§3 ГОСУДАРСТВЕННАЯ И МУНИЦИПАЛЬНАЯ СЛУЖБА И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ

М.В. Костенников, А.В. Куракин, Г.Н. Кулешов, П.В. Несмелов

АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННОЙ ГРАЖДАНСКОЙ СЛУЖБЫ В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ (Ч. 2)

Информационные правоотношения играют важную роль в правовом регулировании государственно-служебных отношений. Как писал в свое время А.Б. Венгеров, «…информационными являются те отношения, которые складываются в сфере управления между работниками, их коллективами в процессе регистрации, сбора, передачи, хранения и обработки информации»[1]. Информация, которая вращается в системе государственной службы, несет в себе различную социальную нагрузку. В системе государственной службы есть информация, которая касается служебной деятельности, есть информация, которая касается непосредственно государственных служащих. Информация в системе государственной службы имеет различный правовой статус или специальный правовой режим.

В Доктрине информационной безопасности РФ указывается на необходимость разработки «основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики», развития и совершенствования «системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам»[2].

Утвержденная Президентом РФ 7 февраля 2008 г. Стратегия развития информационного общества в Российской Федерации вопросы обеспечения информационной безопасности ставит как задачу «обеспечения национальной безопасности в информационной сфере», но не предлагает никаких решений[3].

Важным событием в процессе развития государственной политики в сфере информатизации стало принятие в начале 2008 г. Стратегии развития информационного общества в России, которая

[1] См.: Венгеров А.Б. Право и информация в условиях автоматизации управления. – М., 1978. – С. 27.

[2] См.: Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. – 2008. – № 4. – С. 15.

[3] Там же.

Статья подготовлена при информационной поддержки компании «Консультант Плюс»

задала концептуальную и стратегическую цель для дальнейшего движения к информационному обществу и развития информационного права. Стратегия выступает «основой для подготовки и уточнения доктринальных, концептуальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, а также принципы и механизмы их взаимодействия с организациями и гражданами в области развития информационного общества в Российской Федерации»[4].

Благодаря ее реализации, к 2015 г. Россия должна войти в двадцатку лидеров глобального информационного общества, а по показателю доступности информационной и телекоммуникационной инфраструктуры для граждан и организаций — в десятку стран-лидеров.

Стратегия развития информационного общества в России определила основные принципы государственной политики в сфере информатизации:

- партнерство государства, бизнеса и гражданского общества;
- свобода и равенство доступа к информации и знаниям;
- поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;
- содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;
- обеспечение национальной безопасности в информационной сфере.

Суть Стратегии развития информационного общества в России состоит в том, что государство гарантирует обществу создание таких условий, при которых любой гражданин сможет максимально эффективно пользоваться информационно-коммуникационными технологиями, в том числе для доступа к информации о деятельности органов власти, получения государственных и муниципальных услуг в электронном формате и защиты своих прав[5].

Качество современного уровня правового регулирования отношений по поводу информации во многом определяется степенью учета законодателем этих признаков (свойств). Первое российское легальное определение понятия «информация» было дано в Федеральном законе от 20 февраля 1995 г. «Об информации, информатизации и защите информации»[6], в ст. 2 говорилось, что информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В действующем Федеральном законе от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» определение информации представлено в более общем виде. Информацией являются любые сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность в переводе с латинского означает «доверие» (т.е., передавая такую информацию, мы надеемся на ее сохранность и нераспространение, так как ее разглашение может нанести сторонам определенный ущерб. Конфиденциальная информация — это информация с ограниченным доступом, не содержащая государственную тайну.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

По мнению Д.В. Иванова, это определение небезупречно. Вряд ли можно согласиться с определением конфиденциальной информации опять-таки через информацию с ограниченным доступом, не содержащую государственную тайну[7], во-первых, потому, что такое определение оказывается в замкнутом круге: нельзя определять подобное подобным; во-вторых, государственная тайна — это тоже конфиденциальная информация. Поэтому более правильно, под конфиденциальной информацией понимать легально полученную информацию, которая в силу закона или иного акта, имеющего юридическое значение, доступна строго определенному кругу лиц, и в отношении которой установлен режим той или иной степени секретности[8].

При этом ограниченную в обороте конфиденциальную информацию можно подразделить на следующие разновидности.

Информация, составляющая коммерческую тайну (секрет производства), имеющая действительную или потенциальную коммерческую ценность, доступ

---

[4] Стратегия развития информационного общества в России [Электронный ресурс] // URL: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html

[5] См.: Маслова Н.Р. Состояние и проблемы формирования правовой основы реализации Стратегии развития информационного общества в России на федеральном и региональном уровне // Информационное право. – 2009. – № 2. – С. 18.

[6] См.: СЗ РФ. – 1995. – № 8. – Ст. 609.

[7] См.: Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. – 2008. – № 12. – С. 21.

[8] См.: Там же.

к которой ограничен ее первоначальным обладателем в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации». Информация, составляющая служебную тайну, доступ к которой в соответствии с законом ограничен ее первоначальным обладателем. В связи с этим на обладателя информации возлагается обязанность не разглашать ее.

Информация, составляющая профессиональную тайну, доступ к которой в соответствии с законом ограничен ее первоначальным обладателем, и обязанность не разглашать установлена для отдельных категорий субъектов, осуществляющих определенные виды деятельности в соответствии с федеральными законами и (или) по решению суда. Профессиональные тайны различаются по сферам профессиональной деятельности: адвокатская, банковская, медицинская, нотариальная и др.

Информация, составляющая личную и семейную тайну, доступ к которой в соответствии с законом ограничен ее первоначальным обладателем, и обязанность не разглашать установлена в соответствии с законом для всех третьих лиц (тайна усыновления и др.).

Иные разновидности конфиденциальной информации. Информация, изъятая из оборота, т.е. сведения, составляющие государственную тайну, подразделяется по грифам секретности на три категории:

- информация особой важности;
- совершенно секретная информация;
- секретная информация[9].

По мнению Е. Лобачева, правильный подход к проблеме защиты от утечки конфиденциальной информации содержит следующие шаги:

- формулирование кадровой политики, ведение работы по обеспечению лояльности персонала;
- разработка политики информационной безопасности в части, касающейся конфиденциальной информации;
- проведение организационных мероприятий, направленных на обеспечение юридической ответственности за разглашение конфиденциальной информации;
- разграничение доступа к конфиденциальной информации в соответствии с политикой, устранение путей утечки больших объемов информации;
- контроль, архивирование информационных потоков, идущих наружу; расследование инцидентов утечек информации с привлечением виновных к ответственности вплоть до уголовной;
- учет прочих факторов, вынесенных за рамки данной статьи[10].

