8. Ведомости ВС СССР. 1962. № 8. Ст. 83.
9. Елизаров П.С. Ответственность за посягательство на жизнь, здоровье и достоинство работников милиции и народных дружинников. Киев, 1973. С. 24.
10. Ветров Н.И. Преступления против порядка управления, посягающие на нормальную деятельность органов внутренних дел. М., 1989. С. 34–35.
11. Бюллетень Верховного Суда СССР. 1989. № 6.
12. Поленов Г.Ф. Ответственность за преступления против порядка управления. М., 1966. С. 53.
13. Осипов П.П. Преступления против порядка управления. Курс советского уголовного права. Часть Особенная. Л., 1978. Т. 4. С. 440–441.
14. Сборник постановлений Пленума Верховного Суда РФ. 1961–1993. М., 1994.
15. Карницкий Д.А., Рогинский Г.К., Строгович М.С. Уголовный кодекс РСФСР. Постатейный комментарий. М., 1929. С. 216.
16. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // Рос. газ. 2001. 22 дек. № 249 (ред. от 5 мая 2014 г.).

ВИДЫ ИНФОРМАЦИИ, ЗАЩИЩАЕМОЙ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ

О.С. Скрементова, кандидат юридических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены виды информации, защищаемой законодательством Российской Федерации. Изучено правовое регулирование государственной тайны, правовое регулирование обработки персональных данных, а также служебная и коммерческая тайна.
Ключевые слова: информация, информационные технологии, защита информации, государственная тайна, коммерческая тайна, служебная тайна

INFORMATION TYPES, PROTECTED BY THE LEGISLATION OF THE RUSSIAN FEDERATION

O.S. Skrementova.

The information types, protected by the legislation of the Russian Federation were discussed. The legal regulation of state secret, legal regulation of personal data processing and also official and trade secret were studied.
Keywords: information, information technologies, information security, state secret, trade secret, official secret

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ (ФЗ РФ № 149-ФЗ) «Об информации, информационных технологиях и о защите информации» [1] классифицирует информацию в зависимости от категории доступа к ней и порядка ее предоставления или распространения. По категориям доступа информация подразделяется:

– на общедоступную;

– ограниченного доступа, то есть такую информацию, доступ к которой ограничен федеральными законами.

По порядку предоставления или распространения информация подразделяется:

– на свободно распространяемую;

– предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

– подлежащую предоставлению или распространению в соответствии с Федеральным законом (например, сведения об имущественном положении кандидатов в депутаты);

– ограничиваемую или запрещаемую к распространению в Российской Федерации (например, разжигающую национальную, расовую или религиозную ненависть и вражду).

Право разрешать или ограничивать доступ к информации и определять условия такого доступа принадлежит обладателю информации. Обладатель информации обязан принимать меры по защите информации и ограничивать доступ к ней, если такая обязанность установлена ФЗ РФ № 149-ФЗ [1].

Ограничение доступа к информации возможно только в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства и устанавливается федеральным законом. Статья 9 ФЗ РФ № 149-ФЗ устанавливает обязательность соблюдения конфиденциальности информации ограниченного доступа, то есть «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Информация ограниченного доступа подразделяется на сведения, представляющие собой: государственную, коммерческую, служебную, профессиональную тайны, персональные данные граждан. Помимо прямо указанных в Законе, существуют и иные виды информации ограниченного доступа.

Классификация информации по категориям доступа

В Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» [2] предпринята попытка упорядочить состав конфиденциальной информации. Указом утвержден перечень сведений конфиденциального характера, в котором перечислены шесть видов информации:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, составляющие тайну следствия и судопроизводства;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и федеральными законами Российской Федерации (врачебная, нотариальная, адвокатская тайны, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, (профессиональная тайна);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

– сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

ФЗ РФ № 149-ФЗ в ч. 4 ст. 8 определяет перечень сведений, доступ к которым не может быть ограничен:

– нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

– информация о состоянии окружающей среды;

– информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

– информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

– иная информация, недопустимость ограничения доступа к которой установлена Федеральным законом.

Уголовный кодекс Российской Федерации 1996 г. (УК РФ) впервые установил нормы, объявляющие общественно опасными деяниями действия в сфере компьютерной информации и устанавливающие ответственность за их совершение.

К уголовно наказуемым отнесены неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

В тех случаях, когда общественно опасные действия в области информационных отношений совершаются без применения компьютерных средств, законодатель нередко относит их к другим, соответствующим родовым объектам.

