ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(4) / 2012

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство **ПИ № ФС77-44941** от 05.05.2011

Адрес редакции: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.

Тел./факс: (351) 267-90-65, 267-97-01.

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: i-secur@mail.ru**

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

ТОЧКА ЗРЕНИЯ

ТРИБУНА МОЛОДОГО УЧЕНОГО

ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ

СТЕГАНОГРАФИЯ

РЕГИОНАЛЬНЫЙ АТТЕСТАЦИОННЫЙ ЦЕНТР ЮУрГУ

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

PERSONAL DATA

LEGAL PROTECTION OF PERSONAL DATA

POINT OF VIEW

TRIBUNE FOR YOUNG SCIENTIST

SOFTWARE AND HARDWARE PROTECTION OF INFORMATION

STEGANOGRAPHY

THE REGIONAL ATTESTATIVE CENTER SUSU

REQUIREMENTS TO THE ARTICLESTO BE PUBLISHED IN MAGAZINE

УДК 342.7 + 347(094.5.072)
ББК Х400.323 + Х99(4/8)

Минбалеев А. В.

ПРОБЛЕМНЫЕ ВОПРОСЫ ПОНЯТИЯ И СУЩНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье автор анализирует основные принципы и закономерности, лежащие в основе определения категории «персональные данные». Исследуется зарубежный опыт определения персональных данных в законодательстве. Дается характеристика современному законодательному определению персональных данных, описываются их признаки как вида информации ограниченного доступа.

Ключевые слова: *персональные данные, иностранное законодательство, признаки персональных данных.*

Minbaleev A.V.

PROBLEM QUESTIONS OF CONCEPT AND ESSENCE OF THE PERSONAL DATA

In the article an author analyses basic principles and conformities to law, being the basis of determination of category the "personal data". Foreign experience of determination of the personal data is investigated in a legislation. Description is given to modern legislative determination of the personal data, their signs are described as a type of information of a limit access.

Keywords: *personal data, foreign legislation, signs of the personal data.*

Одним из наименее урегулированных правовых режимом информации ограниченного доступа в информационном праве Российской Федерации является правовой режим персональных данных, в связи с чем сегодня ставится задача скорейшего формирования законодательства о персональных данных. Принятие базового закона «О персональных данных» не устранило данную задачу, а наоборот, только ее обострило.

Правовое регулирование персональных данных традиционно включает в себя правовую охрану персональных данных и их разновидностей – специальных персональных данных, выделяемых на основе критерия «чувствительности». Подобное выделение специальных данных исходит из сложившегося в судебной практике стран общего права принципа, что распространение определенного факта частной жизни (персональных данных)

признается посягательством на частную жизнь, если это распространение высокопредосудительно для «любого благоразумного человека, наделенного обычной чувствительностью»[1]. Согласно данному подходу, закон не защищает сверхчувствительных людей, поскольку каждый должен открывать свою жизнь до определенного обоснованного предела. Поэтому выделяются обычные и чувствительные персональные данные. Конвенция 108 Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» выделяет категорию «высокочувствительных» данных (данные о расовом или национальном происхождении, политических взглядах, религиозных и иных убеждениях, а также данные, касающиеся здоровья, сексуальной жизни, судимости), подлежащих специальной охране[2].

Обработка обычных персональных данных либо допускается без особых ограничений, либо ограничивается законодательно, при этом дополнительно выделяются чувствительные данные как разновидность персональных данных с более строгим режимом их использования. Например, Закон Латвии «Об охране данных физических лиц» помимо персональных выделяет специальную их разновидность – «сенситивные»[3], к которым относит персональные данные, указанные в качестве «высокочувствительных» в Конвенции 108. Закон Венгрии «О защите персональных данных и о публикации данных, представляющих общественный интерес» № LXIII от 1992 года выделяет персональные данные и «специальные данные» (персональные данные, относящиеся к расовой или национальной принадлежности, национальности или этническому статусу, политическим взглядам или партийной принадлежности, религиозным или иным убеждениям; состоянию здоровья, нездоровым пристрастиям, сексуальной жизни и криминальному прошлому). Близкий подход закреплен в Законе Дании о частных записях 1978 г.[4]

Большинство европейских стран выделяют три категории персональных данных. Так, в Бельгии по Законодательному Акту 1992 года о защите данных выделяются «обычные», «чувствительные» и «особо чувствительные» персональные данные[5]. В Испании кроме обычных выделяются «персональные данные, защищаемые особенно тщательно», к которым в соответствии с п. 2 ст. 16 Конституции и пп. 1, 2 ст. 7 Закона «О защите персональных данных»[6] относятся персональные данные, содержащие сведения об идеологии, профсоюзном членстве, религии и вероисповедании. Все они могут быть обработаны только при наличии четкого и письменного согласия субъекта. Также особо охраняются персональные данные, «касающиеся расовой принадлежности, здоровья, сексуальной жизни, которые могут быть получены и подвергнуты обработке, только если это установлено законом ради общественного блага или если имеется ясно выраженное согласие субъекта» (п. 3 ст. 7 Закона Испании «О защите персональных данных»). Согласно Закону Канады «О защите персональной информации и электронных документов» выделяются данные, включающие имя, служебный или деловой адрес либо телефонный номер служащего организации, которые являются открытыми для всех; персональные данные (информация о подлежащем идентификации физическом лице) и персональная информация о здоровье в отношении физического лица, независимо от того, жив он или нет[7]. Выделение «чувствительных данных» характерно также и для Австрии, Германии, Франции, Великобритании и других стран, где осуществляется регулирование персональных данных.

Определение персональных данных в основном строится на критерии «идентифицируемости субъекта данных». При этом, с точки зрения В. П. Иванского, в отношении всех персональных данных, определяемых исходя из данного критерия, устанавливается единый режим правовой защиты – все персональные данные относятся к категории «конфиденциальных данных»[8]. Из этого делается вывод о формировании самостоятельного направления (в противовес критерию «чувствительности») регулирования персональных данных – на основе критерия «идентифицируемости».

Регулирование персональных данных должно сочетать в себе и принцип «идентифицируемости» и принцип «чувствительности». Верность данного подхода подтверждает и зарубежный опыт, так как во многих странах, которые предусматривают регулирование «чувствительных» персональных данных, само понятие «персональные данные» строится именно на основе признака «идентифицируемости». Так, в Латвии – это «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу». По Закону Австрии «О защите персо-

нальных данных» 2000 г. это «сведения, которые идентифицируют определенного или определяемого лица»[9]. Также данный принцип характерен и для Германии (Закон об охране данных 1990 г.), Великобритании (Законы о защите данных 1984 и 1998 гг.), Дании (законодательные акты о регистрах публичных органов власти и о частных регистрах 1979 г.), Франции (Закон об обработке данных, файлах данных и индивидуальных свободах 1978 г.) и многих других стран.

Одной из проблем при построении законодательного определения «персональные данные» является закрепление объема сведений, которые могут быть отнесены к таковым. Необходимо ли специальное указание на конкретные виды сведений, которые могут быть содержанием персональных данных, а также тех, которые таковыми быть не могут? Так, по Закону Швеции «Об охране информации» под персональными данными понимается любая информация, касающаяся того или иного лица[10]. По Закону Таджикистана «Об информации»[11] – это «совокупность документированных или публично объявленных сведений о личности». Чаще всего к персональным данным относится «любая информация о конкретном человеке, которая отождествлена или может быть отождествлена с ним» (ст. 3 Закона Испании «О защите персональных данных») или «данные о физическом лице, позволяющие прямо или косвенно идентифицировать его» (ст. 3 Закона Республики Молдова «Об информатизации и государственных информационных ресурсах»[12]). Такой же подход закреплен в Латвии, Франции, Австрии и других странах. Иногда к персональным данным причисляются дополнительно «выводы, которые могут быть сделаны на основании данных, относящихся к заинтересованному лицу», при этом главное, чтобы была прослежена связь этих данных с заинтересованным лицом (ст. 2 Закона Венгрии). В Германии это «отдельные сведения о личных или деловых отношениях какого-либо определенного или определяемого физического лица» (Федеральный закон об охране данных)[13]. Таким образом, термин «персональные данные» однозначно связывается с личностью и сведениями о ней, но объем этих сведений неоднозначен и зависит от особенностей правовой системы.

В России понятие персональных данных (ранее действовавший Федеральный закон «Об информации, информатизации и защите информации») изначально связывалось только непосредственно со сведениями о фактах, событиях и обстоятельствах жизни гражданина, но данная формулировка могла быть оправдана только при расширительном толковании термина «жизнь». В ряде законопроектов, предлагаемых в период с 1999 по 2005 г. определение персональных данных в основном строилось из определения, даваемого директивой 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных»[14] и директивой 2002/58/ЕС «Об обработке персональных данных и охраны тайны частной жизни в секторе электронных коммуникаций»[15]. Оно основывалось на отнесении к персональным данным любых сведений о конкретном человеке, которые позволяют или могут позволить идентифицировать его (быть отождествлены с ним). Данное определение согласовывалось и с определениями отдельных видов персональных данных, даваемыми в отечественном законодательстве на тот период времени. Так, «персональные данные работника», согласно Трудовому кодексу Российской Федерации, – это «информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника»[16]. 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»[17].

В первой редакции Федерального закона «О персональных данных» под персональными данными понималась «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». В новой редакции персональные данные – это «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Таким образом, законодатель расширил понятие, и в качестве персональных дан-

ных сегодня может быть рассмотрена и информация, по которой можно даже косвенно определить субъекта персональных данных. Это может быть любая личная информация, которая относится к тому или иному человеку, что позволяет существенно расширить не только понятие персональных данных, но и круг операторов, их обрабатывающих.

При характеристике персональных данных в практической сфере часто возникает потребность в закреплении перечня сведений, которые могут быть персональными данными. В информационном праве также предлагалось дать исчерпывающий перечень сведений, которые законом отнесены к категории персональных данных[18]. Однако опыт правового регулирования в других странах опровергает такой подход. Исчерпывающий перечень не должен устанавливаться законом, поскольку любое ограничение содержания персональных данных может способствовать ограничению прав субъекта. Законодательно должны быть закреплены виды персональных данных, которые могут свободно обращаться, и случаи, когда допускается использование персональных данных без согласия заинтересованного лица. Так, например, не должно применяться требование конфиденциальности в полном объеме в отношении фамилии, имени, отчества лица. Данную информацию определяют обычно как «номинативную», но при этом в «определенных ситуациях и эти сведения также могут рассматриваться как конфиденциальные»[19]. В России открытость данной информации в некоторых случаях также прямо предусматривается. Так, согласно постановлению Правительства РФ «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» не могут быть отнесены к сведениям ограниченного доступа фамилии, имена, отчества Председателя и членов Правительства РФ, руководителей федеральных органов исполнительной власти и их структурных подразделений, руководителей организаций и органов, образованных при Правительстве РФ, и некоторых других должностных лиц. Определенные ограничения на запрет использования персональных данных без согласия лица предусматриваются российским законодательством в отношении лиц, работающих на режимных объектах; имеющих доступ к государственной тайне; несовершеннолетних и лиц с психическими отклонениями; лиц, страдающих тяжкими инфекционными заболеваниями; лиц, содержащихся под стражей, отбывающих наказание в местах лишения свободы или находящихся под административным надзором. Некоторые ограничения неприкосновенности частной жизни допустимы в условиях чрезвычайного положения. Также не требуется согласия лица на сбор, хранение, использование и распространение сведений о нем при проведении следствия, дознания, оперативно-розыскных мероприятий.

Ограничение на использование персональных данных лица закрепляется во многих законодательных актах Российской Федерации. Согласно п. 6 ч. 1 ст. 30 и ч. 2 ст. 61 Основ законодательства Российской Федерации об охране здоровья граждан, пациент имеет право на сохранение в тайне информации о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе и иных сведениях, полученных при обследовании и лечении, а органы и лица, которым эти сведения стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, обязаны не допускать их разглашения.

Одной из актуальных проблем правового режима персональных данных является вопрос о возможности применения категории персональных данных к юридическим лицам. Существующие законодательные акты иностранных государств преимущественно отрицательно относятся к данной возможности, однако в некоторых государствах законы о защите персональных данных распространяют свое действие и на юридические лица[20]. Так, исландский законодательный акт 1989 г. о регистрации и обращении с персональными данными распространяет понятие «персональные данные» и на сведения о юридических лицах, признает «корпоративное право на невмешательство в частную сферу»[21]. Также категория «персональные данные» распространяется на юридические лица по законам «О защите персональных данных» Австрии 2000 г. и Швейцарии (Art. 3 lit b Bundesgesetz über den Datenschutz) от 23 марта 1988 г[22]. В России, на наш взгляд, данное право также законодательно закреплено в Федеральном законе «О связи», в ст. 53 которого сведения обо всех абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполне-

ния договора об оказании услуг связи, являются конфиденциальной информацией. К сведениям об абонентах – юридических лицах при этом относятся наименование (фирменное наименование), фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента[23].

Персональные данные традиционно включаются в сферу правового регулирования как объекты, над которыми совершаются определенные действия – обработка, в том числе создание, сбор, хранение, модификация, использование, передача, уничтожение и т. п. Поэтому необходимо обязательное законодательное закрепление определений данным действиям. Такой подход широко распространен за рубежом и основывается на четком разграничении данных действий и создании специальных норм в отношении каждого из них. Например, Закон об охране данных Германии предусматривает определение понятиям «сбор», «обработка», «блокирование», «аннулирование», «использование», «анонимизирование». При этом под обработкой понимают накопление, модификацию, передачу, блокирование и аннулирование персональных данных, а под использованием – любое применение данных, которое не включается в обработку. В Испании по Закону «О защите персональных данных» предусматривается универсальный термин – «действия с персональными данными», то есть операции и технические процессы автоматизированного и неавтоматизированного характера, которые способствовали бы сбору, записи, хранению, разработке, изменению, блокированию и уничтожению, а также передаче персональных данных из сообщений, консультаций, взаимосвязей и перемещений информации. Данная формулировка включает в себя совокупность всех действий с персональными данными и учитывает их автоматизированную обработку. Также дается определение категории «передача или сообщение персональных данных» (любое раскрытие о персональных данных третьему лицу) и «обезличивание персональных данных» (любая обработка личной информации таким образом, чтобы получаемая информация не могла быть отождествлена прямо или косвенно с конкретным человеком).

Персональные данные как разновидность информации ограниченного доступа обладают рядом отличительных признаков, позволяющих говорить об их специальном режиме. Основной особенностью персональных данных является то, что значительное их количество являются открытыми (например, фамилия, имя, отчество лица), но в тот или иной момент времени, применительно к тем или иным обстоятельствам, доступ к ним и их использование могут быть ограничены субъектом персональных данных. Режим же других видов информации ограниченного доступа (преимущественно тайны) исходит из принципа сохранения в тайне этой информации и законодательно закрепляемом запрете ее сбора и распространения. Персональные данные могут охраняться как самостоятельным режимом защиты, так и в режиме государственной тайны или определенного вида информации ограниченного доступа, например, коммерческой тайны или профессиональной тайны. В этом случае персональные данные подобны хамелеону и в зависимости от ситуации «меняют окраску» и охраняются в режиме определенного вида информации ограниченного доступа или при помощи собственных мер, или в режиме совместной охраны. Подобная практика позволяет режиму персональных данных быть очень «гибким» и подстраиваться под те или иные отношения. Обусловливается это тем, что персональными данными могут стать любые сведения, если по ним даже есть косвенная возможность определить физическое лицо.

Примечания

[1] См.: Судебное определение из дела «Диас против Окленд Трибюн, Инкорпорейтед» (139 Cal App3d 118, 1983). Цит. по: Иванский В. П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования : Монография. – М.: Изд-во РУДН, 1999. – С. 8.

[2] См.: Совет Европы. Конвенция о защите личности в связи с автоматической обработкой персональных данных от 28 января 1981. – СПб.: Манускрипт, 1995. – С. 12.

[3] См.: Ст. 2 Закона Республики Латвия «Об охране данных физических лиц» от 06.04.2000 г. –htpp://www.medialaw.ru/exussrlaw/index.htm.

[4] См.: Briat M. Personal data and the free flow of information // Freedom of data flows and EEC Law. – Boston, 1988. – P. 50.

[5] См.: Иванский В. П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий : автореф. дис. … к.ю.н. – М., 1998. – С. 12.

[6] Органический закон Испании «О защите персональных данных» от 13.12.1999. № 15/99 // Официальный государственный бюллетень Испании. – 14.12.1999. – № 298.

[7] См.: Ст. 2 ч. 1 «Защита персональной информации в частном секторе» Закона Канады «О защите персональной информации и электронных документов» от 13.04.2000. № SI/2000-29 // Шамраев А. В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. – М., 2003. – С. 690–691.

[8] См.: Иванский В. П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий : автореф. дис. … к.ю.н. – С. 12.

[9] Art. 2 Bundesgesetz Österreich über den Schutz personenbezogener Daten (DSG 2000) // Bundesgesetzblatt. 1999. Teil I. № 165/1999.

[10] См.: Ст. 1 Закона Швеции «Об охране информации» 1973. № 289 // Защита персональных данных: Опыт правового регулирования. – М.: Галерия, 2001. – 236 с.

[11] Закон Республики Таджикистан «Об информации» от 2 декабря 2002. № 71 // Ахбори Маджлиси Оли Республики Таджикистан. – 2002. – № 11. – Ст. 696.

[12] Закон Республики Молдова «Об информатизации и государственных информационных ресурсах» от 21.11.2003 г. № 467-XV // Официальный монитор Республики Молдова. – 01.01.2004. – № 6–12.

[13] См.: § 3 Bundesdatenschutzgesetz Deutschland vom 20. Dezember 1990 // Bundesgesetzblatt, 1990. Teil I. S. 2954.

[14] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr // Amtsblatt der Europäischen Gemeinschaften. Nr. L 281 vom 23.11.95. – S. 31.

