ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Москва
2018

ББК67.401.26
З-40

Защита персональных данных в органах внутренних дел: учебное пособие / В. И. Лустин, В. И. Бокшицкий, Е. М. Шпагина, Н. Г. Белгородцева. – М. : Московский университет МВД России В.Я. Кикотя, 2018. – 95 с. ISBN978-5-9694-0578-3

Учебное пособие подготовлено для обучающихся по специальности 10.05.05 – Безопасность информационных технологий в правоохранительной сфере, в соответствии с действующим ФГОС ВО. В пособии делается акцент на изучение организационно-правовых основ защиты персональных данных в автоматизированных информационных системах, особенности механизма юридической ответственности за правонарушения в области обращения с персональными данными граждан, а также основные направления научно-правовых исследований по совершенствованию систем и методов защиты персональных данных. Учебное пособие отличает структурирование с учетом профиля подготовки специалистов в Московском университете МВД России имени В.Я. Кикотя.

Учебное пособие предназначено для изучения учебных дисциплин на разных видах занятий курсантами и слушателями очной и заочной форм обучения Московского университета МВД России имени В.Я. Кикотя.

Кроме того, оно может быть использовано в образовательном процессе высших учебных заведений, в том числе ведомственных образовательных учреждений высшего образования в системе МВД России, осуществляющих подготовку в области информационной безопасности.

ББК67.401.26

Рецензенты:

– старший преподаватель кафедры информационной безопасности Воронежского института МВД России, кандидат технических наук, подполковник полиции ***С. В.Зарубин;***

– начальник кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, кандидат экономических наук, полковник полиции ***Н. Р. Шевко***.

ISBN978-5-9694-0578-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы настоящей работы обусловлена в широком аспекте необходимостью обеспечения реализации провозглашенных и закрепленных Конституцией Российской Федерации и нормами международного права основных прав и свобод граждан; интересов общества и государства, задачами обеспечения и поддержания общественной безопасности и правопорядка. В конкретно-прикладном аспекте значимость темы обусловлена тем обстоятельством, что одним из приоритетных и необходимых условий действенной реализации прав и свобод человека и гражданина является эффективная правоприменительная деятельность институтов исполнительной власти государства, необходимым элементом которой является правоохранительная деятельность органов внутренних дел.

Целью работы является целостное отображение деятельности органов внутренних дел по обеспечению прав человека и гражданина в очерченной заданием предметной области. Для достижения названной цели в рамках настоящей работы решались следующие задачи:

– рассмотреть понятие, признаки и структуру персональных данных;

– изучить нормативные правовые акты по тематике защиты персональных данных;

– проанализировать систему защиты персональных данных в органах внутренних дел;

– выявить, обосновать и дать предложения по совершенствованию нормативной правовой базы в сфере обеспечения защиты персональных данных.

В качестве основного метода выполнения работы был избран сравнительно-правовой анализ основополагающих принципов и норм, закрепленных в актах международного права и в нормативных правовых актах Российской Федерации, научной литературе и материалах практики.

I. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

1. Правовой институт защиты персональных данных: основные понятия, структура и источники

В соответствии с пунктом 1 статьи 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[1] персональные данные понимаются как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу – субъекту персональных данных. Поскольку имеются различные категории персональных данных граждан, которые возможно преобразовывать в базы данных, должен быть урегулирован вопрос того, кто имеет право осуществлять обработку этих данных. В Федеральном законе «О персональных данных» дано понятие оператора персональных данных, которым может являться государственный или муниципальный орган, либо юридическое или физическое лицо. Они могут как самостоятельно, так и совместно с другими лицами одновременно организовывать и осуществлять обработку персональных данных, либо лишь одно из этих действий. Эти лица или органы определяют как цель обработки, так и состав персональных данных, а также те действия и операции, которые будут совершены в отношении них.

Совокупность источников права, выражающих и закрепляющих нормы, устанавливающие порядок обращения и защиты персональных данных физического лица, является многоэлементной и имеет сложную многоуровневую структуру. Она включает в себя:

I. *Акты международного права*, содержащие общепризнанные принципы и нормы, признаваемые и применяемые международным сообществом государств в целом, в качестве юридически обязательных, отступление от которых невозможно[2]. Это основы международного со-

---

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. – 2006. – № 4131. – 29 июля.

[2] Постановление Пленума Верховного Суда Российской Федерации от 10 октября 2003 г. № 5 «О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации // Бюллетень Верховного Суда Российской Федерации. – 2003. – № 12; Российская газета. – 2003. – № 244. 2 дек.

трудничества в области обеспечения прав человека и основных свобод для всех, без различия расы, пола, языка и религии, как одной из целей ООН и образуемых ей органов и учреждений – согласно положениям Устава ООН (п. 3 ст. 1; подпункт *b* п. 1 ст. 13; п. *c* ст. 55; п. 2 ст. 62; ст. 68; п. *c* ст. 76)[1]. В Уставе ООН закреплены принципы, на основании которых в последующих документах были конкретизированы и закреплены международно-правовые стандарты в области прав человека. Основными детализирующими актами международного права в области обеспечения прав человека и основных свобод являются:

– Всеобщая декларация прав человека[2];

– Международный пакт о гражданских и политических правах (включая факультативный протокол)[3];

– Международный пакт об экономических, социальных и культурных правах[4];

– Европейская конвенция о защите прав человека и основных свобод от 4 ноября 1950 г.[5]

В качестве источников права перечисленные акты относятся к категории *правовых договоров*.

Все нормы и принципы международного права в области прав и свобод человека, в том числе в информационной сфере, имеют всеоб-

---

[1] Устав Организации Объединенных Наций. Подписан 26 июня 1945 г. в Сан-Франциско на заключительном заседании Конференции Объединенных Наций по созданию Международной Организации, вступил в силу 24 октября 1945 г. (составной частью Устава является Статут Международного Суда) (в ред. от 12 июня 1968 г. – URLhttp: // www.un.org/ru/documents/charter/chapter19.shtml. Дата обращения 15.12.2013.

[2] Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. – URL http: // www.un.org/ru/ documents/decl_conv/ declarations/declhr. Дата обращения 09.08.2014.

[3] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 г. *United Nations, Treaty Series, vol. 999, p. 225-240, 315–317.* URL http: // www.un.org/ru/documents /decl_conv/conventions/pactpol.shtml. Дата обращения 09.08.2014. Вступил в силу 23 марта 1976 г.

[4] Международный пакт об экономических, социальных и культурных правах. Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 г. *United Nations, Treaty Series, vol. 993, p. 35–43*. URL http: // www.un.org/ru/ documents/decl_conv/conventions/pactecon.shtml. Вступил в силу 3 января 1976 г.

[5] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21.09.1970 г., 20.12.1971 г., 01.01.1990 г., 6.11.1990 г., 11.05.1994 г., 13.05.2004 г.). – URL http: // base.garant.ru/ 2540800/#ixzz39vIWoYsb. Дата обращения 09.08.2014.

щий характер. Это значит, что права и свободы людей подлежат обязательному соблюдению во всех государствах и действуют в отношении всех лиц без какой-либо дискриминации. При этом целью выработки международных стандартов в данной области является не унификация национального законодательства, а создание ориентиров для разработки, принятия и исполнения государствами конкретизированных актов национального законодательства, обеспечивающих реализацию прав и свобод личности, закрепленных общепризнанными принципами и нормами международного права.

II. *Акты национального (в контексте целей настоящей работы – российского) законодательства.* Данный массив источников права является наиболее обширным и многообразным. Он включает в себя конституционно-правые акты (Конституцию Российской Федерации, Декларацию прав и свобод человека и гражданина[1], федеральные конституционные законы), федеральные законы, подзаконные акты – указы и распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, акты (приказы, инструктивные письма и т. д.) федеральных органов исполнительной власти, законы и акты органов исполнительной власти субъектов Российской Федерации, акты органов местного самоуправления, акты судебного толкования норм права и иные материалы судебной практики.

Не будет преувеличением считать, что при действующей практике правотворческой деятельности и с учетом современной методологии юридической техники значительная, если не большая, часть выпускаемых нормативных правовых актов в большей или меньшей мере охватывает вопросы информационных прав и свобод физических лиц и полномочий в указанной сфере органов власти и иных юридических лиц (а также обязанности в информационной сфере для всех перечисленных субъектов). Это относится к нормативным правовым актам, регулирующим:

– информационно-правовые общественные отношения;

– иные правоотношения – в части информационного обеспечения их субъектов.

---

[1] Постановление Верховного Совета РСФСР от 22 ноября 1991 г. № 1920-I «О Декларации прав и свобод человека и гражданина» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. – 1991. – № 52, ст. 1865.

Закрепляющие информационно-правовой статус и регулирующие информационно-правовые отношения акты могут быть классифицированы путем отнесения к категориям:

1) материального или процессуального законодательства;

2) регулятивного (позитивного) или правоохранительного.

Первичными критериями отнесения нормативного правового акта к той или иной категории является излагаемое в его вводной части содержание:

1) целей, задач и функций данного акта;

2) регулируемых данным актом правовых отношений – регулятивных или правоохранительных.

Производным критерием может быть признано количественное соотношение положений (статей) нормативного правового акта, закрепляющих соответственно материальные или процессуальные и регулятивные либо охранительные нормы права.

В качестве наиболее значимых примеров актов материального регулятивного законодательства следует указать:

– Гражданский кодекс Российской Федерации[1];

– Федеральный закон «Об информации, информационных технологиях и защите информации»[2];

– Федеральный закон «О персональных данных»;

– Закон Российской Федерации «О средствах массовой информации»[3].

Рассмотрение актов правоохранительного законодательства требует введения для них специальной (дополнительной) классификации. Акты, исключительно или преимущественно закрепляющие охранительные нормы права и регулирующие правоохранительные отношения, могут быть отнесены к следующим категориям:

---

[1] Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ // Собр. законодательства Рос. Федерации. – 1994. – № 32, ст. 330. См. главу 8 ГК РФ «Нематериальные блага и их защита» (здесь и далее – общепринятые сокращения могут использоваться без дополнительных пояснений).

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3448 *(Часть I)*.

[3] Закон Российской Федерации от 27 декабря 1991 г. 2124-I «О средствах массовой информации» // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 7, ст. 300.

1) акты, закрепляющие ограничения на реализацию информационных прав и свобод, устанавливаемые в интересах охраны прав и законных интересов иных субъектов (личности, общества и государства). Примерами таких актов служат Федеральные законы «О противодействии экстремистской деятельности», «О защите детей от информации, причиняющей вред их здоровью и развитию», «О коммерческой тайне», Закон Российской Федерации «О государственной тайне», указы Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне» и «Об утверждении перечня сведений конфиденциального характера».

Указанные и иные источники права образуют, в широком смысле, систему внешних нормативных условий, в которых с объективной необходимостью функционируют организационно-правовые и технические подсистемы обработки и защиты персональных данных. При этом ряд нормативных правовых актов непосредственно регулирует специальные вопросы обращения с персональными данными. Например, норма пункта 4 ст. 5 Закона Российской Федерации «О государственной тайне» охватывает по своему смыслу вопросы обращения с персональными данными физических лиц – субъектов и объектов разведывательной, контрразведывательной и оперативно-разыскной деятельности, а также деятельности в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Наряду с установлением упомянутых ограничений в части реализации информационных прав и свобод в диспозициях норм законодательных актов данной категории часть этих актов включает санкции[1] и меры пресечения и (или) предупреждения нарушений установленных ограничений – например: приостановление деятельности, ликвидацию или запрещение, в порядке гражданского судопроизводства, общественного или религиозного объединения, или средства массовой информации в связи с нарушением ими Конституции и (или) законов Российской Федерации (в соответствии с Федеральным законом «О противодействии экстремистской деятельности» в системной связи с соот-

[1] С прямым или бланкетным способом изложения.

ветствующими положениями законов «Об общественных объединениях», «О политических партиях», «О средствах массовой информации», «О свободе совести и религиозных объединениях» и т. д.);

2) акты материального законодательства, основной функцией которых является закрепление норм об ответственности за правонарушения в сфере информационных прав и свобод (в том числе – за злоупотребление указанными правами и свободами). Очевидными примерами таких актов служат Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, а также законы (кодексы) об административных правонарушениях субъектов Российской Федерации;

3) акты, закрепляющие права, полномочия и обязанности органов и должностных лиц по охране и защите информационных прав и свобод личности, общества и государства. В качестве примеров таких актов могут быть названы: Федеральные конституционные законы «О Конституционном Суде Российской Федерации», «О судебной системе Российской Федерации», «Об Уполномоченном по правам человека в Российской Федерации», «О судах общей юрисдикции в Российской Федерации», Федеральные законы «О Следственном комитете Российской Федерации», «О полиции», «О службе в органах внутренних дел и внесении изменений в отдельные законодательные акты Российской Федерации», «О федеральной службе безопасности», «О судебных приставах», «Об исполнительном производстве», «Об оперативно-розыскной деятельности», Закон Российской Федерации «О прокуратуре Российской Федерации»[1].