Информационные отношения получили уголовно-правовую защиту. В связи с этим безопасность информации стала новым объектом преступления, а информация вообще и охраняемая законом в частности – предметом преступления.

Законодательство Российской Федерации о государственной тайне включает в себя Федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны [3].

Предметом правового регулирования являются отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием, распоряжением этими сведениями, а также их защитой.

Субъекты права в области государственной тайны – органы законодательной, исполнительной и судебной властей (органы государственной власти), местного самоуправления, предприятия, учреждения и организации независимо от их организационно-правовой формы и формы собственности, должностные лица и граждане Российской Федерации, взявшие на себя обязательства либо обязанные по своему статусу исполнять требования законодательства о государственной тайне.

Цель правового регулирования заключается в противодействии угрозам несанкционированного раскрытия сведений, составляющих государственную тайну.

Правовой режим государственной тайны включает в себя:

– порядок отнесения сведений к государственной тайне;

– порядок засекречивания и рассекречивания;

– порядок распоряжения сведениями, составляющими государственную тайну;

– систему защиты сведений, составляющих государственную тайну.

Объект правового режима государственной тайны – защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Отнесение сведений к государственной тайне осуществляется уполномоченными субъектами в соответствии с закрепленным в законодательстве перечнем таких сведений и их отраслевой, ведомственной или программно-целевой принадлежностью.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Субъекты отнесения сведений к государственной тайне: палаты Федерального Собрания Российской Федерации, Президент Российской Федерации, Правительство Российской Федерации, органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий. Отнесение сведений к государственной тайне и их засекречивание заключаются во введении в предусмотренном законодательством порядке для сведений, составляющих государственную тайну, ограничений на их распространение и доступ к их носителям и осуществляются в соответствии с принципами законности, обоснованности и своевременности.

Законность заключается в соответствии засекречиваемых сведений законодательству Российской Федерации о государственной тайне. Обоснованность заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан. Своевременность заключается в установлении ограничений на распространение сведений с момента их получения (разработки) или заблаговременно.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

– о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

– о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

– о фактах нарушения прав и свобод человека и гражданина;

– о размерах золотого запаса и государственных валютных резервах Российской Федерации;

– о состоянии здоровья высших должностных лиц Российской Федерации;

– о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суде.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие их распространения. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «Особой важности», «Совершенно секретно» и «Секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации. Для осуществления единой государственной политики в области засекречивания сведений Межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с перечнем сведений, составляющих государственную тайну, перечень органов государственной власти по распоряжению данными сведениями. Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Рассекречивание сведений и их носителей заключается в снятии ранее введенных в предусмотренном порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основания для рассекречивания сведений:

– взятие международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;

– изменение объективных обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, нецелесообразна.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению Межведомственной комиссии по защите государственной тайны.

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации вправе обратиться в органы государственной власти, на предприятия, в учреждения, организации, в том числе в государственные архивы, с запросом о рассекречивании сведений, отнесенных к государственной тайне. Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, обязаны в течение трех месяцев рассмотреть его и дать мотивированный ответ. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с момента его поступления передается в орган государственной власти, наделенный такими полномочиями либо в Межведомственную комиссию по защите государственной тайны, о чем уведомляются граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжении которого находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ.

Организация контроля эффективности защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора. Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения Межведомственной комиссии о возможности передачи этих сведений.

К органам защиты государственной тайны относят:

– Межведомственную комиссию по защите государственной тайны;

– федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации и их территориальные органы;

– органы государственной власти, предприятия, учреждения, организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны – коллегиальный орган, координирующий деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ

нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Ответственность за организацию защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей. В зависимости от объема работ с использованием государственной тайны руководителями органов государственной власти, предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых работ.

Защита государственной тайны – один из видов основной деятельности органа государственной власти, предприятия, учреждения или организации. Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке и предусматривает:

– принятие на себя обязательств перед государством по нераспространению доверенных сведений, составляющих государственную тайну;

– согласие на частичные, временные ограничения прав в соответствии с законодательством;

– письменное согласие на проведение проверочных мероприятий полномочными органами;

– определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных законодательством;

– ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

– принятие решения руководителем органа государственной власти, предприятия, учреждения или организации об оформлении допуска лица к государственной тайне.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие социальные гарантии:

– процентные надбавки к зарплате в зависимости от степени секретности сведений, к которым они имеют доступ;

– преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Для сотрудников структурных подразделений по защите государственной тайны дополнительно к социальным гарантиям устанавливается процентная надбавка к зарплате за стаж работы в указанных подразделениях.