[15] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) of 12.07.2002. // Official Journal of the European Communities. – 31.07.2002. – L 201/37.

[16] Ст. 85 Трудового кодекса РФ от 30.12.2001. № 197-ФЗ // СЗ РФ. – 2002. – № 1 (Часть I). – Ст. 3.

[17] Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела. Утв. Указом Президента РФ от 30.05.2005. № 609.

[18] См., например: Фатьянов А. А. Тайна и право (основные системы ограничения на доступ к информации в российском праве) : Монография. – М.: МИФИ, 1999. – С. 205.

[19] Терещенко Л.К. Персональные данные в системе конфиденциальной информации. –http://www.infoforum.ru/detail.php?pagedetail=1019.

[20] См.: Becker J. Information und Gesellschaft. – Wien; New-York: Springer-Verlag, 2002. – S. 107.

[21] Иванский В. П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования : Монография. – С. 11.

[22] Druey J. N. Information als Gegenstand des Rechts: Entwurf einer Grundlegung. – S. 371.

[23] ФЗ РФ «О связи» от 07.07.2003. № 126-ФЗ // СЗ РФ. – 2003. № 28 . – Ст. 2895.

Минбалеев Алексей Владимирович, к.ю.н., доцент, доцент кафедры конституционного и административного права ЮУрГУ, доцент кафедры информационного права УрГЮА. E-mail: alexmin@bk.ru

Minbaleev Aleksey Vladimirovich, senior lecturer on Department of Constitutional and Administrative Law in the South Ural State University, senior lecturer on Department of Informative Law in the Ural State Law Academy, Doctor of Law. E-mail: alexmin@bk.ru

УДК 343.13:342.7
ББК Х408.114 + Х400.323:Х408.114

Гарбатович Д. А.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ УГОЛОВНЫМ ПРАВОМ

Автором исследуются возможности защиты персональных данных современным уголовным правом России. Исследуется соотношение понятий «частная жизнь» и «персональные данные». В статье поднимается актуальная сегодня на практике проблема применения ст. 137 Уголовного кодекса Российской Федерации при нарушении прав субъектов персональных данных.

Ключевые слова: *персональные данные, защита, неприкосновенность частной жизни, уголовная ответственность.*

Garbatovich D. A.

PROTECTION OF PERSONAL DATA BY MEANS OF CRIMINAL LAW

The author investigates the possibilities of personal data protection by means of modern criminal law in Russia. The article studies the correlation of concepts "personal life" and "personal data". The work raises the urgent problem of practical application of Article 137 of the Criminal Code of the Russian Federation while infringing on the rights of personal data owner.

Keywords: *personal data, protection, personal life sanctity, criminal liability.*

Любое общество находится в постоянном развитии, что неизбежно ведет к появлению новых институтов, требующих соответствующей защиты со стороны государства.

С момента выделения термина «персональные данные», образования соответствующего правового института, возникла проблема надлежащей его правовой охраны. Началась дискуссия о целесообразности защиты персональных данных посредством установления уголовной ответственности за совершение незаконных действий с указанными данными.

Указанная дискуссия сводится к решению следующих вопросов.

Как соотносятся между собой термины «частная жизнь» и «персональные данные», это по содержанию абсолютно разные понятия или что-то является общим по отношению к другому? Данный вопрос имеет принципиальное значение, так как в УК РФ уже имеется запрещенное деяние в виде нарушения неприкосновенности частной жизни (ст. 137 УК РФ). И если понятие «персональные данные» входит в термин «частная жизнь», установление уголовной ответственности, например, за незаконное собирание, распространение персональных данных, будет признаваться как излишнее загромождение уголовного закона.

Другие вопросы сводятся к дискуссии, насколько незаконные действия с персональными данными являются именно общественно опасными, требующими признания их преступными и уголовно наказуемыми. Решение указанного вопроса имеет принципиальное значение, так как нецелесообразно для защиты определенного права сразу же обра-

щаться к уголовному кодексу, если для эффективной защиты можно использовать потенциал иных отраслей права.

Вопрос о соотношении терминов «частная жизнь» и «персональные данные».

В соответствии со ст. 3 ФЗ «О персональных данных» под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[1].

Фамилия, имя, отчество, место жительства, реквизиты паспорта являются персональными данными, поскольку они прямо относятся к определенному гражданину. Будут являться персональными данными, например, сведения о паспорте транспортного средства, принадлежащего гражданину, сведения из правоустанавливающих документов на принадлежащее ему недвижимое имущество (свидетельство о государственной регистрации права в ЕГРП), вносимые в заявление на страхование или анкету клиента для пользования другого рода услугой, поскольку эти сведения имеют отношение к определенному физическому лицу. Сведения из других документов также могут являться персональными данными, если они прямо или косвенно имеют отношение к определенному или определяемому физическому лицу.[2]

Итак, «персональные данные» – это любая информация, относящаяся к определенному или определяемому на основании такой информации 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. В качестве «другой» информации может выступать биометрическая информация о лице; данные о супруге, детях, других членах семьи; индивидуальные средства коммуникации (номер телефона, адрес электронной почты, ICQ, персональный сайт или иной личный ресурс в Интернете, например блог или страница в социальной сети); сведения о событиях и обстоятельствах жизни лица, позволяющие его идентифицировать, в том числе аудио- и видеофайлы, и т. д. Перечень сведений, которые могут быть отнесены к персональным данным, является открытым[3].

Под частной жизнью понимаются сведения о частной жизни лица, составляющие его личную или семейную тайну. Носителями сведений могут выступать документы, вещи, информация на магнитных носителях, а также сам человек. Обязательное требование, предъявляемое к этим носителям законом, заключается в том, что они должны содержать информацию, образующую личную или семейную тайну лица, т. е. субъективно относимые человеком к скрытым от посторонних лиц данные, касающиеся индивида и его связей в обществе, ранее не разглашавшиеся на публике и носящие как порочащий, так и непорочащий характер[4].

Сведения о частной жизни могут касаться прошлой деятельности лица, привычек, физических недостатков, сексуальной ориентации, духовной жизни, семейных и интимных взаимоотношений, имущественного и профессионального положения и т. п. Частную жизнь составляют те стороны жизни человека, которые он в силу своей свободы не желает делать достоянием других[5].

Б. Н. Кадников считает, что к информации о частной жизни следует относить: общие сведения личного и семейного характера, специальные тайны и персональные данные[6].

Соответственно странным представляется мнение Б. Н. Кадникова, что если персональные данные относятся к частной жизни, тем не менее, персональные данные фактически остаются незащищенными и требуют установления отдельной уголовно-правовой нормы, предусматривающей уголовную ответственность за совершение незаконных действий с персональными данными[7].

Зачем нужна отдельная норма, если, по мнению данного автора, персональные данные относятся к частной жизни, которые уже охраняются соответствующей уголовно-правовой нормой (ст. 137 УК РФ)?

Можно сделать вывод, что тайна частной жизни является общей родовой категорией, включающей профессиональные и непрофессиональные (иные) тайны; тайна персональных данных – одна из видов тайн. Такой вывод вытекает из ст. 2 Закона «О персональных данных», согласно которой его целью «является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну». Следовательно, законодатель рассматривает действия по обработке персональных данных в режиме права на неприкосновенность частной жизни. При этом сами персональные данные в ст. 3

Закона о персональных данных определяются как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[8].

К аналогичному выводу можно прийти и при анализе Указа Президента РФ «Об утверждении перечня сведений конфиденциального характера»[9], в соответствии с которым под сведениями конфиденциального характера понимаются 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.

Право на неприкосновенность частной жизни представляет собой сложный по составу правовой институт, состоящий из множества правомочий индивида. Так, по мнению Е. А. Миндровой, персональные данные являются по своему содержанию сегментом информации о частной жизни лица[10].

Согласно иной позиции право на защиту персональных данных есть одно из правомочий индивида в сфере охраны его частной жизни, исследуемые понятия («частная жизнь» и «персональные данные») частично пересекаются, однако не всегда совпадают. Исследуемые категории представляют собой два различных (хотя и смежных) правовых института, следовательно, правовое регулирование этих двух институтов будет различным[11].

Все персональные данные можно условно разделить на свободно обращаемые, ограниченно обращаемые, обращаемые в специальных целях, запрещенные к обороту[12].

Частично за совершение незаконных действий в отношении отдельных категорий персональных данных уже установлена уголовная ответственность (например, нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), отказ в предоставлении гражданину информации (ст. 140 УК РФ), разглашение тайны усыновления (удочерения), незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), неправомерный доступ к компьютерной информации» (ст. 272 УК РФ)).

Вопрос об установлении специального состава преступления, предусматривающего уголовную ответственность за совершение незаконных действий в отношении персональных данных, является дискуссионным.

Далеко не каждый факт незаконного собирания и распространения сведений, составляющих персональные данные, является общественно опасным и требует защиты со стороны самого репрессивного права, уголовного права.

Даже за распространение сведений о частной жизни привлечение к ответственности виновных является весьма проблематичным. Потерпевшие не всегда считают указанные нарушения особо значимыми, либо, чаще всего, просто не знают о наличии своих прав, их нарушениях и о том, как можно их защитить.[13]

Если вопрос о защите персональных данных посредством установления соответствующей уголовной ответственности будет решен положительно, законодателю нужно будет максимальным образом позаботиться о четком формулировании объективных и субъективных признаков указанного состава преступления (например, существенное нарушение прав, причинение значительного ущерба, корыстные мотивы, цели и т. д.).

При отсутствии конкретных критериев, какое действие в отношении персональных данных является преступным, сложно на практике будет отграничивать, какое нарушение будет считаться преступлением, а какое нарушением, формально содержащим также все признаки состава преступления, но в силу малозначительности не представляющим общественной опасности, не будет признаваться преступным и уголовнонаказуемым.

Примечания

[1] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных» //Российская газета. – 2006. – 29 июля.

[2] Зоркольцев Р. Д. Персональные данные, получаемые через Интернет: практические вопросы // СПС КонсультантПлюс (дата обращения 02.11.2012 г.).

[3] Петрыкина Н. И. Правовое регулирование оборота персональных данных. Теория и практика. – М.: Статут, 2011.

[4] Комментарий к Уголовному кодексу Российской Федерации: (постатейный) (4-е издание) / под ред. Г. А. Есакова. – Проспект, 2012 (КонсультантПлюс).

[5] Комментарий к Уголовному кодексу Российской Федерации: (постатейный) под ред. А. И. Чучаева – «КОНТРАКТ», 2012 (КонсультантПлюс).

[6] Кадников Б. Н. Уголовно-правовая охрана неприкосновенности частной жизни : научно-практическое пособие / под ред. Н. Г. Кадникова. – М.: Юриспруденция, 2011.

[7] Там же.

[8] Гришаев С. П. Право на неприкосновенность частной жизни // СПС КонсультантПлюс (дата обращения 02.11.2012 г.).

[9] Пункт 1 Указа Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005) «Об утверждении Перечня сведений конфиденциального характера» // Российская газета. – 1997. – 14 марта.

[10] Миндрова Е. К. Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества : автореф. дис. ... канд. юрид. наук. – М., 2007. – С. 8.

[11] Петрыкина Н. И. Правовое регулирование оборота персональных данных. Теория и практика. – М.: Статут, 2011.

[12] Там же.

[13] Сулейманова С. Т. К вопросу об уголовной ответственности за нарушение неприкосновенности частной жизни в сфере трудовых отношений // Социальное и пенсионное право. –2009. – N 3. – С. 35–37.

Гарбатович Д. А., декан юридического факультета Челябинского филиала Университета Российской академии образования, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Южно-Уральского государственного университета, доцент кафедры Уголовного права Уральского филиала Российской академии правосудия, кандидат юридических наук. E-mail: garbatovich@mail.ru

Garbatovich D. A., Dean of Law Faculty, Chelyabinsk branch of University of Russian Academy of Education, Associate professor of Criminal Law, Criminology and Criminal Executive Law Department, South Ural State University, Associate professor of Criminal Law Department, Ural branch of Russian Academy of Justice, Candidate of law. E-mail: garbatovich@mail.ru

УДК 342.7:004.056 + 004.7
ББК Х400.323

Кафтанникова В. М.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье анализируются новеллы законодательства о персональных данных, посвященные правовому регулированию информационных систем персональных данных. Автором исследуются понятие, правовой режим и отдельные виды информационных систем персональных данных. Дается анализ уровней защищенности персональных данных при их обработке в информационных системах и требования для каждого из них.

Ключевые слова: *персональные данные, защита, информационные системы, уровни защищенности, автоматизированная обработка.*

Kaftannikova V. M.

LEGAL REGULATION OF PERSONAL DATA INFORMATION SYSTEMS

The article analyses novels of legislation on personal data, devoted to the legal control of personal data information systems. It gives analysis of levels of personal data protection while processing in information systems and requirements for each of them.

Keywords: *personal data, protection, information systems, levels of protection, automatic processing.*

Возникновение информационных систем персональных данных можно приурочить к моменту возникновения информационных систем, т. е. ко времени появления электронно-вычислительных машин. Основную роль в истории защиты персональных данных сыграла Конвенция Совета Европы от 28 января 1981 года (с изменениями 1999 года) «О защите личности в связи с автоматической обработкой персональных данных» (ратифицирована Федеральным законом от 19 декабря 2005 г. № 160-ФЗ) (далее – Конвенция)[1].

В Конвенции еще не дано определение информационным системам персональных данных (далее – ИСПДн), но можно выделить следующие составляющие ИСПДн: «автоматизированная база данных» и «автоматическая обработка». Таким образом, сложив составляющие, можно получить следующее толкование: ИСПДн означает любой набор данных, с которым осуществляются следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств: накопление данных, проведение логических или/и арифметических операций с такими данными, их изменение, стирание, восстановление или распространение. Согласно данной Конвенции, персональные данные в информационных системах должны отвечать следующим требованиям:

• должны быть получены и обработаны добросовестным и законным образом;

• должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;

• должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;

• должны быть точными и в случае необходимости обновляться;

• должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

В 2001 году Российская Федерация подписала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Необходимым шагом Российской Федерации как стороны Конвенции стало принятие Федерального закона № 152-ФЗ «О персональных данных»[2], целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Следует отметить, что еще в 1997 году Указом Президента РФ № 188 были определены сведения конфиденциального характера[3], которые определены как перечень данных, относящихся к персональным (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 и т. д.). В законе «О персональных данных» появляется определение термина: информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

В законе также указываются принципы обработки персональных данных, которым должны следовать операторы (оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными), причем можно отметить, что данные принципы копируют требования, представленные в Конвенции, а именно:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Согласно закону «О персональных данных», оператор должен принимать необходимые правовые, организационные и технические меры при обработке персональных данных в информационных системах или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В отдельную статью в законе «О персональных данных» выделяются особенности обработки персональных данных в государственных или муниципальных ИСПДн, в которой говорится о том, что государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные инфор-

мационные системы персональных данных. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

Контроль и надзор за исполнением требований обработки персональных данных в информационных системах осуществляют регуляторы, к которым относятся следующие службы:

• Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (контроль за исполнением юридических требований закона, осуществление документального контроля).

• ФСТЭК – Федеральная служба по техническому и экспортному контролю (контроль за состоянием информационных систем и средств их защиты, осуществление технического контроля).

• ФСБ – Федеральная служба безопасности (контроль средств защиты информации при необходимости ее шифрования).

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи (Роскомнадзор), является уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям федерального закона №152. В законе «О персональных данных» указываются контрольные и надзорные функции для Роскомнадзора в сфере обработки персональных данных в информационных системах, а именно:

• принятие в установленном законодательством Российской Федерации порядке мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

• обращение в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представление интересов субъектов персональных данных в суде;

• осуществление проверки сведений, содержащихся в уведомлении об обработке персональных данных, или привлечение для осуществления такой проверки иных государственных органов в пределах их полномочий и другие.

Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»[4] установлены требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации. Постановлением Правительства Российской Федерации № 1119 от 1 ноября 2012 года[5] признано утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и установлены новые требования к защите персональных данных при их обработке в информационных системах персональных данных.

Постановлением устанавливаются четыре уровня защищенности персональных данных при их обработке в информационных системах и требования для каждого из них. Отнесение информационных систем к тому или иному уровню защищенности производится в зависимости от вида персональных данных, который обрабатывает информационная система (специальные, биометрические, общедоступные, иные), типа актуальных угроз (1-й, 2-й, 3-й), количества обрабатываемых информационной системой субъектов персональных данных и от того, обрабатываются ли персональные данные о сотрудниках оператора. Постановление позволит операторам информационных систем, обрабатывающих персональные данные, определить требуемый уровень защищенности персональных данных, что в дальнейшем значительно упростит процедуру определения необходимых и достаточных мер по защите персональных

данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Приказом ФСТЭК, ФСБ, Мининформсвязи от 13.02.08 г. № 55/86/20[6] установлен порядок проведения классификации информационных систем персональных данных. В основу классификации легли многие критерии, такие как: режим обработки персональных данных в информационной системе, местонахождение технических средств ИСПДн, структура информационных систем и другие. Во главе основной классификации ИСПДн лежат критерии категории персональных данных и количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе. Согласно законодательству, существуют следующие категории персональных данных (Хпд):

• категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

• категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

• категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

• категория 4 – обезличенные и (или) общедоступные персональные данные.

Количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе, может принимать следующие значения (Хнпд):

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных. данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Таблица 1. Классификация ИСПДн

$X_{пд}$ \ $X_{нпд}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов (табл. 1):

• класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

• класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

• класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

• класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных.

Приказом ФСТЭК России № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»[7] установлены методы и способы защиты информации,

применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, или лицом, которому на основании договора оператор поручает обработку персональных данных. Данный приказ содержит в себе методы и способы защиты информации от несанкционированного доступа, а также методы и способы защиты информации от утечки по техническим каналам. Приложением к Положению о методах и способах защиты информации в информационных системах персональных данных установлены методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности персональных данных в информационных системах в зависимости от класса информационных систем.

