны;
c. общественной безопасности;
d. предотвращения, расследования, раскрытия и обвинения по уголовным преступлениям или нарушений этики в регулируемых профессиях;
e. важных экономических или финансовых интересов государства-участника или Европейского Союза, включая финансовые, бюджетные и налоговые вопросы;
f. мониторинговых, инспекционных или управленческих функций, связанных, хотя бы и случайно, с осуществлением официальных полномочий, указанных в пунктах (c), (d) и (e);
g. защиты субъекта данных или прав и свобод иных лиц.

В 18 статье 9 раздела 2 главы данной директивы указано об обязанности оператора уведомлять надзорный орган. Такое уведомление, по меньшей мере, должно включать:

- имя (наименование) и адрес контролера и его представителя, если таковой имеется;
- цель или цели обработки;
- описание категории или категорий субъекта данных и данных, или категории относящихся к ним данных;
- получателей или категории получателей, которым могут раскрываться данные;
- предполагаемую передачу в третьи страны;
- общее описание, позволяющее произвести предварительную оценку правомерности мер для обеспечения безопасности обработки.

1.1.3 Директива № 2002/58/ЕС Европейского Парламента и Совета ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи

Другим основополагающим нормативным правовым актом являлась директива 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций. В ней

были конкретизированы положения директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных применительно к сектору телекоммуникаций. Данная директива должна была быть адаптирована к изменениям на рынке и в технологиях оказания услуг электронной связи для обеспечения равного уровня защиты персональных данных и информации о частной жизни пользователей общедоступных услуг электронной связи независимо от используемых технологий. В связи с этим указанная директива подлежала отмене и была заменена директивой № 2002/58/ЕС Европейского Парламента и Совета ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи.

Директива № 2002/58/ЕС применяется в отношении обработки персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи коллективного доступа в Сообществе, в том числе в сетях связи коллективного доступа, поддерживающих сбор данных и устройства идентификации. Данный документ обеспечивает гармонизацию национальных положений, необходимых для гарантии соответствующего уровня защиты основных прав и свобод, и, в частности, права на частную жизнь и конфиденциальность информации о частной жизни в связи с обработкой персональных данных в сфере электронных коммуникаций, и для обеспечения свободного движения таких данных, передвижения оборудования для электронной связи и услуг электронной связи в Сообществе.

В 4-ой статье этой директивы рассматривается вопрос обеспечения безопасности обработки данных. В ней говориться, что провайдер общедоступных услуг связи обязан:

- предпринимать необходимые технические и организационные меры для обеспечения безопасности предоставляемых услуг, при необходимости совместно с провайдером сети связи общего доступа, если это касается вопроса безопасности сети. Принимая во внимание уровень развития технологий и стоимость их внедрения, данные меры должны гарантировать уровень безопасности, соответствующий имеющимся угрозам. Данные меры должны по меньшей мере:
    a. гарантировать, что доступ к персональным данным может быть предоставлен только уполномоченному персоналу в разрешенных законом целях;
    b. защищать персональные данные, сохраненные или переданные, от случайного или незаконного уничтожения, случайной потери или изменения, несанкционированного или незаконного хранения, обработки, доступа или раскрытия;
    c. гарантировать введение политики безопасности в отношении обработки персональных данных.

- информировать абонентов при наличии определенной угрозы повреждения системы безопасности сети, в отношении такой угрозы;
- информировать абонентов о любых возможных средствах защиты, включая информацию о затратах на их приобретение в случаях, когда угроза выходит за пределы средств защиты, доступных провайдеру;
- без необоснованного промедления доводить до сведения компетентных национальных органов власти соответствующую информацию в случае повреждения системы безопасности персональных данных;
- без необоснованного промедления уведомлять абонента или индивидуального пользователя о наличии вероятности повреждении системы безопасности персональных в случае, если повреждение такой системы неблагоприятным образом затронет персональные данные или информацию о частной жизни абонента или индивидуального пользователя.

Уведомление абонента или индивидуального пользователя о повреждении безопасности персональных данных не требуется, если провайдер продемонстрировал компетентным органам то, что им были приняты необходимые технологические защитные меры, и то, что эти меры были применены в отношении данных, затронутых в результате повреждения системы безопасности. Такие технологические защитные меры должны представить данные, непонятные любому лицу, не имеющему к ним санкционированного доступа. Уведомление абонента или индивида должно содержать следующую минимальную информацию:

- описание характера повреждения системы безопасности персональных данных;
- указание на контактные пункты, где можно получить дополнительную информацию;
- меры, которые могут быть приняты для того, чтобы смягчить возможные неблагоприятные последствия от повреждения в системе безопасности персональных данных.

Уведомление, обращенное к национальным компетентным органам власти, должно как минимум содержать:

- описание характера повреждения системы безопасности персональных данных;
- описание последствий повреждения системы безопасности персональных данных;
- меры, предложенные и принятые провайдером в отношении адресата.

В 5-ой статье данной директивы описаны обязанности государств-членов ЕС по обеспечению конфиденциальности коммуникаций:

- гарантия конфиденциальности передаваемых сообщений и относящихся к ним данных трафика посредством сети связи общего пользования и общедоступных услуг электронной связи. Исключение составляет законодательно разрешенная запись сообщений и относящихся к ним данных трафика, когда такая запись производится в ходе законной деловой практики для целей предоставления доказательства совершения коммерческой сделки или осуществления любого другого делового взаимодействия.
- гарантия того, что хранение информации или получение доступа к информации, уже сохраненной на терминальном оборудовании абонента или пользователя, допускается только при условии, что заинтересованный абонент или пользователь дали свое согласие, будучи обеспеченными точной и полной информацией в соответствии с директивой 95/46/ЕС, помимо прочего, о целях обработки информации.

В 6-ой статье описывается порядок обработки данных трафика, касающегося абонентов и пользователей:

- данные трафика, касающиеся абонентов и пользователей, обработанные и сохраненные провайдером сети связи общего доступа или провайдером общедоступных услуг электронной связи, должны быть уничтожены или сделаны анонимными, если в них нет дальнейшей необходимости для передачи сообщения;
- данные трафика, необходимые для формирования счетов абонента за пользование связью и соединение, могут быть обработаны. Такая обработка допустима только до истечения периода времени, в течение которого может быть законодательно оспорен счет за услуги или взыскана плата за соединение;
- в целях продвижения услуг электронных коммуникаций или дополнительных услуг провайдер общедоступных услуг электронной связи может осуществлять обработку данных трафика, касающихся абонентов и пользователей. Данная обработка допускается до той степени и на протяжении такого периода времени, какие необходимы для подобных услуг или маркетинга, при условии, что абонент или пользователь, к которым относятся эти данные, дал свое предварительное согласие на их обработку. Абонентам или пользователям должна быть предоставлена возможность отозвать свое согласие на обработку данных трафика в любое время;
- провайдер услуг должен информировать абонента или пользователя о видах данных трафика, находящихся в обработке, и о длительности такой обработки в целях, необходимых для формирования счетов абонента за пользование связью и соединение;

- провайдер услуг должен информировать абонента или пользователя о видах данных трафика, находящихся в обработке до получения их согласия в целях продвижения услуг электронных коммуникаций или дополнительных услуг провайдер общедоступных услуг электронной связи;
- обработка данных трафика должна быть ограничена для лиц, действующих под руководством провайдеров сетей связи общего доступа, провайдеров общедоступных услуг электронной связи, в пределах, необходимых для осуществления данными лицами следующих видов деятельности: управления трафиком или биллингом, рассмотрения требований клиентов, обнаружения мошенничества, продвижения услуг электронной связи или предоставления дополнительных услуг.

В 9-ой статье данной директивы рассмотрен порядок обработки данных о местоположении, отличных от данных трафика:

- в случаях, когда допускается возможность обработки данных местоположения, отличных от данных трафика и имеющих отношение к абонентам или пользователям общедоступных услуг электронной связи, такие данные могут быть обработаны только после того, как они будут сделаны анонимными, или с согласия пользователей или абонентов. При этом такая обработка допускается до той степени и в течение такого периода времени, какие необходимы для оказания дополнительных услуг;
- провайдер услуг должен информировать пользователей или абонентов перед получением их согласия:
    a. о типе данных местоположения, отличных от данных трафика, которые будут обрабатываться;
    b. о длительности и целях обработки;
    c. будут ли передаваться данные третьей стороне в целях оказания дополнительных услуг.
- пользователям или абонентам должна быть предоставлена возможность в любое время отозвать свое согласие на обработку данных местоположения, отличных от данных трафика;
- В случае, когда согласие пользователя или абонента на обработку данных местоположения, отличных от данных трафика, уже получено, у пользователя или абонента должна сохраняться возможность простым способом и бесплатно временно отказаться от обработки таких данных применительно к каждому соединению с сетью или каждой передаче сообщения;
- обработка данных местоположения, отличных от данных трафика должна быть ограничена для лиц, действующих под руководством провайдера сети связи общего доступа или провайдера общедоступных

услуг электронной связи или третьей стороны, предоставляющей дополнительные услуги. Данное ограничение должно осуществляться до пределов, необходимых для предоставления дополнительных услуг.

Также одним из немаловажных факторов, рассмотренных в директиве № 2002/58/ЕС, является использование персональных данных в справочниках абонентах. К применяемым мерам их защиты можно отнести следующее:

- обязанность государств-членов ЕС гарантировать, что абоненты перед включением их в справочник бесплатно проинформированы о цели (целях) печатного или электронного справочника абонентов, находящегося в свободном доступе или запрашиваемого через справочные службы, в которые могут быть включены их персональные данные, и о любых дальнейших возможностях использования, данных, основанных на функциях поиска, встроенных в электронные версии справочника;
- обязанность государств-членов ЕС гарантировать, что абонентам предоставлена возможность определять, включены ли их персональные данные в общедоступный справочник;
- если персональные данные абонентов включены в общедоступный справочник, то абонентам должна быть предоставлена возможность определять, до какой степени эти данные имеют отношение к целям справочника, определенным поставщиком справочника, а также возможность проверять, вносить исправления в данные или отзывать такие данные;
- отказ абонентов от включения их данных в общедоступный справочник абонентов, проверка персональных данных, внесение в них исправлений или отзыв персональных данных из справочника абонентов должны осуществляться бесплатно;
- государства-члены ЕС могут потребовать, чтобы для любых целей общедоступного справочника, иных, чем поиск деталей контакта людей на базе их имени и необходимого минимального количества других идентификационных признаков, было запрошено дополнительное согласие абонентов;
- обязанность государств-членов ЕС гарантировать в рамках законодательства Сообщества и применимого национального законодательства, что законные интересы абонентов, не являющихся физическими лицами, в связи с внесением их в общедоступные справочники достаточно защищены.