Законодательство в области персональных данных состоит из Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других федеральных законах, определяющих случаи и особенности обработки персональных данных [4].

Предмет правового регулирования в области персональных данных – отношения, связанные с обработкой этих данных с применением средств автоматизации или без их применения. Исключение составляют отношения, возникающие:

– в связи с обработкой персональных данных физическими лицами для личных и семейных нужд;

– при формировании и использовании Архивного фонда Российской Федерации;

– при формировании и использовании Единого государственного реестра индивидуальных предпринимателей;

– в случае, если эти данные составляют государственную тайну.

Под персональными данными понимается 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, число и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

К особым категориям персональных данных относится информация о субъекте, касающаяся расы, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также физиологических особенностей, на основании которой можно установить его личность (биометрические персональные данные).

Цель правового регулирования заключается в обеспечении защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Основная угроза безопасности этих прав и свобод – неправомерное использование собираемых персональных данных государственными органами, органами местного самоуправления, юридическими и физическими лицами.

В целях противодействия указанной угрозе законодательно закрепляются:

– принципы и условия обработки персональных данных и их конфиденциальность;

– права субъектов персональных данных;

– обязанности оператора при обработке персональных данных;

– механизм контроля и надзора за соблюдением законодательства.

Под оператором персональных данных понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки этих данных.

Обработка персональных данных должна осуществляться на основе следующих принципов:

– законность целей и способов обработки персональных данных, добросовестность;

– соответствие целей обработки заранее объявленным и заявленным при сборе персональных данных целям, а также полномочиям оператора;

– соответствие объема и характера обрабатываемых персональных данных, способов их обработки заявленным целям;

– достоверность персональных данных, их достаточность для целей обработки и недопустимость их избыточности;

– недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– уничтожение персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Основное условие обработки персональных данных – согласие субъекта этих данных, которое он дает своей волей и в своем интересе. При составлении общедоступных источников персональных данных (в том числе справочников, адресных книг), специальных категорий персональных данных, обработке биометрических персональных данных согласие должно быть дано в письменной форме и включать в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер документа, удостоверяющего личность, сведения о дате выдачи документа и выдавшем его органе,

наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

Предварительное согласие субъекта персональных данных на их использование – обязательное условие использования этих данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи. Обязанность доказывать наличие согласия субъекта персональных данных на обработку персональных данных лежит на операторе.

Государственные и муниципальные органы создают в пределах своих полномочий государственные и муниципальные информационные системы персональных данных. Операторы, получающие доступ к персональным данным, должны обеспечивать их конфиденциальность, за исключением случаев обезличивания данных и обработки общедоступных данных.

Субъект персональных данных обладает правами:

– на доступ к своим персональным данным;

– возражение против принятия решений исключительно на основании автоматизированной обработки персональных данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы;

– обжалование действий или бездействий;

– отзыв согласия на обработку персональных данных.

Право на доступ к своим персональным данным включает в себя:

– получение сведений об операторе, месте его нахождения, наличии у оператора соответствующих персональных данных, а также ознакомление с ними;

– получение сведений, касающихся обработки персональных данных;

– уточнение своих персональных данных, их блокирование или уничтожение в случае, если эти данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Доступ должен быть предоставлен как лично субъекту персональных данных, так и его законному представителю по обращению или запросу этих лиц. Обращение и запрос могут быть отправлены в электронной форме и подписаны электронной цифровой подписью.

Правомочие получения информации, касающейся обработки персональных данных, реализуется субъектом этих данных посредством обращения или запроса. Ответ на обращение или запрос может содержать следующую информацию:

– способы обработки персональных данных, применяемые оператором;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– срок обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Право на обжалование действий или бездействий включает в себя:

– обжалование действия или бездействия оператора, нарушающего права и свободы субъекта персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

– возмещение убытков и компенсацию морального вреда в судебном порядке.

Право на отзыв согласия на обработку персональных данных заключается в возможности запретить соответствующие действия оператора в отношении своих персональных данных. В этом случае оператор обязан прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

При обработке персональных данных на оператора возлагаются следующие обязанности:

– соблюдение установленного порядка сбора персональных данных;

– обеспечение безопасности;

– реагирование на обращения и запросы;

– устранение нарушений законодательства;

– уведомление об обработке персональных данных.