Основными составляющими системы государственного контроля и надзора за обеспечением безопасности персональных данных при их обработке в информационных системах являются:

---

[1] Прокуратора Российской Федерации, не будучи субъектом государственного регулирования в сфере обращения с персональными данными, осуществляет, тем не менее, государственный контроль над соблюдением и исполнением нормативных правовых актов по рассматриваемой деятельности, а также обрабатывает (на постоянной основе) персональные данные граждан при реализации иных функций. Акты охранительного законодательства данной категории обладают столь же значимыми признаками регулятивного законодательства.

• Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Росскомнадзор) – уполномоченный орган по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации – т. е. по защите прав субъектов персональных данных[1];

• Федеральная служба безопасности (ФСБ России) – федеральный орган исполнительной власти, уполномоченный в области обеспечения государственной безопасности;

• Федеральная служба по техническому и экспортному контролю и противодействию иностранным разведкам (ФСТЭК России) – уполномоченный орган в области контроля используемых технических средств защиты;

• Министерство связи и информационных технологий Российской Федерации – уполномоченный орган в области контроля над порядком проведения классификации информационных систем, содержащих персональные данные.

Согласно ст. 22 Федерального закона «О персональных данных» оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи и массовых коммуникаций) о своем намерении осуществлять обработку персональных данных во всех случаях, за исключением перечисленных в части второй указанной статьи, в частности:

– относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

– 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;

– являющихся общедоступными персональными данными;

---

[1] Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций. – Утверждено Постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 // Российская газета. – 2009. – 24 марта.

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– 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.

Представленные выше классификации актов законодательства являются относительными. Например, кодифицирующие акты процессуальных отраслей законодательства – УПК, ГПК и АПК РФ, являясь по своему смыслу актами процессуальными и правоохранительными, содержат также и материальные регулятивные нормы, закрепляющие информационные права участников соответствующих судопроизводств. Аналогичные позитивные положения содержит и такой акт материального охранительного законодательства, как Федеральный закон «Об оперативно-розыскной деятельности» – в части соблюдения прав и свобод человека и гражданина, включая и информационные, при осуществлении оперативно-розыскной деятельности (ст. 5 указанного Федерального закона). КоАП РФ закрепляет как охранительные материальные (административно-деликтные) нормы, обеспечивающие административно-правовую охрану информационных прав и свобод физических и юридических лиц, общества и государства в целом[1], так и административно-процессуальные нормы о формах и порядке производства по делам об административных правонарушениях[2], а также регулятивные материальные нормы об информационных правах участников судебных или административных производств по делам об административных правонарушениях.

---

[1] Например, главы КоАП РФ: 5 – «Административные правонарушения, посягающие на права граждан»; 6 – «Административные правонарушения, посягающие на здоровье, санитарно-эпидемиологическое благополучие населения и общественную нравственность; 13 – «Административные правонарушения в области связи и информации»; 17 – «Административные правонарушения, посягающие на институты государственной власти»; 20 – «Административные правонарушения, посягающие на общественный порядок и общественную безопасность».

[2] Включая положения об обязанностях и полномочиях органов и должностных лиц – данные нормы также могут быть определены как материальные.

Практически все акты материального (регулятивного) законодательства содержат охранительные положения (статьи) об ответственности за их нарушение. В большинстве случаев эти положения излагаются бланкетным способом – указывается, что нарушение норм конкретного акта влечет за собой для виновных субъектов уголовную, административную, гражданско-правовую, материальную или иную предусмотренную законом ответственность. Однако возможно и непосредственное закрепление норм об ответственности в тексте регулятивного акта. Примером могут служить положения ГК РФ – ст.ст. 152 «Защита чести, достоинства и деловой репутации», 152^1 «Охрана изображения гражданина» и 152^2 «Охрана частной жизни гражданина».

Значительный объем процессуальных норм включен в подзаконные акты – утверждаемые актами Президента и Правительства Российской Федерации, приказами министерств и ведомств, положениями и инструкциями, детализирующими порядок применения норм федеральных законов. Актуальным примером такого подзаконного акта применительно к деятельности органов внутренних дел по обеспечению информационных прав и свобод граждан является Инструкция об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации, утвержденная приказом МВД России от 12 сентября 2013 г. № 707[1] и конкретизирующая нормы Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации»[2].

В качестве источников права, подробно раскрывающих значение и место реализации основных прав и свобод граждан в информационной сфере в системе национальных интересов России, следует рассматривать также официальные документы политико-правового характера –

---

[1] Приказ Министерства внутренних дел Российской Федерации от 12 сентября 2013 г. № 707 «Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации. Зарегистрировано в Минюсте России 31 декабря 2013 г. № 30957.

[2] Федеральный закон от 2 мая 2006 г. №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // Собр. законодательства Рос. Федерации. – 2006 – № 19 – ст. 2060; 2010, № 27, ст. 3410; № 31, ст. 4196; 2013, № 19, ст. 2307; № 27, ст. 3474.

Доктрину информационной безопасности Российской Федерации[1] и Стратегию национальной безопасности Российской Федерации до 2020 г.[2] В качестве элементов, обеспечивающих системную связь массивов нормативных правовых актов и государственно-политических документов следует указать Федеральные законы «Об информации, информационных технологиях и защите информации» и «О безопасности»[3].

2. Обзор содержания основных правовых норм, регламентирующих защиту персональных данных

1.2. Общепринятые принципы и нормы международного права, международные договоры Российской Федерации как внешняя правовая среда национальной системы защиты персональных данных

Организацией объединенных наций свобода информации уже давно была признана фундаментальным правом человека. 14 декабря 1946 г. на первой сессии Генеральной Ассамблеи ООН была принята Резолюция 59(1), которая гласила, что: «…Свобода информация есть фундаментальное право человека и…пробный камень всех свобод, которые находятся центре внимания ООН…». В более поздних международных документах по правам человека свобода информации рассматривалась не отдельно, а как часть фундаментального права на свободу слова, которое включает право искать, получать и распространять информацию[4].

---

[1] Доктрина информационной безопасности Российской Федерации – утверждена Президентом Российской Федерации – от 9 сентября 2000 г. № Пр-1895. – URL http: // pravo.gov.ru/proxy/ips/?searchres=&bpas=cd00000&intelsearch=%C4%EE%EA%F2%F0%E8%ED%E0+%E/. Дата обращения 15.06.2014 (действует без изменений).

[2] Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Собр. законодательства Рос. Федерации. – 2009. – № 20, ст. 2444.

[3] Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Собр. законодательства Рос. Федерации. – 2011. – № 1, ст. 2.

[4] Свобода информации. Сравнительное правовое исследование // Тоби Мендел. URL http: // www.unesco.kz/publications/ci/freed_inform_ru.doc/. Дата обращения 20.08.2014. – Опубликовано в 2003 году Региональным Бюро ЮНЕСКО по информации и коммуникации [Office UNESCO House, B-5/29, SafdarjungEnclave, NewDelhi 110029 India/ URL www.unesco.org/webworld]. Составлено и отпечатано MacroGraphicsPvt.Ltd. ЮНЕСКО 2003. Переведено Кластерное бюро ЮНЕСКО в Алматы, Отдел Коммуникации и Информации, URL http: // www.unesco.kz, Июль 2004. Код документа CI/ATA/2009/PI/H/1.

Основы *международно-правового обеспечения* реализации и защиты информационных прав и свобод личности закреплены Всеобщей декларацией прав человека (1948 г.)., в соответствии со ст. 19 которой: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений, искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

Аналогичные положения включает в себя и ст. 19 Международного пакта о гражданских и политических правах (1966 г.), согласно которой:

«1. Каждый человек имеет право беспрепятственно придерживаться своих мнений.

2. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно, или посредством печати или художественных форм выражения, или иными способами по своему выбору».

Исходя из юридического статуса указанного Пакта как универсального международного соглашения, положения пакта носят обязательный характер для всех государств членов Организации Объединенных Наций.

Для стран Европы юридической силой обладает также Европейская конвенция о защите прав человека и основных свобод (1950 г.). Ее положения расширяют и конкретизируют основы информационных прав, заложенные во Всеобщей декларации прав человека. Согласно норме пункта 1 ст. 9 данной Конвенции (Свобода мысли, совести и религии): «Каждый 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».

В соответствии с пунктом 1 ст. 10 Конвенции (Свобода выражения мнения): «Каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу по-

лучать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Настоящая статья не препятствует государствам осуществлять лицензирование радиовещательных, телевизионных или кинематографических предприятий».

По смыслу пункта 1 ст. 11 Конвенции, (Свобода собраний и объединений) и в системной связи со ст.ст. 9 и 10 вышеназванными правами могут реализовываться как отдельные физические лица, так и создаваемые ими коллективные объединения.

В Международном пакте о гражданских и политических правах право на информацию раскрывается не только как право получать и распространять информацию, но и включает право искать информацию. При этом указан также способ поиска, получения и распространения информации: устно, письменно, или посредством печати, или художественных форм выражения, или иными способами по своему выбору.

Как следует из содержания соответствующих статей приведенных актов, в них закрепляется право на информацию. Это право отнесено к основным правам человека, оно тесно корреспондирует с правом свободно выражать свое мнение. Право на информацию раскрывается как право свободно получать и распространять информацию и идеи без какого-либо вмешательства публичных (государственных) властей, т. е. самостоятельно. В юридических доктринах это право часто обозначают как «право общества знать». Причем это право должно осуществляться не только без какого-либо вмешательства публичных властей, но и «независимо от государственных границ». Указанное *право* корреспондирует *обязанности* органов власти и должностных лиц (публичных властей) предоставлять соответствующую информацию гражданам и их объединениям. Определение практических пределов и порядка исполнения данной обязанности (в форме обязательного публичного раскрытия соответствующей информации обязанными субъектами[1] либо

[1] В контексте темы настоящей работы – государственные и муниципальные органы и учреждения, а также, в определенных законом случаях – негосударственные (коммерческие и некоммерческие) организации.

представления ее по запросам управомоченных субъектов[1]) остается предметом широкой дискуссии международных (межгосударственных) организаций, национальных правительств, международных и национальных неправительственных организаций[2].

Статья 13 *Американской Конвенции о правах человека* (АКПЧ), юридически обязательный для исполнения договор – гарантирует свободу слова в формулировке, аналогичной и даже более сильной, нежели документы ООН. В 1985 году Консультативное заключение Межамериканского суда по правам человека (МАСПЧ), интерпретируя Статью 13, признало свободу информации в качестве фундаментального человеческого права, которое важно для свободного общества как свобода слова. Суд объяснил:

«…Статья 13… устанавливает, что те, к кому применима Конвенция, не только имеют право на свободу выражения собственного мнения, но также право и свободу искать, получать и распространять информацию и идеи всякого рода… [Свобода слова предполагает], с одной стороны, что никого нельзя произвольно ограничивать или препятствовать в выражении собственных мыслей. И в этом смысле это право каждого человека. Второй аспект этого права, с другой стороны, предполагает коллективное право получать любую информацию, а также иметь доступ к мнению, высказываемому другими людьми…».

Суд (МАСПЧ) также заявил: «Для среднего гражданина также важно знать мнение других людей или иметь доступ к информации вообще, равно как и распространять собственное мнение», сделав при этом заключение о том, что «общество, которое не информировано достаточно хорошо, не является подлинно свободным обществом»[3].

В то же время информационные права и свободы не абсолютны – их реализация объективно связана с определенными ограничениями. Тесная взаимосвязь прав и обязанностей, связанных с осуществлением информационных прав, проявляется в том, что уже в самих статьях ос-

---

[1] Физические и юридические лица, группы и объединения граждан, международные организации, средства массовой информации и т. д. – претендующие на получение интересующей их информации.

[2] Тоби Мендел. Указ. соч. гл. 2 «Особенности режима С[вободы]И[формации]». С. 36–48.

[3] Тоби Мендел. Указ. соч. С. 19–20.

новных международных актов одновременно с провозглашением права на информацию закрепляются и соответствующие обязанности.

Согласно норме пункта 3 ст. 19 Международного пакта о гражданских и политических правах:

«Пользование предусмотренными в пункте 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

a) для уважения прав и репутации других лиц;

b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения».

Пункт 2 ст. 9 и пункт 2 ст. 10 Европейской конвенции о защите прав человека и основных свобод содержат аналогичные положения, соответственно:

– «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»;

– «Осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия».

Таким образом, объективно необходимыми условиями правомерных ограничений информационных прав и свобод являются те, которые:

– должны быть установлены законом;

– быть обоснованными;

– могут применяться строго в целях уважения прав и репутации других лиц, охраны государственной безопасности, общественного порядка, здоровья или нравственности населения и обеспечения справедливого правосудия.

В части *применения норм международного права* в области информационных прав и свобод межгосударственными судейскими органами претензии, связанные с правом получения информации от государственных органов, непосредственно рассматривались до настоящего времени только Европейским судом по правам человека (ЕСПЧ)[1]. Суд уделяет особое внимание сбалансированности интересов в делах, связанных с правом на информацию. Практика ЕСПЧ показывает, что свобода информации является неотъемлемой частью свободы слова, т. е. право на информацию – это часть свободы слова, и распространение информации, выражение своего мнения обеспечивают эту свободу. По смыслу ст. 10 Европейской конвенции о защите прав человека и основных свобод можно прийти к выводу, что право выражения мнения защищает и форму выражения идей и мнений, и их содержание. Критерии для определения баланса интересов не уточнены, и такие вопросы решаются на основе фактических обстоятельств конкретных дел. Но практика ЕСПЧ устанавливает некоторые важные правила, которые должны соблюдаться при решении дела:

– свобода выражения мнения составляет одну из основ демократического общества;

– толерантность и равное уважение к человеку являются основой демократического и плюралистического общества;

– проблемы, интересные для общества, должны быть раскрыты.