Целями информационного обеспечения государственной гражданской службы являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы организации.

К расходам на защиту информации в системе государственной гражданской службы относится в основном приобретение средств, обеспечивающих ее защиту от неправомерного доступа. Средств обеспечения защиты информации множество, условно их можно разделить на две большие группы. Первая — это средства, которые имеют материальную основу, такие, как сейфы, камеры видеонаблюдения, охранные системы и т.д. Вторая — средства, которые не имеют материальной основы, такие, как антивирусные программы, программы ограничения доступа к информации в электронном виде и т.д.[11]

Для решения задач защиты информации в системе государственной гражданской службы используются следующие способы:

- организационные меры — подписание сотрудниками положений по использованию корпоративной информации, прохождение инструктажа и контроль за соблюдением норм;
- внедрение систем архивирования исходящей почты с возможностью последующего разбора инцидентов;
- разграничение прав доступа к информации, предназначенной для выполнения служебных обязанностей;
- перекрытие компьютерных портов ввода-вывода информации;
- установка на локальные компьютеры программ, следящих за всеми операциями пользователей

[9] См.: Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: Дис. … д-ра юрид. наук. М., 2007. С. 25.

[10] См.: Лобачев Е. Средства защиты информации от утечки из информационных систем // Финансовая газета. Региональный выпуск. – 2009. – № 37. – С. 12.

[11] См.: Щаников В. Учет расходов на защиту информации // Финансовая газета. Региональный выпуск. – 2008. – № 41. – С. 21.

(перехват клавиатуры, контроль операций с буфером обмена);
- физические ограничения — обращение с защищаемой информацией в замкнутом сегменте сети.

По мере использования таких традиционных средств борьбы с внутренними нарушителями стали усугубляться следующие проблемы:
- количество финансово значимых инцидентов утечки информации увеличивается с каждым годом;
- появляются новые источники внутренних угроз (технические пути вывода информации из корпоративной информационной системы);
- малейшие ограничения пользователей информационных систем приводят к нарушению отлаженных бизнес-процессов (сотрудники не могут выполнять свои служебные обязанности);
- юридические департаменты компаний на законной основе противостоят службам безопасности, вскрывающим электронную переписку сотрудников;
- небольшой отдел информационной безопасности должен решать задачи обработки огромного числа событий от разнородных систем безопасности, среди которых приходится вручную выявлять инциденты.

Проблемы информационного обеспечения в системе государственной гражданской службы становятся все более сложными и практически значимыми в связи с массовым переходом информационных технологий управления на безбумажную автоматизированную основу. Информационное обеспечение государственной гражданской службы носит концептуальный характер и предполагает решение комплекса задач поддержания безопасности информационных ресурсов (информации), а иными словами — безопасности отношений складывающихся в целом в системе публичного управления. Безопасность информации в системе государственной гражданской службы в современных условиях компьютеризации информационных процессов имеет принципиальное значение для предотвращения незаконного и часто преступного использования ценных сведений, особенно в связи с вхождением отечественных компьютерных систем в международные компьютерные сети.

Особым объектом правовой защиты информации в системе государственной гражданской службы являются конфиденциальные информационные ресурсы, которые, как иные другие виды ресурсов, защищаются нормами информационного права, нормами административного права, а также иных отраслей права от противоправных посягательств в рамках создания системы мер обеспечения безопасности и защиты информационных ресурсов в системе государственной службы[12].

Решение проблем информационного обеспечения государственной гражданской службы и защиты информации в деятельности государственных служащих осуществляется, посредством реализации ряда организационно-правовым мер:
- организация предупреждения правонарушений в сфере высоких технологий;
- обеспечение правовой охраны программ для ЭВМ;
- определение правового режима компьютерной информации, банка данных;
- правовое регулирование использования систем электронного документооборота и в связи с этим определение правового статуса электронных документов;
- правовая защита компьютерных систем и сетей в виде проведения совокупности мероприятий для создания условий, обеспечивающих предупреждение разглашения, хищения, уничтожения или искажения информации, а также ее несанкционированного использования;
- определение права собственности на компьютерные информационные ресурсы, компьютерные системы, технологии и средства их обеспечения;
- нормативная регламентация порядка функционирования отдельных компьютерных систем общего и специального назначения;
- создание правовых основ для использования глобальных компьютерных сетей, трансграничной передачи данных в рамках международного обмена информации;
- унификация законодательства России в сфере защиты информации и приведение его в соответствие с законодательством зарубежных стран[13].

О безопасности (защищенности) конфиденциальных информационных ресурсов в системе государственной гражданской службы можно говорить лишь в том случае, если создана система мер по защите информации во времени и пространстве от любых объективных и субъективных угроз, возни-

[12] См.: Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. – М., 1998. – С. 22.

[13] См.: Кисляковский А.В. Административно-правовое обеспечение информационной безопасности: Дис. … канд. юрид наук. – М., 2003. – С. 40.

кающих в обычных условиях функционирования общества и государства и в условиях стихийных бедствий, экстремальных ситуаций, других неуправляемых событий и активных попыток некоторых лиц создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных[14].

Любые информационные, а равно и конфиденциальные информационные ресурсы являются весьма уязвимой категорией и при интересе, возникшем к ним со стороны заинтересованных лиц, могут подвергаться объективным и субъективным угрозам утраты носителя или ценности информации.

Под угрозой или опасностью утраты конфиденциальной информации в системе государственной гражданской службы понимается единичное или комплексное, реальное или потенциальное, активное или пассивное появление однотипных и (или) разнохарактерных внешних и (или) внутренних источников возникновения критических (ЧС природно-техногенного характера и т.д.), противоправных ситуаций, оказывающих дестабилизирующее воздействие на защищаемую информацию.

Утрата конфиденциальных информационных ресурсов происходит, как правило, в двух случаях: информация переходит во владение непосредственно к заинтересованному либо к постороннему лицу в силу безответственности персонала и в силу противоправного завладения ею.

По принадлежности к тому или иному виду собственности конфиденциальные информационные ресурсы могут быть государственными и негосударственными и, как элемент состава имущества, находиться в собственности физических и юридических лиц (органов государственной власти, органов местного самоуправления, общественных объединений и т.п.).