Обязанности по соблюдению установленного порядка сбора персональных данных заключаются в следующем:

– предоставление по просьбе субъекта персональных данных информации, касающейся обработки его персональных данных;

– представление в случае получения персональных данных не от субъекта этих данных (за исключением случаев их представления на основании Федерального закона или когда они являются общедоступными) субъекту персональных данных до начала их обработки следующей информации: наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– установление цели обработки персональных данных и ее правовое основание;

– указание предполагаемых пользователей персональных данных;

– соблюдение установленных законом прав субъекта персональных данных.

Обязанности по обеспечению безопасности персональных данных включают в себя:

– принятие необходимых организационных и технических мер, в том числе связанных с использованием криптографических средств, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

– использование и хранение биометрических персональных данных вне информационных систем персональных данных только на материальных носителях информации и с применением таких технологий хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

Обязанности по реагированию на обращения и запросы заключаются в следующем:

– сообщение субъекту персональных данных или его законному представителю информации о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставление возможности ознакомления с этими данными при обращении или запросе субъекта персональных данных или его законного представителя;

– предоставление в письменной форме мотивированного ответа, содержащего ссылку на положения Федерального закона, являющиеся основанием для отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных;

– безвозмездное предоставление субъекту персональных данных или его законному представителю возможности ознакомления с персональными данными, относящимися к субъекту персональных данных;

– внесение в персональные данные необходимых изменений, уничтожение или блокирование соответствующих персональных данных по представлению субъектом

персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– уведомление субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах;

– сообщение в уполномоченный орган по защите прав субъектов персональных данных по его запросу информации, необходимой для осуществления деятельности указанного органа.

Обязанности по устранению нарушений законодательства включают в себя:

– блокирование персональных данных, относящихся к соответствующему субъекту, при обращении или по запросу субъекта персональных данных или его законного представителя в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора;

– уточнение персональных данных и снятие с них блокирования на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных;

– устранение выявленных нарушений в срок, не превышающий трех дней с даты выявления неправомерных действий с персональными данными, либо уничтожение этих данных;

– уведомление субъекта персональных данных или его законного представителя об устранении допущенных нарушений или об уничтожении соответствующих персональных данных;

– прекращение обработки персональных данных и уничтожение их в случае достижения цели обработки, а также в случае отзыва субъектом персональных данных согласия на их обработку.

Обязанности по уведомлению об обработке персональных данных заключаются в уведомлении уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных до начала их обработки.

Обработка персональных данных может осуществляться без уведомления уполномоченного органа по защите персональных данных, если эти данные:

– относятся к субъектам персональных данных, связанным с оператором трудовыми отношениями;

– получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относятся к членам общественного объединения или религиозной организации и обрабатываются соответствующими общественными объединениями или религиозными организациями, действующими в соответствии с законодательством, для достижения целей, предусмотренных их учредительными документами;

– являются общедоступными;

– включают только фамилии, имена, отчества субъектов персональных данных;

– необходимы для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор;

– включены в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы

персональных данных, созданные для защиты безопасности государства и общественного порядка;

– обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными актами, устанавливающими требования к обеспечению безопасности персональных данных при их обработке.

Необходимо остановиться на рассмотрении законодательства о служебной тайне.

Предмет правового регулирования законодательства о служебной тайне составляют отношения, связанные с отнесением информации к служебной тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей служебную тайну, и других участников регулируемых отношений.

В соответствии с действующим законодательством служебная тайна – это информация, доступ к которой ограничен органами государственной власти и федеральными законами (сведения об усыновлении, вкладах граждан в различного рода банках, характере заболеваний пациентов и т.д.).

Служебная тайна не подлежит разглашению, кроме случаев, когда те или иные сведения запрашиваются правоохранительными органами. Согласно Указу Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» [2] разница между служебной тайной и коммерческой тайной состоит в том, что коммерческая тайна – это сведения, связанные с коммерческой деятельностью, доступ к которым ограничен коммерческой организацией, а служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти.

Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1 233 было утверждено «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» [5], в котором определен гриф конфиденциальности информации – «Для служебного пользования». В соответствии с указанным положением к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничение на распространение которой диктуется служебной необходимостью.

Положение предписывает руководителям федеральных органов исполнительной власти в пределах своей компетенции определять категорию должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, обеспечивать ее защиту и т.д. Таким образом, можно утверждать, что потенциальными носителями служебной тайны являются, как минимум, все служащие, которые работают в органах законодательной, исполнительной и судебной власти, а также на подведомственных им предприятиях, в учреждениях и организациях.