Регуляторы информационных систем персональных данных издают документацию, согласно которой следует действовать при обработке персональных данных в информационных системах. К таким актам можно отнести «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»[8] ФСБ России и другие.

ФСТЭК России разработал «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»[9]. Методика предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных.

На данный момент действующими признано около 50 нормативно-правовых актов в сфере защиты персональных данных федерального уровня – постановления правительства, указы президента, федеральные законы. Несмотря на то что проверки регуляторами информационных систем на предмет защищенности в них персональных данных начались относительно недавно, нельзя не заметить общую тенденцию к усилению защиты ИСПДн и повышение уровня грамотности регуляторов и операторов в данной сфере.

Примечания

[1] Конвенция Совета Европы от 28 января 1981 года «О защите личности в связи с автоматической обработкой персональных данных» // URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=3020

[2] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. – 2006 г. – № 165.

[3] Указ Президента № 188 от 1997 г. // Российская газета. – 1997. – 18 марта.

[4] Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. – 2007 г. – № 260.

[5] Постановление Правительства РФ от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // URL: http://government.ru/gov/results/21355/

[6] Приказ ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. № 55/86/20 // URL: http://ispdn.ru/law/530/#text

[7] Приказ ФСТЭК России №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» // Российская газета. – 2010 г. – № 46.

[8] Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных ФСБ России// URL: http://ispdn.ru/law/749/#text

[9] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // URL: www.fstec.ru/_spravs/metodika.doc

В. М. Кафтанникова, аспирант кафедры конституционного и административного права Южно-Уральского государственного университета. E-mail: ladalk@gmail.com

V. M. Kaftannikova, postgraduate student of Constitutional and Administrative Law Department, South Ural State University. E-mail: ladalk@gmail.com

УДК 342.518:004 + 342.7:004.056
ББК Х401.011.11

И. У. Кулдыбаева

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ РАЗВИТИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В статье поднимается актуальная сегодня на практике проблема защиты персональных данных в условиях развития информационного общества и электронного правительства. Автором исследуются угрозы безопасности персональных данных, обрабатываемых в органах государственной власти. Исследуются меры защиты персональных данных.

Ключевые слова: *персональные данные, электронное правительство, несанкционированный доступ, защита.*

I. U. Kuldybaeva

ASSUARANCE OF PERSONAL DATA PROTECTION IN CONDITIONS OF E-GOVERNMENT DEVELOPMENT

The article raises urgent problem of application in practice of personal data protection in conditions of information society and e-Government development. The author investigates the threats of protection of personal data which are processed in the bodies of state authorities. It studies the means of personal data protection.

Keywords: *personal data, e-Government, unauthorized access, protection*

Одним из приоритетных направлений развития информационного общества является электронное правительство, приоритетное направление которого – предоставление государственных услуг в электронной форме.

Под электронным правительством понимается новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов[1]. Развитие системы предоставления государственных и муниципальных услуг в электронном виде является стратегической задачей как для совершенствования государственного управления, так и для становления в России информационного общества.

Использование информационных технологий в процессе предоставления государственных услуг подразумевает создание одного государственного репозитория (баз данных, хранилищ информации, реестров с

персональными данными граждан), которое должно быть защищено в соответствии с законом «О персональных данных»[2], нормативными документами и методическими документами регулирующих органов. Таким образом, будучи операторами персональных данных, государственные и муниципальные органы обязаны принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Распоряжением Правительства Российской Федерации от 15 апреля 2011 г. № 654-р «О базовых государственных информационных ресурсах»[3] утвержден перечень базовых государственных информационных ресурсов, используемых при предоставлении государственных или муниципальных услуг (исполнении государственных или муниципальных функций). Федеральные органы исполнительной власти и Пенсионный фонд Российской Федерации, являющиеся обладателями базовых ресурсов, должны обеспечить круглосуточный непрерывный доступ в электронном виде посредством единой системы межведомственного электронного взаимодействия органов власти и организаций, уполномоченных оказывать государственные и муниципальные услуги. Межведомственное информационное взаимодействие, – осуществляемое в целях предоставления государственных и муниципальных услуг взаимодействие по вопросам обмена документами и информацией, в том числе в электронной форме, между органами, предоставляющими государственные услуги[4].

Для получения государственных и муниципальных услуг заявитель должен предоставить все необходимые документы и информацию, необходимые для предоставления государственной или муниципальной услуги, в том числе и персональные данные. Заявитель – лицо, обратившееся в орган власти или организацию, предоставляющие государственные или муниципальные услуги, с запросом о предоставлении государственной или муниципальной услуги, выраженным в устной, письменной или электронной форме.

В рамках реализации системы электронного правительства планируется обеспечить централизованное хранение персональных данных о получателях услуги, что значительно упростит процедуру сбора персональных данных, но в то же время повлечет возникновение ряда угроз безопасности такого рода информации. Таким образом, получателю услуги не придется каждый раз предоставлять полный пакет документов, так как большинство персональных данных уже содержится в базовых государственных информационных ресурсах и может быть получено посредством межведомственного взаимодействия между органами власти и организациями, предоставляющими государственные и муниципальные услуги.

Применение информационных технологий в деятельности органов государственной власти поднимает вопрос обеспечения безопасности обрабатываемой, хранимой и передаваемой по сетям связи информации, доступ к которой ограничен федеральными законами. В частности, остро стоит проблема защиты персональных данных от несанкционированного доступа.

Проблемы информационной безопасности практически не урегулированы в законодательных и нормативных документах, регулирующих отношения по предоставлению государственных и муниципальных услуг.

В Федеральном законе от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[5], регулирующем отношения, возникающие в связи с предоставлением государственных и муниципальных услуг, затрагиваются следующие вопросы обработки персональных данных:

• в случае, если для предоставления государственной или муниципальной услуги необходимо представление документов и информации об ином лице, не являющемся заявителем, при обращении за получением государственной или муниципальной услуги заявитель дополнительно представляет документы, подтверждающие наличие согласия указанных лиц или их законных представителей на обработку персональных данных указанных лиц, а также полномочие заявителя действовать от имени указанных лиц или их законных представителей при передаче персональных данных указанных лиц в орган или организацию;

• для обработки органами и организациями, предоставляющими государственные и

муниципальные услуги, персональных данных в целях предоставления персональных данных заявителя, имеющихся в распоряжении таких органов или организаций, в орган или организацию, предоставляющий государственную и муниципальную услугу, на основании межведомственных запросов таких органов или организаций для предоставления государственной или муниципальной услуги по запросу заявителя, а также для обработки персональных данных при регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг и на региональных порталах государственных и муниципальных услуг не требуется получение согласия заявителя как субъекта персональных данных в соответствии с требованиями статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Таким образом, вопрос защиты персональных данных сводится лишь к получению согласия субъекта персональных данных на обработку его личной информации, либо узаконивание получения персональных данных заявителя без его согласия при межведомственном обмене персональными данными.

Для получения государственных и муниципальных услуг в орган или организацию, оказывающие такие услуги, предоставляются следующие персональные данные:

- документы, удостоверяющие личность гражданина Российской Федерации;
- документы воинского учета;
- свидетельства о государственной регистрации актов гражданского состояния;
- документы, подтверждающие регистрацию по месту жительства или по месту пребывания;
- документы, подтверждающие предоставление лицу специального права на управление транспортным средством соответствующего вида;
- документы о трудовой деятельности, трудовом стаже и заработке гражданина;
- справки, заключения и иные документы, выдаваемые организациями, входящими в государственную, муниципальную или частную систему здравоохранения;
- правоустанавливающие документы на объекты недвижимости, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
- документы, выдаваемые федеральными государственными учреждениями медико-социальной экспертизы;
- удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки;
- и другие.

В большинстве случаев передаваемые в органы и организации, оказывающие государственные и муниципальные услуги, персональные данные относятся к персональным данным второй категории, а именно персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию. За редким исключением передаются персональные данные специальной категории, в частности, данные о состоянии здоровья субъекта.

В соответствии с законом «О персональных данных» субъект персональных данных должен дать письменное согласие на обработку своих персональных данных специальной категории. В свою очередь, закон дает право обработки персональных данных без согласия субъекта в случае предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг.

Также встает вопрос об обработке биометрических персональных данных, в том числе фотографии, данные, характеризующие особенности сетчатки глаза, что представляют собой сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Вопросы создания системы обеспечения информационной безопасности «электронного правительства» и соблюдения законодательства Российской Федерации в сфере обеспечения безопасности персональных данных при их обработке в информационных системах находятся на стадии обсуждения. По нашему мнению, данные вопросы должны обсуждаться на федеральном уровне, должны быть выработаны единые требования и рекомендации по обеспечению безопасности персональных данных в системе электронного правительства.

Также существует проблема нормативно-правового регулирования требований по защите персональных данных. Принятие изменений, внесенных Федеральным законом от 25.07.2011 № 261-ФЗ, повлекло изменение концепции защиты персональных данных. В соответствии с новыми изменениями Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает уровни защищенности персональных данных при их обработке в информационных системах персональных данных. Таким образом, классы информационных систем персональных данных и связанная с ними нормативно-правовая база перестала быть актуальной.

Учитывая происшедшие изменения, Правительство должно переработать нормативные документы, где классификация информационных систем персональных данных будет заменена уровнями защищенности персональных данных. На сегодняшний день порядок определения уровней защищенности и требования к ним не закреплены.

Пример выполнения установленных законом и подзаконными актами требований должны показывать органы государственной власти, являющиеся операторами персональных данных. Недостаточно только сформулировать «букву закона», требуется сохранить и реализовать эти законы на практике. А на практике все складывается иначе: порталы государственных органов, обрабатывающих сведения о гражданах, не удовлетворяют требованиям по защите персональных данных. Для шифрования персональных данных, передаваемых в сети Интернет на портал и с портала государственных услуг www.Gosuslugi.ru, применяется протокол https, использующий в свою очередь Open SSL, криптографический пакет с открытым исходным кодом, не имеющим сертификата ФСБ. На портале Федеральной налоговой службы любой человек, знающий ИНН субъекта персональных данных, может получить исчерпывающую информацию о его задолженностях по всем налогам. На сайте Службы судебных приставов можно получить информацию об исполнительных производствах в отношении любого гражданина. К тому же указанные государственные структуры, являясь операторами персональных данных, не обозначают цели и способы обработки персональных данных.

В соответствии с Приказом МВД России и ФНС России от 31 октября 2008 года № 948/ММ-3-6/561[6] файлы передачи/корректировки данных со сведениями о транспортных средствах и лицах, на которых они зарегистрированы, представляются в соответствующие органы по электронной почте или на электронных носителях. В рамках такого взаимодействия передаются следующие персональные данные: ФИО, ИНН, дата рождения, пол, серия и номер паспорта или в/у, гражданство, адрес регистрации. При этом в приказе обозначается лишь, что органы обеспечивают защиту информации в соответствии с требованиями к работе с информацией ограниченного доступа. Каким образом осуществляется защита на практике и действительно ли принимаются меры – не известно.

Нормативным «подводным камнем» на сегодняшний день является вопрос обеспечения защиты прав субъектов персональных данных при оказании государственных услуг в электронном виде. Помимо самого закона о защите персональных данных требуется разрабатывать информационную политику по закреплению принципов, например, о децентрализованном хранении персональных данных, о правилах межведомственного обмена данными. Также необходимо включение вопросов обеспечения информационной безопасности в состав критериев экспертной оценки документов, используемых в рамках планирования, создания и использования информационно-коммуникационных технологий в деятельности государственных органов[7].

Для успеха электронного правительства нужно сбалансировать защиту персональных данных и возможность эффективного использования персональных данных для оказания государственных услуг. В ближайшем будущем личная и общественная жизнь граждан неизбежно будет контролироваться все сильнее – как государственными органами, так и заинтересованными коммерческими организациями, поэтому обеспечение безопасности персональных данных граждан должно стать одним из приоритетных направлений в деятельности электронного правительства.

Примечания

[1] Концепция формирования в Российской Федерации электронного правительства до 2010 года. Одобр. распоряжением Правительства Российской Федерации № 632-р от 06 мая 2008 г. // СЗ РФ. – 2008. – № 20. – Ст. 2372.

[2] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. – 2006. – № 31. – Ст. 345.

[3] СЗ РФ. – 2011. – № 17. – Ст. 2465.

[4] См. там же.

[5] Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 г. № 210-ФЗ // СЗ РФ. – 2010. – № 31. – Ст. 4179.

[6] Приказ МВД России и ФНС России от 31 октября 2008 года № 948/ММ-3-6/561 «Об утверждении Положения о взаимодействии подразделений Госавтоинспекции и налоговых органов при представлении сведений о транспортных средствах и лицах, на которых они зарегистрированы» // Российская газета. – 2009. – 28 янв.

[7] Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов // СЗ РФ. – 2010. – № 22. – Ст. 2778.

И. У. Кулдыбаева, аспирант кафедры конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: irinakuldybaeva@mail.ru

I. U. Kuldybaeva, postgraduate student of Constitutional and Administrative Law Department of South Ural State University (national research university). E-mail: irinakuldybaeva@mail.ru

УДК 342.7:004 + 070.133 + 342.7(094.5.072)
ББК Х400.323:Ч600 + Ч600.00

Минбалеев А. В.

ПРОБЛЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЖУРНАЛИСТАМИ И СМИ

В статье исследуются проблемы обработки персональных данных журналистами и средствами массовой информации при осуществлении ими профессиональной деятельности. Анализируются нормы законодательства о персональных данных об ограничении прав субъектов персональных данных при обработке их персональных данных журналистами. Даются рекомендации журналистам и СМИ. Рассматриваются гарантии субъектов персональных данных.

Ключевые слова: *журналист, персональные данные, защита прав, средства массовой информации, профессиональная деятельность.*

Minbaleev A. V.

PROBLEMS OF PROCESSING OF THE PERSONAL DATA JOURNALISTS AND MASS-MEDIA

In the article the problem of processing of the personal data journalists and mass medias is explored at realization by them to professional activity. The norms of legislation are analysed about the personal information about limitation of rights for the subjects of the personal information at processing of their personal data journalists. Given recommendation journalists and mass media. The guarantees of subjects of the personal information are examined.

Keywords: *journalist, personal information, defence right, mass medias, professional activity.*

Журналисты в процессе осуществления профессиональной деятельности постоянно сталкиваются с необходимостью обработки персональных данных своих «героев», интервьюируемых и других лиц. Особенно часто с проблемой персональных данных приходится сталкиваться в ходе журналистских расследований, когда кроме персональных данных обычной чувствительности приходится использовать специальные категории персональных данных. Федеральный закон «О персональных данных» (далее – Закон о персональных данных)[1] в числе специально урегулированных отношений предусмотрел и обработку персональных данных журналистами и средствами массовой информации (далее – СМИ). Насколько свободно сегодня могут обрабатывать персональные данные тех или иных лиц журналисты и СМИ? Где пределы вмешательства журналистов в сферу персональных данных? Эти вопросы сегодня постоянно ставятся редакциями СМИ. Они же

имеют и важную научную значимость, поскольку институт обработки персональных данных в сфере массовой информации является одним из наименее изученных механизмов ограничения права на персональные данные как в российской науке информационного права, так и за рубежом[2].

Правовой основой для законной обработки журналистами персональных данных выступает п. 6 ч. 2 ст. 6 Закона о персональных данных. Персональные данные могут обрабатываться без предварительного получения согласия субъекта персональных данных в случае, когда такая «обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных». При этом под обработкой персональных данных Закон о персональных данных понимает действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных. Таким образом, все эти действия с персональными данными журналист может осуществлять только в целях профессиональной деятельности.

Данное ограничение традиционно связывается с ст. 9 (п. b ч. 2) Конвенции о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 (Страсбург, 28 января 1981 г.), согласно которой договаривающиеся стороны могут отступить от основных принципов защиты данных личного характера, когда это предусмотрено законом государства и является необходимой мерой в демократическом обществе для защиты субъекта данных или прав и свобод других лиц[3]. Ограничение прав субъектов персональных данных при их обработке в процессе профессиональной деятельности журналиста введено в целях защиты свободы массовой информации и свободы слова. Это так называемая «медиапривилегия»[4].

Согласно ст. 2 Закона Российской Федерации «О средствах массовой информации» (далее – Закон о СМИ)[5] под журналистом понимается лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию. Из данного определения явно следует, что в полномочия журналиста не входит распространение информации, а значит и обработка персональных данных в части их распространения. Профессиональная деятельность журналиста неотъемлемо связана с деятельностью редакции СМИ. В связи с этим обработкой персональных данных в части ее распространения занимается редакция СМИ. Между тем, редакция СМИ не названа в п. 6 ч. 2 ст. 6 Закона о персональных данных как субъект, управомоченный обрабатывать персональные данные без предварительного получения согласия субъекта персональных данных. В связи с чем на практике сегодня ряд СМИ задаются вопросом о наличии у них такого права. Представляется, что анализируемую норму необходимо толковать расширительно (включая редакции СМИ в число управомоченных субъектов), поскольку без редакции СМИ журналист не может осуществлять профессиональную деятельность и реализовать свое право на обработку персональных данных. Подтверждением данной мысли является и легальное определение понятия «распространение персональных данных», под которым Закон о персональных данных понимает «действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, *в том числе обнародование персональных данных в средствах массовой информации*, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом». Также необходимо учитывать, что Закон о персональных данных допускает обработку персональных данных без согласия субъекта именно в целях профессиональной деятельности журналиста. Данная цель предполагает, что журналист обязательно действует от редакции СМИ (выполняет трудовые обязанности, исполняет условия гражданско-правового договора, заключенного с редакцией, или действует по поручению редакции), а не от себя лично.