В основном жалобы изучаются на основе конкретных фактов, т. е. усложняется установление общих правил, но практика ЕСПЧ показывает, что примирение интересов и установление баланса между разными аспектами более важно. Основы ограничения этих прав отражены в Конвенции. Однако главная тенденция состоит в том, что основы ограничения права на информацию должны узко толковаться и выполнять-

[1] Уставные документы (статуты) Международного суда ООН и Международного уголовного суда не закрепляют в их юрисдикции производство по делам о нарушениях информационных прав и свобод (вне расширительного толкования).

ся судами государств. В целом право на свободу информации является основой демократического общества и ключевым элементом в самореализации человека[1].

Среди международных актов, защищающих права и свободы человека, тайну его частной и семейной жизни, в том числе и персональные данные, следует назвать Всеобщую декларацию прав человека 1948 г. (ст. 12), Конвенцию о защите прав человека и основных свобод 1950 г. (ст. 8), Международный пакт о гражданских и политических правах 1976 г. (ст. 17), Конвенцию Содружества Независимых Государств о правах и основных свободах человека 1995 г. (ст. 9).

В Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г. (в ней участвуют государства-члены Совета Европы) в понятие «данные личного характера» включается любая информация об определенном или поддающемся определению физическом лице (субъекте данных), что продиктовано пунктом «а» статьи 2.

Российская Федерация произвела ратификацию Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. с поправками от 15 июня 1999 г.[2], но с рядом оговорок:

1) Россия не будет применять Конвенцию к персональным данным:

а) обрабатываемым физическим лицом исключительно для личных и семейных нужд;

б) отнесенным к государственной тайне в порядке, установленном законодательством Российской Федерации о государственной тайне;

2) будет применять Конвенцию к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации;

---

[1] Защита свободы информации в практике Европейского суда по правам человека. Представлено Юридической компанией ЛЕГАС. Москва, Вологда. URL http: // legascom.ru/notes/813-zachita-svobodi-informacii-v-praktike-esph?tmpl= component&print=1&layout=default&page=. Обновлено 23.07.2014 14:05, дата обращения 20.08.2014, – библиография 29 наименований.

[2] Федеральный закон от 19 декабря 2005 г. № 160-ФЗ // Собр. законодательства Рос. Федерации. – 2005. – № 52 (ч. I). Ст. 5573.

3) оставляет за собой право устанавливать ограничения прав субъектов персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

10 февраля 2006 г. Президентом Российской Федерации подписано распоряжение № 54-РП «О подписании дополнительного протокола к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, касающегося наблюдательных органов и трансграничной передачи данных»[1].

2.2. Конституционно-правовые нормы и федеральные законы

На уровне национального (российского) законодательства общепринятые принципы и нормы международного права в части информационных прав и свобод закреплены и конкретизированы Конституцией Российской Федерации и принятыми на ее основе иными нормативными правовыми актами. В соответствии с нормами ч. 1 ст. 17 в Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права и в соответствии с Конституцией Российской Федерации. Согласно ч. 2 указанной статьи основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения.

Согласно норме ст. 18 Права и свободы человека и гражданина являются непосредственно действующими. Они определяют смысл, содержание и применение законов, деятельность законодательной, исполнительной власти, местного самоуправления и обеспечиваются правосудием[2].

В соответствии с нормами ст. ст. 23 и 24 (ч.ч. 1 и 2 соответственно):

– каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения;

---

[1] Распоряжение Президента Российской Федерации от 10 февраля 2006 г. № 54-РП // Собр. законодательства Рос. Федерации. – 2006. – № 7, ст. 769.

[2] Здесь и далее – ссылки на положения Конституции Российской Федерации могут производиться без указания на полное наименование источника, в форме косвенной речи.

– сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом[1].

В Конституции Российской Федерации право на информацию в целом по смыслу совпадает со значением этого права в международных актах, но трактуется шире. Согласно норме ст. 64 Конституции информационные права наряду с другими правами составляют основу правового статуса личности в Российской Федерации, они принадлежат каждому от рождения и являются неотчуждаемыми – не могут быть изменены иначе, как в порядке, установленном Конституцией Российской Федерации. Обязанности по соблюдению информационных прав и обеспечению информационных свобод возлагается на государство.

У обрабатываемых персональных данных, согласно нормам Федерального закона «О персональных данных», имеется собственная видовая структура ст. 10 закрепляет категорию специальных персональных данных, в которую включаются сведения о расовой и национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. Обработка обозначенных персональных данных является недопустимой, за исключением тех случаев, когда эта обработка возможна при условии соблюдения некоторых факторов:

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

2) субъект сделал свои персональные данные общедоступными;

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

4) в соответствии с Федеральным законом от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»[2];

---

[1] Здесь и далее – выделенное курсивом положение выражает содержание *правомерных ограничений* информационных прав и свобод.

[2] Федеральный закон от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения» // Российская газета. – 2002. – №17. – 29 янв.

5) в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

6) для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

7) 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;

8) 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;

9) необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

10) осуществляется в соответствии с законодательством Российской Федерации об обороне, безопасности, противодействии терроризму, транспортной безопасности, противодействии коррупции, оперативно-разыскной деятельности, исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

11) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

12) в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

13) в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

14) в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Согласно пункту 3 указанной статьи обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Идентифицировать личность позволяют, в частности, дактилоскопические данные. Для подразделений органов внутренних дел, предназначенных для борьбы с преступностью, эти данные имеют непосредственное значение. В связи с этим 25 июля 1998 г. был принят Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации»[1]. Для отдельных категорий лиц гражданской государственной службы приняты инструкции, предусматривающие обязательность и порядок проведения дактилоскопической регистрации. Например, Приказом Государственного комитета Российской Федерации по контролю над оборотом наркотических средств и психотропных веществ от 28 января 2004 г. № 18 утверждена «Инструкция о порядке проведения обязательной государственной дактилоскопической регистрации сотрудников органов по контролю за оборотом наркотических средств и психотропных веществ»[2].

В Федеральном законе «О персональных данных» статья 11 регламентирует порядок обращения с биометрическими персональными данными. Это широкое понятие, в которое включаются и дактилоско-

---

[1] Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Российская газета – 1998. – № 145.

[2] Бюллетень нормативных актов федеральных органов исполнительной власти. – 2004. – № 11. – С. 125.

пические данные, ввиду того, что под биометрическими персональными данными понимаются сведения, которые характеризуют биологические и физиологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления персональных данных личности субъекта. Эти данные могут обрабатываться только при наличии письменного согласия субъекта персональных данных.

При этом нормой части второй ст. 11 Федерального закона закреплены условия, при которых обработка может осуществляться и без согласия субъекта персональных данных:

– в связи с реализацией международных договоров Российской Федерации о реадмиссии;

– в связи с осуществлением правосудия и исполнением судебных актов;

– в случаях, предусмотренным законодательством Российской Федерации об обороне, безопасности, противодействии терроризму, транспортной безопасности, противодействии коррупции, оперативно-разыскной деятельности, государственной службе; уголовно-исполнительным законодательством Российской Федерации; законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

В соответствии с частью 1 статьи 17 Федерального закона «О полиции» полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах, при этом обеспечивает защиту информации, содержащуюся в банках данных, от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.

Информация, содержащаяся в банках данных, предоставляется государственным органам и их должностным лицам только в случаях, предусмотренных федеральным законом; правоохранительным органам иностранных государств и международным полицейским организациям – в соответствии с международными договорами Российской Федерации.

В соответствии с частью 7 статьи 14 Федерального закона «О персональных данных» субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

«1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) 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;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами».

Он вправе 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.

Согласно части 8 указанной статьи право субъекта персональных данных на доступ к своим персональным данным ограничивается в случаях, если:

«1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, 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».

До начала обработки персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных[1] о своем намерении осуществлять обработку персональных данных, за исключением следующих случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных»:

1) обрабатываемых в соответствии с трудовым законодательством;

---

[1] Роскомнадзор.

2) 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;

3) 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;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) 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;

8) 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;

9) 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».

В части 3 указанной статьи отмечается, что уведомление должно быть направлено в виде документа на бумажном носителе или в форме электронного документа и подписано уполномоченным лицом. Уведомление должно содержать следующие сведения:

«1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

В случае предоставления неполных или недостоверных сведений уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов (часть 6 указанной статьи).

При изменении данных сведений, 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 (часть 7 указанной статьи).

В ст. 22^1 Федерального закона «О персональных данных», закреплены следующие требования к операторам персональных данных:

1) оператор, являющийся юридическим лицом, обязан назначить лицо, ответственное за организацию обработки персональных данных и подотчетное ему;

2) лицо, ответственное за организацию обработки персональных данных, должно получить указания непосредственно от исполнительного органа организации, являющейся оператором;

3) оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 ст. 22 указанного федерального закона;

4) 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 РФ 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. Полномочия федеральных органов исполнительной власти в сфере защиты персональных данных

В соответствии с нормами Федерального закона «О персональных данных» (части 3 и 4 ст. 19) 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:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Состав и содержание необходимых для выполнения указанных 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[1], и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации[2], в пределах их полномочий.

Согласно нормам частей 8 и 9 на ФСБ и ФСТЭК России возлагается контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных указанной статьей федерального закона – в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. ФСБ и ФСТЭК России могут быть также наделены решением Правительства Российской Федерации и с учетом значимости и содержания обрабатываемых персональных данных 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 аналогично – без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

---

[1] ФСБ России.

[2] ФСТЭК России.

В Положении о Федеральной службе безопасности Российской Федерации, утвержденном Указом Президента Российской Федерации от 11 августа 2003 г. № 960, в части первой Общие положения, пункта первого говорится о том, что Федеральная служба безопасности Российской Федерации является федеральным органом исполнительной власти, в пределах своих полномочий осуществляющая государственное управление в области обеспечения информационной безопасности Российской Федерации.

В основных задачах Федеральной службы безопасности, в подпункте 14 пункта 9 части 2 Основные задачи ФСБ России указаны формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности и организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем (подпункт 15).

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» 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. Согласно части 7 той же статьи проекты указанных нормативных актов подлежат согласованию с ФСБ и ФСТЭК России. Примерами подобных (изданных ранее) нормативных и правовых актов являются:

– Концепция создания системы персонального учета населения Российской Федерации, одобренная Распоряжением Правительства Российской Федерации от 9 июня 2005 г. № 748-р[1];

[1] Бюллетень трудового и социального законодательства Российской Федерации. – 2005. – № 7. – С. 35.

– Положение о паспорте гражданина Российской Федерации, образец бланка и описание паспорта гражданина Российской Федерации, утвержденные Постановлением Правительства Российской Федерации от 8 июля 1997 г. № 828 (с последующими изменениями)[1];

– Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» В соответствии с нормой пункта 4 указанного Постановления оператор связи обязан обеспечить соблюдение тайны информации, передаваемой по сети передачи данных. При этом сведения об абоненте-гражданине, ставшие известными оператору связи в силу исполнения договора об оказании услуг связи по передаче данных, могут использоваться оператором связи для оказания справочных и иных информационных услуг или передаваться третьим лицам только с письменного согласия этого абонента, за исключением случаев, предусмотренных федеральными законами. Согласие абонента-гражданина на обработку его персональных данных в целях осуществления оператором связи расчетов за оказанные услуги связи, а также рассмотрения претензий не требуется[2].

Согласно части 7 статьи 19 Федерального закона «О персональных данных» проекты подобных нормативных актов, подготавливаемые в дальнейшем, подлежат согласованию с ФСБ и ФСТЭК России.

В соответствии с нормами частей 6 и 7 ст. 19 Федерального закона «О персональных данных», наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 указанной статьи, 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,

---

[1] Собр. законодательства Рос. Федерации. – 1997. – № 28, ст. 3444; 1999. – № 41, ст. 4918; 2001. – № 3, ст. 242; 2002. – № 4, ст. 330; 2003. – №27, ст. 2813; 2004. – № 5, ст. 374.

[2] Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» // Собр. законодательства Рос. Федерации. – 2006. – № 5, ст. 553.

характера и способов их обработки. Проекты таких решений также подлежат согласованию с ФСБ и ФСТЭК России. В случаях, когда указанные федеральные органы исполнительной власти отказывают в согласовании представленных им проектов, они обязаны мотивировать свое решение. В сфере защиты информации, составляющей персональные данные граждан, действует также совокупность подзаконных (ведомственных) нормативных правовых актов, основанных на нормах Конституции Российской Федерации и федеральных законов.

Например, в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[1] предлагается выделять персональные данные из информационных систем, содержащих информацию ограниченного доступа и защищаемых в режиме тайны, что во многих случаях не реализуемо. Выделение персональных данных из общего массива охраняемой информации создает для оператора проблему соотношения требований по технической защите информации, а также проблему соотношения прав и обязанностей субъектов в отношении защищаемой информации.