В соответствии с интересами информационного обеспечения государственной гражданской службы и степенью ценности информации (стоимостной (коммерческой) или научно-технической, технологической и т.п.) для общества и государства, а также правовыми, экономическими интересами собственников информационные ресурсы (документы) могут быть:

- открытыми, т.е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях и интервью;
- ограниченного доступа и пользования, т.е. содержащие сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению и контролю.

К информации ограниченного доступа в системе государственной гражданской службы не могут быть отнесены некоторые категории информационных ресурсов, к которым относятся:

- законодательные и другие нормативные правовые акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций, общественных объединений и организаций, а также права, свободы и обязанности граждан, порядок их реализации;
- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, относящихся к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Основными направлениями повышения уровня защищенности объектов общей информационно-технологической инфраструктуры федеральных органов государственной власти являются:

- обеспечение комплексного подхода к решению задач информационной безопасности с учетом необходимости дифференцирования ее уровня в различных федеральных органах государственной власти;
- разработка модели угроз информационной безопасности;
- определение технических требований и критериев определения критических объектов информационно-технологической инфраструктуры, создание реестра критически важных объ-

[14] См.: Там же.

ектов, разработку мер по их защите и средств надзора за соблюдением соответствующих требований;

- обеспечение эффективного мониторинга состояния информационной безопасности;
- совершенствование нормативной правовой и методической базы в области защиты государственных информационных систем и ресурсов, формирование единого порядка согласования технических заданий на обеспечение информационной безопасности государственных информационных систем и ресурсов;
- проведение уполномоченными федеральными органами государственной власти аттестации государственных информационных систем и ресурсов, используемых в деятельности федеральных органов государственной власти, и контроль их соответствия требованиям информационной безопасности;
- создание физически обособленного телекоммуникационного сегмента специального назначения, обеспечивающего возможность обмена в электронном виде информацией, содержащей государственную тайну, ограниченным кругом органов государственной власти;
- развитие средств защиты информации, систем обеспечения безопасности электронного документооборота, системы контроля действий государственных служащих по работе с информацией, развитие и совершенствование защищенных средств обработки информации общего применения, систем удостоверяющих центров в области электронной цифровой подписи, а также систем их сертификации и аудита.

Документы, содержащие информацию ограниченного или конфиденциального характера, могут быть классифицированы по различным основаниям. Конфиденциальными документами независимо от принадлежности можно признать также любые персональные (личные) данные о гражданских служащих, а также сведения, содержащие профессиональную тайну, технические и технологические новшества (до их патентования) и т.п.

Специальный правовой режим касается персональных данных государственного служащего. Как отмечает М.М. Лебедева, «…выделение специального правового режима персональных данных было произведено по специальному объекту информации»[15]. В настоящее время достаточно много внимание уделяется защите персональных данных в системе государственной службы. В этой связи вполне справедливо мнение Э.А. Цадыковой, «…само по себе распространение персональных данных не столько наносит ущерб личности, сколько создает возможность для причинения ущерба. Защита персональных данных подстраховывает от возможных нарушений неприкосновенности частной жизни …»[16].

Персональные данные объективно присуще любому человеку, они подчеркивают правовой статус человека и гражданина. Персональные данные содержат необходимый объем информации о человеке, который участвует в соответствующих правоотношениях. Персональные данные принадлежат непосредственно человеку, и он в их несанкционированном распространении, как правило, не заинтересован, в этой связи неслучайно, что персональные данные охраняются различными правовыми средствами. Исходя из этого, вполне логично, что доступ к персональным данным имеет весьма ограниченный круг лиц: работодатель, сотрудники кадровых служб и др. Персональные данные находятся в правовом поле, в этой связи есть смыл кратко рассмотреть правовую основу, которая регламентирует режим оборота и использования персональных данных, а затем рассмотреть меры административной ответственности, применяемой за нарушение законодательства о персональных данных. В настоящее время правовое регулирование персональных данных привлекает внимание ученых и специалистов-практиков. В частности, О.Б. Просветова отмечает, что «персональные данные — это сведения о фактах, событиях и обстоятельствах жизни конкретного физического лица или его семьи, позволяющие отождествлять его с конкретным индивидом и отражающие особенности последнего по отношению к другим людям»[17].

Н.Г. Беляева пишет о том, что «представляют собой данные, содержащие информацию о частной жизни живого индивида (субъекта данных), который может быть идентифицирован на основании этой ин-

---

[15] См.: Лебедева М.М. Специальные правовые режимы информации: Автореф. дис. … канд. юрид. наук. – Саратов, 2009. – С. 12.

[16] См.: Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. – 2007. – № 14. – С. 15.

[17] См.: Просветова О.Б. Защита персональных данных: Автореф. дис. … канд. юрид. наук. Воронеж, 2005. С. 11.

формации (или с помощью этой информации), если, с точки зрения любого нормального человека, наделенного обычной чувствительностью, субъект данных вправе считать такую информацию конфиденциальной и контролировать ее распространение»[18].

Приведенное определение достаточно широкое и позволяет использовать его применительно к любым правоотношениям, в которых участвует соответствующий гражданин.

Согласно Федеральному закону от 27 июля 2006 г. «О персональных данных»[19] персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ст. 3). Указ Президента РФ от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера»[20], определяет, что сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, являются — персональными данными.

Согласно Указу Президента РФ от 30 мая 2005 г. «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»[21] под персональными данными гражданского служащего понимаются сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего либо подлежащие включению в его личное дело.

Согласно Трудовому кодексу РФ персональные данные работника — информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ст. 85). Федеральный закон от 2 марта 2007 г. «О муниципальной службе в Российской Федерации»[22] определяет, что персональные данные муниципального служащего — это информация, необходимая представителю нанимателя (работодателю) в связи с исполнением муниципальным служащим обязанностей по замещаемой должности муниципальной службы и касающаяся конкретного муниципального служащего. Как отмечает С.Е. Чанов, «…законодателем был избран различный порядок к правовому регулированию режима персональных данных на государственной гражданской и муниципальной службе»[23].

Согласно Федеральному закону от 15 ноября 1997 г. «Об актах гражданского состояния»[24] сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат (ст.2).

Как видим, наряду с общим законом о персональных данных существует еще целый ряд законодательных актов, которые регламентируют общественные отношения, связанные с защитой и регулированием персональных данных. Как отмечает Е. Волчинская, «обращение с информацией персонального характера требует особой регламентации»[25].