Порядок работы с незапрашиваемыми сообщениями указан в 13-ой статье данной директивы. В положения данного порядка входит:

- использование систем связи автоматического повтора вызова без человеческого вмешательства (устройства автоматического дозвона), факсимильных аппаратов (факсов) или электронной почты в целях прямого маркетинга допускается только в отношении абонентов или пользователей, давших свое предварительное согласие;
- в случаях когда физическое или юридическое лицо получает от своих клиентов адрес электронной почты в связи с продажей товара или оказанием услуги, в соответствии с директивой 95/46/ЕС то же самое физическое или юридическое лицо может использовать эти адреса в целях прямого маркетинга своих собственных аналогичных товаров и услуг при условии, что клиентам ясно и отчетливо предоставляется возможность возражать бесплатно и простым способом против такого использования их электронных адресов во время предоставления ими своих адресов и при получении ими каждого сообщения в том случае, если клиент первоначального не отказался от использования своего электронного адреса;
- в иных случаях государства-члены ЕС должны принять соответствующие меры для гарантии недопущения отправки незапрашиваемых сообщений в целях прямого маркетинга, как без согласия заинтересованных абонентов и пользователей, так и в отношении абонентов или пользователей, не желающих получать такие сообщения;
- государства-члены ЕС также должны принять меры для определения разницы в национальном законодательстве между этими двумя возможностями неполучения абонентами незапрашиваемых сообщений, принимая в расчет, что обе эти возможности должны быть бесплатными для абонента или пользователя;
- в любом случае должна быть запрещена практика отправки в целях прямого маркетинга электронной почты, маскирующей или скрывающей идентификацию отправителя в нарушение статьи 6 директивы 2000/31/ЕС, отправка сообщений с недействительного адреса, на который получатель не может отправить запрос о прекращении отправки таких сообщений, либо отправка в нарушение указанной статьи почты, побуждающей получателей посещать вэб-сайты;
- государства-члены ЕС должны также гарантировать, в рамках законодательства Сообщества и применимого национального законодательства, что законные интересы абонентов, не являющихся физическими лицами, в отношении незапрашиваемых сообщений достаточно защищены.
- государства-члены ЕС должны гарантировать, что любое физическое или юридическое лицо, ощутившее на себе неблагоприятные последствия нарушений национальных положений, принятых согласно настоящей статье и в связи с этим имеющих законный интерес в

прекращении или запрещении подобных нарушений, включая провайдера услуг электронной связи, защищающего свои законные деловые интересы, может начать судебное разбирательство в отношении таких нарушений;

- государства-члены ЕС могут установить особые правила о штрафах, применимых к провайдерам услуг электронной связи, которые в результате своей небрежности способствуют нарушению национальных положений, принятых в соответствии с настоящей статьей.

1.2 Нормативно-правовая документация Российской Федерации в области защиты персональных данных

В Российской Федерации долгое время политике в области защиты персональных данных не уделялось должного внимания. Одним из немногих законодательных актов, ранее регулирующих процесс обработки персональных данных, являлся Указ Президента Российской Федерации от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера". И только после подписания Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в 2001 году были изданы основные законодательные акты, которые регулируют организацию процессов, связанных с защитой персональных данных на современном этапе. Сейчас список документов в данной области достаточно обширен, но пробелов в обеспечении защиты персональных все равно достаточно. К таким законодательным актам относят:

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера";
- Федеральный закон Российской Федерации 30 декабря 2001 г. № 197-ФЗ "Трудовой кодекс Российской Федерации (14 глава)";
- Федеральный закон от 19 декабря 2005 г. N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных";
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- Федеральный закон Российской Федерации от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации";
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Постановление Правительства Российской Федерации 2 июня 2008 г. № 419 "О федеральной службе по надзору в сфере связи и массовых коммуникаций";
- Приказ ФСТЭК России от 11 февраля 2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
- Приказ ФСТЭК России от 18 февраля 2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Приказ Роскомнадзора от 05 сентября 2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных";
- Постановление Правительства Российской Федерации от 21 марта 2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";
- Постановление Правительства Российской Федерации от 01 ноября 2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год;
- Приказ ФСТЭК России от 31 августа 2010 г. N 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 N 149/54-144);

- «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203);
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 N 149/6/6-622).

В Федеральном законе Российской Федерации № 197-ФЗ «Трудовом кодексе Российской Федерации» в 14 статье рассматривается защита персональных данных работника, в частности:

- общие требования при обработке персональных данных работника и гарантии их защиты;
- хранение и использование персональных данных работников;
- передача персональных данных работника;
- права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя;
- ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" является основным законодательным актом, которым должны руководствоваться операторы персональных данных при осуществлении своей деятельности, в нем регламентирован ряд условий, обязательных для обеспечения должного уровня безопасности информации конфиденциального характера, в частности персональных данных. Также в нем указаны права субъектов персональных данных и ответственность за нарушение порядка обработки персональных данных.

Федеральный закон Российской Федерации от 3.12.2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации" также регламентирует порядок обработки персональных данных. Согласно данному законодательству, государственная геномная регистрация - деятельность, осуществляемая указанными в настоящем Федеральном законе государственными органами и учреждениями по получению, учету, хранению, использованию, передаче и уничтожению биологического материала и обработке геномной информации, где биологический материал - содержащие геномную информацию ткани и выделения человека или тела (останков) умершего человека, а геномная информация - персональные данные, включающие кодированную информацию об определенных фрагментах

дезоксирибонуклеиновой кислоты физического лица или неопознанного трупа, не характеризующих их физиологические особенности. Такая государственная геномная регистрация должна проводится с соблюдением общепризнанных прав и свобод человека и гражданина в соответствии с принципами законности, гуманизма, конфиденциальности, сочетания добровольности и обязательности.

В постановлении Правительства Российской Федерации от 15.09.2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" указаны требования к обработке персональных данных, осуществляемой без использования средств автоматизации, которые должны применятся в устанавливаемых нормативных правовых актах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальных актах организации.

Постановление Правительства Российской Федерации от 6.07.2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" устанавливает требования, которые применяются при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне информационных систем персональных данных, где под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность. Настоящие требования не распространяются на отношения, возникающие при:

- использовании оператором информационной системы персональных данных (далее - оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;
- использовании бумажных носителей для записи и хранения биометрических персональных данных.

В Постановлении Правительства Российской Федерации 2.06.2008 г. № 419 "О федеральной службе по надзору в сфере связи и массовых коммуникаций" рассмотрены полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), а также организация ее деятельности. Данная служба является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных

требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

В приказах ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" рассмотрены меры по обеспечению безопасности персональных данных, которые должны приниматься для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения такой информации, а также от иных неправомерных. И в зависимости от того, является ли организация, осуществляющая работу с информацией конфиденциального характера, в том числе и персональными данными, государственной или негосударственной, меры соблюдаемые при организации процесса работы с персональными данными, будут различаться. Органы государственной власти при осуществлении своей деятельности должны руководствоваться приказом ФСТЭК России от 11.02.2013 N 17. Негосударственные организации - приказом ФСТЭК России от 18.02.2013 N 21.

В приказе ФСТЭК России от 31.08.2010 г. N 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» рассматриваются требования, которые распространяются на федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации, и являющиеся обязательными для операторов информационных систем общего пользования при разработке и эксплуатации информационных систем общего пользования.

Еще одним нормативным документом в области защиты персональных данных являются «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 N 149/54-144). Данными методическими рекомендациями необходимо руководствоваться в случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств (за исключением случая, когда оператором является физическое лицо, использующее персональные данные исключительно для личных и семейных нужд), а также при обеспечении безопасности персональных данных при обработке в информационных системах,

отнесенных к компетенции ФСБ России. В частности, Методическими рекомендациями необходимо руководствоваться:

- при обеспечении с использованием криптосредств безопасности персональных данных при их обработке в государственных информационных системах персональных данных (часть 5 Федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);
- при использовании криптосредств для обеспечения персональных данных в случаях, предусмотренных п. 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

Данные методические рекомендации не распространяются на информационные системы персональных данных, в которых:

- персональные данные обрабатываются без использования средств автоматизации;
- обрабатываются персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну;
- технические средства частично или целиком находятся за пределами Российской Федерации.

Согласно постановлению Правительства Российской Федерации от 02.06.2008 года № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации» Министерство связи и массовых коммуникаций Российской Федерации является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в следующих сферах:

- информационные технологии (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним);
- электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи;
- массовых коммуникаций и средств массовой информации (в том числе электронных), печати, издательской и полиграфической деятельности;
- обработки персональных данных.

Выделенный функционал с позиции отраслевого нормативного регулирования можно отнести к федеральным законам, формирующим правоотношения для сфер деятельности вышеназванного министерства:

- Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 07 июля 2003 года № 126-ФЗ «О связи»;
- Закон Российской Федерации от 27.12.1991 года № 2124-1 «О средствах массовой информации»;
- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных».

Таким образом, часть законов, регулирующих деятельность вышеуказанного министерства, относятся к области защиты информации, в том числе и персональных данных.

Еще одним законодательным актом, которым руководствуется Минкомсвязь при осуществлении своей деятельности, является «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203). Данная модель угроз безопасности персональных данных содержит систематизированный перечень угроз безопасности персональных данных при их обработке в типовых информационных системах персональных данных организации. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости, характерные для данной информационной системы персональных данных, реализуя тем самым угрозы информационной безопасности.

Говоря о нормативных правовых актах в области обеспечения защиты персональных данных, стоит упомянуть о таком документе, как «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 N 149/6/6-622).

Данным документом устанавливаются требования, которые:

- являются обязательными для оператора, осуществляющего обработку персональных данных, а также лица, которому на основании договора оператор поручает обработку персональных данных и (или) лица, которому на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности защиты персональных данных при их обработке в информационной системе с использованием криптосредств. При этом существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их

обработке в информационной системе в случаях, предусмотренных действующим законодательством;

- распространяются на криптосредства, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, все технические средства которых находятся в пределах Российской Федерации, а также в системах, технические средства которых частично или целиком находятся за пределами Российской Федерации.
- не отменяют требования иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

1.3 Федеральный закон «О персональных данных»

Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" является основным законом в области обеспечения безопасности персональных данных. В нем прописаны принципы осуществления обработки информации ограниченного доступа, в частности персональных данных, обязанности оператора, осуществляющего такую обработку, а также права субъекта персональных данных. Данным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Согласно тексту данного закона, основной его целью 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.

Во 2-ой главе данного документа рассматриваются принципы и условия обработки персональных данных, а именно:

- принципы обработки персональных данных;

- условия обработки персональных данных;
- конфиденциальность персональных данных;
- общедоступные источники персональных данных;
- согласие субъекта персональных данных на обработку своих персональных данных;
- специальные категории персональных данных;
- биометрические персональные данные;
- трансграничная передача персональных данных;
- особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.