Примерами служебной тайны являются:

– налоговая тайна. В соответствии с Налоговым кодексом Российской Федерации, налоговую тайну составляют любые сведения о налогоплательщике, полученные налоговым органом, органом государственного внебюджетного фонда и таможенным органом. Данные о налогоплательщике – физическом лице, также являются его личной тайной – персональными данными;

– тайна записи актов гражданского состояния. В соответствии с Федеральным законом Российской Федерации от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния» сведения, ставшие известными работнику органа записи актов гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат. Акты гражданского состояния – это действия граждан или события, влияющие на возникновение, изменение или прекращение прав и обязанностей [6].

Положением определен перечень информации, которая не может иметь статус служебной тайны:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Перечень информации, составляющей служебную тайну, может, в частности, включать и в себя:

– информацию о руководителях организации, других работниках (судимость, опыт работы, профессиональные знания, деловые связи);

– информацию о структуре управления производством, методику обучения персонала;

– информацию об участии в капиталах других организаций, о вложении средств в ценные бумаги, на депозитные счета банков;

– информацию об источниках финансирования;

– сведения о заключенных сделках, применяемых ценах;

– информацию о кредитоспособности данной организации;

– сведения о системе организации охраны на предприятии;

– сведения о состоянии материально-технической базы данной организации и др.

Сведения, относящиеся к служебной тайне, не являются обычно предметом самостоятельных сделок, однако их разглашение может причинить имущественный ущерб организации и вред ее деловой репутации. Служебная тайна относится к негосударственной тайне, однако ее правовой режим устанавливается государственными и негосударственными структурами – владельцами и обладателями информации. Таким образом, к служебной тайне, за исключением информации, составляющей государственную тайну, относится информация о деятельности государственных органов и их служащих, представляющая не коммерческий, а государственный интерес, а также иная конфиденциальная информация, составляющая частную, коммерческую тайну субъекта, полученная государственным органом в пределах своей компетенции для выполнения, возложенных на него функций.

Лица, незаконными методами получившие информацию, которая составляет служебную тайну или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную тайну или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном.

Основной задачей, стоящей перед государством и специалистами в данной области, является разработка и принятие комплекса законодательных актов, эффективных при реализации прав граждан в информационной сфере.

Литература

1. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ // Рос. газ. 2006. 29 июля. № 4131.

2. Об утверждении Перечня сведений конфиденциального характера: Указ Президента Рос. Федерации от 6 марта 1997 г. № 188. Доступ из справ.-правовой системы «КонсультантПлюс».

3. О государственной тайне: Федер. закон Рос. Федерации от 21 июля 1993 г. № 5485-1 // Рос. газ. 2010. 19 нояб. № 5341.

4. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. // Рос. газ. 2006. 29 июля. № 4131.

5. Об утверждении «Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление Правительства Рос. Федерации от 3 ноября 1994 г. № 1 233 Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об актах гражданского состояния: Федер. закон Рос. Федерации от 15 нояб. 1997 г. № 143-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ОБЕСПЕЧЕНИЯ РАДИАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

О.Л. Узун, кандидат юридических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены исторические аспекты открытия радиоактивности, применения атомной энергии, обобщены данные о нормировании радиоактивного воздействия, рассмотрена система нормативных правовых актов, регулирующих радиационную безопасность в Российской Федерации, проанализированы проблемы в сфере радиационной безопасности и предложены правовые способы совершенствования радиационной безопасности Российской Федерации.

Ключевые слова: радиация, радиоактивность, радиационная безопасность, атомное право

TO A QUESTION OF LEGAL REGULATION OF ENSURING RADIATION SAFETY IN THE RUSSIAN FEDERATION

O.L. Uzun. Saint-Petersburg university of the State fire service of EMERCOM of Russia

Historical aspects of discovery of radioactivity, application of atomic energy are considered, data on rationing of radioactive influence are generalized, the system of regulations regulating radiation safety in the Russian Federation is considered; problems in the sphere of radiation safety are analysed and legal ways of improvement of radiation safety of the Russian Federation are offered.

Keywords: radiation, radioactivity, radiation safety, nuclear law

В истории человечества есть немало открытий, изменивших жизнь людей и всего человечества. Одним из таких событий является открытие радиоактивности.

Открытие радиоактивности было непосредственно связано с открытием Рентгена. Более того, некоторое время считалось, что это один и тот же вид излучения. Конец XIX в. вообще был богат на открытия различного рода не известных до того «излучений». В 1880-е гг. английский физик Джозеф Джон Томсон приступил к изучению элементарных