Согласно пункту 5 Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[2] указанные требования применяются при обработке в государственной информационной системе информации, содержащей персональные данные наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119[3].

---

[1] Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. – 2013. – № 107. – 22 мая.

[2] Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. – 2013. – № 6112. – 26 июня.

[3] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. – 2012. – №5929. – 7 нояб.

3. Действующая в органах внутренних дел система защиты персональных данных: состояние, проблемы и пути их решения

Защита информации, в том числе персональных данных, осуществляется в системе МВД России в соответствии с нормами законодательства Российской Федерации о защите информации, а также иными нормативными правовыми актами Российской Федерации и государственными стандартами.

Обработка персональных данных в системе органов внутренних дел может осуществляться в следующих целях:

1) трудоустройства, содействия сотруднику в прохождении службы в органах внутренних дел, обучении и должностном росте, обеспечении личной безопасности сотрудника и работника, учете результатов выполнения им служебных обязанностей;

2) обработки данных физических лиц, совершивших административные правонарушения или уголовные преступления, осуществляемой для установления личности, документирования обстоятельств совершения административного правонарушения или уголовного преступления, составления протокола по делу об административном правонарушении или заполнения бумаг в уголовном деле, обеспечения установленного порядка производства по делам об административных правонарушениях или уголовных преступлениях.

Обработка персональных данных сотрудника включает производимые органами внутренних дел в лице уполномоченных его представителей (как правило – сотрудников кадрового аппарата) операции (действия):

а) по получению;

б) хранению;

в) комбинированию;

г) передаче персональных данных работника или иному их использованию.

Согласно норме Федерального закона от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» для сотрудников внутренних дел, в отличие от военнослужа-

щих, отдельно прописана защита их персональных данных, что означает дополнительное предоставление гарантий по их защите:

– обработка персональных данных сотрудника осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, настоящего Федерального закона, других законодательных актов Российской Федерации;

– защита персональных данных сотрудника от неправомерного их использования или утраты обеспечивается за счет средств федерального органа исполнительной власти в сфере внутренних дел в порядке, установленном настоящим Федеральным законом и другими федеральными законами.

Обработка персональных данных осуществляется операторами, являющимися государственными или муниципальными органами в соответствии с Федеральным законом «О персональных данных», Федеральным законом «О полиции», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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, а также другими нормативными правовыми актами Российской Федерации в области защиты информации.

В системе Министерства внутренних дел Российской Федерации вопросы указанных нормы федерального законодательства регламентированы, в частности, Положением о централизованном учете персональных данных сотрудника органов внутренних дел Российской Федерации и ведении его личного дела и Положением о централизованном учете персональных данных гражданина Российской Федерации, поступающего на службу в органы внутренних дел Российской Федерации[1].

В соответствии с п.п. 2–3 Положения о централизованном учете персональных данных сотрудника органов внутренних дел Российской

[1] Утверждены Приказом МВД России от 28 апреля 2014 г. № 381 «О некоторых вопросах централизованного учета персональных данных сотрудников ОВД Российской Федерации, граждан Российской Федерации, поступающих на службу в органы внутренних дел Российской Федерации». – С Прил. №№ 1, 2 // Российская газета. – 2014. – 6 авг. Федеральный выпуск №6447 (зарег. в Минюсте 4.06.2014 г., рег. № 32562).

Федерации и ведении его личного дела в органах внутренних дел Российской Федерации ведутся личные дела, документы учета сотрудников, банки данных о сотрудниках, содержащие персональные данные сотрудников, сведения об их служебной деятельности и стаже службы, а также персональные данные членов семей сотрудников. Централизованный учет персональных данных сотрудника осуществляют кадровые подразделения главных управлений, департаментов, управлений МВД России, Национального центрального бюро Интерпола МВД России, территориальных органов МВД России, образовательных, научных, медико-санитарных и санаторно-курортных организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел. Сотрудник, виновный в нарушении норм, регулирующих получение, хранение, обработку, использование и передачу персональных данных другого сотрудника, либо в утрате таких данных, несет ответственность в соответствии с Федеральным законом от 30 ноября 2011 г. 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» и другими федеральными законами.

Без уведомления уполномоченного органа по защите прав субъектов персональных данных органы внутренних дел осуществляют обработку персональных данных в следующих случаях:

1) когда персональные данные обрабатываются в соответствии с трудовым законодательством;

2) получены 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;

3) субъект персональных данных сделал свои персональные данные общедоступными;

4) персональные данные включают в себя только фамилии, имена и отчества субъектов персональных данных;

5) необходимы в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

6) включены в информационные системы персональных данных, имеющих 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;

7) обрабатываются 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.

Координация и контроль деятельности по защите персональных данных при их автоматизированной обработке в системе органов внутренних дел осуществляется Департаментом информационных технологий, связи и защиты информации МВД России, который является единым координирующим и контролирующим органом по вопросам защиты персональных данных при их автоматизированной обработке.

В территориальных органах МВД России функции по осуществлению мероприятий по защите персональных данных при их автоматизированной обработке и контроле за их проведением подразделениями территориального органа возложены на подразделения информационных технологий, связи и защиты информации.

Руководители подразделений МВД России могут издавать локальные правовые акты по вопросам защиты персональных данных при ее обработке в информационных системах персональных данных.

Ответственными за соблюдение требований по защите персональных данных при их автоматизированной обработке являются руководители подразделений МВД России, эксплуатирующих, а также использующих информационные системы персональных данных, администраторы информационных систем персональных данных, пользова-

тели информационных систем персональных данных, непосредственно обрабатывающие персональные данные в информационных системах и инженерно-технический персонал, имеющий доступ к информационной системе.

Обязанности данных должностных лиц отражаются в соответствующих должностных регламентах (должностных инструкциях).

В системе органов внутренних дел действует утвержденная Приказом МВД России от 6 июля 2012 г. № 678 Инструкция по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации (далее – Инструкция)[1] и Методические рекомендации по обеспечению безопасности персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации от 1 октября 2013 г., исходящий № 1/9116.

Министерство внутренних дел Российской Федерации в соответствии со статьей 3 Федерального закона № 152-ФЗ, а также пунктом 3 Инструкции является оператором, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Обеспечение выполнения требований законодательства о направлении оператором уведомления об обработке персональных данных в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций возлагается на Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации. Подразделение-оператор информационной системы персональных данных указанные уведомления в Роскомнадзор не направляет, поскольку подразделения МВД России операторами персональных данных не являются.

Непосредственно обработку персональных данных в информационной системе персональных данных осуществляют подразделения МВД

---

[1] Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» // Российская газета. – 2012. – № 5903. – 5 окт.

России, определенные оператором в приказе МВД России о вводе информационной системы персональных данных в эксплуатацию.

Подразделения МВД России являются подразделениями-операторами информационной системы персональных данных при условии, что они осуществляют деятельность по эксплуатации информационной системы персональных данных, в том числе по обработке информации, содержащейся в ее базах данных.

В случаях, когда реализация мер по организации и обработке персональных данных в информационной системе персональных данных возлагается на несколько подразделений МВД России, вопросы разграничения полномочий между ними отражаются в инструкции по эксплуатации соответствующей информационной системы персональных данных, утверждаемой приказом о вводе ее в эксплуатацию.

Инструкция также определяет порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, в том числе полученных при трансграничной передаче, устанавливает методы и способы защиты информации в информационных системах персональных данных, а также определяет обязанности должностных лиц. Однако в Инструкции не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

Согласно пункту 4 Инструкции, координацию и контроль деятельности по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, осуществляет также подразделение центрального аппарата МВД России, выполняющее функции головного подразделения МВД России по вопросам защиты персональных данных при их автоматизированной обработке.

Согласно пункту 5 Инструкции, оператор определяет подразделения органов внутренних дел Российской Федерации, осуществляющие обработку персональных данных в эксплуатируемых информационных системах.

В случаях, когда реализация мер по организации и обработке персональных данных в информационных системах персональных данных возлагается на несколько подразделений МВД Российской Федерации, вопросы разграничения полномочий между ними отражаются в инструкции по эксплуатации соответствующей информационной системы.

Часть вторая Инструкции посвящена вопросам организации работ по обеспечению безопасности персональных данных при их автоматизированной обработке.

Согласно пункту 3 в целях обеспечения безопасности персональных данных создается средство защиты персональных данных, которое должно обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

Средство защиты персональных данных включает в себя организационные и технические меры, средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии.

В пункте 6 констатируется, что классификация информационной системы проводится подразделением-оператором информационной системы на этапе создания или модернизации информационной системы или при изменении состава обрабатываемых персональных данных.

Подразделения-операторы информационной системы, которые осуществляли обработку персональных данных, должны обеспечить средства защиты ранее введенных и (или) модернизирующихся информационных систем в соответствии с требованиями Инструкции.

Для проведения классификации информационной системы персональных данных (ИСПДн[1]) приказом руководителя подразделения-оператора информационной системы назначается комиссия, в состав которой включаются представители подразделения, эксплуатирующего

[1] Полный перечень применяемых в настоящей работе основных обозначений, сокращений и определений понятий представлен в Приложении.

информационную систему, а также специалисты подразделения МВД России, осуществляющего функции в сфере информационных технологий, связи и защиты информации (пункт 12 Инструкции). Оформление результатов классификации информационной системы производится соответствующим актом подразделения-оператора информационной системы (пункт 13 Инструкции). В соответствии с пунктом 11 Приказа ФСТЭК № 17 условием успешного проведения классификации является применение в составе ИСПДн сертифицированных средств защиты информации (пункт 9 Инструкции).

В том случае, если объект информатизации содержит информационные системы, введенные в эксплуатацию до введения в действие Инструкции, они подлежат аттестации по требованиям безопасности информации в целях официального подтверждения эффективности комплекса используемых на рассматриваемом объекте информатизации мер и средств защиты информации (пункт 11 Инструкции).

Помещения, в которых размещены объекты информатизации, содержащие информационные системы персональных данных, должны соответствовать требованиям по обеспечению их сохранности, пожарной безопасности, а также защите от несанкционированного проникновения посторонних лиц (пункт 15 Инструкции).

В соответствии с пунктами 16 Инструкции для каждой ИСПДн на этапе ее создания или модернизации разрабатываются модель угроз, а также документы, отражающие вопросы резервного копирования информации, содержащей персональные данные, парольной защиты, проведения антивирусного контроля, порядка удаления (изменения) персонифицированных записей из (в) ИСПДн, обезличивания персональных данных, проведения технического обслуживания ИСПДн, работы с машинными носителями персональных данных. При этом действующая редакция Инструкции не закрепляет разработчика модели.

Согласно положению пункта 21 Инструкции для каждой ИСПДн предусматривается ведение следующих журналов:

1) учета эксплуатирующего персонала, в том числе администраторов безопасности ИСПДн, администраторов ИСПДн, пользователей ИСПДн, непосредственно обрабатывающих персональные данные в ИСПДн, и инженерно-технического персонала, имеющего доступ к

ИСПДн в целях обеспечения устойчивого функционирования информационной системы при ее использовании;

2) учета и выдачи машинных носителей персональных данных;

3) проведения инструктажей по обеспечению безопасности персональных данных;

4) проверки исправности технических средств и технического обслуживания.

Создание (модернизация) информационных систем, обрабатывающих персональные данные, а также их отдельные элементы осуществляется с учетом требований приказа МВД России от 18 марта 2013 г. № 150 «Об организации научного обеспечения и применении положительного опыта в органах внутренних дел Российской Федерации и внутренних войсках МВД России».

Эксплуатация информационных систем персональных данных МВД России без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности, не допускается.

Технические средства, предназначенные для обработки информации, содержащейся в информационных системах персональных данных, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

При создании информационной системы персональных данных использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи.

При создании и эксплуатации информационных систем персональных данных МВД России, используемые в целях защиты персональных данных методы и способы ее защиты должны соответствовать требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, Федеральной службой безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, Федеральной службой по техническому и экспертному контролю, в пределах их полномочий.

Защита персональных данных, содержащихся в информационных системах, обеспечивается путем выполнения обладателем персональных данных требований к организации защиты персональных данных и требований к мерам их защиты, содержащимся в информационных системах персональных данных.

Работы по обеспечению защиты персональных данных в установленном порядке включаются в план основных организационных мероприятий МВД России (планы работ подразделений МВД России). Ответственность за организацию обеспечения защиты персональных данных, содержащихся в информационных системах персональных данных, и организацию подготовки объекта информатизации к аттестации на соответствие требованиям безопасности информации возлагается на подразделение МВД России, являющееся подразделением-оператором информационной системы персональных данных. Объективная необходимость выполнения данного условия на практике выявила актуальность дополнительных мероприятий по-доукомплектованию указанных подразделений-операторов специалистами по технической защите информации.

В целях создания и модернизации информационных систем персональных данных, а также средств защиты, соответствующие работы могут включаться в план научного обеспечения деятельности органов внутренних дел и внутренних войск МВД России в установленном порядке.

Мероприятия по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных включают в себя:

– формирование требований к защите персональных данных, содержащихся в информационных системах персональных данных;

– разработку средств защиты персональных данных информационных систем персональных данных;

– внедрение средств защиты персональных данных в информационные системы;

– аттестацию информационных систем персональных данных по требованиям защиты информации и ввод их в эксплуатацию;

– обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

– обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки персональных данных.