Согласно данному закону, обработка персональных данных должна осуществляться при наличии согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 данного Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и с учетом следующих 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 также 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.

При работе с персональными данными оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность такой информации за исключением следующих случаев:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

В общедоступные персональные данные могут быть включены фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные субъекта при наличии письменного согласия этого субъекта. При этом такие сведения могут быть изъяты из

общедоступного источника по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Данные о расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни к общедоступным данным не могут быть отнесены. Такие данные относятся к специальным категориям персональным данных, обработка которых не допускается за исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных":

- 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 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;
- 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;
- 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;
- обработка персональных данных необходима в связи с осуществлением правосудия;
- 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.

При передаче персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу оператор обязан

убедиться, что после завершения передачи будет обеспечиваться адекватная защита прав субъектов персональных данных.

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных;
- предусмотренных международными договорами Российской Федерации по вопросам выдачи виз, а также международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

В 3-ей главе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" прописаны права субъекта персональных данных, в частности:

- право субъекта персональных данных на доступ к своим персональным данным;
- права субъектов персональных данных при обработки их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;
- права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных;
- право на обжалование действий или бездействий оператора.

В следующей главе данного закона рассмотрены обязанности оператора персональных данных при осуществлении обработки такой информации:

- обязанности оператора при сборе персональных данных;
- меры по обеспечению безопасности персональных данных при их обработке;
- обязанности оператора при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

- обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;
- уведомление об обработке персональных данных.

В 5-ой главе рассмотрен порядок осуществления контроля и надзора за обработкой персональных данных, которые реализуются уполномоченным органом по защите прав субъектов персональных данных - федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи. Также в данной главе определена ответственность за нарушение требований данного Федерального закона.

Контрольные вопросы:

1. Какими документами на международном уровне регулируется вопрос о защите персональных данных?
2. Какие условия обработки персональных данных обязаны обеспечить государства-участники ЕС?
3. В каких случаях возможна обработка персональных данных согласно директиве 95/46/ЕС?
4. Что входит в обязанности оператора согласно директиве 2002/58/ЕС?
5. Какие обязанности есть у государств-участников ЕС по обеспечению конфиденциальности коммуникаций?
6. Какие меры защиты должны быть реализованы по отношению к персональным данным, используемым в справочниках абонентов, согласно директиве 2002/58/ЕС?
7. Какими основными законодательными актами регулируется вопрос защиты персональных данных на территории Российской Федерации?

2. Права субъекта и обязанности оператора при обработке персональных данных

2.1 Субъект персональных данных и его права при обработке персональных данных

Отношения, связанные с обработкой персональных данных, регулируются Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных". Согласно ему субъектом персональных данных является физическое лицо, которое может быть прямо или косвенно определено или определяемо при использовании персональных данных.

Согласно положениям данного закона, субъект персональных данных обладает следующими правами на доступ к своим персональным данным:

1. Правом на получение сведений, касающихся обработки его персональных данных.
2. Правом требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
3. Правом на получение от оператора сведений, касающихся обработки его персональных данных, в доступной форме, без содержания в них персональных данных, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.
4. Правом на получение сведений, касающихся обработки его персональных данных, предоставляемых субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Такой запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации и должен содержать:

   - номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
   - сведения о дате выдачи указанного документа и выдавшем его органе;
   - сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

5. Право на повторное обращение к оператору, в случае, если сведения, касающиеся обработки персональных данных субъекта, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу.
6. Право направить оператору повторный запрос в целях получения сведений, касающихся обработки персональных данных субъекта, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления

первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7. Право на повторное обращение к оператору или направление ему повторного запроса в целях получения сведений, касающихся обработки персональных данных субъекта, а также в целях ознакомления с обрабатываемыми персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.
8. Право потребовать от оператора представления доказательств отказа в выполнении повторного запроса.
9. Право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

   - подтверждение факта обработки персональных данных оператором;
   - правовые основания и цели обработки персональных данных;
   - цели и применяемые оператором способы обработки персональных данных;
   - наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
   - обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
   - сроки обработки персональных данных, в том числе сроки их хранения;
   - порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
   - информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект персональных данных может быть ограничен в праве на доступ к его персональным данным в соответствии с федеральными законами, в том числе если:

1. обработка персональных данных, включая персональные данные, полученные 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. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
4. доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
5. обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

В случае обработки персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации субъект персональных данных имеет право:

- давать свое согласие на обработку персональных данных, оператору. Обработка персональных данных, в выше указанных целях, без

предварительного согласия со стороны субъекта персональных данных не допускается;
- отзывать свое согласие на обработку персональных данных, у оператора. Оператор обязан немедленно прекратить обработку персональных данных по требованию субъекта персональных данных.

При принятии решений на основании исключительно автоматизированной обработки персональных данных, субъект персональных данных имеет право:

- запретить 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;
- требовать у оператора предоставления разъяснений:
  - о порядке принятия решений на основании исключительно автоматизированной обработки его персональных данных;
  - о возможных юридических последствий такого решения;
  - о порядке защиты его прав и законных интересов.
- требовать у оператора предоставления возможности заявления возражения против такого решения. В случае поступления возражений со стороны субъекта персональных данных, оператор обязан в течении 30 дней, со дня получения возражений, рассмотреть поступившие возражения и сообщить о результатах его рассмотрения.

В случае, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных" или иным образом нарушает его права и свободы, субъекта персональных данных имеет право:

- обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

В соответствии с частью 4, статьи 9 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом от 06.04.2011 N 63–ФЗ "Об электронной подписи" электронной подписью.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.2 Оператор персональных данных

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

На официальном портале Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, уполномоченного органа по защите прав субъектов персональных данных, в разделе персональных данных можно осуществить поиск оператора персональных данных по существующему реестру, который содержит в себе информацию о всех зарегистрированных операторах, осуществляющих обработку персональных данных.

В организации могут быть назначены лица, ответственные за организацию обработки персональных данных:

- оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных;
- лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему;
- оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных";
- лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

    - осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
    - доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных,

локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.3 Обязанности оператора при обработке персональных данных

В соответствии с положениями 152 федерального закона, оператор при сборе персональных данных обязан:

а) Предоставить субъекту персональных данных по его просьбе следующую информацию:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных";
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

б) Разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление

персональных данных является обязательным в соответствии с федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных".

в) Предоставить субъекту персональных данных до начала обработки таких персональных данных, в случае, если персональные данные получены не от субъекта персональных данных, следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных;
- источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

В случае получения обращения и\или запроса со стороны субъекта персональных данных (или его представителя) или уполномоченного органа по защите прав субъектов персональных данных, оператор обязан:

- сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", субъекту персональных данных или его представителю информацию о наличии

персональных данных, относящихся к соответствующему субъекту персональных данных,

- предоставить возможность ознакомления с персональными данными относящихся к соответствующему субъекту персональных данных, при обращении субъекта персональных данных или его представителя, либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;
- дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных" закона или иного федерального закона, который являлся основанием в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;
- безвозмездно предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- внести изменения в персональные данные в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются неполными, неточными или неактуальными;
- уничтожить персональные данные в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;
- сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

В случае нарушения законодательства при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных оператор обязан:

- осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных, в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных;
- осуществить блокирование персональных данных, относящихся к субъекту персональных данных, в случае выявления в них неточностей при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;
- уточнить персональные данные и снять блокирование либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных в течение семи рабочих дней со дня представления таких сведений;
- прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора, в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;
- уничтожить персональные данные или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, в случае, если обеспечить правомерность обработки таких персональных данных невозможно;
- уведомить субъекта персональных данных или его представителя, об устранении допущенных нарушений или об уничтожении персональных данных, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, уведомить указанный орган;
- прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется

другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае достижения цели обработки персональных данных. Данные действия должны быть реализованы в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" или другими федеральными законами;

- прекратить обработку персональных данных или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами;
- уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных. Данные действия должны быть реализованы в срок, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами;
- осуществить блокирование персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отсутствия возможности уничтожения таких персональных данных в

течение срока, указанного в частях 3 – 5 статьи 21 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", и обеспечить уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Также в Федеральном законе от 27.07.2006 N 152–ФЗ "О персональных данных" отдельно оговорены обязанности оператора по уведомлению об обработке персональных данных. До начала обработки персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

– оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

  - обрабатываемых в соответствии с трудовым законодательством;
  - полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
  - относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых 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 или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;
  - сделанных субъектом персональных данных общедоступными;
  - включающих в себя только фамилии, имена и отчества субъектов персональных данных;
  - необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
  - включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
- обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

– уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

- уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 статьи 22 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными;
- на оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов;
- в случае предоставления неполных или недостоверных сведений, указанных в части 3 статьи 22 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", 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, указанных в части 3 статьи 22 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

2.4 Меры по обеспечению выполнения оператором своих обязанностей

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных":

- оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено

Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" или другими федеральными законами. К таким мерам могут, в частности, относиться:

- назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
- издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных";
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;
- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

– оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
– оператор, осуществляющий сбор персональных данных с использованием информационно–телекоммуникационных сетей,

обязан опубликовать в соответствующей информационно–телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно–телекоммуникационной сети;

- Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами;
- оператор обязан представить документы и локальные акты, указанные в части 1 статьи 18.1 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных" настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 статьи 18.1 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", по запросу уполномоченного органа по защите прав субъектов персональных данных.

2.5 Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Обеспечение безопасности персональных данных достигается, в частности:

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

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

Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 статьи 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных" требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области

противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно–правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки;

Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

Проекты нормативных правовых актов, указанных в части 5 статьи 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 статьи 19 Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных", подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным;

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в

соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных;

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных;

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения;

Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Контрольные вопросы:

1. Укажите, какими международными нормативными документами регламентируются вопросы, связанные с персональными данными.
2. В каком году Российская Федерация ратифицировала Европейскую конвенцию по правам человека?
3. Перечислите основные положения Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных".
4. Что такое персональные данные?
5. Что относится к специальным категориям персональных данных?
6. Укажите основополагающие принципы обработки персональных данных.
7. В каком году в Российской Федерации был принят Федеральный закон от 27.07.2006 N 152–ФЗ "О персональных данных"?
8. Перечислите, какую минимальную информацию обязан предоставить оператор персональных данных субъекту персональных данных или его законному представителю согласно положениям Директивы ЕС?
9. Перечислите, какую минимальную информацию обязан предоставить оператор персональных данных субъекту персональных данных или его законному представителю согласно положениям Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных".
10. При каком условии оператор персональных данных может начать осуществлять обработку персональных данных?
11. Существуют ли временные ограничения на обработку персональных данных?
12. В каких случая оператор персональных данных не может осуществлять их обработку?