Спорным вопросом является и возможность «льготной» обработки персональных данных всеми журналистами. С точки зрения

юридического статуса в качестве журналиста может быть любое физическое лицо, уполномоченное редакцией (например, внештатные корреспонденты, работающие по заданию редакции). Возникает вопрос о том, кто будет гарантировать в данном случае выполнение данным лицом требований конфиденциальности персональных данных. Особенно это актуально в тех случаях, когда внештатные корреспонденты работают в другом регионе, и, еще сложнее, если сбор персональных данных происходит за рубежом.

Анализируемому ограничению прав субъектов персональных данных на их обработку корреспондирует обязанность журналистов и средств массовой информации соблюдать требования о недопустимости нарушения прав и свобод субъектов персональных данных. Прежде всего, это права субъектов персональных данных, закрепленные Законом о персональных данных. В частности, право на доступ к своим персональным данным, в том числе право требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав (ст. 14 Закона о персональных данных).

Права субъектов, персональные данные которых обрабатываются журналистами в процессе профессиональной деятельности, также вытекают из ряда обязанностей журналистов, закрепленных в Законе о СМИ и других законах, регулирующих отношения в сфере массовой информации. Так, ст. 41 Закона о СМИ запрещает редакции СМИ без согласия несовершеннолетнего и его законного представителя разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие. Без согласия несовершеннолетнего и (или) его законного представителя запрещается разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, признанного потерпевшим. Согласно ст. 50 Закона о СМИ распространение сообщений и материалов, подготовленных с использованием скрытой аудио- и видеозаписи, кино- и фотосъемки, допускается только, если это не нарушает конституционных прав и свобод человека и гражданина; если это необходимо для защиты общественных интересов и приняты меры против возможной идентификации посторонних лиц, а также если демонстрация записи производится по решению суда.

При работе с персональными данными СМИ и журналистам необходимо учитывать, что освобождение журналистов от предварительного получения согласия субъекта персональных данных на их обработку при осуществлении профессиональной журналистской деятельности не освобождают СМИ от этой обязанности при обработке персональных данных в иных отношениях и в иных целях кроме профессиональной деятельности по созданию и распространению массовой информации. Например, в случаях обработки персональных данных читателей, зрителей, слушателей, подписчиков, клиентов в целях исследования общественного мнения, повышения рейтинга и т. д. Не освобождены они и от обязанности принимать меры по охране конфиденциальности, установленные законодательством о персональных данных. Соблюдение конфиденциальности персональных данных возлагается как на СМИ в качестве оператора, так и любого журналиста, получившего доступ к персональным данным. Это требование вытекает не только из статей 3 и 7 Закона о персональных данных, но и ст. 49 Закона о СМИ, согласно которой при осуществлении профессиональной деятельности журналист обязан: уважать права, законные интересы, честь и достоинство граждан и организаций; проверять достоверность сообщаемой им информации; сохранять конфиденциальность информации и (или) ее источника; при получении информации от граждан и должностных лиц ставить их в известность о проведении аудио- и видеозаписи, кино- и фотосъемки.

Современная судебная практика пока скупа по вопросам использования персональных данных журналистами. Можно отметить лишь решение по сетевому изданию «Листок» в г. Горно-Алтайск. По данному делу в статье «Детектив на окраине» была опубликована информация, с помощью которой, по словам истца, «его можно идентифицировать, то есть однозначно определить, что

речь идет именно о нем, т.к. указаны фамилия, адрес, место работы. Своего согласия газете «Листок в Горно-Алтайске» на обработку и распространение такой информации он не давал. Поскольку, в этой статье о нем излагается в негативном свете, считает нарушенными свои права»[6]. Из судебного решения следует, что А. А. Макогонский, являясь главным редактором печатного издания «Листок в Горно-Алтайске», в силу ст. 19 Федерального закона «О средствах массовой информации», неся ответственность за выполнение требований, предъявляемых к деятельности средств массовой информации, допустил публикацию в газете «Листок в г. Горно-Алтайске» № 40 от 06.10.2010 года, содержащую персональные данные гражданина Ананьева И. В., его фамилию, место работы, адрес, обстоятельства частной жизни, без письменного согласия последнего. В связи с чем в действиях А. А. Макогонского усматривается состав административного правонарушения, предусмотренного ст. 13.11 КоАП РФ.

По данному делу сначала мировой судья, а затем судья апелляционной инстанции даже не рассмотрели вопрос о возможности применения специальной нормы, предусмотренной п. 6 ч. 2 ст. 6 Закона о персональных данных. В решении лишь говорится об общих требованиях закона, в том числе, что «поскольку, из части 1 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» следует, что субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Таким образом, согласие гражданина на использование его персональных данных в указанном случае являлось обязательным. Статьей 6 названного Закона в качестве условия обработки персональных данных также указано на обязательное наличие согласия субъекта персональных данных». Представляется, что подобное решение как минимум подлежит пересмотру в вышестоящей инстанции, поскольку судом не применены специальные нормы и не рассматривался вопрос о специальном статусе журналиста при обработке персональных данных.

В ходе профессиональной деятельности журналистов их персональные данные также часто подлежат обработке, например, при их использовании в рамках аккредитации журналистов. И в этом случае также речь может идти об обработке аккредитующими организациями персональных данных без согласия их субъектов (журналистов), если это осуществляется в целях профессиональной деятельности журналистов. Интересно в этом отношении определение Верховного Суда Российской Федерации от 27 февраля 2008 г., в котором было принято решение по жалобе прокурора Республики Коми о признании противоречащими федеральному законодательству и недействующими со дня принятия ряда норм Положения об аккредитации представителей средств массовой информации при Главе Республики Коми, утвержденного Указом Главы Республики Коми «Об аккредитации представителей средств массовой информации при Главе Республики Коми» от 19 декабря 2006 г. № 143, в частности, подпункта 1 пункта 9 в той части, в какой он предусматривает представление редакцией средства массовой информации в Управление по связям с общественностью и информации администрации Главы Республики Коми и Правительства Республики Коми сведений о фактическом адресе, почтовом (электронном) адресе, номерах служебных и мобильных (домашних) телефонов каждого из аккредитуемых журналистов; подпункта 2 пункта 15 в той части, в какой он предусматривает возможность отказа в аккредитации при представлении средством массовой информации заявки, не содержащей сведений о фактическом адресе, почтовом (электронном) адресе, номерах служебных и мобильных (домашних) телефонов каждого из аккредитуемых журналистов.

Заявитель в своей жалобе ссылался на тот факт, что Глава Республики Коми не относится в силу положений Федерального закона «О персональных данных» к операторам, осуществляющим обработку персональных данных. Кроме того, в соответствии с названным Указом персональные данные аккредитуемых журналистов должны были предоставляться в обязательном порядке, то есть без их согласия, что, по мнению заявителя, противоречит общим принципам обработки персональных данных, установленных законом.

Проверив материалы дела, изучив доводы кассационного представления прокурора, Судебная коллегия по гражданским делам Верховного Суда Российской Федерации нашла ранее принятое решение Верховного суда Республики Коми подлежащим оставлению без изменения по следующим основаниям. В силу ст. 1, 38, 39, 48 Закона Российской

Федерации «О средствах массовой информации» редакция средства массовой информации с целью оперативного получения полной информации о деятельности государственных органов, организаций, учреждений, органов общественных объединений и доведения этой информации до граждан вправе подать заявку на аккредитацию при указанных выше органах, организациях, учреждениях своих журналистов. Судом обоснованно обращено внимание на то, что правила аккредитации журналистов при государственных органах, организациях, учреждениях, органах общественных объединений устанавливаются данными субъектами самостоятельно. То есть Глава Республики Коми действительно имеет статус оператора, имеющего право устанавливать принципы и цели обработки персональных данных.

Аккредитовавшие журналистов органы, организации, учреждения обязаны предварительно извещать их о заседаниях, совещаниях и других мероприятиях, обеспечивать стенограммами, протоколами и иными документами, создавать благоприятные условия для производства записи. Для исполнения указанной обязанности они должны располагать сведениями о фактическом адресе, почтовом (электронном) адресе, номерах служебных и мобильных (домашних) телефонов каждого из аккредитованных журналистов, поскольку непредставление редакцией средства массовой информации данного минимума персональных данных может привести как к нарушению предусмотренных статьями 47, 48 Закона Российской Федерации «О средствах массовой информации» прав журналистов, так и к ущемлению права граждан на получение оперативной и достоверной информации о деятельности органов, организаций и учреждений, аккредитовавших журналистов.

Существенное значение в данном случае имеет и то обстоятельство, что в силу требований Закона Российской Федерации «О средствах массовой информации» аккредитация журналиста возможна только на основании его волеизъявления, в связи с чем предполагается согласие этого журналиста на передачу редакцией соответствующих персональных данных.

Судом также правильно обращено внимание на то, что аккредитация журналиста непосредственно связана с его профессиональной деятельностью по поиску, получению и распространению информации, и поэтому, в соответствии с п. 6 ч. 2 ст. 6 Федерального закона «О персональных данных», необходимый для реализации требований статьи 48 Закона «О средствах массовой информации» минимум персональных данных журналиста может передаваться в орган, осуществляющий его аккредитацию, и без согласия этого журналиста[7].

Анализ практики обработки журналистами персональных данных в процессе профессиональной деятельности свидетельствует, что пока в журналистской среде нет достаточного понимания, каким же образом необходимо осуществлять обработку персональных данных. Многие правоприменители также не готовы использовать специальные нормы, регулирующие особое положение журналистов, обрабатывающих персональные данные. Во многом это объясняется нечеткими формулировками Закона о персональных данных, а также отсутствием разъяснений по этому вопросу уполномоченных органов государственной власти.

Примечания

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.

[2] См.: Zulauf R. Informationsqualitet. Ein Beitrag zur journalistischen Qualitetsdebatte aus der Sicht des Informationsrechts: Dissertation / Genehmigt auf Antrag vor Prof. Dr. Rolf H. Weber. Zurich: Schulthess Juristische Medien AG, cop. 2000. 164 s.; Beckmann E. Der Schutz personenbezogener Daten im sozialen Sicherungssystem: Auf der Basis des deutschen, osterreichischen und europaischen Rechts. 1.Aufl. Baden-Baden: Nomos, 2000. 221 s. (Frankfurter Studien zum Datenschutz; Bd.15); Kugelmann D. Die informatorische Rechtsstellung des Burgers: Grundlagen und verwaltungsrechtliche Grundstrukturen individueller Rechte auf Zugang zu Informationen der Verwaltung. Tubingen: Mohr, 2001. XII, 399 s. (Jus publicum; Bd. 65); Smith Graham J.H. Internet law and regulation / By Graham J. H. Smith and contributors from Bird & Bird: Simon Chalton et al. 3. ed., reprint. London: Sweet & Maxwell, 2002. – XLVII, 737 p.

[3] Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS N 108). Заключена в г. Страсбурге 28.01.1981 // Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью. – М.: СПАРК, 1998. – С. 106–114.

[4] См.: Fechner F. Medienrecht: Lehrbuch des gesamten Medienrechts unter besonderer Berecksichtigung von Presse, Rundfunk und Multimedia. – Stuttgart, 2008. – S. 160–161.

[5] Закон РФ от 27.12.1991 № 2124-1 (ред. от 25.12.2008) «О средствах массовой информации» // Ведомости СНД и ВС РФ. – 1992. – № 7. – Ст. 300.

[6] Решение Горно-Алтайского городского суда Республики Алтай от 16 февраля 2011 года г. Горно-Алтайск. – http://www.listock.ru/15928.

[7] См.: Определение Верховного Суда Российской Федерации от 27 февраля 2008 г. № 3-Г08-3 «Об оставлении без изменения решения Верховного Суда Республики Коми от 28.11.2007, которым частично удовлетворено заявление о признании противоречащими федеральному законодательству и недействующими со дня принятия ряда норм Положения об аккредитации представителей средств массовой информации при Главе Республики Коми, утвержденного Указом Главы Республики Коми «Об аккредитации представителей средств массовой информации при Главе Республики Коми» от 19.12.2006 № 143». URL: http://www.supcourt.ru/stor_text.php?id=20192255.

Минбалеев Алексей Владимирович, к.ю.н., доцент, доцент кафедры конституционного и административного права ЮУрГУ, доцент кафедры информационного права УрГЮА. E-mail: alexmin@bk.ru

Minbaleev Aleksey Vladimirovich, senior lecturer on Department of Constitutional and Administrative Law in the South Ural State University, senior lecturer on Department of Informative Law in the Ural State Law Academy, Doctor of Law. E-mail: alexmin@bk.ru

УДК 342.7:347.965 + 347.965.3
ББК Х75 + Х400.323

Циулина Н. Е.

КРИТЕРИИ ПРАВОМЕРНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ АДВОКАТОМ

В статье анализируются законодательные и нормативные акты, регламентирующие адвокатскую деятельность. Автор исследует законодательно установленные права адвоката, выявляет определение адвокатской тайны и приходит к выводу о невозможности привлечения адвоката к ответственности за нецелевое использование полученной информации. Автор считает, что обработка адвокатом персональных данных третьих лиц должна осуществляться при условии получения согласия этих лиц в любой подтверждающей этот факт форме.

Ключевые слова: *федеральный закон, персональные данные, адвокатская деятельность, адвокатская тайна, документ, защита информации, согласие, доверитель, доверенность, специальный правовой статус.*

Tsyulina N. E.

CRITERIA FOR THE LAWFULNESS OF PROCESSING PERSONAL DATA BY ATTORNEY

This paper analyzes the legislation and normative acts that regulate the lawyers's practice. The author examines statutory rights of the lawyer, explores the notion of revealing the lawyer's secrecy and concludes about the impossibility of a lawyer to become a subject to liability for a non target usage of information. The author believes that the processing of third parties' personal data by a lawyer should be a subject to consent by these parties in any given valid form.

Keywords: *Federal Law, personal data, advocacy, lawyer's secrecy, document, information security, consent, trustee, procuracy, special legal status.*

Адвокатская деятельность, а также функции, полномочия и обязанности адвоката определены Федеральным законом от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»[1]. Ст. 1 определяет адвокатскую деятельность как квалифицированную юридическую помощь, оказываемую на профессиональной основе лицами, получившими статус адвоката, в целях защиты их прав, свобод и интересов, а также обеспечения доступа к правосудию, что согласуется со ст. 45 Конституции РФ «каждый вправе защищать свои права и свободы всеми способами, не запрещенными законом», ст. 48 Конституции, которая гарантирует каждому гражданину право на получение квалифицированной юридической помощи и ст. 123: «судопроизводство осуществляется на основе состязательности и равноправия сторон».

Вместе с тем, практика реализации Федерального закона создает предпосылки для уточнения его отдельных положений, в частности предоставления персональных данных по письменному запросу адвоката.

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает, что целью данного Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. В основе закона лежат конституционные положения, гарантирующие защиту прав на неприкосновенность частной жизни, личную и семейную тайну, запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, а также положения, определяющие допустимость ограничения названных конституционных прав граждан нормами других федеральных законов.

Анализ ст. 6 Федерального закона «О персональных данных» свидетельствует о возможности обработки, в том числе и передачи персональных данных при условии осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей. А ст. 10 Федерального закона определяет специальные категории персональных данных, условия обработки которых предусматривают специальный правовой режим доступа к ним.

В соответствии с п. 3. ст. 6 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат вправе собирать сведения, необходимые для оказания юридической помощи, в том числе запрашивать справки, характеристики и иные документы от органов государственной власти, органов местного самоуправления, а также общественных объединений и иных организаций. Указанные органы и организации обязаны выдать адвокату запрошенные им документы или их заверенные копии не позднее, чем в месячный срок со дня получения запроса адвоката. П. 5 ст. 6 этого же закона запрещает адвокату «разглашать сведения, сообщенные ему доверителем в связи с оказанием последнему юридической помощи, без согласия доверителя». Любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю, являются адвокатской тайной (ст. 8). Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката допускается только на основании судебного решения.

Законодатель защитил от неправомерного использования любую информацию о лице, полученную адвокатом в процессе профессиональной деятельности, в том числе и от оператора.

Однако наступление дисциплинарной ответственности непосредственно за нарушение тайны предполагается только в случае разглашения адвокатом сведений, сообщенных ему доверителем, без согласия последнего (подп. 5 п. 4 ст. 6). Однако привлечь адвоката к ответственности за нецелевое использование профессионально значимой информации, за исключением случаев разглашения, практически невозможно, поскольку на правоприменительном уровне норма подп. 1 п. 1 ст. 9 Кодекса профессиональной этики адвоката[2] не позволяет в полной мере учитывать специфику адвокатской тайны.

На наш взгляд, пока отсутствует правовая норма, четко определяющая критерии правомерного использования информации адвокатом, уверенности, что адвокат понесет ответственность в случае любого злоупотребления сведениями, у доверителей не будет. Это касается не только доверительных тайн, но и сведений, полученных адвокатом о третьих лицах без их согласия, например: персональных данных участников процесса, содержание их документов и показаний; данные опроса третьих лиц; иная информация, полученная в ходе адвокатского производства по делу или в связи с ним. Представляется, что для использования такой информации, в частности, для оказания помощи доверителям, адвокат должен заручиться разрешением всех лиц, которых она касается[3].

Согласно п. 2 ст. 6 адвокат представляет доверителя на основании доверенности. Доверенность по своей юридической природе – сделка односторонняя, и потому для ее действительности и действия достаточно соответствующего закону волеизъявления представляемого (доверителя). Содержание воли доверителя должно свидетельствовать о его желании уполномочить представителя совершить от его имени и в его интересах юридическое действие. Исходя из общих правил представительства, доверенное лицо, заклю-

чая сделку или совершая иные правомерные действия, на которые у него имеются полномочия, действует от имени представляемого и для представляемого наступают правовые последствия: создаются, изменяются или прекращаются гражданские права и обязанности, таким образом, правоотношения возникают между представляемым и третьим лицом[4]. Выдаваемая гражданином доверенность должна содержать подпись доверителя[5], что согласуется с требованием ст. 9 Федерального закона «О персональных данных», когда согласие субъекта персональных данных на обработку его персональных данных может быть дано субъектом в любой форме, позволяющей подтвердить факт его получения. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочие данного представителя на дачу согласия от имени субъекта персональных данных проверяется оператором .