Мероприятия по обеспечению защиты данных при их обработке в информационных системах проводятся в соответствии с пунктами 14–19 Требований о защите информации, не составляющей государственную тайну.

При формировании требований к защите персональных данных, содержащихся в информационных системах, наряду с их классификацией устанавливается уровень защищенности персональных данных, обрабатываемых в этой системе.

Обеспечение защиты персональных данных, содержащихся в информационной системе, осуществляется в соответствии с разделом 3 Требований о защите информации, с учетом раздела 2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21.

В случае, когда установленный класс защищенности информационной системы не обеспечивает установленного уровня защищенности персональных данных, содержащихся в системе, соответствующий адаптивный базовый набор мер защиты информации уточняется с учетом аналогичных мер защиты, установленных приказом ФСТЭК России от 18 февраля 2013 г. № 21 и обеспечивающих необходимый уровень защищенности персональных данных.

Формирование требований к средствам защиты персональных данных информационных систем рекомендуется осуществлять с учетом «Системного проекта подсистемы информационной безопасности единой системы информационно-аналитического обеспечения деятельности МВД России», с учетом особенностей «облачной» архитектуры.

Информационные системы персональных данных, которые введены в эксплуатацию в установленном порядке на основании пункта 3.1 приказа МВД России от 6 июля 2012 г. № 678, подлежат включению в

Перечень информационных систем персональных данных, который утверждается актом руководителя МВД России.

В целях своевременного внесения изменений в Перечень подразделения МВД России при вводе в эксплуатацию информационных систем или выводе их из эксплуатации в течение 10 дней после издания соответствующего приказа МВД России предоставляют в Департамент информационных технологий, связи и защиты информации МВД России для актуализации Перечня, в том числе реквизиты приказа МВД России о вводе и выводе в эксплуатацию информационных систем.

4. Механизм юридической ответственности за правонарушения в области обращения с персональными данными граждан

В соответствии с нормой статьи 24 Федерального закона «О персональных данных» на лиц, виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством Российской Федерации ответственность. Объектом противоправных посягательств, влекущих за собой реализацию указанных видов ответственности, выступают общественные отношения в сфере обращения персональных данных граждан, а предметом – информация, содержащая указанные данные.

Административная ответственность для операторов (за исключением лиц, для которых обработка персональных данных является профессиональной деятельностью и подлежит лицензированию) предусмотрена[1]:

– за отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо их несвоевременное предоставление, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 КоАП РФ);

– нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных (ст. 13.11 КоАП РФ);

---

[1] В соответствии со ст. 2.5. КоАП РФ за административные правонарушения, указанные в настоящем разделе, лица, имеющие специальные звания органов внутренних дел, несут дисциплинарную ответственность.

– разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет за собой уголовную ответственность), лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Деяниями, влекущими за собой уголовную ответственность, являются:

– незаконные сбор 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 произведении или средствах массовой информации (ст. 137 УК РФ);

– неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и 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 (ст. 140 УК РФ);

– неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло за собой уничтожение, блокировку, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272 УК РФ).

В рассматриваемой сфере общественных отношений наряду с административной и уголовной действует также механизм гражданско-правовой ответственности. Статьей 17 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусмотрено, что лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным ее неправомерным использованием, могут обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации в соответствии с порядком гражданского судопроизводства.

Федеральным законом от 2 июля 2013 г. № 142-ФЗ Гражданский кодекс Российской Федерации (часть первая) дополнен статьей 152^2 «Охрана частной жизни гражданина», в соответствии с нормами которой не допускаются без согласия гражданина 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 – за исключением случаев, когда иное прямо предусмотрено законом. При этом не является нарушением указанных правил сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле (п. 1 ст. 152^2 ГК РФ). Согласно п. 2 указанной статьи: стороны обязательства (в контексте настоящей работы – оператор персональных данных) 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. В соответствии с нормой пункта 3 указанной статьи 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. Согласно соответственно нормам п.п. 4 и 5:

– 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;

– право требовать защиты частной жизни гражданина способами, предусмотренными пунктом 2 ст. 150 и ст. 152^2 ГК РФ, в случае его смерти имеют дети, родители и переживший супруг такого гражданина.

В Постановлении от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» Пленум Верховного Суда Российской Федерации указал, что судам в практике их деятельности необходимо отграничивать дела о защите чести, достоинства и деловой репутации (ст. 152 ГК РФ) от дел о защите других нематериальных благ, перечисленных в ст. 150 ГК РФ, нарушенных в связи с распространением о гражданине сведений, неприкосновенность которых специально охраняется Конституцией Российской Федерации и законами, и распространение которых может причинить моральный вред даже в случае, когда эти сведения соответствуют действительности и не порочат честь, достоинство и деловую репутацию истца. В частности, при разрешении споров, возникших в связи с распространением информации о частной жизни гражданина, необходимо учитывать, что в случае, когда имело место распространение без согласия истца или его законных представителей соответствующих действительности сведений о его частной жизни, на ответчика может быть возложена обязанность компенсировать моральный вред, причиненный распространением такой информации (ст.ст. 150, 151 ГК РФ). Исключение составляют случаи, когда средством массовой информации была распространена информация о частной жизни истца в целях защиты общественных интересов на основании пункта 5 статьи 49 Закона Российской Федерации «О средствах массовой информации». Эта норма корреспондируется со статьей 8 Конвенции о защите прав человека и основных свобод. Если же имело место распространение не соответствующих действительности порочащих сведений о частной жизни истца, то ответчик может быть обязан опровергнуть эти сведения и компенсировать моральный вред, причиненный распространением такой информации, на основании ст. 152 ГК РФ[1].

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Бюллетень Верховного Суда Российской Федерации. – 2005. – № 4.

Судебное толкование относит к сведениям, неприкосновенность которых специально охраняется законами Российской Федерации, сведения, включенные в Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 г. № 188. В соответствии с пунктом 1 указанного Перечня к таковым отнесены сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях[1].

В соответствии с п.п. 28 и 29 Инструкции[2] дисциплинарную ответственность за нарушение режима защиты информационных систем для обработки персональных данных (ИСПДн) несут руководители подразделений МВД России, эксплуатирующих, а также использующих ИСПДн, администраторы ИСПДн, пользователи ИСПДн, непосредственно обрабатывающие ПДн в ИСПДн, и инженерно-технический персонал, имеющий доступ к ИСПДн в целях обеспечения устойчивого функционирования информационной системы при ее использовании, что отражается в должностных регламентах (должностных инструкциях) указанных лиц. Дисциплинарная ответственность реализуется совокупным действием норм Федеральных законов «О службе в органах внутренних дел и о внесении изменений в некоторые законодательные акты Российской Федерации» и «О полиции», Дисциплинарным уставом органов внутренних дел Российской Федерации, утвержденным указом Президента Российской Федерации от 14 октября 2012 г. № 1377, иными подзаконными актами по вопросам деятельности органов внутренних дел и организации полиции и ведомственными актами МВД России.

---

[1] Обзор практики рассмотрения судами Российской Федерации дел о защите чести, достоинства и деловой репутации, а также неприкосновенности частной жизни публичных лиц в области политики, искусства, спорта // Бюллетень Верховного Суда Российской Федерации. – 2007. – № 12; Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // Собр. законодательства Рос. Федерации. – 1997. – № 10, ст. 1127.

[2] Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» // Российская газета. – 2012 . – № 5903. – 5 окт.

5. Согласование законодательства о защите персональных данных с правовым регулированием в других сферах
(результаты мониторинга правоприменения)

Анализ судебной практики показывает, что при включении в правовую систему Российской Федерации законодательных норм, обеспечивающих защиту персональных данных, не было осуществлено их должного согласования с ранее принятым действующим законодательством. Конфликты законодательных норм возникают в судебной практике достаточно часто, и если некоторые из них решаются судами в целом единообразно, то по многим другим единых подходов в судебной практике не выработано. Ни сам Закон «О персональных данных», ни другие законодательные акты не содержат принципов и критериев, которые послужили бы ориентирами в разрешении коллизий, оставляя для правоприменителей множество затруднений.

Первая и наиболее очевидная проблема согласования законодательства о защите персональных данных с другими правовыми актами проявляется в ограничении пределов обеспечения конституционных прав на свободный оборот информации и на получение информации о деятельности государственных органов**.** Сам по себе конфликт между правом на защиту частной жизни (и соответственно ограничением доступа к персональным данным) и правом на получение информации носит вполне объективный характер. Законодателю следовало бы найти необходимый баланс между этими двумя конституционными правами, однако, это сделано недостаточно определенно, что оставляет правоприменительным органам широкое поле для усмотрения, а принятые решения не всегда выглядят убедительным решением проблемы поиска такого баланса[1].

Вторая проблема связана с ограничением возможностей передачи информации, содержащей персональные данные, тем лицам и организациям, которым она необходима для выполнения их функций или полномочий, либо обязательств по договорам.

---

[1] Согласование законодательства о защите персональных данных правовым регулированием в других сферах. Информация о результатах мониторинга правоприменени за февраль 2014 года. – URL http: // monitoring.law.edu.ru/otchety/2014/ fevral_2014_goda // Lfnfj,hfotybz – 13/09/2015/. Дата обращения 13.08.2015. Упоминаемые в данном разделе судебные решения цитируются по указанному источнику.

Работодатель, осуществляющий расследование дисциплинарного проступка, с точки зрения судов не вправе запрашивать информацию о работнике у третьих лиц без согласия на это самого работника, а при проведении служебной проверки Следственным комитетом и органом внутренних дел неправомерно были истребованы сведения, составляющие врачебную тайну, без согласия субъекта персональных данных[1].

Применение законодательства о защите персональных данных зачастую происходит таким образом, что фактически создаются препятствия для реализации прав, гарантированных другими законодательными актами – прежде всего, права на доступ к информации**,** необходимой для реализации прав конкретного лица.

При рассмотрении дел об оценке правомерности отказов в предоставлении информации суды иногда весьма своеобразно и не всегда последовательно определяют, какая информация затрагивает права заявителя непосредственно и поэтому должна быть предоставлена несмотря на содержащиеся в ней персональные данные, а в каких случаях защита персональных данных не позволяет предоставить эту информацию.

При проведении конкурса на замещение должности государственной службы суд признал за соискателем должности право получить возможность ознакомиться с протоколом заседания конкурсной комиссии, определяющим уровень профессиональной подготовки победившего кандидата[2]. При этом в рамках самой процедуры конкурса на замещение публичной должности (главы муниципального образования) истребование характеристики на одного из претендентов с прежнего места работы – органа внутренних дел – было признано судом незаконным[3]. Положения законодательства об административных правонарушениях трактуются в судебной практике как предоставляющие абсолютное право лицу, в отношении которого ведется производство, знакомиться со всеми материалами дела, в том числе с заявлением гражданина, инициировавшего это производство. Суды не принимают во

---

[1] Решение Кировского районного суда г. Кемерово от 14 июня 2011 г. по делу № 2-349-11; Решение Верховного Суда Республики Башкортостан от 4 сентября 2011 г. (номер дела обезличен).

[2] Решение Свердловского районного суда города Белгорода от 30 марта 2011 г. по делу № 2-941/2011.

[3] Решение Пестяковского районного суда Ивановской области от 3 ноября 2010 г. по делу № 2–254/ 10.

внимание не только защиту персональных данных, но и опасность угроз и преследований со стороны лица, в отношении которого ведется производство[1].

Законодательные акты, непосредственно не регулирующие вопросы оборота персональных данных, в некоторых случаях дают основания для их обработки, в некоторых случаях ссылки на подобные основания суды признают необоснованными. Законодательство о социальной защите, возлагающее на органы публичной власти полномочия по обеспечению социальной защиты граждан, может рассматриваться как основание для оборота персональных данных без согласия гражданина, в частности меры социальной помощи могут оказываться без заявления самого гражданина по инициативе уполномоченного органа[2].

Управление юстиции в субъекте Российской Федерации на основании части третьей ст. 8 Федерального закона «О свободе совести и о религиозных объединениях» может проводить проверку достоверности представленного перечня членов местной религиозной организации, в том числе с уточнением их места жительства и возраста, несмотря на то, что сведения о религиозной принадлежности относятся к особо охраняемым законом персональным данным[3].

Законодательство о государственной службе дает основания для признания правомерной передачи личного дела уволенного со службы госслужащего из одного органа в другой в пределах системы налоговых органов[4]. В то же время размещение на сайте государственного органа сведений о бывшем служащем (сведения об имуществе и доходах), размещенных в соответствии с требованием закона до его увольнения со службы, признано неправомерным, поскольку прекращение служебных отношений лишает размещение такой информации на сайте правового основания[5].

---

[1] Апелляционное определение судебной коллегии по гражданским делам Свердловского областного суда от 25 сентября 2012 г. по делу №33-11387/2012.

[2] Решение Измайловского районного суда г. Москвы от 20 января 2011 г. (номер дела обезличен).

[3] Решение Мытищинского городского суда Московской области от 17 марта 2011 г. (номер дела обезличен).

[4] Определение Нижегородского областного суда от 18 января 2011 г. № 33-66/11.

[5] Решение Железнодорожного районного суда г. Улан-Удэ от 27 апреля 2011 г. по делу № 2-1162/2011.