3. Нарушители безопасности персональных данных

3.1 Классификация нарушителей безопасности информационных систем персональных данных

В условиях современных тенденций функционирования организаций большинство работников во время исполнения служебных обязанностей так или иначе сталкиваются с информацией ограниченного доступа, что делает их как объектом, так и субъектом информационных угроз. То есть одним из немаловажных факторов, который необходимо учитывать при построении системы защиты информации на предприятии в общем, и системы защиты персональных данных в частности, является человеческий фактор. Для этого необходимо обеспечить:

1. Правильный подход к подбору персонала и дальнейшую организацию работы с ним, включая:

   - проведение семинаров и инструктажей по общим вопросам и правилам обработки информации ограниченного доступа, в том числе и персональных данных;
   - повышение общего уровня знаний и компетенции каждого сотрудника по вопросам обеспечения информационной безопасности в организации;
   - формирование наиболее благоприятных рабочих условий, отвечающих требованиям внешних и внутренних нормативных документов в сфере защиты информации и персональных данных;
   - формирование единой корпоративной культуры по вопросам обеспечения информационной безопасности в организации, с доведением до сведения персонала о возможных последствиях нарушения данной корпоративной культуры.

2. Организацию контролируемой зоны, включая:

   - определение границ контролируемой зоны;
   - определение мер и средств физической защиты информации;
   - определение мер и средств технической защиты информации;
   - организация КПП в организации;
   - организация пропускного режима;
   - регламентацию работы и допуска персонала к защищаемой информации, в том числе и персональных данных;

– формирования правил учета лиц, получивших доступ к работе с информацией ограниченного доступа, в том числе и персональных данных.

Согласно положениям «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК РФ 15.02.2008, контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

В случае, если получение информации ограниченного доступа происходит в обход правил предоставления доступа, лица, получившие такую информацию, являются нарушителями информационной безопасности.

Нарушитель информационной безопасности, согласно положениям ГОСТ Р 53114–2008 – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

По наличию права постоянного, временного или разового доступа в контролируемую зону нарушители подразделяются на два типа:

1. Нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители.
2. Нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Внешними нарушителями могут быть:

– разведывательные службы государств;
– криминальные структуры;
– конкуренты (конкурирующие организации);
– недобросовестные партнеры;
– внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

– осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
– осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры информационной системы персональных данных, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к информационной системе персональных данных.

3.2 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно–технических мер защиты, в том числе по допуску физических лиц к персональным данным и контролю порядка проведения работ. Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к персональным данным.

К первой категории относятся лица, имеющие санкционированный доступ к информационной системе персональных данных, но не имеющие доступа к персональным данным. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование информационной системы персональных данных. Лицо этой категории может:

- иметь доступ к фрагментам информации, содержащей персональные данные и распространяющейся по внутренним каналам связи информационной системы персональных данных;
- располагать фрагментами информации о топологии информационной системы персональных данных (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;
- располагать именами и вести выявление паролей зарегистрированных пользователей;
- изменять конфигурацию технических средств информационной системы персональных данных, вносить в нее программно–аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам информационной системы персональных данных.

Ко второй категории относятся зарегистрированные пользователи информационной системы персональных данных, осуществляющие ограниченный доступ к ресурсам информационной системы персональных данных с рабочего места. Лицо этой категории:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;
- располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству персональных данных должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи информационной системы персональных данных, осуществляющие удаленный доступ к персональным данным по локальным и (или) распределенным информационным системам. Лицо этой категории:

- обладает всеми возможностями лиц первой и второй категорий;
- располагает информацией о топологии информационной системы персональных данных на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств информационной системы персональных данных;
- имеет возможность прямого (физического) доступа к фрагментам технических средств информационной системы персональных данных.

К четвертой категории относятся зарегистрированные пользователи информационной системы персональных данных с полномочиями администратора безопасности сегмента (фрагмента) информационной системы персональных данных. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) информационной системы персональных данных;
- обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) информационной системы персональных данных;

- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) информационной системы персональных данных;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) информационной системы персональных данных;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) информационной системы персональных данных.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора информационной системы персональных данных. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;
- обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных;
- имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;
- обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

Системный администратор выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от несанкционированного доступа.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности информационной системы персональных данных. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией об информационной системе персональных данных;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы персональных данных;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты–разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на информационной системе персональных данных;
- обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии информационной системе персональных данных и технических средствах обработки и защиты персональных данных, обрабатываемых в информационной системе персональных данных.
- К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на информационную систему персональных данных.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на информационную систему персональных данных. Лицо этой категории:

- обладает возможностями внесения закладок в технические средства информационной системы персональных данных на стадии их разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии информационной системы персональных данных и технических средствах обработки и защиты информации в информационной системе персональных данных.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации угрозы безопасности персональных данных.

Таким образом видно, что при должной мотивации нарушителем безопасности персональных данных может быть любой человек включая сотрудников организации. Исключить полностью данный фактор невозможно, но при хорошо организованной работе с персоналом, а также совокупности других организационных и технических мер, можно минимизировать вероятность его возникновения.

Контрольные вопросы:

1. Дайте определение понятию «Нарушитель информационной безопасности».
2. Какие типы нарушителей информационной безопасности существуют согласно действующим правилам разграничения доступа к информации?
3. На сколько категорий делится внутренний нарушитель информационной безопасности и по каким критериям?
4. Укажите, кто относится к первой категории внутренних нарушителей безопасности информации.
5. Укажите, кто относится ко второй категории внутренних нарушителей безопасности информации.
6. Укажите, кто относится к третьей категории внутренних нарушителей безопасности информации.
7. Укажите, кто относится к четвертой категории внутренних нарушителей безопасности информации.
8. Укажите, кто относится к пятой категории внутренних нарушителей безопасности информации.
9. Укажите, кто относится к шестой категории внутренних нарушителей безопасности информации.
10. Укажите, кто относится к седьмой категории внутренних нарушителей безопасности информации.
11. Укажите, кто относится к восьмой категории внутренних нарушителей безопасности информации.
12. Какими возможностями обладают лица, отнесенные к первой категории внутренних нарушителей?
13. Какими возможностями обладают лица, отнесенные ко второй категории внутренних нарушителей?
14. Какими возможностями обладают лица, отнесенные к третьей категории внутренних нарушителей?
15. Какими возможностями обладают лица, отнесенные к четвертой категории внутренних нарушителей?
16. Какими возможностями обладают лица, отнесенные к пятой категории внутренних нарушителей?
17. Какими возможностями обладают лица, отнесенные к шестой категории внутренних нарушителей?
18. Какими возможностями обладают лица, отнесенные к седьмой категории внутренних нарушителей?
19. Какими возможностями обладают лица, отнесенные к восьмой категории внутренних нарушителей?
20. Что такое информационная система персональных данных?

4. Государственные регуляторы и их нормативно-правовая документация в области защиты персональных данных

4.1 Государственные органы исполнительной власти, осуществляющие надзор за соблюдением требований законодательства в области обработки персональных данных

Контроль за соблюдением установленных требований является неотъемлемой частью всего общего процесса обработки персональных данных, и для должной реализации данной процедуры в законодательной базе Российской Федерации определены необходимые регламентирующие документы. В данных документах прописаны требования, которые являются обязательными для соблюдения операторами при осуществлении обработки персональных данных. Проверка реализации необходимых требований, в области защиты персональных данных, является одной из обязанностей государственных регулирующих органов, таких как:

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- Федеральная служба по техническому и экспортному контролю;
- Федеральная служба безопасности Российской Федерации.

Полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Служба) определены Постановлением Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций".

Согласно данному постановлению Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций с целью реализации полномочий в установленной сфере ведения имеет право:

- запрашивать и получать в установленном порядке сведения, необходимые для принятия решений по вопросам, отнесенным к компетенции Службы;
- проводить необходимые расследования, испытания, экспертизы, анализы и оценки, а также научные исследования по вопросам, отнесенным к компетенции Службы;
- привлекать в установленном порядке для проработки вопросов, отнесенных к компетенции Службы, научные и иные организации, а также ученых и специалистов;

- давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к компетенции Службы;
- применять меры профилактического и пресекательного характера, направленные на недопущение нарушений юридическими лицами и гражданами обязательных требований в этой сфере и (или) ликвидацию последствий таких нарушений, в порядке и в случаях, которые установлены законодательством Российской Федерации;
- создавать совещательные и экспертные органы (советы, комиссии, группы и коллегии), в том числе межведомственные, в установленной сфере ведения;
- осуществлять контроль за деятельностью территориальных органов Службы, а также за деятельностью подведомственных организаций;
- утверждать образцы служебных удостоверений;
- привлекать к формированию и ведению единого реестра оператора единого реестра - организацию, зарегистрированную на территории Российской Федерации, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации.

Федеральная служба по техническому и экспортному контролю (далее - ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. Полномочия данной Службы приведены в указе Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю". В соответствии с данным документом ФСТЭК России в целях реализации своих полномочий в сфере обработки персональных данных имеет право:

- вносить в установленном порядке Президенту Российской Федерации, в Правительство Российской Федерации и Совет Безопасности Российской Федерации предложения по нормативно-правовому регулированию в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также в области экспортного контроля;
- осуществлять контроль деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти (в Минобороны России, СВР России, ФСБ России, ФСО России и ГУСПе - по согласованию с руководителями указанных органов), в органах исполнительной власти

субъектов Российской Федерации, органах местного самоуправления и организациях, определять порядок, формы и методы осуществляемого в пределах своей компетенции контроля;

- контролировать с применением технических средств эффективность защиты:

  - объектов, на которых выполняются работы, связанные со сведениями, составляющими государственную и (или) служебную тайну;
  - образцов вооружения и военной техники при их разработке, производстве и полигонных испытаниях (военных объектов, образцов вооружения и военной техники при испытаниях на полигонах Минобороны России - по согласованию с Минобороны России, а на полигонах, находящихся в иностранных государствах, - и по согласованию с СВР России);
  - информации в ключевых системах информационной инфраструктуры, в информационных системах, в средствах и системах связи и управления, в том числе от специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней (в отношении технических средств и систем Минобороны России, СВР России, ФСБ России, ФСО России и ГУСПа, а также объектов и технических средств федеральных органов государственной власти, защита которых входит в их компетенцию, - по согласованию с руководителями указанных органов).