Конституционный Суд Российской Федерации вынес определение от 29 сентября 2011 г. № 1063-О-0, что информация, в силу статьи 24 (часть 2) Конституции Российской Федерации любая затрагивающая права и свободы гражданина (за исключением сведений, содержащих государственную тайну, сведений о частной жизни, а также конфиденциальных сведений, связанных со служебной, коммерческой, профессиональной и изобретательской деятельностью), должна быть ему доступна, при условии, что законодателем не предусмотрен специальный правовой статус такой информации в соответствии с конституционными принципами, обосновывающими необходимость и соразмерность ее особой защиты. Исходя из приведенной правовой позиции Конституционного Суда Российской Федерации, исключение информации, относящейся к персональным данным, которая была запрошена заявителем, из режима свободного доступа полностью соответствует предписаниям статьи 24 (часть 2) Конституции Российской Федерации. В противном случае под угрозой оказалось бы гарантированное статьями 23 (часть 1) и 24 (часть 1) Конституции Российской Федерации право на неприкосновенность частной жизни.

Таким образом, заявитель, запрашивая персональные данные лиц, вместе с запросом должен предоставить: либо доверенности от этих лиц, заверенные установленным порядком, либо их согласие на обработку персональных данных в любой подтверждающей этот факт форме.

При этом заявитель не лишен возможности при рассмотрении судом конкретного дела с участием его доверителя обратиться к суду с ходатайством об истребовании доказательств, в том числе сведений, содержащих конфиденциальную информацию.

Проведенный анализ свидетельствует, что условия обработки (передачи) персональных данных лиц, в том числе и по запросу адвоката, решается на законодательном уровне. Вместе с тем, наличествуют проблемы, которые могут привести к злоупотреблениям адвокатом персональными данными, особенно третьих лиц. На наш взгляд, необходимо дополнить п. 2 ст. 6 Федерального закона от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» следующей нормой: «В случаях, предусмотренных федеральным законом, адвокат представляет доверителя на основании доверенности. Обработка адвокатом персональных данных третьих лиц осуществляется с их согласия в любой подтверждающей этот факт форме».

Примечания

[1] Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (с изменениями от 28 октября 2003 г., 22 августа, 20 декабря 2004 г., 24 июля, 3 декабря 2007 г., 23 июля 2008 г., 11 июля, 21 ноября 2011 г.) [Электронный ресурс] // http://base.garant.ru

[2] Кодекс профессиональной этики адвоката (принят Первым Всероссийским съездом адвокатов 31 января 2003 г.) (с изменениями и дополнениями, утвержденными Третьим Всероссийским съездом адвокатов 5 апреля 2007 г.) [Электронный ресурс] // http://base.garant.ru/12130519/

[3] Пилипенко Ю. С. Адвокатская тайна: теория и практика. – М.: «Информ-Право», 2009. – С. 131

[4] Постатейный комментарий к Основам законодательства Российской Федерации о нотариате [Электронный ресурс] // http://www.6pl.ru/dogovor/dover.htm

[5] Постатейный комментарий к Гражданскому кодексу Российской Федерации / Комментарий к главе 10. Представительство. Доверенность [Электронный ресурс] // http://www.6pl.ru/dogovor/gk_dover_com.htm

Циулина Наталья Евгеньевна, начальник службы делопроизводства Южно-Уральского государственного университета. E-mail: cne@susu.ac.ru

Tsiulina Natalya Evgenjevna, head of office administration service of South Ural State University. Email: cne@susu.ac.ru

УДК 342.7:004.056 + 342.9.086
ББК Х400.323 + Х401.114

Брызгин А. А., Минбалеев А. В.

ПРАВОВОЙ РЕЖИМ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье поднимается актуальная сегодня в теории и на практике проблема понимания сущности биометрических персональных данных. Авторами дается анализ легального определения биометрических персональных данных. Исследуются сущностные признаки биометрических персональных данных.

Ключевые слова: *биометрические персональные данные, обработка, правовой режим.*

Bryzgin A. A., Minbaleev A. V.

LEGAL REGIME OF BIOMETRICAL PERSONAL DATA

The article raises the urgent theoretical and practical issues of understanding the essence of biometrical personal data. The authors give an analysis of legal definition of biometrical personal data. They investigate essential characteristics of biometrical personal data.

Keywords: *biometrical personal data, processing, legal regime.*

Одной из основных проблем формирующегося законодательства в области персональных данных в Российской Федерации является нечеткость формулировок терминов и определений. Результатом подобной нечеткости становится размытие границ применимости норм, закрепленных законами и подзаконными нормативными актами. Это, в свою очередь, приводит к отсутствию единой позиции регуляторов по ряду вопросов, а впоследствии, и к неоправданному завышению ряда требований по защите информации, составляющей персональные данные граждан, особенно при проверках на местах.

Анализ практики защиты персональных данных позволяет выявить проблему формулировки термина «биометрические персональные данные», приводящую в ряде случаев к несогласию оператора персональных данных с результатами проверок. Несогласие, в частности, касается отнесения к разряду биометрических персональных данных фотографических изображений граждан и их копий на бумажных носителях, а также копий гражданских паспортов на бумажных носителях, содержащих фотографические изображения граждан при использовании означенных изображений, их копий и копий докумен-

тов в кадровом делопроизводстве и, кроме того, к требованиям по сбору согласий на обработку таких данных у субъектов.

Целями настоящей статьи являются анализ обоснованности подобного отнесения и соответствующих требований, рассмотрение последствий отнесения части информации, обрабатываемой оператором, к биометрическим персональным данным, а также выработка стратегии и тактики действий оператора в преддверии проверочных мероприятий.

Достигнуть целей предполагается посредством анализа определения биометрических персональных данных, приведенного в Федеральном законе «О персональных данных» № 152-ФЗ, а также его соотнесения с положениями и формулировками данного закона и иных нормативных правовых актов и государственных стандартов, касающихся биометрической идентификации и аутентификации.

В начале статьи хотелось бы уделить внимание примеру неверного толкования понятия биометрических персональных данных операторами персональных данных.

Часть 1 ст. 11 ФЗ «О персональных данных» № 152-ФЗ от 27.07.2006 в редакции от 25.07.2011 г. гласит: «*Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи*».

Именно этот текст дает определение термина биометрических персональных данных, и именно в его толковании совершают ошибки многие операторы, выводя в качестве определения биометрических персональных данных следующую формулировку: «**биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных**». Данная формулировка, по сути, снимает с оператора ответственность за декларирование факта обработки сведений, которые формально являются биометрическими, однако фактически не используются им для установления личности субъекта персональных данных.

Анализируя же исходный пункт грамматически, мы видим, что термин, указанный в скобках, логически обобщает лишь следующую формулировку «**Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность**», а оставшаяся часть «*и которые используются оператором*…» относится уже к требованию наличия согласия субъекта на обработку таких данных за исключением случаев, перечисленных в части 2 той же статьи.

Вторая же часть данной статьи определяет следующее: «*2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию*». Как видим, исключения не касаются большей части операторов и относятся только к операторам, являющимся государственными органами РФ.

Таким образом, в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ от 27.07.2006 в редакции от 25.07.2011 г. определением биометрических персональных данных является следующее определение:

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Кроме того, в соответствии с законом, согласие субъекта необходимо получать только на обработку тех биометрических персональных данных, которые используются оператором для установления личности субъекта, получение же согласия для биометрических персональных данных, используемых для

определения личности, необходимо за исключением вышеперечисленных случаев.

Можем допустить, что такое определение косвенно подтверждает справедливость отнесения к биометрическим персональным данным ксерокопий паспорта гражданина Российской Федерации (в части фотографического изображения) и фотографий в личном деле сотрудника, однако, не влечет никаких последствий для оператора в силу текста части первой ст. 11 ФЗ «О персональных данных», то есть в силу того, что такие данные фактически не используются оператором для установления личности субъекта, а обрабатываются в основном в силу соблюдения традиций кадрового делопроизводства, и всякие требования по сбору согласий на обработку биометрических персональных данных при хранении ксерокопий паспорта и фотографии в личном деле сотрудника являются превышением полномочий регуляторов, в случае если оператором будет доказано отсутствие факта использования хранимых данных для установления личности субъекта (биометрической идентификации), причем именно идентификации, а не аутентификации (подтверждения подлинности личности). По факту же обращение к обозначенным в статье носителям информации производится лишь при недоверии к подлинности субъекта или предъявляемого им документа, следовательно, речь может идти только об аутентификации, то есть подтверждении, а не установлении личности субъекта.

Вообще же стоит обратиться к принципам и условиям обработки ПД, перечисленным в ст. ст. 5 и 6 Закона «О персональных данных» № 152-Ф. В пункте 2 статьи 5 сказано: «Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных», в пункте 4 этой же статьи говорится: «Обработке подлежат только персональные данные, которые отвечают целям их обработки», а в пункте 5 в том числе сказано: «…*Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки*». Пункт 1 статьи 6 Закона описывает 11 условий, при которых обработка персональных данных субъектов возможна, в том числе, десять условий обработки персональных данных без согласия субъекта. Вот эти условия:

«1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) закон-

ной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом».

Наиболее применимыми к исследуемой ситуации видятся подпункты 1, 2 и 5 настоящего пункта ст. 6 федерального закона, то есть необходимо определить, имеются ли у оператора права или обязанности по обработке биометрических категорий персональных данных в соответствии с законами, подзаконными нормативными актами, договорами с субъектом и договорами, где субъект выступает в роли поручителя или выгодоприобретателя, а также существуют ли у данного вида обработки статистические или исследовательские цели.

Таким образом, оператору до проверки, а лучше еще на этапе создания системы обработки персональных данных, следует разобраться с целями такой обработки и с законодательными требованиями к ее условиям. Это относится ко всем категориям персональных данных, а не только к тем, которые рассматриваются в исследовании.

Что же касается рассматриваемых спорных категорий персональных данных, то авторам видится, что наиболее используемая часть законодательства РФ не содержит требований или предписаний по хранению фотографических изображений сотрудников или клиентов и, тем более, копий их основных документов, сложно представить себе и договорные обязательства, для осуществления которых такая обработка была бы необходима. Следовательно, в общем случае цель обработки данных материалов действительно определяется и формулируется самим оператором и, соответственно, обработка должна согласовываться с субъектом независимо от того, причисляет оператор рассматриваемые в исследовании данные к биометрическим или нет.

Начиная данное исследование, авторы, кроме прочего, не согласны вообще с отнесением подобных данных к биометрическим персональным данным, и потому применили для уточнения результатов исследования также систематический способ толкования правовых норм, о результатах применения которого рассказано ниже.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утвержденные постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512, подпунктом «б» пункта 3 выводят из-под своего регулирования отношения, возникающие при использовании бумажных носителей для записи и хранения биометрических персональных данных. Таким образом, заявлена возможность бумажной формы хранения биометрических персональных данных, но не формулирует никаких требований к обработке соответствующих данных в конкретной бумажной форме, логично предположить, что подобная обработка должна производиться в соответствии с требованиями «**Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,** утвержденного постановлением Правительства Российской Федерации № 687 от 15.09.2008.

Показательным примером подхода законодателя к определению биометрии можно считать введение новой формы бланков паспортов (т. н. «биометрические» паспорта), о биометрическом характере которых заговорили лишь после того, как было сообщено о факте хранения внутри бланка паспорта специально структурированной информации на материальном электронном носителе.

Правительство РФ, в том числе, формулирует свои взгляды на предмет биометрических персональных данных в статье 2 **соглашения о сотрудничестве в создании государственных информационных систем изготовления, оформления и контроля паспортно-визовых документов нового поколения и дальнейшем их развитии и**

использовании в государствах – участниках Содружества Независимых Государств, утвержденного распоряжением Правительства Российской Федерации от 13 ноября 2008 г. № 1654-р, в которой сказано, в частности, следующее: *««биометрические персональные данные» – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (цифровая фотография, отпечатки пальцев, изображение радужной оболочки глаз и другие биометрические персональные данные), которые могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных в соответствии с законодательством каждого из государств Сторон».*

Несмотря на то что перечень данных, приведенный в соглашении, является открытым, мы видим ряд категорий, содержащих формализуемые биометрические признаки и составляющих биометрические персональные данные, в который, тем не менее, изображения лица гражданина на бумажном носителе совершенно не вписываются, для фотографического изображения явно указана цифровая форма.

Подкрепляет вышеозначенную позицию и содержания **перечня персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию**, установленного постановлением Правительства РФ № 125 от 4 марта 2010 г. Обозначенный перечень включает в себя следующие категории данных:

«1. Номер документа

2. Фамилия и имя владельца документа

3. Гражданство владельца документа

4. Дата рождения владельца документа

5. Пол владельца документа

6. Цветное цифровое фотографическое изображение лица владельца документа (биометрические персональные данные владельца документа)».

Как видно из пункта 6 перечня, именно цветное цифровое фотографическое изображение лица владельца документа составители назвали биометрическими персональными данными.

Продолжая систематический анализ, авторы изучили семейство национальных стандартов ГОСТ Р ИСО/МЭК 19794-х-хххх, которые и определяют требования к формированию наборов биометрических персональных данных, позволяющих определять личность субъекта, и, в частности ГОСТ Р ИСО/МЭК 19794-1-2008 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными».

Пункт 3.2 данного стандарта определяет термин «биометрия» (biometrics) как «Автоматическое распознавание личности человека, основанное на его поведенческих и биологических характеристиках», что еще раз приводит нас к выводу о том, что целевые носители сведений о гражданах не относятся к биометрическим.

Стоит, однако, заметить и то, что п. 1 ст. 1 Федерального закона «О персональных данных» № 152-ФЗ гласит о том, что данный закон регулирует отношения, связанные с обработкой персональных данных с использованием средств автоматизации или без использования таких средств, подразумевая, таким образом, неавтоматизированную биометрическую аутентификацию.

Это еще более усложняет проблему правильного формулирования в силу того, что 152-ФЗ развивает положения **европейской конвенции о защите физических лиц при автоматической обработке их персональных данных.** Как несложно заметить из названия, конвенция затрагивает лишь вопросы автоматической обработки личных данных, а регулирование неавтоматизированной обработки в 152-ФЗ появилось при ратификации данной конвенции в 2005 г. 160-ФЗ.

В силу возможностей, оставленных в ст. 11 конвенции, в соответствии с которой Российская Федерация обеспечивает расширенную защиту интересов граждан, формируя требования, в том числе и к способам неавтоматизированной обработки. Таким образом, говорить о несоответствии Закона международному акту, которым является «Евроконвенция», некорректно, но некорректно и обращаться к тексту конвенции для уточнения возможности неавтоматизированной обработки биометрических персональных данных.

В завершение статьи хотелось бы обратиться к анализу этимологии слова. Слово «биометрия» имеет греческое происхождение и образовано от двух слов: βίο — жизнь

и μετρέω — мерить. Подобная расшифровка термина, особенно его второй составной части, верно соотносится с основными методами и способами современной биометрии как науки, изученными авторами во время подготовки статьи, так, все стандарты под биометрическими признаками подразумевают измеряемые характеристики человеческого тела, снятые с определенной точностью и подразумевающие автоматизацию процессов снятия реальных характеристик и их сравнения с эталонными, приводящего к формированию решения задачи идентификации/аутентификации.

Таким образом, мы постарались доказать, во-первых, отсутствие юридических последствий хранения фотографий и ксерокопий паспортов граждан РФ в части изображений, если таковые не применяются для установления личности субъекта персональных данных (но если их обработка прямо или косвенно вытекает из требований законодательства и соотносится с целями обработки персональных данных), в том числе доказана возможность не получать согласие субъекта на обработку таких данных. Данный вывод, бесспорно, является скорее теоретическим и не подразумевает широких возможностей использования фотографий граждан операторами (исключения составляют группы операторов, являющихся органами исполнительной власти, финансовыми учреждениями и некоторые другие, в силу федеральных законов и подзаконных нормативных актов обязанные или наделенные правом хранить фотографические изображения граждан и ксерокопии их основных документов в части изображения), а на практике, в случае обработки таких данных без отнесения их к биометрическим, необходимо получение согласия субъекта на обработку дополнительных категорий его персональных данных.

Оценивая описанную в начале статьи ситуацию, можно заключить правомерность требований регулятора в части необходимости получения согласия на обработку фотографий субъекта и копии его паспорта, однако некорректно объяснять эту необходимость отнесением данных видов информации к биометрическим персональным данным. Обработка дополнительной информации подобного рода должна быть согласована с субъектом в силу того, что выходит за пределы требований законов и подзаконных нормативных актов, и если оператор считает подобную обработку необходимой для достижения поставленных целей и выполнения законных обязанностей, то это должно быть отражено также и в документах, определяющих подход оператора к обработке персональных данных.

Во-вторых, предпринята попытка доказать несоответствие таких физических проявлений персональных данных, как фото субъекта на бумажном носителе или копия паспорта, определению биометрических данных, сформулированному прямо или косвенно в нормативно-правовых актах, в том числе международных. Отмечено также то, что Федеральный закон Российской Федерации «О персональных данных» определяет возможности как автоматизированной, так и неавтоматизированной обработки таких данных, и потому прямое соотнесение данного определения с большинством российских и международных стандартов и договоров некорректно.

Однако равнозначно некорректным можно считать и введение особого подхода к биометрическим персональным данным (в том числе и на бумажных носителях) без определения, тем не менее, методики обработки и защиты таких данных.

Что касается бумажных носителей персональных данных, авторам представляется возможность столь экзотичного явления, однако, исходя из выведенной сущности биометрии вообще и биометрических персональных данных в частности, содержать такой носитель должен скорее биолого-математические данные, снятые по описанным в нормативной документации правилам, или пригодные для формализации и объективной оценки изначальные сведения, а не изображения в относительно свободной форме. Подобные измышления подкреплены выдержками из нормативно-правовой документации.