В этой связи правильно, что лица, виновные в нарушении законодательства о персональных данных, несут гражданскую, уголовную, административную, дисциплинарную ответственность. Следует отметить, что персональные данные — это информация о гражданине, его социальном статусе, которую он не хотел бы широко распространять, поскольку данная информация может быть использована в корыстных целях или интересах третьих лиц или групп. Персональные данные позволяют идентифицировать человека. Как отмечает Э.А. Цадыкова, «… персональные данные — это лишь информация позволяющая идентифицировать личность»[26]. Кроме идентификации личности информация о персональных данных позволяют оказывать негативное воздействие на человека, доставляя ему массу проблем. Поэтому персональные данные охраняются различными правовыми средствами, в том числе мерами административной ответственности.

И. Бачило говорит о том, что персональные данные — это такие сведения о личности, которые включаются в информационную систему государственных, общественных и частных, корпоратив-

---

[18] См.: Беляева Н.Г. Право на неприкосновенность частной жизни и доступ к персональным данным // Правоведение. – 2001. – № 1. – С. 101.

[19] См.: СЗ РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[20] См.: СЗ РФ. – 1997. –№ 10. – Ст. 1127.

[21] См.: СЗ РФ. – 2005. – № 23. – Ст. 2242.

[22] См.: СЗ РФ. – 2007. – № 10. – Ст. 1152.

[23] См.: Чаннов С.Е. Правовой режим персональных данных на государственной и муниципальной службе // Российская юстиция. – 2008. – № 1. – С. 21.

[24] См.: СЗ РФ. – 2007. – № 10. – Ст. 5340.

[25] См.: Волчинская Е. Информационная безопасность бизнеса: правовые аспекты // Закон. – 2002. – № 12. – С. 3.

[26] Цадыкова Э.А. Указ.раб. С. 15.

ных организаций по инициативе индивида или в силу закона в целях реализации его прав и обязанностей в процессе участия в самых разных социальных процессах и отношениях. Это та частной жизни, которая определенным образом представлена и присутствует в публичном и гражданском секторах правовых отношений индивида с другими субъектами права[27].

Так, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрена административная ответственность (ст. 13.11 КоАП РФ). Персональные данные являются информацией ограниченного характера, поэтому за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, предусмотрена административная ответственность (ст. 13.14 КоАП).

Административные правонарушения в области связи и информатизации весьма разнообразны, они касаются не только информационной сферы, они посягают также и на конституционные права граждан, касающиеся личной, семейной тайны, частной жизни и т.д. Любое административное правонарушение носит противоправный, виновный и наказуемый характер. Не являются исключением и административные правонарушения, посягающие на режим использования, хранения и оборота персональных данных.

Объектом посягательства деяния, предусмотренного ст. 13.11, являются общественные отношения, связанные с порядком сбора, хранения, использования или распространения информации о гражданах.

В этой связи неслучайно, что разглашение персональных данных работника — это грубое нарушение трудовой дисциплины, а также закона. Помимо увольнения виновного работника он может быть привлечен к административной ответственности.

Следует сказать, что правонарушение, предусмотренное ст. 13.11 КоАП РФ, посягает на конституционное право, в этой связи вопрос об административной ответственности может быть поставлен, если деяние не содержит в себе признаков преступления, ответственность за которое определена в УК РФ.

Преступлениями, влекущими за собой уголовную ответственность, являются:

- незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации (ст. 137 УК РФ);
- неправомерный отказ должностного лица в представлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо представление 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 (информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети), если это деяние повлекло за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272 УК РФ).

Объективная сторона административного правонарушения, посягающего на порядок оборота персональных данных, — это его внешнее выражение. Следует сказать, что рассматриваемое правонарушение может быть совершено как форме действия, так и в форме бездействия.

Субъектом правонарушения, связанного с нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) являются физические, должностные и юридические лица.

Данное правонарушение может совершаться как умышленно, так и по неосторожности. При этом умысел может быть как прямой, так и косвенный, неосторожность может быть как небрежность, так и самонадеянность. Состав правонарушения, который предусмотрен в ст. 13.11 КоАП РФ, носит универсальный характер. Мерами административной ответственности охраняются различные правоотношения, в которых используются персональные данные. Необходимо сказать, что данный подход не совсем оправдан, поскольку персональные данные весьма разнообразны, они могут носить как общий, так и специальный характер. Поэтому и меры административной ответственности должны носить весьма дифференцированный характер. В этой связи можно подержать позицию Н.И. Петрыкиной, которая отметила, что в КоАП РФ необходимо предусмотреть ответственность за незаконный сбор, хранение, ис-

[27] См.: Бачило И.Л. Персональные данные в сфере бизнеса // Закон. – 2002. – № 12. – С. 26.

пользование и разглашение информации, относящийся к специальным категориям персональных данных; несоблюдение установленных законодательством правил сбора и обработки персональных данных; за осуществление деятельности по сбору и обработке персональных данных оператором без уведомления уполномоченного органа по защите персональных данных, если федеральным законодательством такое уведомление обязательно, за нарушение прав субъектов персональных данных, при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации[28].

Сбор персональных данных осуществляется в формах предусмотренных законом. Так, при заключении трудового договора работодатель получает от работника необходимую ему информацию, документы, сведения и т.п. Которые приобщает к личному делу, работодателю запрещено требовать документы, которые не предусмотрены законом. Как отмечают Е.Л. Никитин и А.А. Тимошенко, перечень общих требований, которые обязан соблюдать работодатель при обработке персональных данных, следует дополнить указанием на запрет получения работодателем от лица, поступающего на работу, и работника следующих сведений:

- информации, составляющей государственную тайну или иную охраняемую законом конфиденциальную информацию, которая стала известна работнику до возникновения трудовых правоотношений с работодателем;
- сведений о прошлой политической или общественной деятельности работника или лица, устраивающегося на работу;
- сведений об имевших место в прошлом случаях привлечения к уголовной ответственности (за исключением ограничений, установленных для лиц, устраивающихся в органы правоохранительной системы РФ и правосудия, на работу, связанную с воспитанием, обучением детей, иную социально значимую работу, а также связанных с назначением наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью);
- данных об имущественном положении (исключение для лиц, претендующих на занятие выборных должностей);
- сведений о национальности самого работника, его близких родственников, родственников, близких лиц, иных лиц;
- иных подобных данных[29].

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания, обрабатываемых персональных данных работника, работодатель должен руководствоваться Конституцией РФ, а также законами РФ;
- все персональные данные работника следует получать у него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законом;

[28] См.: Петрыкина Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС (сравнительно-правовое исследование): Автореф. дис. … канд. юрид. наук. – М., 2007. – С. 20.