- осуществлять радиоконтроль за соблюдением установленного порядка передачи служебной информации должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную и\или служебную тайну, при использовании открытых каналов радио-, радиорелейных, тропосферных, спутниковых и других линий и сетей радиосвязи, доступных для радиоразведки;
- осуществлять мониторинг безопасности информации в ключевых системах информационной инфраструктуры;
- осуществлять контроль за организацией противодействия техническим разведкам и технической защиты информации при проведении мероприятий по мобилизационной подготовке и мобилизации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;
- выдавать предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций в случае выявления в ходе

осуществления контроля нарушений норм и требований, касающихся противодействия техническим разведкам и технической защиты информации;

- запрашивать и получать от федеральных органов исполнительной власти, иных государственных органов, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, а также от организаций и должностных лиц необходимые для осуществления деятельности ФСТЭК России информацию, документы и материалы, в том числе добытые по специальным каналам;
- приостанавливать или отменять действие выданных сертификатов;
- вносить в установленном порядке представления о применении мер ответственности за нарушения законодательства Российской Федерации по вопросам ее деятельности;
- рассматривать в пределах своей компетенции дела об административных правонарушениях;
- издавать в пределах своей компетенции нормативные правовые акты, методические документы и индивидуальные правовые акты;
- отказывать при наличии соответствующих оснований в выдаче лицензий, осуществлять контроль за соблюдением соответствующих лицензионных требований и условий организациями, имеющими лицензии ФСТЭК России, при осуществлении ими лицензируемых видов деятельности, приостанавливать в установленном порядке действие выданных лицензий;
- заслушивать на заседаниях коллегии ФСТЭК России должностных лиц, уполномоченных руководителями федеральных органов исполнительной власти, по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также должностных лиц, ответственных за организацию противодействия техническим разведкам и технической защиты информации в органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях.

Федеральная служба безопасности Российской Федерации (далее - ФСБ России) является федеральным органом исполнительной власти, в пределах своих полномочий осуществляющим государственное управление в области обеспечения безопасности Российской Федерации, борьбы с терроризмом, защиты и охраны государственной границы Российской Федерации, охраны внутренних морских вод, территориального моря, исключительной экономической зоны, континентального шельфа Российской Федерации и их природных ресурсов, обеспечивающим информационную безопасность Российской Федерации и непосредственно реализующим основные направления деятельности органов федеральной службы безопасности, определенные законодательством Российской Федерации, а также координирующим

контрразведывательную деятельность федеральных органов исполнительной власти, имеющих право на ее осуществление. Основными задачами ФСБ России являются:

- координация осуществляемых федеральными органами исполнительной власти контрразведывательных мероприятий и мер по обеспечению собственной безопасности, включая защиту персональных данных;
- организация выявления, предупреждения, пресечения и раскрытия преступлений, включая нарушения законодательства в сфере информационной безопасности и защиты персональных данных, осуществление досудебного производства по которым отнесено к ведению органов безопасности;
- обеспечение производства по делам об административных правонарушениях, рассмотрение которых отнесено Кодексом Российской Федерации об административных правонарушениях к ведению органов безопасности;
- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности.

4.2 Нормативно-правовая документация государственных органов исполнительной власти, осуществляющих надзор за соблюдением требований законодательства в области обработки персональных данных

Нормативно-правовая база в Российской Федерации является основным источником, регламентирующим вопросы порядка обработки персональных данных. В данной области можно выделить следующий перечень документов:

- Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
- Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных"
- Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"

- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"
- "Трудовой Кодекс Российской Федерации" (ТК РФ) от 30.12.2001 N 197-ФЗ статья 89
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год
- Приказ ФСТЭК России от 31 августа 2010 г. N 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 N 149/54-144)
- «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203)
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 N 149/6/6-622)

Каждый из данных документов позволяет операторам наиболее правильно реализовать меры по организации работ с персональными данными.

В зависимости от того, является ли организация, осуществляющая работу с информацией конфиденциального характера, в том числе и персональными данными, государственной или негосударственной, меры соблюдаемые при организации процесса работы с персональными данными, будут различаться. Органы государственной власти при осуществлении своей деятельности должны руководствоваться приказом ФСТЭК России от 11.02.2013 N 17. Негосударственные организации - приказом ФСТЭК России от 18.02.2013 N 21. В этих документах рассмотрены меры по обеспечению безопасности

персональных данных, которые должны приниматься для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения такой информации, а также от иных неправомерных действий в отношении персональных данных.

Существующие меры, направленные на предотвращение актуальных угроз должны быть реализованы в соответствии с требованиями к защите персональных данных при их обработке в информационных системах, которые утверждены постановлением Правительства Российской Федерации от 01.11.2012г. N 1119. В данном постановлении также определены уровни защищенности персональных данных.

Также основной перечень мер, направленных на обеспечение выполнение обязанностей, для государственных организаций, предусмотренный Федеральным законом от 27.07.2006 N 152-ФЗ, указан в постановлении Правительства РФ от 21.03.2012 N 211.

В случае, если обработка информации должна происходить без использования средств автоматизации и осуществляется при непосредственном участии человека, Оператор должен руководствоваться положениями, указанными в постановлении Правительства Российской федерации от 15.09.2008 г. N 687. В данном документе указаны особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации, в частности:

- правила фиксации персональных данных на материальных носителях;
- правила ознакомления лиц, осуществляющих обработку персональных данных без использования средств автоматизации, с их обязанностями;
- условия, которые должны быть соблюдены, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных;
- условия, которые должны быть соблюдены, при ведении журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор;
- меры по обеспечению раздельной обработки персональных данных, которые должны быть приняты при несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных отдельно от других зафиксированных на том же носителе персональных данных;
- порядок уничтожения, обезличивания персональных данных, обрабатываемых без использования средств автоматизации;

- порядок уточнения персональных данных, обрабатываемых без использования средств автоматизации;
- меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Чтобы снизить уровень защищенности информационной системы персональных данных, а соответственно упростить требования, предъявляемые к организации системы защиты обработки, Оператор может провести процедуру по обезличиванию такой информации. Данная необходимость может появиться в случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей. Также обезличивание персональных данных происходит при необходимости обработки такой информации в статистических или иных исследовательских целях. Согласно Федеральному закону от 27.07.2006 N 152-ФЗ, обезличивание персональных данных – это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Для проведения данной процедуры Оператор, осуществляющий обработку информации ограниченного доступа, в том числе персональных данных, должен руководствоваться положениями приказа Роскомнадзора от 05.09.2013 N 996, где рассмотрены следующие требования и методы по обезличиванию персональных данных:

- свойства обезличенных данных;
- характеристика методов обезличивания персональных данных;
- требования к методам обезличивания;
- требования к свойствам получаемых обезличенных данных;
- требования к свойствам методов обезличивания;
- метод введения идентификаторов;
- метод изменения состава или семантики;
- метод декомпозиции;
- метод перемешивания.

После проведения процедуры обезличивания персональных данных появляется возможность их использования для целей организации без запроса согласия субъекта на обработку такой информации.

При проектировании системы защиты информации Оператор должен иметь представления о возможных угрозах безопасности персональных данных при процессе их обработки в информационных системах. Для этих целей был разработан документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год». В нем содержится систематизированный перечень угроз, которые обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или

организаций, а также криминальных группировок, создающих условия для нарушения безопасности персональных данных, которое ведет к ущербу жизненно важных интересов личности, общества и государства. В частности, в данном документе рассмотрены:

- классификация угроз безопасности персональных данных;
- угрозы утечки информации по техническим каналам:
  - угрозы утечки акустической (речевой) информации;
  - угрозы утечки видовой информации;
  - угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.
- угрозы несанкционированного доступа к информации в информационной системе персональных данных:
  - общая характеристика источников угроз несанкционированного доступа в информационной системе персональных данных;
  - общая характеристика уязвимостей информационной системы персональных данных:
    a. общая характеристика уязвимостей системного программного обеспечения;
    b. общая характеристика уязвимостей прикладного программного обеспечения;
  - общая характеристика угроз непосредственного доступа в операционную среду информационной системы персональных данных;
  - общая характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия;
  - общая характеристика угроз программно-математических воздействий;
  - общая характеристика нетрадиционных информационных каналов;
  - общая характеристика результатов несанкционированного или случайного доступа.
- типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных:
  - типовая модель угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

- типовая модель угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности персональных данных, обрабатываемых в локальных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности персональных данных обрабатываемых в локальных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Применение модели угроз позволяет решить следующие задачи:

- разработка частных моделей угроз безопасности персональных данных в конкретных информационных систем персональных данных с учетом их назначения, условий и особенностей функционирования;
- анализ защищенности информационной системы персональных данных от угроз безопасности персональных данных в ходе организации и выполнения работ по обеспечению безопасности такой информации;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты такой информации, предусмотренных для соответствующего класса информационной системы персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональных данных и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы персональных данных, в результате которого может быть нарушено их функционирование;

– контроль обеспечения уровня защищенности персональных данных.

Также при построении модели угроз Оператор должен руководствоваться «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.» ФСТЭК России, 2008 год. В данном документе определен порядок выявления актуальных угроз безопасности персональных данных в информационных системах персональных данных.

4.3 Обеспечение выполнение мер, утвержденных постановлением Правительства Российской Федерации от 21.03.2012 г. N 211

Данный документ предназначен для государственных или муниципальных органов при создании организационной системы защиты информации, в том числе и персональных данных. В нем указаны меры, направленные на обеспечение выполнения обязанностей операторами, которые предусмотрены Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", по результатам реализации которых должен быть составлен комплект организационно-распорядительной документации, утвержденной актом руководителя, и формализующей политику в части обработки персональных данных внутри организации.

К таким мерам относятся:

– назначение ответственного за организацию обработки персональных данных из числа служащих. Для этого создается инструкция ответственного за организацию обработки персональных данных в информационных системах, в которой прописаны обязанности данного ответственного лица, его права, ответственность, действия данного лица при нештатных ситуациях. Также к данному документу прилагается лист ознакомления с настоящей инструкцией;
– формализация правил обработки персональных данных, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в сфере персональных данных. Данная мера реализуется за счет написания положения о персональных данных, обрабатываемых в организации. В нем указаны цели обработки персональных данных, содержание таких данных, категории субъектов обрабатываемых персональных данных, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, права и обязанности работника и работодателя в области обработки персональных данных работника, ответственность за нарушение данного положения;

- ведение журнала обращений субъектов персональных данных или их представителей. Такой журнал должен содержать в себе дату, данные субъекта, цель обращения и перечень используемых сведений;
- определение правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленными Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных". Для этого утверждается план внутренних проверок режима обработки информации ограниченного доступа, в котором указаны все мероприятия, их периодичность, а также лица, ответственные за их проведение вместе с журналом учета мероприятий по контролю за соблюдением требований по обработке информации ограниченного доступа (персональных данных);
- регламентация правил работы с обезличенными данными внутри организации осуществляется при помощи инструкции, в которой прописаны: порядок обезличивания персональных данных, обязанности сотрудника, допущенного к работе с такой информацией, его ответственность, также должен прилагаться лист ознакомления с положениями данного документа;
- ведения перечня информационных систем персональных данных. В нем должны быть рассмотрены следующие пункты: наименование системы, цель создания системы, эксплуатирующее подразделение и, при необходимости, примечания;
- ведение перечня персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций, с указанием: содержания персональных данных, местом хранения, местом обработки и списком лиц, допущенных к работе с такой информацией;
- ведение перечня должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных вместе с приказом руководителя о назначении ответственных лиц;
- ведение перечня должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- регламентация обязанностей ответственного лица за организацию обработки персональных данных, а также его прав и действий в случае наступления нештатной ситуации прописана в должностной инструкции ответственного за организацию обработки персональных данных в государственном или муниципальном органе;
- формализация типового обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку

персональных данных, в случае расторжения с ним государственного или муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей. Для этого предусмотрено соглашение о неразглашении персональных данных, при подписании которых сотрудник принимает на себя обязательства по неразглашению информации ограниченного доступа;

- формализация типовой формы согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные. Согласие вступает в силу с момента его подписания на срок действия трудового договора с организацией и в течение трех лет после окончания срока действия трудового договора и может быть отозвано путем подачи письменного заявления со стороны сотрудника;
- регламентация порядка доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных. Данные помещения определены приказом об определении помещений, предназначенных для обработки информации ограниченного доступа, где указаны помещения и лица, ответственные за организацию обработки информации ограниченного доступа в этих помещениях, приказом об утверждении списка лиц, имеющих право вскрытия и закрытия помещений, в которых обрабатывается информация ограниченного доступа, а также приказом о назначении должностных лиц, допущенных к обработке информации ограниченного доступа вместе с журналом учета лиц (организаций), получивших доступ к информации ограниченного доступа;
- регламентация правил обработки персональных данных без использования средств автоматизации. Данные положения прописываются в инструкции по обработке персональных данных, осуществляемой без использования средств автоматизации, в организации. В ней определяются: порядок обработки персональных данных, обязанности сотрудника, допущенного к обработке персональных данных, а также ответственность, которая наступает в случае несоблюдения установленных правил. К данном документу прилагается лист ознакомления;
- определение порядка ознакомления служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных. Данное требование утверждается

приказом руководителя, где определен обязательный перечень информации для ознакомления, а также ответственные лица;
- организация регламента уведомления уполномоченного органа по защите прав субъекта персональных данных об обработке такой информации;
- формирование документов, определяющих политику в отношении обработки персональных данных, с дальнейшим опубликованием на официальном сайте государственного или муниципального органа в течении 10 дней после их утверждения.

Данные документы должны быть утверждены актом руководителя государственного или муниципального органа.

Контрольные вопросы:

1. Что такое модель угроз безопасности персональных данных?
2. О чем говорится в постановлении Правительства РФ от 21.03.2012 N 211?
3. Какие основные задачи призвана решать модель угроз безопасности персональных данных?
4. Укажите, какими документами необходимо пользоваться в случае необходимости построения модели угроз безопасности персональных данных?
5. Укажите, какими документами необходимо пользоваться в случае необходимости построения модели угроз безопасности персональных данных, с использованием средств шифрования?
6. Какими возможностями обладает Федеральная Служба Безопасности Российской Федерации в части решения вопросов по защите и обработке персональных данных?
7. Какими возможностями обладает Федеральная Служба Технического и Экспертного Контроля Российской Федерации в части решения вопросов по защите и обработке персональных данных?
8. Укажите название органа исполнительной власти Российской Федерации уполномоченного по вопросам защиты законных интересов субъектов персональных данных?
9. В какой период времени должны быть опубликованы на официальном сайте государственного или муниципального органа документы, определяющие политику в отношении обработки персональных данных?
10. Какие документы по защите и обработке персональных данных должны быть опубликованы на официальном сайте государственного или муниципального органа в соответствии с положениями постановления Правительства РФ от 21.03.2012 N 211?

5. Осуществление проверки соблюдения правил в области защиты персональных данных и ответственность за их нарушение

5.1 Контроль за соблюдением требований законодательства в области защиты персональных данных

Контроль за соблюдением установленных требований является неотъемлемой частью процесса обработки персональных данных. На территории Российской Федерации функции контроля за соблюдением требований законодательств в области защиты персональных данных выполняют следующие уполномоченные органы государственной власти:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций. В его функции входит рассмотрение обращений субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принятия соответствующего решения.

Уполномоченный орган по защите прав субъектов персональных данных обладает следующими правами и обязанностями:

- уполномоченный орган по защите прав субъектов персональных данных имеет право:
  - запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
  - осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления

такой проверки иные государственные органы в пределах их полномочий;

- требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;
- направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, следующие сведения:

    a. описание мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных»;
    b. описание мер по обеспечению безопасности персональных данных при их обработке, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств.

- 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;
- 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;

- вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;
- привлекать к административной ответственности лиц, виновных в нарушении Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

– 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:

- организовывать в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» и других федеральных законов защиту прав субъектов персональных данных;
- 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;
- вести реестр операторов;
- осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;
- 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;
- информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;
- выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.2 Лицензирование деятельности по технической защите конфиденциальной информации

В зависимости от деятельности осуществляемой организацией определяется необходимость получения лицензии в соответствии с Федеральным законом «О

лицензировании отдельных видов деятельности» от 04.05.2011 N 99-ФЗ. В части 1 статьи 12 данного законодательного акта указаны все лицензируемые виды деятельности организаций, к которым относятся:

- разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и производство средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- производство и реализация защищенной от подделок полиграфической продукции;
- разработка, производство, испытание и ремонт авиационной техники;
- разработка, производство, испытание, установка, монтаж, техническое обслуживание, ремонт, утилизация и реализация вооружения и военной техники;
- разработка, производство, испытание, хранение, ремонт и утилизация гражданского и служебного оружия и основных частей огнестрельного оружия, торговля гражданским и служебным оружием и основными частями огнестрельного оружия;
- разработка, производство, испытание, хранение, реализация и утилизация боеприпасов (в том числе патронов к гражданскому и служебному оружию и составных частей патронов), пиротехнических изделий IV и V классов в соответствии с национальным стандартом, применение пиротехнических изделий IV и V классов в соответствии с техническим регламентом;

- деятельность по хранению и уничтожению химического оружия;
- эксплуатация взрывопожароопасных и химически опасных производственных объектов I, II и III классов опасности;
- деятельность по тушению пожаров в населенных пунктах, на производственных объектах и объектах инфраструктуры, по тушению лесных пожаров (за исключением деятельности добровольной пожарной охраны);
- деятельность по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений;
- производство лекарственных средств;
- производство и техническое обслуживание (за исключением случая, если техническое обслуживание осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) медицинской техники;
- оборот наркотических средств, психотропных веществ и их прекурсоров, культивирование наркосодержащих растений;
- деятельность в области использования возбудителей инфекционных заболеваний человека и животных (за исключением случая, если указанная деятельность осуществляется в медицинских целях) и генно-инженерно-модифицированных организмов III и IV степеней потенциальной опасности, осуществляемая в замкнутых системах;
- деятельность по перевозкам внутренним водным транспортом, морским транспортом пассажиров;
- деятельность по перевозкам внутренним водным транспортом, морским транспортом опасных грузов;
- деятельность по перевозкам воздушным транспортом пассажиров (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по перевозкам воздушным транспортом грузов (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по перевозкам пассажиров автомобильным транспортом, оборудованным для перевозок более восьми человек (за исключением случая, если указанная деятельность осуществляется по заказам либо для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по перевозкам железнодорожным транспортом пассажиров;
- деятельность по перевозкам железнодорожным транспортом опасных грузов;

- погрузочно-разгрузочная деятельность применительно к опасным грузам на железнодорожном транспорте;
- погрузочно-разгрузочная деятельность применительно к опасным грузам на внутреннем водном транспорте, в морских портах;
- деятельность по осуществлению буксировок морским транспортом (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по обезвреживанию и размещению отходов I - IV классов опасности;
- деятельность по организации и проведению азартных игр в букмекерских конторах и тотализаторах;
- частная охранная деятельность;
- частная детективная (сыскная) деятельность;
- заготовка, хранение, переработка и реализация лома черных металлов, цветных металлов;
- оказание услуг по трудоустройству граждан Российской Федерации за пределами территории Российской Федерации;
- оказание услуг связи;
- телевизионное вещание и радиовещание;
- деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование данных объектов авторских и смежных прав в силу федерального закона или договора);
- деятельность в области использования источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности);
- образовательная деятельность (за исключением указанной деятельности, осуществляемой частными образовательными организациями, находящимися на территории инновационного центра «Сколково»);
- космическая деятельность;
- геодезические и картографические работы федерального назначения, результаты которых имеют общегосударственное, межотраслевое значение (за исключением указанных видов деятельности, осуществляемых в ходе инженерных изысканий, выполняемых для подготовки проектной документации, строительства, реконструкции, капитального ремонта объектов капитального строительства);
- производство маркшейдерских работ;
- работы по активному воздействию на гидрометеорологические и геофизические процессы и явления;

- деятельность в области гидрометеорологии и в смежных с ней областях (за исключением указанной деятельности, осуществляемой в ходе инженерных изысканий, выполняемых для подготовки проектной документации, строительства, реконструкции объектов капитального строительства);
- медицинская деятельность (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра «Сколково»);
- фармацевтическая деятельность;
- деятельность по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации;
- деятельность по проведению экспертизы промышленной безопасности;
- деятельность, связанная с обращением взрывчатых материалов промышленного назначения.

Порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями, которая не содержит сведения, составляющие государственную тайну, регламентирован Постановлением Правительства РФ от 03.02.2012 N 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

На территории Российской Федерации уполномоченным органом, осуществляющим лицензирование деятельности по технической защите конфиденциальной информации, является Федеральная служба по техническому и экспортному контролю.

В данном случае под технической защитой конфиденциальной информации понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:

- контроль защищенности конфиденциальной информации от утечки по техническим каналам в:

    - средствах и системах информатизации;
    - технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

- помещениях со средствами (системами), подлежащими защите;
- помещениях, предназначенных для ведения конфиденциальных переговоров;

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
– сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);
– аттестационные испытания и аттестация на соответствие требованиям по защите информации:

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- помещениях, предназначенных для ведения конфиденциальных переговоров.

– проектирование в защищенном исполнении:

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- помещениях, предназначенных для ведения конфиденциальных переговоров.

– установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

К соискателю лицензии на осуществление деятельности по технической защите конфиденциальной информации предъявляются следующие требования:

- наличие у соискателя лицензии на осуществление деятельности по технической защите конфиденциальной информации:

  - юридического лица - специалистов, находящихся в штате соискателя лицензии, имеющих высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
  - индивидуального предпринимателя - высшего профессионального образования в области технической защиты информации либо высшего технического или среднего профессионального (технического) образования при условии прохождения им переподготовки или повышения квалификации по вопросам технической защиты информации.