6. Основные направления научно-правовых исследований по совершенствованию систем и методов защиты персональных данных

Информатизация современного общества, создание и широкое использование различными государственными и частными структурами компьютеризированных баз данных о гражданах, активное участие России в международном информационном обмене придают особую актуальность задаче обеспечения правовой защиты информации о частной жизни граждан.

Одна из главных проблем защиты личной информации состоит в латентном характере посягательств на частную жизнь граждан: субъект данных может и не догадываться о незаконном сборе, обработке, хранении, уничтожении, передаче его персональных данных, а также о внесении в эти данные преднамеренных искажений. Применяемые правоохранительными органами меры не всегда адекватны степени возникающих угроз в этой сфере, что обусловливает необходимость применения дополнительных мер защиты информации в целях обеспечения информационной безопасности страны, защиты частной жизни граждан от преступных посягательств. Деятельность, связанная с защитой личных секретов человека, его персональных данных требует комплексного подхода, сочетающего в себе применение эффективных правовых, организационных и технических мер[1].

По мнению аналитиков, основная проблема в области защиты персональных данных – это большое количество операторов ПДн, их общее число составляет 5–7 млн, а на сегодняшний день в реестре Роскомнадзора зарегистрировано всего 190 тысяч. Вторая проблема – запутанность регулирования в области ПДн. В это вовлечено много ведомств, включая ФСБ, ФСТЭК, Роскомнадзор, Роструд, для банков – Банк России, которые часто предъявляют противоречивые требования. С другой стороны, ответственность за несоблюдение норм 152-ФЗ такова, что некоторые организации придерживаются позиции, что де-

[1] Даукаев И. М., Журавленко Н. И. Проблемы правовой и организационной защиты персональных данных : монография. Уфа : БашГУ // Международный журнал экспериментального образования. – 2013. – № 9. – С. 62.

шевле платить штрафы, чем реализовать весь комплекс мер по защите ПДн согласно закону.

Проблема защиты персональных данных связана и со степенью развитости институтов гражданского общества. К сожалению, в России низкий уровень развития подобных институтов, низкая правовая культура граждан, а также недостаточный уровень активности граждан и большая степень закрытости власти. Именно поэтому вопросы защиты персональных данных, как, впрочем, и многие другие, обсуждаются и прорабатываются сравнительно небольшой группой специалистов и правозащитных организаций, при этом сами граждане либо не считают эти вопросы значимыми, либо, чаще всего, просто не знают о наличии своих прав, их нарушениях и о том, как можно их защитить. При этом ущерб при неправомерном доступе и распространении информации о персональных данных наносится, в первую очередь, интересам самих граждан. Таким образом, наряду с правовыми и организационно-техническими мероприятиями необходимо повышать степень открытости власти и уровень информированности граждан о своих правах, законных интересах и о методах их защиты.

Повышение уровня безопасности личности в современных условиях делового оборота, информационного общества и активного применения интегрированных электронных информационных систем представляет собой крупную научную проблему, в рамках которой необходимо решение следующих научных задач:

– идентификации и аутентификации личности в виртуальном пространстве и в электронных информационных системах (включая, как частный случай, дистанционную идентификацию и аутентификацию);

– определения прав личности при выполнении экономически и юридически значимых действий;

– создания системы санкционирования действий субъектов, пользующихся электронными информационными системами;

– создания средств и методов установления истинного хода событий и действий в ретроспективе;

– разработки методик широкомасштабного обучения безопасному существованию и безопасной деловой активности в условиях совре-

менного информационного общества при непосредственном использовании электронных информационных систем;

– интеграции технических задач информационной безопасности с задачами педагогики безопасности в области осуществления мер по обеспечению безопасности личности[1].

Анализ зарубежного опыта свидетельствует о том, что модернизация европейского законодательства в области защиты персональных данных направлена на усиление региональной интеграции. В Европейском Союзе предполагается передача отдельных областей правового регулирования их защиты на наднациональный уровень. Исследуются вопросы формирования особого юридического пространства за пределами национальных юрисдикций для сторон «Конвенции о защите физических лиц при автоматизированной обработке персональных данных»[2].

При этом вопрос об установлении специального состава преступления, предусматривающего уголовную ответственность за совершение незаконных действий в отношении персональных данных, является дискуссионным. Далеко не каждый факт незаконного собирания и распространения сведений, составляющих персональные данные, является общественно опасным и требует защиты со стороны самого репрессивного права, уголовного права. Даже за распространение сведений о частной жизни привлечение к ответственности виновных является весьма проблематичным. Потерпевшие не всегда считают указанные нарушения особо значимыми, либо, чаще всего, просто не знают о наличии своих прав, их нарушениях и о том, как можно их защитить[3].

Исходя из изложенного выше представляется необходимым:

---

[1] Сиротский А. А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде // Интернет-журнал «Технологии техносферной безопасности» (http: // ipb.mos.ru/ttb) Выпуск № 4 (50). – 2013.

[2] Егошина Г. Г. Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции // Теория и практика общественного развития. – 2014. – № 3. – С. 128.

[3] Гарбатович Д. А. Защита персональных данных уголовным правом // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2(4); Сулейманова С. Т. К вопросу об уголовной ответственности за нарушение неприкосновенности частной жизни в сфере трудовых отношений // Социальное и пенсионное право. – 2009. – № 3. – С. 35–37.

1) конкретизировать случаи предоставления персональных данных заинтересованным органам и лицам без согласия субъектов персональных данных. При этом во избежание двоякого толкования норм следует уйти от общих формулировок, таких как «для осуществления правосудия», «в целях защиты основ конституционного строя»;

2) при предоставлении неограниченному кругу лиц доступа к информации о деятельности судов и органов государственной власти для обеспечения безопасности субъектов персональных данных необходимо установить ответственность должностных лиц за несоблюдение требований обезличивания персональных данных;

3) усовершенствовать комплекс организационно-технических мероприятий по защите персональных данных, вводимых в государственные информационные системы во избежание хищения или использования персональных данных граждан в противоправных целях.

Законодатель допускает использование обезличенных персональных данных без согласия их субъекта в целях проведения статистических, социологических, исторических, медицинских и других научных и практических исследований.

В Федеральном законе «О персональных данных» с обезличиванием связана: статья 3, пункт 9: «Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных».

Процедура обезличивания персональных данных регламентирована Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утвержденных приказом Роскомнадзора от 5 сентября 2013 г. № 996[1].

---

[1] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Зарегистрировано в Минюсте России 10 сентября 2013 г., рег. № 2993 // Российская газета. – 2013. – № 208. – 18 сен.; Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. ФС по надзору в сфере связи, информационных технологий и массовых коммуникаций 13.12.2013 г., текст методических рекомендаций официально опубликован не был).

II. УГРОЗЫ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, МОДЕЛЬ НАРУШИТЕЛЯ

Рассматриваемая в настоящей работе модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн, обрабатывающих специальные категории персональных данных. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный (природный) характер, воздействующих на уязвимости ИСПДн, характерных для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн. Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, приведенные в настоящей Модели, подлежат адаптации в ходе разработки частных (детализированных) моделей угроз.

1. Исходная информация: характеристики объекта информатизации, обрабатываемых персональных данных и показателей безопасности

Исходя из основных характеристик, особенностей ИСПДн и решаемых ими задач в качестве объекта информатизации выступают:

1) автономные автоматизированные рабочие места (АРМ);

2) локальные вычислительные сети (ЛВС);

3) распределенные вычислительные сети;

4) информационные (автоматизированные) системы, в том числе состоящие из ЛВС и автономных средств вычислительной техники.

В зависимости от характеристик и особенностей отдельных объектов часть средств вычислительной техники подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта

ПДн), так и с электронных носителей информации. ИСПДн предполагают как распределенную (на АРМ), так и централизованную (на выделенных файловых серверах сети) обработку и хранение ПДн.

Согласно положениям «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК РФ 15 февраля 2008 г., 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.

Контролируемая зона (КЗ) ИСПДн охватывает здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

Учитывая особенности обработки ПДн, а также виды и категории обрабатываемых в ИСПДн персональных данных, основными показателями безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность понимается как обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Целостность понимается как состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность понимается как состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, копи-

рование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов.

В дополнение к перечисленным выше основным характеристикам безопасности в ИСПДн могут рассматриваться также и другие характеристики безопасности:

– отказоустойчивость;

– журналирование событий;

– идентификация и аутентификация;

– адекватность.

Отказоустойчивость понимается как способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.

Журналирование событий понимается как обеспечение того, что действия субъекта по отношению к объекту (ПДн) могут быть прослежены уникально по отношению к субъекту.

Аутентичность понимается как свойство, гарантирующее, что субъект или ресурс ПДн идентичны заявленным.

Адекватность понимается как свойство соответствия преднамеренному поведению и результатам.

2. Способы нарушения характеристик безопасности персональных данных

Исходя из перечня персональных данных, обрабатываемых в специальных ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

− хищение персональных данных сотрудниками для использования в корыстных целях;

− передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;

− несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам;

− несанкционированное получение персональных данных третьими лицами;

− уничтожение финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− модификация финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− блокирование финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− передача некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− искажение архивной информации по субъекту ПДн.

3. Угрозы безопасности персональных данных при их обработке в специальных информационных системах персональных данных

(содержание угроз и их источники)

Норма Федерального закона «О персональных данных» (ч. 11 ст. 19) закрепляет дефиницию «угрозы (угроз) безопасности персональных данных» как 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.

Под угрозами безопасности персональных данных при их обработке в ИСПДн подразумевается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные

действия могут исходить и от сотрудников в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

− по видам возможных источников угроз;

− типу ИСПДн, на которые направлена реализация угроз;

− виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

− способам реализации угроз;

− используемой уязвимости;

− объекту воздействия.

Для специальных ИСПДн существуют следующие классы угроз безопасности ПДн:

По видам возможных источников угроз безопасности персональных данных:

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИР ИСПДн, включая пользователей, реализующих угрозы непосредственно в ИСПДн;

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

– угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

– угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

− угрозы безопасности данных, обрабатываемых в ИСПДн на базе автоматизированных рабочих мест;

− угрозы безопасности данных, обрабатываемых в ИСПДн на базе локальных информационных систем;

− угрозы безопасности данных, обрабатываемых в ИСПДн на базе распределенных систем.

По способам реализации угроз выделяют следующие классы угроз:

− угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);

− угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);

− угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующие классы угроз:

− угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации.

− приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;

− приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.

По используемой уязвимости выделяются следующие классы угроз:

− реализуемые с использованием уязвимости системного программного обеспечения (ПО);

− реализуемые с использованием уязвимости прикладного ПО;

− возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;

− реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

− возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;

− реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

− реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия выделяются следующие классы угроз:

− угрозы безопасности ПДн, обрабатываемых на АРМ;

− угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т. п.);

− безопасности ПДн, передаваемых по сетям связи;

− прикладным программам, с помощью которых обрабатываются ПДн;

− системному ПО, обеспечивающему функционирование ИСПДн.

При разработке частных (детализированных) моделей угроз должны учитываться подходы, изложенные в настоящей Модели, с детализацией угроз в соответствии с документом ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

3.1. Антропогенные источники угроз безопасности персональных данных

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким

источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т. п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизация работы, вывод систем предприятия из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками предприятий отрасли, имеющими доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

– непредумышленное искажение или удаление программных компонентов;

– внедрение и использование неучтенных программ;

– игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации, в частности:

• нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);

• предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;

• настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

• несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

− угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников предприятия, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);

− угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель) (в случае распределенных ИСПДн);

− угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.

3.2. Техногенные источники угроз безопасности персональных данных

Техногенные источники угроз напрямую зависят от свойств техники. Источники данной категории могут также быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т. п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки.

Аппаратная закладка. Аппаратные закладки могут быть конструктивно встроенными и автономными. Конструктивно встроенные аппаратные закладки создаются в ходе проектирования и разработки аппаратного обеспечения, применяемого в ИСПДн и могут проявляться в виде недекларированных возможностей различных элементов вычислительной системы. Автономные аппаратные закладки являются законченными устройствами, выполняющими определенные функции перехвата, накопления, передачи или ввода/вывода информации. Например, функции автономной аппаратной закладки может выполнять сотовый телефон, несанкционированно подключаемый к ТС ИСПДн.

Учитывая, что аппаратные закладки представляют собой некоторый элемент технических средств (ТС), скрытно внедряемый или подключаемый к ИСПДн и обеспечивающий при определенных условиях реализацию несанкционированного доступа или непосредственное выполнение некоторых деструктивных действий, в них, как правило, содержатся микрокоманды, обеспечивающие взаимодействие закладки с программно-техническими средствами (ПТС) ИСПДн.

Аппаратные закладки могут реализовать угрозы:

− сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;

− формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях (этапах) жизненного цикла ИСПДн.

Носитель вредоносной программы. В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющий роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

− внешний машинный (отчуждаемый) носитель, т. е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т. п.;

− встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства – видеоадаптера, сетевой платы, устройств ввода/вывода магнитных жестких, оптических и лазерных дисков, блока питания и т. п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

− микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т. п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

− пакеты передаваемых по сети ИСПДн сообщений;

− файлы (исполняемые, текстовые, графические и т. д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

3.3. Природные (стихийные) источники угроз безопасности персональных данных

Стихийные источники угроз отличаются большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к предприятию. Это различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Следует отметить, что, защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, в основном регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн и действующей нормативной базы.