[29] См.: Никитин Е.Л., Тимошенко А.А. К вопросу о правовой природе персональных данных работника // Журнал российского права. – 2006. – № 7. – С. 42.

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном законом;
- работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
- работники не должны отказываться от своих прав на сохранение и защиту тайны;
- работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников (ст. 86 ТК РФ).

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном законом;
- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном законом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций (ст. 87 ТК РФ).

За разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, работодатель может расторгнуть трудовой договор с работником по собственной инициативе (ст. 81 ТК РФ).

Как отмечают Е.Л. Никитин и А.А. Тимошенко, «…персональные данные работника органически включены в систему персональных данных лица, составляют отдельное правовое образование — институт трудового права, носят информационный характер, подлежат комплексной правовой защите всеми способами и средствами, установленными для защиты государственной тайны и конфиденциальной информации»[30].

При получении, обработке, хранении и передаче персональных данных гражданского служащего кадровая служба государственного органа обязана соблюдать следующие требования:

- обработка персональных данных гражданского служащего осуществляется в целях обеспечения соблюдения Конституции РФ, федеральных законов и иных нормативных правовых актов РФ, содействия гражданскому служащему в прохождении государственной гражданской службы РФ (далее — гражданская служба), в обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества государственного органа, учета результатов исполнения им должностных обязанностей;

[30] Никитин Е.Л., Тимошенко А.А. Указ. раб. – С. 42.

- персональные данные следует получать лично у гражданского служащего. В случае возникновения необходимости получения персональных данных гражданского служащего у третьей стороны следует известить об этом гражданского служащего заранее, получить его письменное согласие и сообщить гражданскому служащему о целях, предполагаемых источниках и способах получения персональных данных;
- запрещается получать, обрабатывать и приобщать к личному делу гражданского служащего не установленные федеральными законами персональные данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;
- при принятии решений, затрагивающих интересы гражданского служащего, запрещается основываться на персональных данных гражданского служащего, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;
- защита персональных данных гражданского служащего от неправомерного их использования или утраты обеспечивается за счет средств государственного органа в порядке, установленном федеральными законами;
- передача персональных данных гражданского служащего третьей стороне не допускается без письменного согласия гражданского служащего, за исключением случаев, установленных федеральным законом.

В целях обеспечения защиты персональных данных, хранящихся в личных делах гражданских служащих, гражданские служащие имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные гражданского служащего, за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Гражданский служащий при отказе представителя нанимателя или уполномоченного им лица исключить или исправить персональные данные гражданского служащего имеет право заявить в письменной форме представителю нанимателя или уполномоченному им лицу о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера гражданский служащий имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требовать от представителя нанимателя или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные гражданского служащего, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействия представителя нанимателя или уполномоченного им лица при обработке и защите персональных данных гражданского служащего.

К личному делу гражданского служащего приобщаются:

- письменное заявление с просьбой о поступлении на гражданскую службу и замещении должности государственной гражданской службы РФ;
- собственноручно заполненная и подписанная гражданином РФ анкета установленной формы с приложением фотографии;
- документы о прохождении конкурса на замещение вакантной должности гражданской службы (если гражданин назначен на должность по результатам конкурса);
- копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;
- копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;
- копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);
- копии решений о награждении государственными наградами РФ, Почетной грамотой Президента РФ, об объявлении благодарности Президента РФ, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);
- копия акта государственного органа о назначении на должность гражданской службы;
- экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт;

- копии актов государственного органа о переводе гражданского служащего на иную должность гражданской службы, о временном замещении им иной должности гражданской службы;
- копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- копия акта государственного органа об освобождении гражданского служащего от замещаемой должности гражданской службы, о прекращении служебного контракта или его приостановлении;
- аттестационный лист гражданского служащего, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;
- экзаменационный лист гражданского служащего и отзыв об уровне его знаний, навыков и умений (профессиональном уровне) и о возможности присвоения ему классного чина государственной гражданской службы РФ;
- копии документов о присвоении гражданскому служащему классного чина государственной гражданской службы РФ (иного классного чина, квалификационного разряда, дипломатического ранга);
- копии документов о включении гражданского служащего в кадровый резерв, а также об исключении его из кадрового резерва;
- копии решений о поощрении гражданского служащего, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;
- копии документов о начале служебной проверки, ее результатах, об отстранении гражданского служащего от замещаемой должности гражданской службы;
- документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности гражданской службы связано с использованием таких сведений;
- сведения о доходах, имуществе и обязательствах имущественного характера гражданского служащего;
- копия страхового свидетельства обязательного пенсионного страхования;
- копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ;
- копия страхового медицинского полиса обязательного медицинского страхования граждан;
- медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению;
- справка о результатах проверки достоверности и полноты представленных гражданским служащим сведений о доходах, имуществе и обязательствах имущественного характера, а также сведений о соблюдении гражданским служащим ограничений, установленных федеральными законами.

В личное дело гражданского служащего вносятся также письменные объяснения гражданского служащего, если такие объяснения даны им после ознакомления с документами своего личного дела. К личному делу гражданского служащего приобщаются иные документы, предусмотренные федеральными законами и иными нормативными правовыми актами РФ. Документы, приобщенные к личному делу гражданского служащего, брошюруются, страницы нумеруются, к личному делу прилагается опись. Учетные данные гражданских служащих в соответствии с порядком, установленным Президентом РФ, хранятся кадровой службой государственного органа на электронных носителях. Кадровая служба обеспечивает их защиту от несанкционированного доступа и копирования. В обязанности кадровой службы государственного органа, осуществляющей ведение личных дел гражданских служащих, входит:

- обеспечение сохранности личных дел гражданских служащих;
- обеспечение конфиденциальности сведений, содержащихся в личных делах гражданских служащих, в соответствии с федеральным законом, иными нормативными правовыми актами РФ;
- представление сведений о доходах, имуществе и обязательствах имущественного характера федеральных гражданских служащих, назначение на должность и освобождение от должности которых осуществляются Президентом РФ или Правительством РФ, для опубликования общероссийским средствам массовой информации по их обращениям;
- представление сведений о доходах, имуществе и обязательствах имущественного характера соответствующих гражданских служащих субъектов РФ для опубликования общероссийским и региональным средствам массовой информации по их обращениям;
- ознакомление гражданского служащего с документами своего личного дела не реже одного раза в год, а также по просьбе гражданского служаще-

го и во всех иных случаях, предусмотренных законодательством РФ.