- наличие помещений для осуществления лицензирования деятельности по технической защите конфиденциальной информации, соответствующих установленным законодательством Российской Федерации техническим нормам и требованиям по технической защите информации и принадлежащих соискателю лицензии на праве собственности или на ином законном основании;
- наличие на праве собственности или на ином законном основании контрольно-измерительного оборудования (прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку) и маркирование), производственного и испытательного оборудования, соответствующего требованиям по техническим характеристикам и параметрам, устанавливаемым Федеральной службой по техническому и экспортному;
- наличие на праве собственности или на ином законном основании средств контроля защищенности информации от несанкционированного доступа, сертифицированных по требованиям безопасности информации, в соответствии с перечнем, утверждаемым Федеральной службой по техническому и экспортному контролю;
- наличие автоматизированных систем, предназначенных для обработки конфиденциальной информации, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
- наличие предназначенных для осуществления лицензируемого вида деятельности программ для электронно-вычислительных машин и баз

данных, принадлежащих соискателю лицензии на праве собственности или на ином законном основании;

- наличие технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, в соответствии с утверждаемым Федеральной службой по техническому и экспортному контролю перечнем и принадлежащих соискателю лицензии на праве собственности или на ином законном основании;
- наличие системы производственного контроля в соответствии с установленными стандартами.

Для получения лицензии соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:

- заявление о предоставлении лицензии, документы (копии документов):
  - копии учредительных документов юридического лица, засвидетельствованные в нотариальном порядке;
  - опись прилагаемых документов.
- копии документов, подтверждающих квалификацию специалистов по защите информации (дипломов, удостоверений, свидетельств);
- копии правоустанавливающих документов на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);
- копии технических паспортов и аттестатов соответствия защищаемых помещений требованиям безопасности информации;
- копии технических паспортов автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации, планов размещения основных и вспомогательных технических средств и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации, а также перечень защищаемых в автоматизированных системах ресурсов, описание технологического процесса обработки информации в автоматизированных системах;

- копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;
- документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;
- документы, содержащие сведения об имеющихся технической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных частью 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации;
- копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами.

К лицензионным требованиям, которые предъявляются к лицензиату при осуществлении лицензируемого вида деятельности, относится:

- выполнение работ и (или) оказание услуг лицензиатом:

  - юридическим лицом - с привлечением специалистов, находящихся в штате лицензиата, имеющих высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
  - индивидуальным предпринимателем - при наличии у него высшего профессионального образования в области технической защиты информации либо высшего технического или среднего профессионального (технического) образования и при условии прохождения переподготовки или повышения квалификации по вопросам технической защиты информации.

- наличие помещений для осуществления лицензируемого вида деятельности, соответствующих установленным законодательством Российской Федерации техническим нормам и требованиям по

технической защите информации и принадлежащих лицензиату на праве собственности или на ином законном основании;

- использование на праве собственности или на ином законном основании контрольно-измерительного оборудования (прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку) и маркирование), производственного и испытательного оборудования, соответствующего требованиям по техническим характеристикам и параметрам, устанавливаемым Федеральной службой по техническому и экспортному контролю;
- использование на праве собственности или на ином законном основании средств контроля защищенности информации от несанкционированного доступа, сертифицированных по требованиям безопасности информации, в соответствии с перечнем, утверждаемым Федеральной службой по техническому и экспортному контролю;
- использование для обработки конфиденциальной информации автоматизированных систем и средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
- использование предназначенных для осуществления лицензируемого вида деятельности программ для электронно-вычислительных машин и баз данных, принадлежащих лицензиату на праве собственности или на ином законном основании;
- наличие технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных частью 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, в соответствии с утверждаемым Федеральной службой по техническому и экспортному контролю перечнем и принадлежащих лицензиату на праве собственности или на ином законном основании;
- наличие системы производственного контроля в соответствии с установленными стандартами.

При намерении лицензиата выполнять новые работы и (или) оказывать новые услуги, подлежащие лицензированию в соответствии с частью 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, в заявлении о переоформлении лицензии указываются сведения о работах (услугах), которые лицензиат намерен выполнять (оказывать), а также следующие сведения, подтверждающие соответствие лицензиата лицензионным требованиям, установленным частью 6 Положения о лицензировании деятельности по технической защите конфиденциальной информации:

- сведения, подтверждающие квалификацию специалистов по защите информации (с указанием реквизитов дипломов, удостоверений, свидетельств);
- сведения, подтверждающие наличие аттестованных по требованиям безопасности информации защищаемых помещений;
- сведения, подтверждающие наличие аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, сведения о защищаемых в автоматизированных системах ресурсах;
- сведения, подтверждающие наличие на праве собственности или на ином законном основании программ для электронно-вычислительных машин и баз данных, планируемых к использованию при осуществлении лицензируемого вида деятельности;
- сведения, подтверждающие наличие контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, сведения о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также сведения, подтверждающие право соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;
- сведения об имеющихся технической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных частью 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации;
- сведения, подтверждающие наличие необходимой системы производственного контроля в соответствии с установленными стандартами.

При намерении лицензиата осуществлять лицензируемый вид деятельности по адресу места его осуществления, не указанному в лицензии, в заявлении о переоформлении лицензии указываются этот адрес и следующие сведения, подтверждающие соответствие лицензиата лицензионным требованиям, установленным частью 6 Положения о лицензировании деятельности по технической защите конфиденциальной информации:

- сведения, подтверждающие наличие помещений, предназначенных для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

- сведения, подтверждающие наличие аттестованных по требованиям безопасности информации защищаемых помещений;
- сведения, подтверждающие наличие аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, и сведения о защищаемых в автоматизированных системах ресурсах;
- сведения, подтверждающие наличие на праве собственности или на ином законном основании программ для электронно-вычислительных машин и баз данных, планируемых к использованию при осуществлении лицензируемого вида деятельности;
- сведения, подтверждающие наличие необходимой системы производственного контроля в соответствии с установленными стандартами.

При проведении проверки сведений, содержащихся в представленных соискателем лицензии (лицензиатом) документах, лицензирующий орган запрашивает необходимые для предоставления государственных услуг в области лицензирования сведения, находящиеся в распоряжении органов, предоставляющих государственные и муниципальные услуги, иных государственных органов, органов местного самоуправления либо подведомственных им организаций, в порядке, установленном Федеральным законом «Об организации предоставления государственных и муниципальных услуг». Лицензионный контроль осуществляется лицензирующим органом в соответствии с Федеральным законом от 26.12.2008 N 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» и статьей 19 Федерального закона «О лицензировании отдельных видов деятельности» от 04.05.2011 N 99-ФЗ.

5.3 Ответственность за нарушения установленных правил по обработке персональных данных

Для осуществления должного контроля необходимо вводить не только требования, которые должны быть соблюдены, но и ответственность, наступающую в случае их несоблюдения. Так в статье 24 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» сказано, что лица, виновные в нарушении требований данного закона, будут нести предусмотренную законодательством Российской Федерации ответственность, в частности:

- уголовную;
- административную;

– гражданско-правовую;

– дисциплинарную и др.

При этом моральный вред, который был причинен субъекту персональных данных вследствие нарушения его прав или правил обработки персональных данных, установленных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации, независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Уголовная ответственность наступает в следствии нарушения положений Уголовного Кодекса Российской Федерации от 13.06.1996 N 63-ФЗ. Данный Кодекс основывается на Конституции Российской Федерации и общепризнанных принципах, и нормах международного права. Его основными задачами являются: охрана прав и свобод человека, и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений. И для их реализации в Кодексе прописаны основания и принципы уголовной ответственности, определяющие, какие опасные действия для личности, общества или государства являются преступлениями, также установлены виды наказаний и иные меры уголовно-правового характера за совершение преступлений.

В Уголовном Кодексе Российской Федерации указаны следующие нарушения в сфере защиты персональных данных, представленные в таблице 5.3.1.

Таблица 5.3.1 – Ответственность за нарушения УК РФ в части персональных данных.

Статья УК РФ	Вид нарушения	Наказание
Статья 137. Нарушение неприкосновенности частной жизни, пункт 1.	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 демонстрирующемся	Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо принудительными

	произведении или средствах массовой информации.	работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.
Статья 137. Нарушение неприкосновенности частной жизни, пункт 2.	Те же деяния, совершенные лицом с использованием своего служебного положения.	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо принудительными работами на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности

		или заниматься определенной деятельностью на срок до 5 лет.
Статья 137. Нарушение неприкосновенности частной жизни, пункт 3.	Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия.	Штраф в размере от 150 000 до 350 000 рублей или в размере заработной платы или иного дохода осужденного за период от 18 месяцев до 3 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет.
Статья 140. Отказ в предоставлении гражданину информации.	Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и	Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев либо

	материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.	лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.
Статья 171. Незаконное предпринимательство, пункт 1.	Осуществление предпринимательской деятельности без регистрации или без лицензии в случаях, когда такая лицензия обязательна, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере.	Штраф в размере до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период до 2 лет, либо обязательными работами на срок до 480 часов, либо арестом на срок до 6 месяцев
Статья 171. Незаконное предпринимательство, пункт 2.	То же деяние: а) совершенное организованной группой; б) сопряженное с извлечением дохода в особо крупном размере.	Штраф в размере от 100 000 до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на срок до 5 лет со штрафом в размере до 80 000 рублей или в размере заработной платы или иного дохода осужденного за период до 6 месяцев либо без такового.

Статья 272. Неправомерный доступ к компьютерной информации, пункт 1.	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.	Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок.
Статья 272. Неправомерный доступ к компьютерной информации, пункт 2.	То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности.	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до 4 лет, либо арестом на срок до 6 месяцев, либо лишением свободы на тот же срок.
Статья 272. Неправомерный доступ к компьютерной информации, пункт 3.	Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.	Штраф в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением

		свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок.
Статья 272. Неправомерный доступ к компьютерной информации, пункт 4.	Те же деяния, но если они повлекли тяжкие последствия или создали угрозу их наступления.	Лишение свободы на срок до 7 лет.

Административная ответственность наступает, как и уголовная, в результате нарушений законодательств в сфере обработки персональных данных, но наносящих меньшее количество ущерба нежели преступления. Согласно статье 2.1 Кодекса РФ об административных правонарушениях от 30.12.2001 N 195-ФЗ административным правонарушением признается противоправное виновное действие (бездействие) физического или юридического лица, за которое настоящим Кодексом или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность, представленная в таблице 5.3.2.

Таблица 5.3.2 – Ответственность за нарушения КоАП РФ в части персональных данных.