4. Модель нарушителя безопасности персональных данных

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации.

2. Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований.

3. СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

4.1. Классификация нарушителей

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.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

− категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;

− категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются:

− на внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

− бывшие сотрудники;

− посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;

− представители преступных организаций.

Внешний нарушитель может осуществлять:

− перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

− деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ;

− несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;

− перехват информации, передаваемой по сетям связи общего пользования, или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами;

− атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К первой группе относятся сотрудники, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации. Лицо данной группы может:

− располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

− изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

2. Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей. Лицо данной группы:

− обладает всеми возможностями лиц первой категории;

− знает, по меньшей мере, одно легальное имя доступа;

− обладает всеми необходимыми атрибутами, например, паролем, обеспечивающим доступ к ИР ИСПДн;

− располагает ПДн, к которым имеет доступ.

3. К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной или распределенной сети предприятий. Лицо данной группы:

− обладает всеми возможностями лиц второй категории;

− располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;

− имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

4. К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн. Лицо данной группы:

− обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;

− обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;

− имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;

− имеет доступ ко всем техническим средствам сегмента ИСПДн;

− обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

5. К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа. Лицо данной группы:

− обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;

− обладает полной информацией о ТС и конфигурации ИСПДн;

– имеет доступ ко всем ТС ИСПДн и данным;

− обладает правами конфигурирования и административной настройки ТС ИСПДн.

6. К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор. Лицо данной группы:

− обладает полной информацией об ИСПДн;

− имеет доступ к средствам защиты информации и протоколирования, а также, к части ключевых элементов ИСПДн;

− не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7. К седьмой группе относятся лица из числа программистов-разработчиков сторонней организации, являющихся поставщиками ПО, и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн. Лицо данной группы:

− обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

− обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

− может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

8. К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн. Лицо данной группы:

− обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;

− может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

4.2. Моделируемые алгоритмы действий нарушителей

Для получения исходных данных о ИСПДн нарушитель (как I, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

К указанным приведенным возможностям, которыми обладают различные группы внутренних нарушителей, может быть приведен ряд дополнительных возможностей, которые присущи всем группам внутреннего нарушителя.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные:

− на предотвращение и пресечение несанкционированных действий;

− подбор и расстановку кадров;

− допуск физических лиц в контролируемую зону и к средствам вычислительной техники;

− контроль над порядком проведения работ.

В силу указаного внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты, и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности. Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

4.3. Средства, применяемые нарушителями, и используемые каналы атак

Предполагается, что нарушитель имеет все необходимые средства для проведения атак по доступным ему каналам атак.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

− доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;

− специально разработанные технические средства и программное обеспечение;

− средства перехвата и анализа информационных потоков в каналах связи;

− специальные технические средства перехвата информации по ТКУИ;

− штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных

средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

Возможные каналы атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

− каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);

− электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;

− бумажные носители информации;

− штатные программно-аппаратные средства ИСПДн;

− кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;

− незащищенные каналы связи;

− технические каналы утечки информации.

5. Меры противодействия нарушителям

(минимальные требования)

В соответствии с нормой Федерального закона «О персональных данных» (часть 1 ст. 19) 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.

Часть вторая указанной статьи конкретизирует меры и условия, необходимые для решения этой задачи. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) 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;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) 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;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Согласно части 10 указанной статьи 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.

В условиях современных тенденций функционирования организаций большинство работников в процессе исполнения служебных обязанностей так или иначе сталкиваются с информацией ограниченного доступа, что делает их как объектом, так и субъектом информационных угроз. Таким образом, персонал (для органов внутренних дел – личный состав) становится важным человеческим фактором, который необходимо учитывать при построении системы защиты информации в орга-

низации и, в частности, системы защиты персональных данных. Для решения указанных задач необходимо обеспечить[1]:

1) правильный подход к подбору персонала и организацию дальнейшей работы с ним, включающей:

– проведение семинаров и инструктажей по общим вопросам и правилам обработки информации ограниченного доступа, в том числе 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;

– формирование единой культуры деятельности по вопросам обеспечения информационной безопасности в организации, включая информирование персонала о возможных последствиях нарушения установленных принципов и норм.

2) проектирование и организация контролируемой зоны, включая:

– определение границ контролируемой зоны;

– определение мер и средств физической защиты информации;

– определение мер и средств технической защиты информации;

– организацию пунктов пропуска/проезда на территорию организации;

– организацию пропускного режима;

– регламентацию работы и допуска персонала к защищаемой информации, включая персональные данные сотрудников и иных граждан;

– формирование правил учета лиц, получивших доступ к работе с информацией ограниченного доступа, в том числе – с персональными данными.

[1] Исаев А. С., Хлюпина Е. А. Правовые основы организации защиты персональных данных. СПб. : НИУ ИТМО, 2014. С. 55.

ЗАКЛЮЧЕНИЕ

1. Совокупность источников права, выражающих и закрепляющих нормы, устанавливающих порядок обращения и защиты персональных данных физического лица, является многоэлементной и имеет сложную многоуровневую структуру. Она включает в себя:

– акты международного права, содержащие общепризнанные принципы и нормы, признаваемые и применяемые международным сообществом государств в целом, в качестве юридически обязательных, отступление от которых невозможно. В качестве источников права перечисленные акты относятся к категории правовых договоров;

– акты национального (в контексте целей настоящей работы – российского) законодательства. Данный массив источников права является наиболее обширным и многообразным. Он включает конституционно-правые акты (Конституцию Российской Федерации, Декларацию прав и свобод человека и гражданина, федеральные конституционные законы), федеральные законы, подзаконные акты – Указы и Распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, акты (приказы, инструктивные письма и т. д.) федеральных органов исполнительной власти, законы и акты органов исполнительной власти субъектов Российской Федерации, акты органов местного самоуправления, акты судебного толкования норм права и иные материалы судебной практики.

2. Закрепляющие информационно-правовой статус и регулирующие информационно-правовые отношения акты могут быть классифицированы путем отнесения к категориям:

– материального или процессуального законодательства;

– регулятивного (позитивного) или правоохранительного.

Один из первичных критериев отнесения нормативного правового акта к той или иной категории является излагаемое в его вводной части содержание:

– целей, задач и функций данного акта;

– регулируемых данным актом правовых отношений – регулятивных или правоохранительных.

Производным критерием может быть признано количественное соотношение положений (статей) нормативного правового акта, закреп-

ляющих соответственно материальные или процессуальные и регулятивные либо охранительные нормы права.

3. Основными составляющими системы государственного контроля и надзора за обеспечением безопасности персональных данных при их обработке в информационных системах являются:

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – уполномоченный орган по защите прав субъектов персональных данных;

– Федеральная служба безопасности – федеральный орган исполнительной власти, уполномоченный в области обеспечения государственной безопасности и применения средств шифрования;

– Федеральная служба по техническому и экспортному контролю и противодействия иностранным разведкам – уполномоченный орган в области контроля используемых технических средств защиты;

– Министерство связи и информационных технологий Российской Федерации – уполномоченный орган в области контроля над порядком проведения классификации информационных систем, содержащих персональные данные.

4. Практически все акты материального (регулятивного) законодательства содержат охранительные положения (статьи) об ответственности за их нарушение. В большинстве случаев эти положения излагаются бланкетным способом: указывается, что нарушение норм конкретного акта влечет за собой для виновных субъектов уголовную, административную, гражданско-правовую, материальную или иную предусмотренную законом ответственность. Однако возможно и непосредственное закрепление норм об ответственности в тексте регулятивного акта. Примером могут служить положения ГК РФ – ст.ст. 152 «Защита чести, достоинства и деловой репутации», 152^1 «Охрана изображения гражданина» и 152^2 «Охрана частной жизни гражданина».

5. В соответствии с частью 1 статьи 17 Федерального закона от № 3-ФЗ «О полиции» полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах, при этом обеспечивает защиту информации, содержащейся в

банках данных, от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.

Информация, содержащаяся в банках данных, предоставляется государственным органам и их должностным лицам только в случаях, предусмотренных федеральным законом; правоохранительным органам иностранных государств и международным полицейским организациям в соответствии с международными договорами Российской Федерации.

6. Защита информации, в том числе персональных данных, осуществляется в системе МВД России в соответствии с нормами законодательства Российской Федерации о защите информации, а также иными нормативными правовыми актами Российской Федерации и государственными стандартами.

Обработка персональных данных в системе органов внутренних дел может осуществляться в следующих целях:

1) трудоустройства, содействия сотруднику в прохождении службы в органах внутренних дел, обучении и должностном росте, обеспечения личной безопасности сотрудника и работника, учета результатов выполнения им служебных обязанностей;

2) обработки данных физических лиц, совершивших административные правонарушения или уголовные преступления, осуществляемых для установления личности, документирования обстоятельств совершения административного правонарушения или уголовного преступления, составления протокола по делу об административном правонарушении или заполнения бумаг в уголовном деле, обеспечения установленного порядка производства по делам об административных правонарушениях или уголовных преступлениях.

Обработка персональных данных сотрудника включает в себя производимые органами внутренних дел в лице уполномоченных его представителей (как правило, сотрудников кадрового аппарата) следующие операции (действия):

а) по получению; б) хранению; в) комбинированию; г) передаче персональных данных работника или иному их использованию.

Руководители подразделений МВД России могут издавать локальные правовые акты по вопросам защиты персональных данных при их обработке в информационных системах персональных данных.

7. Рассмотренная в работе модель угроз безопасности персональных данных представляет собой основу для разработки частных (детализированных) моделей угроз безопасности персональных данных для специальных ИСПДн конкретных подразделений или их групп с учетом назначения, условий и особенностей функционирования, учитывающих:

− структуру информационной системы;

− наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

− режим обработки персональных данных;

− режим разграничения прав доступа пользователей информационной системы;

− местонахождение технических средств информационной системы, а также проведение оценки актуальности угроз безопасности персональных данных.

8. В условиях современных тенденций функционирования организаций большинство работников в процессе исполнения служебных обязанностей так или иначе сталкиваются с информацией ограниченного доступа, что делает их как объектом, так и субъектом информационных угроз. Таким образом, персонал (для органов внутренних дел – личный состав) становится важным человеческим фактором, который необходимо учитывать при построении системы защиты информации в организации и, в частности, системы защиты персональных данных. Для решения указанных задач необходимо обеспечить: 1) правильный подход к подбору персонала и организацию дальнейшей работы с ним; 2) проектирование и организацию контролируемой зоны организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Акты международного права

1. Устав Организации Объединенных Наций. Подписан 26 июня 1945 г. в Сан-Франциско на заключительном заседании Конференции Объединенных Наций по созданию Международной Организации, вступил в силу 24 октября 1945 г. (составной частью Устава является Статут Международного Суда) – в редакции на 12 июня 1968 г. URL http://www.un.org/ru/documents/charter/chapter19.shtml. Дата обращения 15.12.2013.

2. Всеобщая декларация прав человека. Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. URL http://www.un.org/ru/documents/decl_conv/declarations/declhr. Дата обращения 09.08.2014.

3. Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 г. *UnitedNations, TreatySeries, vol. 999, p. 225-240, 315–317.* – URL http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml. Дата обращения 09.08.2014. Вступил в силу 23 марта 1976 г.

4. Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г., 13 мая 2004 г.). URL http://base.garant.ru/2540800/#ixzz39vIWoYsb. Дата обращения 09.08.2014.

5. Статут Международного Суда Организации Объединенных Наций (глава XIV Устава ООН:Международный Суд / Приложение к Уставу ООН). URL http://www.un.org/ru/icj/statut.shtml. Дата обращения 20.08.2014

6. Римский статут Международного Уголовного Суда. / Принят на Дипломатической конференции полномочных представителей под эгидой ООН по учреждению Международного Уголовного Суда, Рим, 17 июля 1998 г. МИД РФ. URL http://www.mid.ru/ns-dmo.nsf/f1010b0687f6c452432569f400359178/389cbd5310e3b88943256beb00259854. Дата обращения 20.08.2014.

7. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Российская газета. – 1993. – № 237[1]. – 25 дек.

8. Постановление Верховного Совета РСФСР от 22 ноября 1991 г. № 1920-I «О Декларации прав и свобод человека и гражданина». Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. – 1991. – № 52, ст. 1865.

9. Закон Российской Федерации от 27 декабря 1991 г. 2124-I «О средствах массовой информации». Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 7, ст. 300.

10. Закон Российской Федерации от 17 января 1992 г. № 2202-I «О прокуратуре Российской Федерации». Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 8, ст. 366; Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 1992 г., № 8, ст. 366.

11. Федеральный конституционный закон от 27 июля 1994 г. № 1-ФКЗ «О Конституционном Суде Российской Федерации». Собр. законодательства Рос. Федерации. – 1994. – № 13, ст. 1447.

12. Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ // Собр. законодательства Рос. Федерации. – 1994. – № 32, ст. 330.

13. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» // Собр. законодательства Рос. Федерации. – 1995. – № 15, ст. 1269.

14. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собр. законодательства Рос. Федерации. – 1995. – № 33, ст. 3349.

[1] Здесь и далее (если не указаны иные источники правовой информации) использовались официальные тексты (в действующей редакции) нормативных правовых актов, размещенные в информационно-правовой системе «Законодательство России» официального интернет-портала правовой информации (Государственная система правовой информации): URL http: // www.pravo.gov.ru/.

15. Семейный кодекс Российской Федерации от 29 декабря 1995 г. № 223-ФЗ. Собр. законодательства Рос. Федерации. – 1996. – № 1, ст. 16.

16. Гражданский кодекс Российской Федерации. Часть вторая, от 26 января 1996 г. № 14-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 5, ст. 41.

17. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

18. Федеральный конституционный закон от 31 декабря 1996 г. № 1-ФКЗ «О судебной системе Российской Федерации» // Собр. законодательства Рос. Федерации. – 1997. – № 1, ст. 1.

19. Федеральный закон от 21 июля 1997 г. № 118-ФЗ «О судебных приставах». // Собр. законодательства Рос. Федерации. – 1997. – № 30, ст. 3590.

20. Федеральный закон от 25 июля 1998 г. «О государственной дактилоскопической регистрации в Российской Федерации». // Российская газета. – 1997. – № 145. – 1 авг.

21. Федеральный конституционный закон от 26 февраля 1997 г. «Об Уполномоченном по правам человека в Российской Федерации» // Собр. законодательства Рос. Федерации. – 1997. – № 9, ст. 1011.

22. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собр. законодательства Рос. Федерации. – 2001. – № 52, ст. 4921.

23. Федеральный закон от 25 января 2002 г. № 8-ФЗ «О всероссийской переписи населения» // Российская газета. – 2002. – №17. – 29 янв.

24. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 1, ст. 1.

25. Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // Собр. законодательства Рос. Федерации. – 2006. – № 19, ст. 2060; 2010. – № 27, ст. 3410; № 31, ст. 4196; 2013. – № 19, ст. 2307; № 27, ст. 3474.

26. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3448 *(Часть I).*

27. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»// Собр. законодательства Рос. Федерации. – от 2006 г., № 31, ст. 3451 (Часть I); «Российская газета» от 29.7.2006 г. (№ 165); «Парламентская газета». – 2006. – № 126-127. – 03 авг.

28. Федеральный закон от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве» // Собр. законодательства Рос. Федерации. – 2007. – № 41, ст. 4849.

29. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности». // Собр. законодательства Рос. Федерации. – 2011. – № 1, ст. 2.

30. Федеральный закон от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации» // Собр. законодательства Рос. Федерации. – 2011. – № 1, ст. 15.

31. Федеральный конституционный закон от 7 февраля 2011 г. № 1-ФКЗ «О судах общей юрисдикции в Российской Федерации» // Собр. законодательства Рос. Федерации. – 2011. – № 7, ст. 898.

32. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Собр. законодательства Рос. Федерации. – 2011. – № 7, ст. 900.

33. Федеральный закон от 30 декабря 2011 г. № 342-ФЗ «О службе в органах внутренних дел и внесении изменений в отдельные законодательные акты Российской Федерации» // Собр. законодательства Рос. Федерации. – 2011. – № 49, ст. 7020 *(Часть I).*

34. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // Собр. законодательства Рос. Федерации. – 1997. – № 10, ст. 1127.

35. Указ Президента Российской Федерации от 12.мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Собр. законодательства Рос. Федерации. – 2009. – № 20, ст. 2444.

36. Указ Президента Российской Федерации от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации» (об утверждении Положения о Министерстве внутренних дел

Российской Федерации) // Собр. законодательства Рос. Федерации. – 2011. – № 10, ст. 1334.

37. Указ Президента Российской Федерации от 1 марта 2011 г. № 250 «Вопросы организации полиции» // Собр. законодательства Рос. Федерации. – 2011. – № 10, ст. 1336.

38. Указ Президента Российской Федерации от 14 октября 2012 г. № 1377 «О Дисциплинарным уставе органов внутренних дел Российской Федерации» // Собр. законодательства Рос. Федерации. – 2012. – № 43, ст. 5808.

39. Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» // Собр. законодательства Рос. Федерации. – 2006. – № 5, ст. 553.

40. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». // Российская газета. – 2012. – № 5929. – 7 нояб.

41. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». // Российская газета. – 2013. – № 6112. – 26 июня.

42. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». // Российская газета. – 2013. – № 107. – 22 мая.

43. Приказ Министерства внутренних дел Российской Федерации от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации». // Российская газета. – 2012. – № 5903. – 5 окт.

44. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г.

№ 996 «Об утверждении требований и методов по обезличиванию персональных данных». Зарегистрировано в Минюсте России 10 сентября 2013 г., регистрационный № 2993. Российская газета. – 2013. – № 208. – 18 сент.

45. Приказ Министерства внутренних дел Российской Федерации от 12 сентября 2013 г. № 707 «Об утверждении инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации. Зарегистрировано в Минюсте России 31 декабря 2013 г. № 30957.

46. Приказ МВД России от 28 апреля 2014 г. № 381 «О некоторых вопросах централизованного учета персональных данных сотрудников органов внутренних дел Российской Федерации, граждан Российской Федерации, поступающих на службу в органы внутренних дел Российской Федерации»: с Приложениями №№ 1, 2. Российская газета. 6 августа 2014 г. Федеральный выпуск №6447. Зарегистрировано в Минюсте 4 июня 2014 г., регистрационный № 32562.

47. Доктрина информационной безопасности Российской Федерации – утверждена Президентом Российской Федерации, от 5 декабря 2016 г. № Пр-1895.

Специальная литература

48. Бабурина И. А., Сафронов В. В. Защита персональных данных. – Основные тенденции развития российского законодательства. – Красноярск, 2012.

49. Гарбатович Д. А. Защита персональных данных уголовным правом // Вестник УрФО. Безопасность в информационной сфере № 2(4). – 2012.

50. Даукаев И. М., Журавленко Н. И. Проблемы правовой и организационной защиты персональных данных: монография. *БашГУ, Уфа. //* Международный журнал экспериментального образования. – 2013. – №9.

51. Додонов В. Н., Ермаков В. Д., Крылова М. А. и др. Большой юридический словарь. – М., 2001.

52. Долгушина С. В. Теория государства и права. Введение в юриспруденцию. / [С.В. Долгушина и др.]; под ред. В. П. Малахова, С. В. Долгушиной. – М., 2012.

53. Егошина Г. Г. Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции / Теория и практика общественного развития. – 2014. – № 3. – С. 128.

54. Журавленко Н. И. Тайна частной жизни и защита персональных данных: монография. Уфа: РИЦ БашГУ, 2013.

55. Защита свободы информации в практике Европейского суда по правам человека. – Представлено Юридической компанией ЛЕГАС. – Москва, Вологда. URL http://legascom.ru/notes/813-zachita-svobodi-informacii-v-praktike-esph?tmpl=component&print=1&layout=default&page=. Обновлено 23.07.2014 14:05, дата обрашения 20.08.2014.

56. Зыкова С. В., Кулакова Ю. Ю., Лановая Г. М. Юридическая техника : учебное пособие. – М. : Московский университет МВД России, 2008.

57. Исаев А. С., Хлюпина Е. А. Правовые основы организации защиты персональных данных. СПб. : НИУ ИТМО, 2014.

58. Кашанина Т. В. Юридическая техника. – М. : Норма, ИНФРА М, 2013.

59. Кучин И. Ю. Защита конфиденциальности персональных данных с помощью обезличиывния // Вестник АГТУ Сер.: Управление, вычислительная техника и информатика. – 2010. – № 2.

60. Сиротский А. А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде**.** / Интернет-журнал «Технологии техносферной безопасности» (http://ipb.mos.ru/ttb). – 2013. – № 4 (50).

61. Согласование законодательства о защите персональных данных правовым регулированием в других сферах. / эксперт – к.ю.н., доцент кафедры государственного и административного права СПбГУ Белов С. А. – Информация о результатах мониторинга правоприменени за февраль 2014 года. URL http://monitoring.law.edu.ru/otchety/2014/fevral_2014_goda//Lfnfj,hfotybz – 13/09/2015/. Дата обращения 13.09.2015.

62. Справочник по теории государства и права: основные категории и понятия / автор-сос. А. А. Иванов. – 2-е изд. стереотип. – М. : Экзамен, 2007.

63. Тоби Мендел. Свобода информации. Сравнительное правовое исследование. URL http://www.unesco.kz/publications/ci/freed_inform_ru.doc/. Дата обращения 20.08.2014. Опубликовано в 2003 году Региональным Бюро ЮНЕСКО по информации и коммуникации [Office UNESCO House, B-5/29, SafdarjungEnclave, NewDelhi 110029 India/ URL www.unesco.org/webworld]. Составлено и отпечатано Macro GraphicsPvt.Ltd. ЮНЕСКО 2003. Переведено Кластерное бюро ЮНЕСКО в Алматы, Отдел Коммуникации и Информации, URL http://www.unesco.kz, Июль 2004. Код документа CI/ATA/2009/PI/H/1.

64. Яковец Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации: учебное пособие. 2-е ид., доп. и перераб. М. : Юрлитинформ, 2014.

Акты применения права и материалы судебной практики

65. Резолюция Комиссии ООН по правам человека о правах на свободу убеждений и их свободное выражение. – принята Комиссией ООН по правам человека 23 апреля 2002 г. на 58-й сессии, без голосования. – URL http://www.hri.ru/docs/?content=doc&id=189. Дата публикации 17.04.2003, дата обращения 10.06.2014.

66. Определение Конституционного Суда Российской Федерации от 9 июля 2013 г. № 1053-О об отказе в принятии к рассмотрению жалобы гражданина Кочемарова Владислава Сергеевича на нарушение его конституционных прав положениями пунктов 1 и 3 статьи 1 и части третьей статьи 13 Федерального закона «О противодействии экстремистской деятельности». Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 18.7.2013 г. *(№ 0001201307180044)*.

67. Постановление Конституционного Суда Российской Федерации от 9 июля 2013 г. № 18-П по делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации в связи с жалобой гражданина Е.В.Крылова // Собр. законодательства Рос. Федерации. – 2013. – № 29, ст. 4019.

68. Постановление Пленума Верховного Суда Российской Федерации от 10 октября 2003 г. № 5 «О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации». URL http://www.vsrf.ru/vscourt_detale.php?id=1177/. Дата обращения 11.01.2014. Бюлле-

тень Верховного Суда Российской Федерации, декабрь 2003, № 12; Российская газета, 2 декабря 2003 г, № 244.

69. Постановление Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц». Бюллетень Верховного Суда Российской Федерации 2005 г., № 4.

70. Обзор практики рассмотрения судами Российской Федерации дел о защите чести, достоинства и деловой репутации, а также неприкосновенности частной жизни публичных лиц в области политики, искусства, спорта. Бюллетень Верховного Суда Российской Федерации. 2007 г., № 12.

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ И ПОНЯТИЯ, ПРИМЕНЯЕМЫЕ В РАБОТЕ

Обозначения и сокращения

АИС – автоматизированная информационная система

АРМ – автоматизированное рабочее место

АСЗИ – автоматизированная система в защищенном исполнении

ИР – информационный ресурс

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

ПТС – программно-технические средства

ПЭМИН – побочные электромагнитные излучения и наводки

РД – руководящий документ

СЗИ – система защиты информации

СрЗИ – средство защиты информации

СКЗИ – средства криптографической защиты информации

УЗ – уровень защищенности

ФСБ – Федеральная служба безопасности

ФСО – Федеральная служба охраны

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ОСНОВНЫЕ ПОНЯТИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Государственный стандарт Российской Федерации «Комплекс стандартов на автоматизированные системы. Автоматизированные системы», (далее – ГОСТ 34.003–90).

Защита информации (далее – ЗИ) от НСД – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации (Государственный стандарт Российской Федерации «Защита информации. Основные термины и определения», (далее – ГОСТ Р 50922–2006).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922–2006).

Информационная система персональных данных – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее 152-ФЗ).

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее 149-ФЗ).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной

информации определить принадлежность персональных данных конкретному субъекту персональных данных (152-ФЗ).

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (149-ФЗ).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (152-ФЗ).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (152-ФЗ).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (152-ФЗ).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (152-ФЗ).

Поставщик информации – специализированная компания, предоставляющая разнообразные сведения для анализа и принятия инвестиционных решений (149-ФЗ).

Потребитель информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею (149-ФЗ).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (152-ФЗ).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (Государственный стандарт Российской Федерации «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования», далее ГОСТ Р 51624–2000).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Лустин Владимир Иванович;
Бокшицкий Владимир Иосифович,
кандидат технических наук;
Шпагина Елена Михайловна;
Белгородцева Н. Г.,
кандидат психологических наук

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор *Чеботарева С. О.*
Компьютерная верстка *Татариновой О. А.*

Подписано в печать 10.12.2018 г.	Формат 60×84 1/16	Тираж 274 экз.
Заказ № 1985	Цена договорная	Объем 4,54 уч.-изд. л. 5,52 усл. печ. л.

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12