П.В. Несмелов

К ВОПРОСУ О КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АДМИНИСТРАТИВНОМ ПРАВЕ

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[1].

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»[2], 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[3], 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[4].

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 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 деятельно-

[1] 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.

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

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

[4] См.: Там же.

сти: 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[5].

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[6].

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.[7]

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.).

---

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

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

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

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 объектов, 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»[8]. 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 …»[9].

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»[10].

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 информации (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»[11].

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»[12] 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»[13], 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»[14] под персональными данными

---

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

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

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

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

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

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

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

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»[15] 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»[16].

Согласно Федеральному закону от 15 ноября 1997 г. «Об актах гражданского состояния»[17] 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»[18].

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»[19]. 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, корпоративных 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[20].

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).

---

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

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

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

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

[19] Цадыкова Э.А. Указ.раб. – С. 15.

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

Библиографический список:

1. Беляева Н.Г. Право на неприкосновенность частной жизни и доступ к персональным данным // Правоведение. — 2001. — № 1.
2. Бачило И.Л. Персональные данные в сфере бизнеса // Закон. — 2002. — № 12.
3. Волчинская Е. Информационная безопасность бизнеса: правовые аспекты // Закон. — 2002. — № 12.
4. Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: Дис. … д-ра юрид. наук. — М., 2007.
5. Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. — 2008. — № 12.
6. Лобачев Е. Средства защиты информации от утечки из информационных систем // Финансовая газета. Региональный выпуск. — 2009. — № 37.
7. Лебедева М.М. Специальные правовые режимы информации: Автореф. дис. … канд. юрид. наук. — Саратов, 2009.
8. 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.
9. Просветова О.Б. Защита персональных данных: Автореф. дис. … канд. юрид. наук. — Воронеж, 2005.
10. Щаников В. Учет расходов на защиту информации // Финансовая газета. Региональный выпуск. — 2008. — № 41.
11. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. — 2007. — № 14.
12. Чаннов С.Е. Правовой режим персональных данных на государственной и муниципальной службе // Российская юстиция. — 2008. — № 1.

References (transliteration):

1. Belyaeva N.G. Pravo na neprikosnovennost’ chastnoy zhizni i dostup k personal’nym dannym // Pravovedenie. — 2001. — № 1.
2. Bachilo I.L. Personal’nye dannye v sfere biznesa // Zakon. — 2002. — № 12.
3. Volchinskaya E. Informatsionnaya bezopasnost’ biznesa: pravovye aspekty // Zakon. — 2002. — № 12.
4. Zvereva E.A. Pravovoe regulirovanie informatsionnogo obespecheniya predprinimatel’skoy deyatel’nosti v Rossiyskoy Federatsii: dis. … d-ra yurid. nauk. — M., 2007.
5. Ivanov D.V. Istochniki pravovogo regulirovaniya konfidentsial’noy informatsii kak usloviya trudovogo dogovora // Trudovoe pravo. — 2008. — № 12.
6. Lobachev E. Sredstva zashchity informatsii ot utechki iz informatsionnykh sistem // Finansovaya gazeta. Regional’nyy vypusk. — 2009. — № 37.
7. Lebedeva M.M. Spetsial’nye pravovye rezhimy informatsii: avtoref. dis. … kand. yurid. nauk. — Saratov, 2009.
8. 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.
9. Prosvetova O.B. Zashchita personal’nykh dannykh: Avtoref. dis. … kand. yurid. nauk. — Voronezh, 2005.
10. Shchanikov V. Uchet raskhodov na zashchitu informatsii // Finansovaya gazeta. Regional’nyy vypusk. — 2008. — № 41.
11. Tsadykova E.A. Garantii okhrany i zashchity personal’nykh dannykh cheloveka i grazhdanina // Konstitutsionnoe i munitsipal’noe pravo. — 2007. — № 14.
12. Channov S.E. Pravovoy rezhim personal’nykh dannykh na gosudarstvennoy i munitsipal’noy sluzhbe // Rossiyskaya yustitsiya. — 2008. — № 1.