В части рекомендаций операторам персональных данных необходимо тщательно изучить состав фактически обрабатываемых на предприятии/в организации персональных данных и для каждой выявленной категории определить законное основание обработки и цель, на достижение которой направлена обработка данной категории. Для категорий, обработка которых прямо не предписывается законами или подзаконными нормативными актами, необходим сбор согласий на их обработку.

Что же касается биометрических персональных данных, то можно прийти к выводу, что неавтоматизированная их обработка на сегодняшний день не накладывает на оператора никаких дополнительных обязанностей сверх требований ст. 11 Федерального закона «О персональных данных» (обязанность согласования обработки с субъектом персональных данных либо обоснования возможности производить таковую обработку без согласия субъекта), а также требований **Положения об особенностях обработки персональных данных без использования средств автоматизации,** утвержденного Постановлением Правительства РФ № 687 от 15.09.2018, выполнение которых не связано со значительными трудовыми и финансовыми затратами.

С дополнительными материальными и временными затратами связана обработка биометрических персональных данных с использованием средств автоматизации, то есть компьютерной обработки, которая выходит за пределы темы данной статьи. Тем не менее мы считаем необходимым предупредить операторов о том, что в соответствии с **Требованиями к защите персональных данных при их обработке в информационных системах персональных данных**, установленными Постановлением Правительства РФ № 1119, для информационных систем персональных данных, содержащих биометрические персональные данные, должны быть обеспечены более высокие уровни защищенности по сравнению со стандартными категориями персональных данных. Именно поэтому учету и обоснованию законности и обоснованности автоматизированной обработки персональных данных оператору следует уделить особое внимание.

Брызгин А. А., студент магистратуры кафедры конституционного и административного права ЮУрГУ. E-mail: andreybryzgin@gmail.com

Минбалеев А. В., к.ю.н., доцент, зам. декана юридического факультета ЮУрГУ. E-mail: alexmin@bk.ru

Bryzgin A. A., graduate student of Constitutional and Administrative Law Department of South Ural State University. E-mail: andreybryzgin@gmail.com

Minbaleev A. V., candidate of law, associate professor, deputy dean of Law Faculty of South Ural State University. E-mail: alexmin@bk.ru

УДК 342.951:347.118 + 347.188:004.056 + 004.056
ББК Х401.131 + Х401.114

Захаров М.

ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ВОЕННОСЛУЖАЩИХ

Автором исследуется специальный режим персональных данных военнослужащих. Исследуется законодательство о персональных данных военнослужащих. Производится разграничение регулирования государственной тайны и персональных данных военнослужащих.

Ключевые слова: *персональные данные, защита, военнослужащие, государственная тайна.*

Zakharov M.

PECULIARITIES OF MILITARIES' PERSONAL DATA PROTECTION

The author investigates the special regime of militaries' personal data. The article studies the legislation on militaries' personal data. It makes distinctions of state secret and militaries' personal data control.

Keywords: *personal data, protection, militaries, state secret.*

Персональные данные сравнительно недавно вошли в нашу жизнь, но уже прочно вошли в наше сознание как информация, защита которой во многом зависит от наших действий. Согласно Федеральному закону «О персональных данных» от 8 июля 2006 года персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Действие данного закона распространяется на отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с задан-

ным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

При этом Федеральный закон «О персональных данных» не распространяется на отношения, возникающие при: «1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных; 2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации; 3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну; 4) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации».

Таким образом, закон разграничивает режим государственной тайны и персональных данных. Между тем соотношение данных категорий в ряде случаев вызывает ряд проблем. Органами государственной власти, где циркулирует наибольшее количество сведений, составляющих государственную тайну, являются силовые ведомства, в которых предусмотрена военная служба: Министерство обороны, Министерство внутренних дел, Федеральная служба безопасности, Федеральная служба охраны, Служба внешней разведки. Так, актуальным представляется выяснить, являются ли персональные данные военнослужащих данных ведомств государственной тайной и подпадают ли под действие Федерального закона «О персональных данных».

Государственной тайной, согласно Закону Российской Федерации «О государственной тайне» от 21 июля 1993 года № 5485-1, является: «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемых Законом. Данный перечень утвержден указом Президента Российской Федерации от 30 ноября 1995 года № 1203.

Согласно законодательству о государственной тайне часть персональных данных военнослужащих выходит из-под действия Федерального закона «О персональных данных». Данный перечень не охватывает весь объем данных, циркулирующих в области национальной безопасности, поскольку помимо сведений о сотрудниках внешней разведки и тех, кто борется с терроризмом, существуют и те военнослужащие, которые обеспечивают обороноспособность нашей страны в штабах и обычных гарнизонах. Например, формирование кадров Вооруженных Сил России начинается с призыва граждан на военную службу. При планировании, подготовке и проведении призыва на военную службу собирается большое количество персональных данных, которые хранятся в Министерстве обороны.

Следует обратиться к перечню лиц, способных относить информацию к государственной тайне. Данный перечень утвержден распоряжением Президента Российской Федерации от 16 апреля 2005 г. № 151-рп. Согласно данному перечню, руководители органов государственной власти, где предусмотрена военная служба, имеют право относить сведения к государственной тайне, но они не имеют право по своему желанию относить любые сведения к государственной тайне.

Одним из фактов, свидетельствующих о том, что персональные данные военнослужащих не являются государственной тайной, свидетельствует то, что летом 2011 года разгорелся скандал в связи с запросом следователями Следственного управления Следственного комитета Российской Федерации по Чеченской Республике сведений о военнослужащих, принимавших участие в контртеррористических операциях на территории Северного Кавказа. Тогда силовые ведомства отказали в предоставлении требуемой информации следователям. После того, как стало известно о данных запросах, лидер ЛДПР в середине июня направил официальное обращение министру обороны РФ Анатолию Сердюкову, в котором заявил о необходимости засекретить такого рода сведения.

Необходимо отметить, что согласно Федеральному закону «О службе в органах вну-

тренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30.11.2011 № 342-ФЗ для сотрудников внутренних дел в отличие от военнослужащих отдельно прописана защита их персональных данных, что означает дополнительное предоставление гарантий при защите их персональных данных:

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

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

Персональные данные же большинства военнослужащих подпадают под действие Федерального закона «О персональных данных» на общих основаниях с другими субъектами персональных данных, кроме тех, что указаны в Перечне сведений, отнесенных к государственной тайне. В случае дальнейшего изменения и дополнения Перечня сведений о государственной тайне персональная информация военнослужащих либо полностью выйдет из-под действия Федерального закона «О персональных данных», либо частично: сведения о военнослужащих, принимавших участие в горячих точках или служащих на режимных объектах, будут секретными (отнесение к государственной тайне этих сведений необходимо, поскольку рискующие своей жизнью военнослужащие должны быть уверены в защите и безопасности), а данные о тех, кто служит в «обычных» гарнизонах, будут просто персональными данными и будут охраняться в соответствующем режиме.

Захаров М., студент магистратуры кафедры конституционного и административного права ЮУрГУ. E-mail: zakharoff.m@mail.ru

Zakharov M., graduate student of Constitutional and Administrative Law of South Ural state University. E-mail: zakharoff.m@mail.ru

УДК 342.7 + 004.056
ББК Х400.323

Никольская К.

ЗНАЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В статье анализируется значение персональных данных в современном мире в условиях развития информационного общества. Исследуется система правового регулирования персональных данных. Анализируются основные нормативные правовые акты в сфере персональных данных.

Ключевые слова: *персональные данные, информационное общество, информационные технологии, законодательство.*

Nikolskaya K.

MEANING OF PERSONAL DATA IN THE CENTURY OF INFORMATION TECHNOLOGIES

The article analyses the meaning of personal data in modern world in conditions of information society development. It investigates the system of legal control of personal data. The work analyses the principle normative legal acts in the sphere of personal data.

Keywords: *personal data, information society, information technologies, legislation.*

XXI век характеризуется все большим наступлением информационных технологий на жизнь человечества. Все больше и больше различных «гаджетов» входит в нашу жизнь. Меняется все: от учебного процесса в школах и вузах до способов получения заработной платы. Параллельно с наступлением информационной эры в нашу жизнь стал входить термин «персональные данные».

Согласно Федеральному закону «О персональных данных» от 27.07.2006 № 152-ФЗ персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Согласно Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., персональными данными является информация, касающаяся конкретного или могущего быть идентифицированным лица («субъекта данных»).

История развития законодательства о защите персональных данных в мире насчитывает не одно десятилетие. Основным международным документом является Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS-108 (Страсбург, 28 января 1981 г.), которая была принята государствами-членами Совета Европы с целью обеспечения на территории каждой из сторон договора уважения прав и основных свобод каждого человека независимо от его гражданства или места жительства, и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой его персональных данных.

Российской Федерацией данная конвенция была ратифицирована только 19 декабря 2005 года Федеральным законом № 160-ФЗ. Именно с этого момента можно говорить о начале развития законодательства о защите персональных данных в России.

Основными документами, регулирующими отношения в сфере персональных данных на международном уровне, являются:

1. Директива Организации по экономическому сотрудничеству и развитию (ОЭСР) «О защите неприкосновенности частной жизни и международных обменов персональными данными» 1980 г.;

2. Директива 95/46/ЕС и № 2002/58/ЕС от 24 октября 1995 Европейского парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных;

3. Директива 97/66/ЕС от 15 декабря 1997 года по обработке персональных данных и защите конфиденциальности в телекоммуникационном секторе;

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

5. Трудовой кодекс Российской Федерации;

6. Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

7. Распоряжение Правительства Российской Федерации от 15 августа 2007 г. № 1055-р «Об утверждении Плана подготовки проектов нормативных правовых актов, необходимых для реализации Федерального закона «О персональных данных».

Также все больше вносится изменений в существующие нормативные акты, что показывает, насколько актуальными и важными становятся персональные данные. В связи с возрастающей важностью персональных данных они требуют все большей защиты: в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» организации, обрабатывающие персональные данные граждан Российской Федерации, обязаны обеспечить защиту этих данных до 01 января 2011 года. Контроль исполнения положений этих документов возложен на ФСТЭК России, ФСБ России и Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Также принимаются различные нормативные и методические документы для защиты персональных данных: «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», (утв. ФСБ РФ 21.02.2008 № 149/54-144), Приказ Роскосмоса от 05.12.2011 № 200 «О защите персональных данных федеральных государственных гражданских служащих Федерального космического агентства» и т. п. Данные документы все больше усиливают внимание на защите персональных данных, актуализируя вопрос их безопасности как обеспечение конституционных прав граждан.

Персональные данные все больше становятся важной частью нашей жизни и все больше требуют внимания. Несмотря на то что уже сейчас имеется достаточная нормативная база, она несовершенна и требует дальнейшего развития и где-то корректировки, так как наша страна относительно недавно стала на путь развития данной сферы. Также требуется развитие «особого» мировоззрения в нашей стране для того, чтобы повысить уровень ответственности и внимания граждан к обращению со своими персональными данными.

Никольская К., студент магистратуры кафедры конституционного и административного права ЮУрГУ. E-mail: zakharoff.m@mail.ru

Nikolskaya K., graduate student of Constitutional and Administrative Law Department of South Ural State University. E-mail: zakharoff.m@mail.ru

УДК 004.41.056.5 + 004.45.056.5 + 004.72.056.5
ББК Х401.114

Нагибин Д. В., Рабушко А. Г.

КОНЦЕПЦИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ КЛЮЧЕВОГО НОСИТЕЛЯ

Рассматривается проблема разработки универсального программного обеспечения на основе ключевого носителя, позволяющего защищать любое представление конфиденциальной информации на рабочих станциях пользователей, с возможностью централизованного и распределенного администрирования системы. Разграничиваются понятия «локальная и удаленная пользовательская информация», а также каналы передачи информации.

Ключевые слова: *автоматизированная система защиты конфиденциальной информации, ключевой носитель, разделяемость ключей, генерация исполняемых файлов.*

Nagibin D. V., Rabushko A. G.

A CONCEPT OF SYSTEM DESIGN INVOLVING PROTECTION OF CONFIDENTIAL DATA USING KEY CARRIER

In the paper we consider the development of universal software based on key token that allows protecting any confidential data on user workstations with the possibility of centralized and distributed administration of the system. We differentiate the notions of local and remote user data, and also that of data transmission channels.

Keywords: *automatic system of confidential data protection, token, key differentiation, executable file generation.*

Введение

Практически в любой организации остро встает вопрос защиты конфиденциальной информации (КИ), представляющей коммерческую или служебную тайну. Для приемлемой надежности сохранности информации каждой организации необходимо закупить или разработать, а также внедрить систему контроля обрабатываемых данных.

Последние помимо бумажного варианта могут быть представлены и в электронном виде: документом, интерпретируемым сторонними приложениями, программным комплексом с собственной базой данных или се-

тевым программным комплексом с удаленной базой данных (БД). Эти три случая требуют более детального рассмотрения.

В первом случае мы имеем право обмениваться документами между сотрудниками, подразумевая ситуацию, что программа-интерпретатор установлена на многих рабочих станциях. В этом случае объектом защиты становится сам документ, к которому необходимо применять универсальные методы защиты.

Во втором случае объектами защиты могут выступать как стационарная база данных, так и программа, обрабатывающая данные. Подход к защите такого взаимодействия должен состоять из криптографических методов и технологий сокрытия сведений в существующих базах данных без нарушения целостности структуры БД и работоспособности систем управления базами данных.

В третьем случае мы сталкиваемся с каналами передачи данных, которые представляют наиболее уязвимое место в системе защиты сведений. С этим вопросом напрямую связана проблема локальной защиты клиентского программного обеспечения.

Условия для реализации данного подхода защиты КИ

Главным условием описываемого в работе подхода является наличие ключевого носителя, в качестве которого может выступать любой flash-накопитель или же магнитный жесткий диск. Для включения его в процесс взаимодействия необходима инициализация на нем хранилища ключей для любого типа обрабатываемых данных. Действие по подготовке носителя сводится к тому, что на нем создается раздел фиксированного размера, данные о котором записываются в главную загрузочную запись, но при этом признак активности обнуляется, вследствие чего данный раздел становится невидим операционной системой, а также любыми средствами диагностики жестких дисков. Также для уже существующего раздела выделенное место становится зарезервированным, то есть неактивным. Узнать о наличии скрытого раздела можно только сравнив истинный размер диска без файловой системы с размером видимого раздела. Для уменьшения риска обнаружения секретного раздела на него отводится всего несколько мегабайт. В этом разделе будут храниться только части ключей и идентификаторы защищаемой информации (рис. 1).

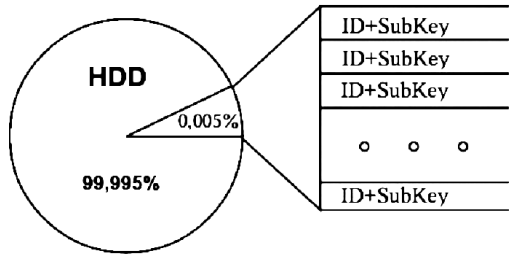

Рис. 1. Структура HDD

Для увеличения парольной энтропии, а также стойкости криптографических преобразований используются методы разделения паролей, где носителями выступают: пользователь либо администратор – носитель мастер-пароля, ключевой носитель и сам объект защиты, если это возможно (рис. 2).

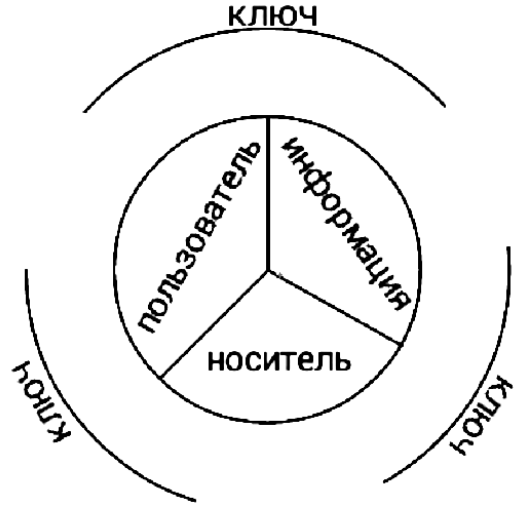

Рис. 2. Разделяемость ключей

Процедура взаимодействия

Рассмотрим более детально процедуру взаимодействия, способы и методы защиты для первого случая. Файл-документ, расположенный на любом носителе, проходит первичную подготовку статическими средствами созданного нами программного комплекса, в результате которой формируется исполняемый файл. Данный exe-файл – это шаблонный, универсальный код, который может применяться лишь в подобных ситуациях. В ресурсы данному файлу попадают: пользовательский документ и прикрывающая программа, которая может состоять из нескольких exe-файлов (рис. 3).

Все ресурсы шифруются уникальным ключом, разделенным между сформированным exe-файлом и ключевым носителем, при

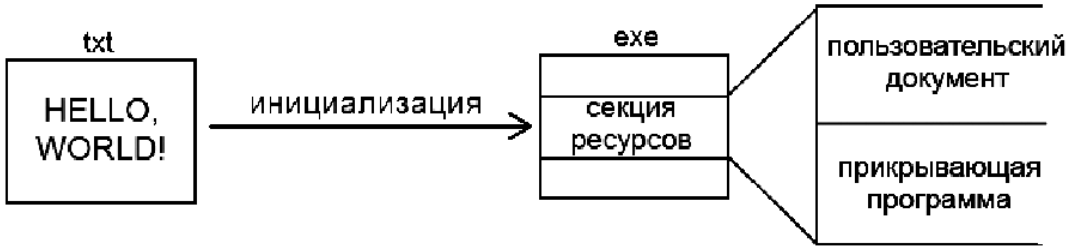

Рис. 3. Подготовка пользовательского документа

этом исходными данными для разделения ключей стало преобразование: ***hash(мастер-пароль) XOR rand()***, где мастер-пароль знает только пользователь либо администратор, а rand() – это случайным образом генерируемая последовательность на основе многих параметров с большой энтропией. Нужно заметить, что hash() и rand() не ограничиваются каким-либо количеством разрядов, потому что рассматривается лишь модель взаимодействия, идеальным вариантом будет создание в результате операции XOR 1024- или 2048-битной последовательности.