В этой связи неслучайно, что разглашение персональных данных государственного гражданского служащего работника — это грубое нарушение служебной дисциплины, а также законодательства о государственной службе. Помимо увольнения виновного служащего, он может быть привлечен к административной, дисциплинарной, уголовной ответственности и др.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, 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. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее — оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой безопасности РФ. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее — уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

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

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков. В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации. При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями — периодически проводимые тематические исследования.

Конкретные сроки проведения контрольных тематических исследований определяются Федеральной службой безопасности РФ. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для

обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий.

К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий. Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ в пределах их полномочий. Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности РФ.

Таким образом, если под конфиденциальной информацией в системе государственной гражданской службы понимается документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ, то персональные данные — это сведения о фактах событиях и обстоятельствах жизни конкретного гражданина или субъекта этих данных, личность которого можно идентифицировать.

По существу, персональные документы образуют круг конфиденциальных документов, содержащих персональные данные о гражданине, которые отражают его личную или семейную жизнь и содержащиеся в паспорте, трудовой книжке, военном билете, дипломе и т.д., а также документы, раскрывающие характер его правоотношений с государством (представление к назначению на должность, аттестационный лист и т.п.) или другими лицами (резюме, объяснительная записка, личное, исковое заявление, решение судебного органа и т.п.

Итак, конфиденциальный документ — это одновременно и носитель ценной, защищаемой информации, и основной источник накопления и объективного распространения этой информации, обязательный объект правовой зашиты от неправомерного разглашения или утечки.

Конфиденциальные документы, включающие и персональные документы, отражают их сущность как носителей информации ограниченного доступа и определяют содержание элементов системы ее защиты.

Одним из элементов системы защиты конфиденциальной информации является установление разрешительного порядка доступа к конфиденциальной информации, включающего процедуру оформления лица на доступ к информации ограничительного распространения и на основании правового акта согласия (разрешения) собственника или владельца информации на передачу ее для работы конкретному лицу. Угрозы утраты конфиденциальной информации имеют особенности. Так, риск угрозы утраты информационных ресурсов данной категории создают не только стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, но, главное, подобную угрозу могут создать заинтересованные и незаинтересованные в ее возникновении лица, а к угрозам подобного рода относятся: несанкционированное уничтожение документов, ускорение угасания (старение) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Как видно, для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации, (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам проявляется повышенный интерес со стороны различного рода лиц, не имеющих права владения ими и использования.

Особую опасность представляет «утечка» конфиденциальной информации или, говоря иначе, неконтролируемый выход конфиденциальной информации за пределы охраняемой зоны.

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ заинтересованного или постороннего лица (т.е. любого лица, не имеющего отношения к деятельности того или иного учреждения (посетители, работники учреждения, но не имеющие права доступа в определенное помещение, к конкретному

документу, базе данных и т.п.) к документированной информации и как результат — овладение информацией и противоправное ее использование или совершение иных действий: видоизменение, уничтожение, подмена и т.п.

Несанкционированный доступ к конфиденциальной информации в системе государственной гражданской службы, как правило, осуществляется через определенные каналы доступа, т.е. через совокупность незащищенных или слабо защищенных направлений возможной утечки конфиденциальной информации, которая может использоваться для получения необходимых сведений либо преднамеренного незаконного доступа к защищаемой информации.

Наличие канала несанкционированного доступа к конфиденциальной информации обязательно влечет за собой ее утрату, исчезновение ее носителя, а в основе его выявления лежит взаимодействие лица с источником информации или преобразование канала объективного распространения информации в канал ее утраты, т.е. перехода информации в категорию общедоступной, общеизвестной или информации открытого доступа.

По существу, утрата конфиденциальной информации происходит в основном как результат безответственных действий персонала (опубликование конфиденциальных сведений, включение этих сведений в открытый документ, их разглашение), нарушения разрешительной системы доступа конфиденциальной информации, утраты документа, носителя или их временного нахождения у постороннего лица, их копирование, перехват данной информации по незащищенным каналам.

Защита конфиденциальной информации в системе государственной гражданской службы представляет собой регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и обеспечивающий надежную безопасность информации в процессе правоохранительной деятельности. Задачи обеспечения информационного обеспечения и защиты конфиденциальной информации в системе государственной гражданской службы реализуются комплексом мер, органической частью которого является организация с соблюдением с соответствующих научно-методических требований сбора и анализа сведений об эффективности системы защиты и направлениях совершенствования составляющих ее элементах[31].

Основной характеристикой системы является комплексность, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты, оптимальное соотношение которых обеспечивает индивидуальность ее построения, неповторимость и необходимый заданный уровень защиты с учетом ценности информации и стоимости системы. Главное предназначение системы защиты конфиденциальной информации состоит в обеспечении реальной и потенциальной информационной безопасности путем реализации совокупности мер, снижающих уязвимость информации и препятствующих несанкционированному доступу к конфиденциальной информации, ее разглашению или утечке (утрате конфиденциальной сущности).

Необходимый уровень, а главное — перспективные направления обеспечения безопасности информационных ресурсов в системе государственной гражданской службы определяются в процессе аналитико-прогностических исследований, данные которых предопределяют структуру и требуемую эффективность системы защиты этих ресурсов с учетом финансовых возможностей предприятий, учреждений и организаций.

Основными элементами системы защиты информации, по общему признанию специалистов, являются: правовой, организационный, инженерно-технических, программно-аппаратный и криптографический. Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений сторон (например, гражданина и государства) по поводу правомерности использования системы защиты информации, соблюдения установленных собственником информации ограничительных и технологических мер защитного характера, а также ответственности за нарушение порядка защиты конфиденциальной информации.

Административно-правовые средства защиты информации в виде норм соответствующих отраслей права (административного, гражданского, уголовного и т.д.) устанавливают различные виды юридической ответственности за совершение в сфере информации правонарушений (преступлений), нарушение авторских прав программистов, порядка контроля за разработчиками компьютерных систем, порядка исполнения международных договоров об ограничении действия компьютерных систем, если они образуют или могут образовать угрозу информационной, а по этой причине и национальной безопасности страны.

[31] См.: Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г. Шаваева. – М., 1998. – С. 3.

Организационный элемент системы мер защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие соблюдать правила защиты конфиденциальной информации:

- организации деятельности службы безопасности и службы конфиденциальной документации;
- организации регулярных инструктажей персонала, работающего с защищаемой информацией;
- установления разрешительной системы разграничения доступа к защищаемой информации и т.п.