Статья КоАП РФ	Вид нарушения	Наказание
Статья 5.39. Отказ в предоставлении информации	Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	Административный штраф на должностных лиц в размере от 1 000 до 3 000 рублей.
Статья 13.11. Нарушение установленного законом порядка	Нарушение установленного законом порядка сбора, хранения,	Предупреждение или наложение административного штрафа на граждан в

сбора, хранения, использования или распространения информации о гражданах (персональных данных).	использования или распространения информации о гражданах (персональных данных)	размере от 300 до 500 рублей; на должностных лиц - от 500 до 1 000 рублей; на юридических лиц - от 5 000 до 10 000.
Статья 13.12. Нарушение правил защиты информации, пункт 2.	Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).	Административного штраф на граждан в размере от 1 500 до 2 500 рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от 2 500 до 3 000 рублей; на юридических лиц - от 20 000 до 25 000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.
Статья 13.13. Незаконная деятельность в области защиты информации, пункт 1.	Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна)	Административный штраф на граждан в размере от 500 до 1 000 рублей с конфискацией средств защиты информации или без таковой; на должностных лиц – от 2 000 до 3 000 рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от 10 000 до 20 000 рублей с конфискацией средств защиты информации или без таковой.
Статья 13.14. Разглашение информации с	Разглашение информации, доступ к которой ограничен	Влечет наложение административного штрафа на граждан в

ограниченным доступом.	федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.	размере от 500 до 1 000 рублей; на должностных лиц - от 4 000 до 5 000 рублей.
Статья 19.4. Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль), пункт 1.	Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль).	Предупреждение или наложение административного штрафа на граждан в размере от 500 до 1 000 рублей; на должностных лиц - от 2 000 до 4 000 тысяч рублей.
Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), пункт 1.	Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства.	Административный штраф на граждан в размере от 300 до 500 рублей; на должностных лиц - от 1 000 до 2 000 рублей или дисквалификацию на срок до 3 лет; на юридических лиц - от 10 000 до 20 000 рублей.
Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица),	Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его	Административный штраф на должностных лиц в размере от 5 000 до 10 000 рублей или дисквалификацию на срок до 3 лет; на юридических лиц - от

осуществляющего государственный надзор (контроль), пункт 2.	территориального органа.	200 000 до 500 000 рублей.
Статья 19.6. Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения.	Непринятие по постановлению (представлению) органа (должностного лица), рассмотревшего дело об административном правонарушении, мер по устранению причин и условий, способствовавших совершению административного правонарушения.	Административный штраф на должностных лиц в размере от 4 000 до 5 000 рублей.
Статья 19.7. Непредставление сведений (информации).	Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде.	Предупреждение или наложение административного штрафа на граждан в размере от 100 до 300 рублей; на должностных лиц - от 300 до 500 рублей; на юридических лиц - от 3 000 до 5 000 рублей.

Гражданско-правовая ответственность наступает в случае нарушения имущественных и личных неимущественных прав граждан и организаций. Правонарушитель в результате неправомерных действий несет определенные материальные убытки, которые служат компенсацией за причинённый вред другому лицу. Основным законодательным актом, регулирующим отношения в

данном виде правонарушений является Гражданский кодекс РФ (ГК РФ) от 30.11.1994 N 51-ФЗ.

Согласно статье 8 Гражданского Кодекса РФ (ГК РФ) от 30.11.1994 N 51-ФЗ гражданские права и обязанности возникают:

- из договоров и иных сделок, предусмотренных законом, а также из договоров и иных сделок, хотя и не предусмотренных законом, но не противоречащих ему;
- из решений собраний в случаях, предусмотренных законом;
- из актов государственных органов и органов местного самоуправления, которые предусмотрены законом в качестве основания возникновения гражданских прав и обязанностей;
- из судебного решения, установившего гражданские права и обязанности;
- в результате приобретения имущества по основаниям, допускаемым законом;
- в результате создания произведений науки, литературы, искусства, изобретений и иных результатов интеллектуальной деятельности;
- вследствие причинения вреда другому лицу;
- вследствие неосновательного обогащения;
- вследствие иных действий граждан и юридических лиц;
- вследствие событий, с которыми закон или иной правовой акт связывает

В сфере обработки и защиты персональных данных Гражданским кодексом предусмотрена защита нематериальных благ, принадлежащих лицу. В частности, к ним могут быть отнесены:

- личная неприкосновенность;
- деловая репутация;
- неприкосновенность частной жизни;
- личная и семейная тайна;
- имя гражданина;
- иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом.

В случае, если нематериальные блага принадлежат умершему, они могут защищаться другими лицами в порядке, который предусмотрен данным законом.

Согласно 151 статье Гражданского Кодекса РФ (ГК РФ) от 30.11.1994 N 51-ФЗ в случае признания факта нанесения морального вреда (физических или нравственных страданий) действиями, которые нарушают его личные неимущественные права либо посягают на принадлежащие гражданину

нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Во внимание принимаются степень вины нарушителя и иные обстоятельства.

В статье 152.2 данного законодательного акта более подробна рассмотрена охрана частной жизни гражданина:

- без согласия гражданина не допускается сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни;
- стороны обязательства не вправе разглашать ставшую известной им при возникновении и (или) исполнении обязательства информацию о частной жизни гражданина, являющегося стороной или третьим лицом в данном обязательстве, если соглашением не предусмотрена возможность такого разглашения информации о сторонах;
- неправомерным распространением полученной с нарушением закона информации о частной жизни гражданина считается, в частности, ее использование при создании произведений науки, литературы и искусства, если такое использование нарушает интересы гражданина;
- в случаях, когда информация о частной жизни гражданина, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно.

Также в части 7 пункта 1 статьи 243 Трудового кодекса РФ (ТК РФ) от 30.12.2001 N 197-ФЗ указано о материальной ответственности работника в случае разглашения сведений конфиденциального характера. Таким образом при невыполнении требований по обработке и защите персональных данных оператором, ему будут предъявлены соответствующие санкции со стороны государственных и иных органов, осуществляющих контроль в данной сфере деятельности.

Контрольные вопросы:

1. Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по защите персональных данных?

2. Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по обработке персональных данных?
3. Какими статьями Уголовного Кодекса Российской Федерации предусмотрена ответственность за нарушения требований по обработке\защите персональных данных?
4. Какая ответственность предусмотрена за нарушение трудового законодательства Российской Федерации в части персональных данных?
5. Какая ответственность предусмотрена за нарушение гражданского кодекса Российской Федерации в части персональных данных?
6. Какая ответственность предусмотрена за нарушение статьи 5.39 кодекса административных правонарушений Российской Федерации?
7. Какая ответственность предусмотрена за нарушение статьи 13.11 кодекса административных правонарушений Российской Федерации?
8. Какая ответственность предусмотрена за нарушение статьи 13.12 кодекса административных правонарушений Российской Федерации?
9. Какая ответственность предусмотрена за нарушение статьи 5.13 кодекса административных правонарушений Российской Федерации?
10. Какая ответственность предусмотрена за нарушение статьи 13.14 кодекса административных правонарушений Российской Федерации?
11. Какая ответственность предусмотрена за нарушение статьи 19.4 кодекса административных правонарушений Российской Федерации?
12. Какая ответственность предусмотрена за нарушение статьи 19.5 пункта 1 кодекса административных правонарушений Российской Федерации?
13. Какая ответственность предусмотрена за нарушение статьи 19.5 пункта 2 кодекса административных правонарушений Российской Федерации?
14. Какая ответственность предусмотрена за нарушение статьи 19.6 кодекса административных правонарушений Российской Федерации?
15. Какая ответственность предусмотрена за нарушение статьи 19.7 кодекса административных правонарушений Российской Федерации?
16. Какая ответственность предусмотрена за нарушение статьи 137 уголовного кодекса Российской Федерации?
17. Какая ответственность предусмотрена за нарушение статьи 140 уголовного кодекса Российской Федерации?
18. Какая ответственность предусмотрена за нарушение статьи 272 уголовного кодекса Российской Федерации?
19. Какая ответственность предусмотрена за нарушение статьи 171 уголовного кодекса Российской Федерации?
20. О чем говорится в части 7 пункта 1 статьи 243 Трудового кодекса Российской Федерации?

Литература

1) Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.).
2) Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.).
3) Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных.
4) Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 года относительно обработки персональных данных и защите частной жизни в электронном коммуникационном секторе.
5) Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера".
6) Федеральный закон Российской Федерации 30 декабря 2001 г. № 197-ФЗ "Трудовой кодекс Российской Федерации (14 глава)".
7) Федеральный закон от 19 декабря 2005 г. N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных".
8) Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных".
9) Федеральный закон Российской Федерации от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации".
10) Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
11) Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".
12) Постановление Правительства Российской Федерации 2 июня 2008 г. № 419 "О федеральной службе по надзору в сфере связи и массовых коммуникаций".
13) Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
14) Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
15) Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных".

16) Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".
17) Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
18) Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
19) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год.
20) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год.
21) Приказ ФСТЭК России от 31 августа 2010 г. N 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».
22) «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 N 149/54-144).
23) «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203).
24) «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 N 149/6/6-622).
25) Постановление Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций".
26) Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю".
27) Указ Президента РФ от 11.08.2003 N 960 "Вопросы Федеральной службы безопасности Российской Федерации".
28) ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

29) Федеральный закон от 02.12.1990 N 395-1) "О банках и банковской деятельности".
30) Приказ Роскомнадзора от 16.07.2010 N 482 "Об утверждении образца формы уведомления об обработке персональных данных".
31) Приказ Россвязькомнадзора от 17.07.2008 года N 8 "Об утверждении образца формы уведомления об обработке персональных данных"
32) "Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных".
33) Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 5 февраля 2010 г. N 58 г. Москва "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных".
34) Приказ Минкомсвязи России от 21.12.2011 N 346 "Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных" (Зарегистрировано в Минюсте России 29.03.2012 N 23650).

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ

Институт комплексного военного образования (ИКВО) был создан в январе 1997 года на базе факультета военного обучения. Является структурным подразделением Университета на правах факультета. На факультете обучается более 1000 студентов и 15 аспирантов. ИКВО включает в себя две выпускающие кафедры:

- Мониторинга и прогнозирования информационных угроз (МиПИУ);
- Военную кафедру.

А также три базовые кафедры:

- Инновационных технологий защиты информации;
- Специального приборостроения защиты информации;
- Бортовых приборов вооружения и военной техники.

Сегодня в ИКВО работает более 60 сотрудников, включая преподавателей и учебно-вспомогательный персонал. ИКВО располагает высоко квалифицированными профессорско-преподавательскими кадрами, в числе которых 3 академика различных Академий, 3 профессора, доктора наук, 8 кандидатов наук и доцентов.

Исаев Александр Сергеевич, Хлюпина Екатерина Анатольевна

Правовые основы организации защиты персональных данных

Учебное пособие

В авторской редакции

Компьютерный набор и верстка А.С. Исаев

Дизайн обложки М.С. Чичев

Редакционно-издательский отдел НИУ ИТМО

Зав. РИО Н.Ф. Гусарова

Лицензия ИД № 00408 от 05.11.99

Подписано к печати

Заказ №

Тираж 100 экз.

Отпечатано на ризографе