Описание взаимодействия программного обеспечения и сетевых программных комплексов

Для большего понимания возможностей данного подхода рассмотрим пример запуска конкретного зашифрованного документа. Пользователь запускает на выполнение сформированный exe-файл, алгоритмом работы которого является:

- поиск ключевых носителей, их идентификация (свой/чужой);
- поиск нужного ключа по известному идентификатору файла;
- сборка ключа;
- дешифрование ресурсов;
- запуск прикрывающей программы.

Исполняемый файл не обладает большой функциональностью, поэтому существует возможность применения максимального количества антиотладочных приемов на минимальном количестве кода для создания наиболее защищенного продукта. Прикрывающая программа обладает большей функциональностью, поэтому требует более серьезного и комплексного подхода к защите. Она имеет две стратегии работы: с автоматическим контролем файла и без контроля. Их выбирает и настраивает пользователь в процессе подготовки. При работе логики программы по первой стратегии должна проверяться ассоциация на файл, а если таковой не имеется, пользователь должен вручную выбрать программу-интерпретатор для документа. При запуске прикрывающей программы последняя создает файл на диске с именем и расширением как у пользовательского. Данными в этом документе будет любой произвольный «мусор», отданный файловой системой. По ассоциации на данный файл находится программа-интерпретатор и запускается с параметром – путь к новосозданному пользовательскому документу. Программа-обработчик начинает обращаться к файловой системе с целью получения порций данных документа, в это же время прикрывающая программа может поставить hooks на обращение к данному файлу или же установить «сквозной» драйвер-фильтр, как, например, делает программа FileMon от sysinternals. При этом алгоритм выбирается в соответствии с правами пользователя. Перехватив сообщение на чтение секторов, программа «на лету» дешифрует нужную порцию данных из вложенного ресурса и подменяет ответ операционной системы, тем самым постепенно заполняя загружаемый документ (рис. 4). Далее она получает разделяемый доступ к данному файлу, чтобы избежать дальнейшего изъятия или подмены данных в процессе работы программы-интерпретатора.

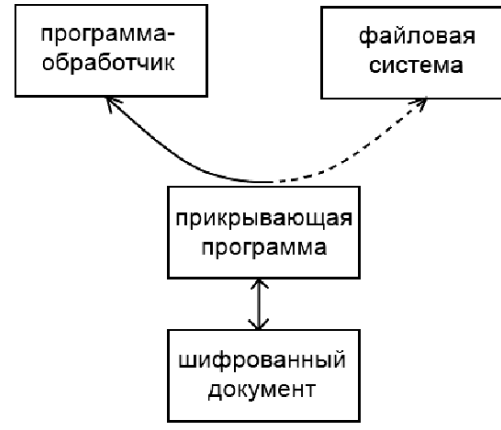

Рис. 4. Открытие пользовательского документа

На этом активная часть работы программы заканчивается и начинается пассивная, которая заключается в перехвате обращений к файловой системе на запись данного документа, автоматическое изменение вложенного ресурса и ожидании наступления одного из трех возможных событий: завершение программы-обработчика, успешное завершение диалоговых окон «Открыть» или «Сохранить», при этом возможны три различные исхода. Первый исход характеризуется отпусканием handle-процесса и передачей монопольного доступа к документу прикрывающей программе. Затем содержимое файла многократно перезаписывается и данный файл безвозвратно удаляется. Также прикрывающая программа со специальным модификатором вызывает заново сформированный исполняемый файл со следующим алгоритмом работы:

• нахождение прикрывающей программы по переданным данным;

• легальная деактивация прикрывающей программы;

• полное удаление прикрывающей программы с рабочей станции.

В результате мы получаем новый exe-файл и чистое рабочее место.

Второй исход получатся, когда пользователь нажимает кнопку «Ok» или «Открыть», при этом действия прикрывающей программы аналогичны первому случаю, за исключением того, что программа-обработчик остается открытой и далее снимаются все hooks. Результатом является неактивный сохраненный исполняемый файл. Третий исход комбинирует в себе два предыдущие подхода. После нажатия пользователем кнопки «Ok» или «Сохранить» прикрывающая программа определяет место, куда будет сохранен файл и перехватывает поток записи в файл, и также «на лету» шифрует его, помещая, на первом этапе, в оперативную память, далее создается шаблонный exe-файл и шифрованный документ помещается ему в ресурсы; на носитель записывается ключ к данному файлу и посылается команда закрытия программы-обработчика. При положительном исходе следующие действия прикрывающей программы аналогичны первому случаю, за исключением того, что при ее закрытии запускается процесс инициализации новосозданного исполняемого файла. В результате мы получаем зашифрованный неактивный старый exe-файл и новый активный исполняемый файл.

При работе по стратегии без контроля за файлом логика работы аналогична, но нас будет интересовать только первая обратившаяся к документу программа. Как только она закрывается, прикрывающая программа шифрует файл документа и помещает его обратно в ресурсы исходному exe-файлу. При таком подходе существует угроза первого обращения нелегальной программы, поэтому настоятельно рекомендуется использовать данный подход только в случае, когда программа-интерпретатор не имеет ассоциации и не способна на вход принимать файл в аргументах запуска.

Рассмотрим случай взаимодействия программного комплекса с системой управления базой данных (СУБД) с целью выполнения запросов на получение, добавление и удаление информации. Для защищенного получения данных в схеме такого взаимодействия (рис. 5) первоначальную подготовку проходит база данных, в которой шифруются все кортежи всех таблиц. В результате мы получаем полностью защищенное содержимое БД. Сегодня существует немного развитых систем управления базами данных, поэтому для разработчика не составит труда разобраться в механизмах взаимодействия СУБД с клиентским программным обеспечением. Центральная идея этого взаимодействия заключается

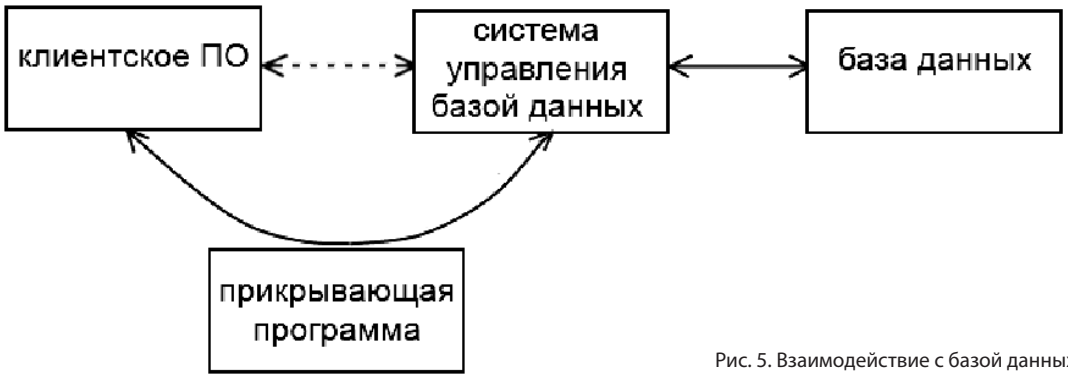

Рис. 5. Взаимодействие с базой данных

в том, что прикрывающая программа, перехватив запрос от клиентского ПО, обратится к СУБД и получит запрашиваемую информацию в зашифрованном виде. Далее произведет дешифрование и отправит программе-получателю, запросы на запись будут выполняться аналогично. В дальнейшем с очевидностью появится возможность шифровать наименования таблиц, столбцов и служебной информации. Использовать современные алгоритмы асимметричного шифрования не получится, т. к. существует спецификация о названиях таблиц, столбцов и т. д., поэтому для сокрытия этих данных будет необходимо использовать лишь алгоритмы «замены», причем алфавит подбирается под конкретную СУБД.

Чаще всего клиентское ПО представлено одним exe-файлом и набором dll-файлов. Для его защиты может применяться подход из первого случая:

• пользовательские exe- и dll-файлы шифруются и помещаются в ресурсы шаблонному исполняемому файлу;

• в процессе запуска эти файлы дешифруются и запускается только пользовательский exe-файл;

• прикрывающая программа ожидает закрытия приложения на его handle.

После завершения приложения все файлы удаляются с жесткого диска.

В результате получаем чистое рабочее место.

В случае взаимодействия пользовательского ПО с удаленной базой данных возникают две возможные ситуации:

• нет доступа к удаленному компьютеру;

• имеется доступ к программному обеспечению удаленного компьютера.

В первой ситуации нет возможности защитить сетевой обмен данными, а только лишь локальное клиентское ПО.

Во втором случае мы можем защитить как БД, так и сетевой обмен информацией. При этом необходимо понимать, что у сетевого программного комплекса будут пользователи как с установленным ПО для защиты канала связи, так и без него, поэтому перед установкой соединения какими-либо средствами необходимо определить группу подключающегося пользователя или, если это возможно, использовать два независимых канала общения. Рассмотрим вариант с созданием виртуального модема, имеющего функциональные возможности:

• определение группы пользователя;

• обзор политики безопасности и возможных разрешений на доступ к системе;

Рис. 6. Структура клиент-серверного взаимодействия

• работа с серверным ПО и клиентским ПО, пересылка данных.

Основным назначением данного виртуального модема является реализация следующих функций: шифрование вложений в TCP и UDP пакетов; распознавание принадлежности пакетов к данной системе; фильтрация отправляемых данных на предмет безопасности взаимодействия. Порты и IP-адрес сервера задаются в настройках виртуального модема на клиентской стороне, а на стороне сервера выстраивается политика безопасности, представленная: ACL, мандатным или дискреционным управлением доступом. В данной ситуации в роли прикрывающей программы выступает приложение, создающее виртуальный модем и поддерживающее стабильное сетевое соединение пользователей системы. Все остальные функциональные возможности остаются прежними и не требуют кардинальных изменений.

Канал передачи данных является таким же объектом защиты, как и документ пользователя, поэтому для его защиты могут применяться те же самые средства и методы. Для наилучшего функционирования системы разработчикам рекомендуется в код прикрывающей программы внести функции мониторинга за наличием установленного ключевого носителя путем отслеживания сообщений операционной системы об извлечении или установке USB устройств с дальнейшей проверкой подключенных устройств, т. к. основным условием должно быть – «один ключевой носитель – один человек – одно рабочее место». Если следовать данному правилу, то для одновременного открытия одного зашифрованного файла или работы с одним каналом будет актуальна возможность обмена ключами между пользователями, но и этот обмен должен быть защищен, т.к. рассматривается модель максимальной защищенности системы.

Для передачи доступа к пользовательскому ресурсу предлагается использовать следующий алгоритм:

1. Пользователь, желающий получить доступ к ресурсу, с помощью своего ПО генерирует запрос, в котором располагается открытый ключ общего алгоритма асимметричного шифрования, полученный операцией XOR из hash парольной фразы и функции rand, а закрытый ключ сразу помещается на ключевой носитель.

2. Запрос отправляется владельцу информации или ресурса по незащищенному каналу передачи информации.

3. Владелец, обрабатывая запрос, в режиме реального времени снимает свою защиту и шифрует пользовательский файл присланным ключом и формирует исполняемый файл, который может передаваться по незащищенному каналу без опасения за конфиденциальность информации.

Заключение

Описанный в работе подход позволяет использовать заложенные заводом-изготовителем функциональные возможности накопителя, а также наиболее безопасно использовать последний для хранения ключевой информации. Соблюдением всех вышеописанных методов и способов защиты мы охватываем очень большое количество клиентских приложений. При этом пользователь не испытает дискомфорта при работе с программой, т. к. подготовку документов может производить в том числе и администратор безопасности, а в пользовательском функционале кардинальных отличий от нормального взаимодействия не наблюдается.

Результатом данной работы стало создание прототипа программы, позволяющей реализовывать первый и второй подходы, описанные во введении.

Нагибин Дмитрий Владимирович, студент 5-го курса кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: 19asdek91@gmail.com

Рабушко Артур Германович, ст. преп. кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: artr@kgsu.ru

Nagibin Dmitry Vladimirovich, student of the last year of the Department «Safety information and automated systems» Kurgan State University. E-mail: 19asdek91@gmail.com

Rabushko Artur Germanovich, Sr. Lecturer of the Department «Safety information and automated systems» Kurgan State University. E-mail: artr@kgsu.ru

УДК 004.7 + 0049:519.654
ББК Ч86 + Х401.114

Бряков А. И., Везнер А. Н., Файзуллин Р. Т.

КРИТЕРИИ ВЫБОРА ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА ДЛЯ LSB-МЕТОДА

Статья посвящена определению классов изображений, в наибольшей степени подходящих для выполнения роли изображения-контейнера для передачи дополнительной информации без потери визуального качества. Определен полезный объем изображения-контейнера при различном количестве замен младших значащих битов изображения-контейнера.

Ключевые слова: *LSB-метод, метод наименьших квадратов, закон Вебера – Фехнера, BMP-формат, стеганография.*

Bryakov A. I., Faizullin R. T., Vezner A. N.

IMAGE SELECTION CRITERIA OF IMAGE-CONTAINER FOR LSB-METHOD

This article is about images that are most suited to perform the role of the image-container. See the most efficient transfer of information with help of the image-container without disturbing the volume, integrity, information content and visualization of the transmitted image. Determine the utility of the volume image container with various numbers of substitutions least significant bits of the image-container.

Keywords: *LSB-method, the method of least squares, the Weber-Fechner law, BMP-format steganography.*

Одним из практических применений компьютерной стеганографии [1,2,3] является создание дополнительного канала передачи информации с помощью LSB-метода.

Метод *LSB* (*Least Significant Bits*)[4] заключается в изменении младшего бита каждой цветовой составляющей изображения. Данный метод позволяет передать информацию в виде изображения, объем которого равен объему исходного изображения, но при этом оно будет нести в себе дополнительное изображение, которое будет информационно-емким.

От метода внедрения данных и от выбора контейнера зависит объем секретного сообщения, а также устойчивость стегоконтейне-

ра к различным видам анализа: визуального или статистического. Способов сокрытия данных много, однако проблема выбора подходящего контейнера до сих пор не решена.

Потеря качества изображений будет зависеть от степени сокрытия передаваемой информации. Чем ближе к оригиналу исходное изображение, тем больше теряет качество вложенное изображение, и наоборот. Одним из применений метода *LSB* является создание дополнительного канала для передачи информации и сокрытия факта передачи. Наиболее информационно-емким форматом является *bmp*-формат[5]. Данный метод позволяет увеличить информативность изображений, проходящих через один и тот же канал, при этом не нарушая объема данной информации.

Цель данной работы – определить, какие изображения в наибольшей степени подходят для выполнения роли изображения – контейнера, добиться наиболее эффективной передачи информации посредством изображения-контейнера, не нарушая объема, целостности, информативности и визуализации передаваемого изображения, определить полезный объем изображения-контейнера при различном количестве замен младших значащих битов изображения-контейнера.

Рассмотрим наиболее часто используемый формат изображений, а именно *BMP*-файл с глубиной цвета 24 бита на пиксель.

Для реализации метода *LSB* нами была составлена программа на языке *Pascal*. Применяя программу для замены разного количества младших битов изображения-контейнера старшими битами изображения скрываемого, можно получать «заполненные» изображения-контейнеры и «вытащенные из них» скрытые изображения различного качества.

Для примера рассмотрим два изображения.

Рис. 1. «Вставляемое» изображение

Рис. 2. Изображение-контейнер

Рис. 3. Изображение-контейнер с изображением, «вставленным» посредством замены 2-х младших значащих битов

Рис. 4. Передаваемое изображение в изображении-контейнере посредством замены 2-х младших значащих битов

Рис. 5. Изображение-контейнер с изображением, «вставленным» посредством замены 3-х младших значащих битов

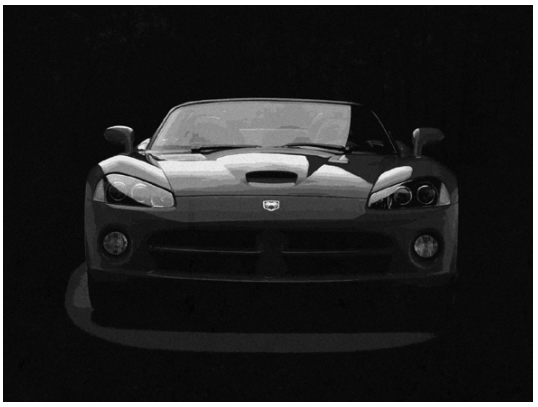

Рис. 6. Передаваемое изображение в изображении-контейнере посредством замены 3-х младших значащих битов

Для получения статистических данных о том, как люди воспринимают «заполненные» изображения-контейнеры, был проведён опрос.

Опрашиваемым было представлено 20 одинаковых по параметрам (формат, разрешение, размер, глубина цвета), но разных по визуальному содержанию изображений. Опрос состоял из двух частей. Первая часть включала в себя опрос из десяти изображений, пять из которых были изменены посредством замены их двух младших битов двумя старшими битами остальных пяти неизменных изображений. Ни одно изображение-контейнер и ни одно изображение-вставка не повторяются. Вторая часть опроса была аналогична первой, за исключением того, что замене подвергались три бита изображения-контейнера.

Опрашиваемым был поставлен вопрос: «Искажено ли изображение?». Время, данное для оценки изображения и ответа, не превышало пятнадцати секунд. В опросе приняли участие 62 человека, среди которых 30 женщин и 32 мужчины.

Результаты показаны на диаграммах рис. 7 и 8.