Организационный элемент защиты информации в системе государственной гражданской службы реализуется в форме регламентации информационной деятельности и взаимоотношений исполнителей таким образом, чтобы несанкционированный доступ к конфиденциальной информации стал невозможным или существенно затруднен за счет организации физической охраны объекта, подбора и расстановки персонала и т.п. организационных элементов системы защиты информации.

Инженерно-технические элементы системы защиты информации в системе государственной гражданской службы предназначены для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудованных с помощью комплексов научно-технических средств.

К техническим мерам защиты информации в системе государственной гражданской службы, представляющие собой различные аппаратные способы защиты информации, относятся, например, экранирование помещений, в которых установлены компьютеры, установка различных генераторов шумов, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку резервных систем энергопитания, автоматической сигнализации на случай неправомерного доступа к компьютерной информации[32].

Необходимо отметить, что систему мер обеспечения информационной безопасности и защиты информации государственной гражданской службы можно рассматривать в статике как состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах личности, общества и государства, а в динамике как способность государства обеспечить противодействие информационным опасностям и угрозам, негативным информационным воздействиям на общественное сознание и психику людей, а также на компьютерные сети и источники информации.

Как правильно резюмируют Е.А. Степанов и И.К. Корнеев, «... безопасность информации в современных условиях компьютеризации информационных процессов имеет принципиальное значение для предотвращения незаконного и частью преступного использования ценных сведений. Задачи обеспечения безопасности информации реализуются комплексной системой защиты информации, которая по своему назначению способна решить множество проблем, возникающих в процессе работы с конфиденциальной информацией и документами. Основным условием информационного обеспечения государственной гражданской службы является организация аналитических исследований, построенных на современном научном уровне и позволяющих иметь постоянные сведения об эффективности системы защиты и направлениях ее совершенствования в соответствии с возникающими ситуационными проблемами»[33].

В последние годы в зарубежных странах все большую актуальность приобретают две проблемы: зашита прав владения информацией и зашита информации от искажения и использования не по назначению.

Первая проблема связана с правовыми вопросами владения информацией, т.е. с правами лиц определять, при каких условиях, когда и кому может быть передана относящаяся к ним информация; вторая — связана с безопасностью, т.е. с защитой информации от случайного или преднамеренного (несанкционированного) ее раскрытия, изменения или разрушения. При этом под данными, содержащимися в банках данных, понимаются именно фактические данные, а не мнения тех или иных лиц, включая должностных лиц компетентных органов.

Критерием информационной открытости государственной гражданской службы является решение задач по совершенствованию информационной политики РФ, ориентированной на развитие системы правового информирования населения о направлениях деятельности органов государственной власти в целях развития демократических основ нашего общества. Административно-правовую основу информационной открытости государственной службы,

[32] См.: Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. – М., 1999. – С. 4.

[33] См.: Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. – М., 2001. – С. 47.

составляют Конституция РФ, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[34], Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[35].

Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» определяет, что доступ к информации о деятельности государственных органов и органов местного самоуправления может обеспечиваться следующими способами:

- обнародование (опубликование) государственными органами и органами местного самоуправления информации о своей деятельности в средствах массовой информации;
- размещение государственными органами и органами местного самоуправления информации о своей деятельности в сети Интернет;
- размещение государственными органами и органами местного самоуправления информации о своей деятельности в помещениях, занимаемых указанными органами, и в иных отведенных для этих целей местах;
- ознакомление пользователей информацией с информацией о деятельности государственных органов и органов местного самоуправления в помещениях, занимаемых указанными органами, а также через библиотечные и архивные фонды;
- присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, государственных органов и органов местного самоуправления, на заседаниях коллегиальных государственных органов и коллегиальных органов местного самоуправления, а также на заседаниях коллегиальных органов государственных органов;
- представление пользователям информацией по их запросу информации о деятельности государственных органов и органов местного самоуправления;
- другими способами, предусмотренными законами и (или) иными нормативными правовыми актами, а в отношении доступа к информации о деятельности органов местного самоуправления — также муниципальными правовыми актами[36].

Государственная политика в сфере использования информационных технологий направлена на решение следующих основных задач:

- реализация стратегических приоритетов в использовании информационных технологий в государственном управлении, формирование единого механизма межведомственной координации реализации государственных программ и проектов создания государственных информационных систем и ресурсов в соответствии с целями социально-экономического развития;
- формирование общей информационно-технологической инфраструктуры для обеспечения деятельности федеральных органов государственной власти;
- распространение практики предоставления гражданам и организациям доступа к открытой информации о деятельности федеральных органов государственной власти, соответствующим государственным информационным ресурсам, в том числе через сеть Интернет;
- организация интерактивного информационного обслуживания граждан и организаций с использованием современных информационных технологий;
- обеспечение информационной безопасности деятельности федеральных органов государственной власти и элементов информационно-технологической инфраструктуры;
- развитие единой защищенной телекоммуникационной инфраструктуры для государственных нужд, системы удостоверяющих центров в области электронной цифровой подписи и электронной среды взаимодействия, обеспечивающей эффективный межведомственный информационный обмен;
- разработка стандартов в сфере использования информационных технологий в деятельности федеральных органов государственной власти, создания государственных информационных систем, их интеграции и совместного использования в рамках создания общего информационного пространства федеральных органов государственной власти;
- централизованное создание общих государственных информационных ресурсов (регистров, кадастров, реестров, классификаторов), содержащих полную, непротиворечивую, достоверную, актуальную информацию, необходимую для выполнения основных функций государственного

[34] См.: СЗ РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

[35] См.: СЗ РФ. – 2009. – № 7. – Ст. 776.

[36] См.: Ковалева Н.Н., Холодная Е.В. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // подготовлен для системы Консультант Плюс, 2007.

управления, обеспечения доступности соответствующих данных на межведомственном уровне, а также для граждан и организаций в соответствии с требованиями, установленными законодательством РФ;

- построение единой системы управления процессом использования информационных технологий в деятельности федеральных органов государственной власти, обеспечивающей эффективную межведомственную координацию реализуемых государственных программ и проектов, их согласованное и взаимоувязанное выполнение в соответствии с основными приоритетами социально-экономического развития;
- распространение на уровне федеральных органов государственной власти практики долгосрочного планирования государственных программ и проектов использования информационных технологий, повышение эффективности управления их выполнением;
- увеличение объемов, объединение и централизация закупок однотипной продукции в сфере информационных технологий в интересах федеральных органов государственной власти для получения эффекта экономии на масштабе;
- создание единой системы мониторинга и контроля эффективности использования информационных технологий в деятельности федеральных органов государственной власти;
- реализация комплексных программ подготовки и повышения квалификации государственных служащих в части использования информационных технологий, развитие необходимой образовательной инфраструктуры и методического обеспечения;
- совершенствование законодательной и иной нормативной правовой базы в целях повышения эффективности использования информационных технологий в деятельности федеральных органов государственной власти с учетом международной практики;
- защита интеллектуальной собственности, недопущение использования в деятельности федеральных органов государственной власти программного обеспечения, не имеющего соответствующей лицензионной поддержки[37].