Заметим, что изображение «8» (рис. 7) было отмечено как искаженное большим количеством опрошенных, нежели остальные изображения. Данное изображение вызывает большее сомнение в его оригинальности, потому, что в нём присутствуют наложенные эффекты – дымка (туман). Поэтому не следует применять в качестве изображений-контейнеров изображения, на которых содержатся наложенные эффекты.

При сравнении диаграмм «на 2» и «на 3» заметно, что процент правильных ответов значительно больше при замене 3-х младших значащих битов, нежели 2-х.

Так как опрашиваемые должны дать

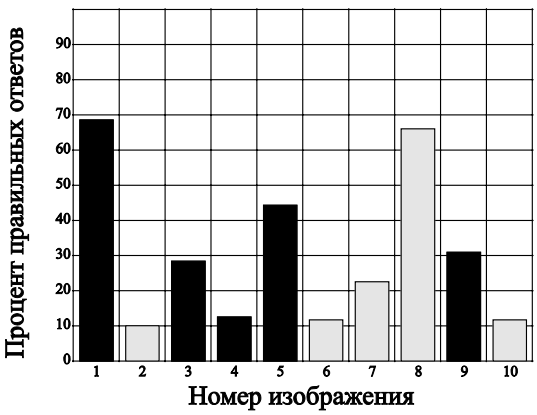

Рис. 7. Проценты ответов с пометкой «искажено» на опрос относительно изображений-контейнеров с заменой 2-х младших значащих битов (красным показаны искаженные изображения, синим – неискаженные).

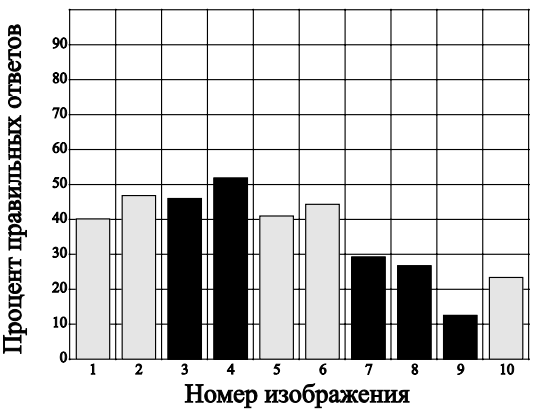

Рис. 8. Проценты ответов с пометкой «искажено» на опрос относительно изображений-контейнеров с заменой 3-х младших значащих битов (красным показаны искаженные изображения, синим – неискаженные).

оценку как искаженным, так и не искаженным изображениям, целесообразно учитывать правильность ответов не только относительно искаженных изображений, но и относительно неискаженных. Поэтому, введем «Коэффициент компетентности эксперта». Чем выше значение коэффициента компетентности эксперта, тем выше качество информации, полученной от опрошенного, то есть исключая ответы людей с низким коэффициентом компетентности эксперта, можно вести наиболее достоверную статистику.

Общий коэффициент компетентности эксперта, полученный при опросе в случае сокрытия изображения в 2-х младших значащих битах, равен -15,48 (отрицательный), что свидетельствует о том, что увидеть какие-либо визуальные искажения изображения-контейнера достаточно сложно. Коэффициент, полученный при опросе в случае сокрытия изображения в 3-х младших значащих битах, 8,39 (положительный), но мал, так как при полностью правильном ответе этот коэффициент был бы равен 100. Это говорит о том, что сокрытие в 2-х младших битах эффективнее, чем сокрытие в 3-х младших битах. Тем не менее, визуальная устойчивость изображений-контейнеров с заменой 3-х младших битов достаточно высока. Такие изображения пригодны для использования в качестве изображения-контейнера при соблюдении некоторых условий (выводы – пункты 2, 3).

Для уточнения результатов оценки статистических данных и выявления возможных закономерностей количество опрошенных людей было увеличено до 120 человек. На основе базы данных, составленной из ответов опрошенных, построены гистограммы, одна из которых представлена на рис. 9. На ней отражены статистические данные относительно 60 опрошенных в эксперименте с заменой 2-х значащих битов изображения.

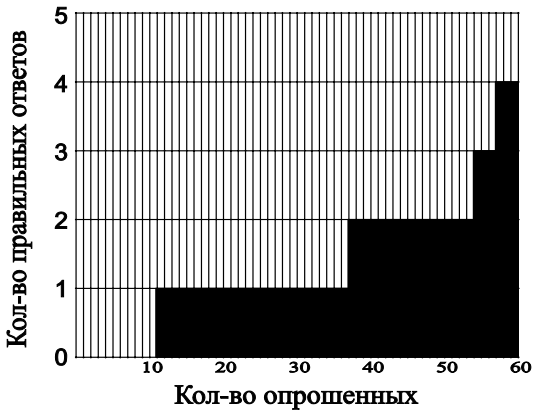

Рис. 9. Диаграмма, отражающая статистические данные относительно 60 опрошенных в эксперименте с заменой 2-х значащих битов изображения

Взяв срединные значения участков гистограмм, показывающих количество опрошенных, одинаково назвавших то или иное количество правильных ответов, рассчитаем ощущение восприятия по закону Вебера – Фехнера[6].

$$S = k * \log(I)$$

где S – ощущение восприятия, k – отношение Вебера для данного эксперимента (отношение количества замененных битов к общему количеству битов в байте), I – срединные значения участков гистограмм, показывающих количество опрошенных, одинаково назвавших то или иное количество правильных ответов.

Исходя из закона Вебера – Фехнера, можем получить зависимость ощущения восприятия от количества правильных ответов, график, которой показан на рис. 10 для двух заменяемых битов, и на рис. 11 для трех заменяемых битов. Судя по форме графика, мы можем сказать, что эта зависимость является логарифмической.

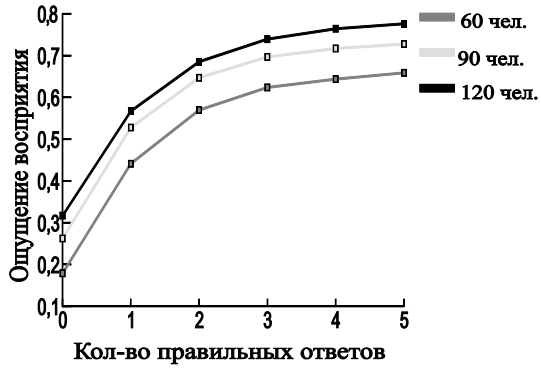

Рис. 10. График зависимости ощущения восприятия от количества правильных ответов на 2 заменяемых бита

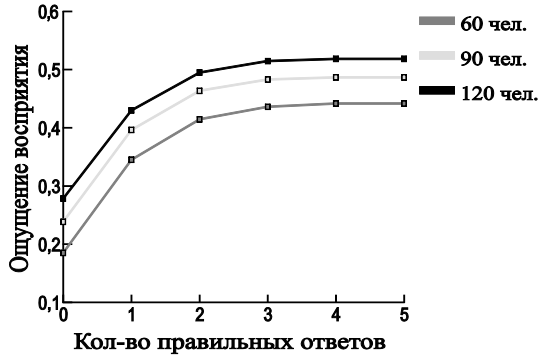

Рис. 11. График зависимости ощущения восприятия от количества правильных ответов на 3 заменяемых бита

Все три графика зависимости при 60, 90 и 120 человек схожи. Отличаются лишь величиной смещения. Обозначим эту величину буквой *A*. Построим график зависимости значений 1/*A* от количества опрошенных. По методу наименьших квадратов[7] рассчитаем асимптоту полученного графика. При двух заменяемых битах она будет иметь значение 1,8036, при трех – 0,6208. Мы выбрали асимптотическую зависимость и получили гиперболу, что свидетельствует о том, что при увеличении количества опрошенных график будет стремиться к асимптоте. Это доказывает достаточность количества опрошенных.

В процентном соотношении количество людей, давших пять правильных ответов (максимум), мало, и поэтому этой категорией людей можно пренебречь. Для эксперимента с заменой двух младших битов этот процент равен 0, так как максимальное количество правильных ответов составило 4, а для трех заменяемых битов это соотношение составило 5%.

Рассмотрим статистические данные отдельно мужчин и женщин. У мужчин коэффициенты компетентности эксперта приблизительно в два раза выше, чем у женщин, это позволяет сказать, что мужчины более компетентны в оценке изображений на наличие искажений.

Заключение:

1. С точки зрения незаметности проведённых манипуляций над изображениями, сокрытие старших битов изображений-вставок в двух младших битах изображений-контейнеров эффективней, чем сокрытие старших битов изображений-вставок в трех младших битах изображений-контейнеров, в 1,49 раза.

2. Для наиболее успешного сокрытия изображения (для того, чтобы сложнее было обнаружить искажение изображения-оригинала) следует применять изображения-носители, на которых изображены естественные природные пейзажи и животные, изображения эти должны быть в оранжево-коричневой гамме и быть достаточно пестрыми, с обилием естественных теней и мелких деталей.

Также подходящими изображениями-носителями являются изображения, близкие к чёрно-белой цветовой гамме.

3. Следует избегать применения в качестве изображений-носителей монотонных изображений (так как на них наиболее заметны «размытия», возникающие из-за вставки «скрываемых» изображений) и изображений с искусственно наложенными эффектами (дымка, размытие, нечёткости), так как они вызывают большее подозрение среди опрашиваемых людей, нежели естественные резкие изображения.

4. Такую технологию сокрытия информации можно использовать в потоковом видео для расширения канала передачи информации без видимого дефекта качества для большинства людей. Тем самым можно использовать в качестве инструмента для сжатия информации без потерь информативности.

Примечания

[1] Chandramouli R. A mathematical framework for active steganalysis / R. Chandramouli // ACM Multimedia Systems. – 2003. – Vol. 9, No. 3. – P. 303–311.

[2] Fridrich J., Goljan M., Du R. Detecting LSB Steganography in color andgrayscale images // IEEE Multimedia 8(4), 2001. – P. 22–28.

[3] Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006. — 288 с.

[4] Fridrich J., Goljan M., Du R. Detecting LSB Steganography in color andgrayscale images // IEEE Multimedia 8(4), 2001. – P. 22–28.

[5] Микрюков В. Ю. Компьютерная графика. – Ростов н/Д: «Феникс», 2006. – 240 с.

[6] Чукова Ю .П. Закон Вебера – Фехнера. – М.:«МП Гигиена», 2009. – 144 с.

[7] Линник Ю. В. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений – М.: «Наука», 1958. – 336 с.

Бряков Антон Игоревич, студент, Омский государственный технический университет. E-mail: extremal24@mail.ru

Везнер Алексей Николаевич, студент, Омский государственный технический университет. E-mail: Vezner_Alexey@mail.ru

Файзуллин Рашит Тагирович, доктор технических наук, профессор, заведующий кафедрой «Комплексная защита информации», Омский государственный технический университет. E-mail: r.t.faizullin@mail.ru

Bryakov Anton Igorevich, Omsk State Technical University, a student. E-mail extremal24@mail.ru

Vezner Alexey Nikolaevich, Omsk State Technical University, a student. E-mail: Vezner_Alexey@mail.ru

Faizullin Rashit Tagirovich, head of Integrated Information Protection Department, Omsk State Technical University, doctor of engineering science, professor.E-mail: r.t.faizullin@mail.ru

РЕГИОНАЛЬНЫЙ АТТЕСТАЦИОННЫЙ ЦЕНТР ЮУрГУ

«Региональный аттестационный центр» создан на основании решения Ученого совета Южно-Уральского государственного университета от 25.06.2007 г. № 10 по согласованию с Управлением ФСБ России по Челябинской области. Основными функциями «Регионального аттестационного центра» являются:

1) всестороннее обследование предприятий-заявителей на предмет их готовности к выполнению работ, связанных с использованием сведений, составляющих государственную тайну;

2) осуществление мероприятий по оказанию услуг в данной области;

3) повышение квалификации сотрудников режимно-секретных подразделений.

Решением Межведомственной комиссии по защите государственной тайны № 95 от 06 апреля 2005 года Южно-Уральский государственный университет включен в перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну» (в зачет государственной аттестации).

Категория слушателей: руководители организаций, заместители руководителей организаций, ответственные за защиту сведений, составляющих государственную тайну.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации, которое дает право руководителям предприятий, учреждений, организаций на освобождение от государственной аттестации.

Форма обучения – очно-заочная (48 часов заочная, 24 часа – очная форма обучения).

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске, учебным пособием курса лекций.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну».

Категория слушателей: руководители и сотрудники структурных подразделений по защите государственной тайны.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации.

Форма обучения – очная (72 часа). Обучение слушателей осуществляется с отрывом от производства – 2 недели.

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске.

Программа предусматривает изучение следующих дисциплин:

1) Правовое и нормативное обеспечение защиты государственной тайны;

2) Организация комплексной защиты информации в организациях;

3) Организация режима секретности в организации;

4) Организация защиты информации, обрабатываемой средствами вычислительной техники;

5) Организация защиты информации при осуществлении международного сотрудничества;

6) Допуск граждан к сведениям, составляющим государственную тайну;

7) Организация и ведение секретного делопроизводства;

8) Ответственность за нарушение законодательства РФ по защите государственной тайны. Порядок проведения служебного расследования по нарушениям.

«Региональный аттестационный центр» на договорной основе предоставляет предприятиям, учреждениям и организациям услуги в сфере защиты государственной тайны:

• оказание методической и консультационной помощи работникам режимно-секретных подразделений предприятий и организаций;

• специальное обслуживание предприятий, не имеющих в своей структуре режимно-секретных подразделений:

1) ведение допускной работы в соответствии с требованиями «Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне», утвержденной постановлением Правительства РФ от 06 февраля 2010 г. № 63;

2) выделение для проведения секретных работ помещений, соответствующих требованиям Инструкции по обеспечению режима секретности в Российской Федерации, утвержденной постановлением Правительства РФ от 05.01.2004 № 3-1 (далее – Инструкция № 3-1-04 г.);

3) выделение для хранения секретных документов помещений, соответствующих требованиям Инструкции № 3-1-04 г.;

4) организация и ведение секретного делопроизводства в соответствии с общими нормативными требованиями Инструкции № 3-1-04 г.;

5) обеспечение защиты государственной тайны при обработке и хранении секретной информации на средствах вычислительной техники и (или) в автоматизированных системах;

6) подготовка Заключения о фактической осведомленности работников в сведениях, составляющих государственную тайну;

7) разработка нормативно-методической документации по вопросам защиты государственной тайны;

8) профессиональная подготовка и обучение работников Заказчика, допущенных к работам с носителями секретной информации;

9) осуществление мероприятий по подготовке к проведению специальной экспертизы Заказчика на предмет получения и продления лицензии на право работ с использованием сведений, составляющих государственную тайну, а также к проведению государственной аттестации его руководителя, ответственного за защиту сведений, составляющих государственную тайну.

Контактные адреса и телефоны:

Юридический адрес: 454080, г. Челябинск, пр. им. В. И. Ленина, д. 76
Фактический адрес: г. Челябинск, пр. им. В. И. Ленина, д. 85, ауд. 512/3
Телефоны: (351) 267-91-55, 267-93-14, 267-92-85
E-mail: rac512@mail.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ «ВЕСТНИК УрФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ».

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцом оформления рукописи, а также приложить к статье сведения о себе (см. Сведения об авторе).

Сведения об авторе

ФИО (полностью)	
Ученая степень	
Ученое звание	
Должность и место работы (полностью)	
Домашний адрес	
Контактные телефоны	
e-mail	
Тема статьи	
Являетесь ли аспирантом (если да, то указать дату приема в аспирантуру и научного руководителя)	

Структура статьи (суммарный объем статьи – не более 40 000 знаков):

1. УДК, ББК, название (не более 12–15 слов), список авторов.
2. Аннотация (не более 500 знаков, включая пробелы), список ключевых слов.
3. Основной текст работы.
4. Примечания

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, аннотация на русском языке объемом до 50 слов, ниже отдельной строкой — ключевые слова. Инициалы и фамилия автора (авторов), название статьи, аннотация и ключевые слова должны быть переведены на английский язык.

В случае непрямого цитирования источников и литературы в начале соответствующего примечания указывается «См.:».

Цитируемая литература дается не в виде подстрочных примечаний, а общим списком в конце статьи с указанием в тексте статьи ссылки порядковой надстрочной цифрой (Формат — Шрифт — Надстрочный) (например, [1]). Запятая, точка с запятой, двоеточие и точка ставятся после знака сноски, чтобы показать, что сноска относится к слову или группе слов, например: по иску собственника[1]. Вопросительный, восклицательный знак, многоточие и кавычки ставятся перед знаком сноски, чтобы показать, что сноска относится ко всему предложению, например: …все эти положения закреплены в Федеральном законе «О ветеранах»[1].

Литература дается в порядке упоминания в статье.

При подготовке рукописи автору рекомендуется использовать ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (Полный текст ГОСТ Р размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии).

В конце статьи должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок.

Обязательно для заполнения: В конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — ученая степень, ученое звание, должность, кафедра, вуз; рабочий адрес, электронный адрес и контактные телефоны.

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Информационная безопасность.

Порядок прохождения рукописи

1. Все поступившие работы регистрируются, авторам сообщается ориентировочный срок выхода журнала, в макет которого помещена работа.

2. Поступившая работа проверяется на соответствие всем формальным требованиям и при отсутствии замечаний, в случае необходимости, направляется на дополнительную экспертизу.

3. Для публикации работы необходима положительная рецензия специалиста из данной или смежной области. На основании рецензии принимается решение об опубликовании статьи (рецензия без замечаний) или о возврате автору на доработку, в этом случае рукопись может проходить экспертизу повторно. При получении второй отрицательной рецензии на работу редакция принимает решение об отказе в публикации.

Материалы к публикации отправлять по адресу
E-mail: urvest@mail.ru в редакцию журнала «Проблемы права».

Или по почте по адресу:
Россия, 454091, г. Челябинск, ул. Васенко, д. 63, оф. 401.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(4)/2012

Подписано в печать 07.09.2012. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 6,30. Тираж 300 экз. Заказ
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.