Степень информационной открытости и обеспеченности органов государственной власти и государственной гражданской службы должна определяться в соответствии с перечисленными выше нормативными правовыми актами, а также в соответствии с определенными критериями информационной открытости.

Библиографический список:

1. Бачило И.Л. Персональные данные в сфере бизнеса // Закон. — 2002. — № 12.
2. Беляева Н.Г. Право на неприкосновенность частной жизни и доступ к персональным данным // Правоведение. — 2001. — № 1.
3. Венгеров А.Б. Право и информация в условиях автоматизации управления. — М., 1978.
4. Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. — 2008. — № 4.
5. Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: Дис. … д-ра юрид. наук. — М., 2007.
6. Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. — 2008. — № 12.
7. Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. — М., 1998.
8. Кисляковский А.В. Административно-правовое обеспечение информационной безопасности: Дис. … канд. юрид наук. — М., 2003.
9. Ковалева Н.Н., Холодная Е.В. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // подготовлен для системы Консультант Плюс, 2007.
10. Лобачев Е. Средства защиты информации от утечки из информационных систем // Финансовая газета. Региональный выпуск. — 2009. — № 37.
11. Лебедева М.М. Специальные правовые режимы информации: Автореф. дис. … канд. юрид. наук. — Саратов, 2009.
12. Маслова Н.Р. Состояние и проблемы формирования правовой основы реализации Стратегии развития информационного общества в России на федеральном и региональном уровне // Информационное право. — 2009. — № 2.

[37] См.: Ковалева Н.Н., Холодная Е.В. Указ. раб.

13. Никитин Е.Л., Тимошенко А.А. К вопросу о правовой природе персональных данных работника // Журнал российского права. — 2006. — № 7.
14. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г. Шаваева. — М., 1998. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. — М., 1999.
15. Просветова О.Б. Защита персональных данных: Автореф. дис. … канд. юрид. наук. Воронеж, 2005.
16. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. — М., 2001.
17. Стратегия развития информационного общества в России [Электронный ресурс] // URL: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html
18. Щаников В. Учет расходов на защиту информации // Финансовая газета. Региональный выпуск. — 2008. — № 41.
19. Чаннов С.Е. Правовой режим персональных данных на государственной и муниципальной службе // Российская юстиция. — 2008. — № 1.
20. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. — 2007. — № 14.

References (transliteration):

1. Bachilo I.L. Personal'nye dannye v sfere biznesa // Zakon. — 2002. — № 12.
2. Belyaeva N.G. Pravo na neprikosnovennost' chastnoy zhizni i dostup k personal'nym dannym // Pravovedenie. — 2001. — № 1.
3. Vengerov A.B. Pravo i informatsiya v usloviyakh avtomatizatsii upravleniya. — M., 1978.
4. Volchinskaya E.K. Rol' gosudarstva v obespechenii informatsionnoy bezopasnosti // Informatsionnoe pravo. — 2008. — № 4.
5. Zvereva E.A. Pravovoe regulirovanie informatsionnogo obespecheniya predprinimatel'skoy deyatel'nosti v Rossiyskoy Federatsii: Dis. … d-ra yurid. nauk. — M., 2007.
6. Ivanov D.V. Istochniki pravovogo regulirovaniya konfidentsial'noy informatsii kak usloviya trudovogo dogovora // Trudovoe pravo. — 2008. — № 12.
7. Kurakov L.P., Smirnov S.N. Informatsiya kak ob'ekt pravovoy zashchity. — M., 1998.
8. Kislyakovskiy A.V. Administrativno-pravovoe obespechenie informatsionnoy bezopasnosti: Dis. … kand. yurid nauk. — M., 2003.
9. Kovaleva N.N., Kholodnaya E.V. Kommentariy k Federal'nomu zakonu ot 27 iyulya 2006 g. № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» // podgotovlen dlya sistemy Konsul'tant Plyus, 2007.
10. Lobachev E. Sredstva zashchity informatsii ot utechki iz informatsionnykh sistem // Finansovaya gazeta. Regional'nyy vypusk. — 2009. –
11. Lebedeva M.M. Spetsial'nye pravovye rezhimy informatsii: Avtoref. dis. … kand. yurid. nauk. — Saratov, 2009.
12. Maslova N.R. Sostoyanie i problemy formirovaniya pravovoy osnovy realizatsii Strategii razvitiya informatsionnogo obshchestva v Rossii na federal'nom i regional'nom urovne // Informatsionnoe pravo. — 2009. –№ 2.
13. Nikitin E.L., Timoshenko A.A. K voprosu o pravovoy prirode personal'nykh dannykh rabotnika // Zhurnal rossiyskogo prava. — 2006. — № 7.
14. Organizatsiya i sovremennye metody zashchity informatsii / Pod obshch. red. S.I. Dieva, A.G. Shavaeva. — M., 1998. Rassledovanie nepravomernogo dostupa k komp'yuternoy informatsii / pod red. N.G. Shurukhnova. — M., 1999.
15. Prosvetova O.B. Zashchita personal'nykh dannykh: Avtoref. dis. … kand. yurid. nauk. Voronezh, 2005.
16. Stepanov E.A., Korneev I.K. Informatsionnaya bezopasnost' i zashchita informatsii. — M., 2001.
17. Strategiya razvitiya informatsionnogo obshchestva v Rossii [Elektronnyy resurs] // URL: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html
18. Shchanikov V. Uchet raskhodov na zashchitu informatsii // Finansovaya gazeta. Regional'nyy vypusk. — 2008. — № 41.
19. Channov S.E. Pravovoy rezhim personal'nykh dannykh na gosudarstvennoy i munitsipal'noy sluzhbe // Rossiyskaya yustitsiya. — 2008. — № 1.
20. Tsadykova E.A. Garantii okhrany i zashchity personal'nykh dannykh cheloveka i grazhdanina // Konstitutsionnoe i munitsipal'noe pravo. — 2007. — № 14.

Начало смотрите в № 10-2012.