ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3–4(5–6) / 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**

В НОМЕРЕ

ПРАВОВОЙ АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРАКТИЧЕСКИЙ АСПЕКТ

LEGAL ASPECT OF INFORMATION SECURITY

PROTECTION OF PERSONAL DATA

INFORMATION ENGINEERING PROTECTION

THE PRACTICAL ASPECT

УДК 343.98 + 004.056
ББК Х401.114 + Х401.02

Майоров В. И., Якупов В. Р.

ИНСАЙДЕРСКАЯ ИНФОРМАЦИЯ: ОПРЕДЕЛЕНИЕ ПОНЯТИЯ

В статье произведен анализ легальной дефиниции понятия «инсайдерская информация», обозначены недостатки данной законодательной конструкции и представлена авторская позиция по определению категории «инсайдерская информация».

Ключевые слова: *инсайдерская информация, признаки инсайдерской информации, достоверная информация, тайная информация, распространение информации, определение понятия «инсайдерская информация».*

Mayiorov V. I., Yakupov V. R.

INSIDER INFORMATION: DETERMINATION OF THE CONCEPT

The article analyzed the legal definition of the concept of "inside informa-tion", identified shortcomings of the legal structure and represented the author's position about the definition of the category of "inside information".

Keywords: *insider information, the signs of insider information, reliable information, secret information, dissemination of information, the definition of "insider information".*

Инсайдерская информация – новый для российского законодательства вид информации, мало исследованный в отечественной юридической науке[1], необходимость появления которого в рамках отечественной правовой материи была обусловлена стремлением законодателя повысить эффективность государственного противодействия одному из проявлений недобросовестной конкуренции на организованном рынке – инсайдерской торговле (неправомерному использованию инсайдерской информации). В этих целях в июле 2010 года был принят Федеральный закон «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»[2] (далее по тексту – ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком»), а ст. 15.21 Кодекса Российской Федерации об административных правонарушениях[3] (далее по тексту – КоАП РФ), ранее устанавливавшая административную ответственность за использование служебной информации на рынке ценных бумаг, была изложена в новой редакции (ст. 15.21 КоАП РФ «Неправомерное использование инсайдерской информации»).

Итак, категория «инсайдерская информация» относится сегодня к числу легальных. Определение категории «инсайдерская информация» закреплено в п. 1 ст. 2 ФЗ «О противодействии неправомерному использова-

нию инсайдерской информации и манипулированию рынком», где указано, что «инсайдерская информация – точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг (далее – эмитент), одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (далее – управляющая компания), одного или нескольких хозяйствующих субъектов, указанных в п. 2 ст. 4 настоящего Федерального закона, либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров) и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, указанный в статье 3 настоящего Федерального закона».

Для целей настоящего исследования данную весьма громоздкую законодательную конструкцию следует существенно сократить. Если не акцентировать внимание на нюансах и выделить в определении наиболее существенные моменты, современная дефиниция понятия «инсайдерская информация» примет следующий вид: это точная и конкретная информация, которая не была распространена или предоставлена, распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров и которая в соответствии с действующим законодательством относится к информации, включенной в соответствующий перечень инсайдерской информации.

Такой сокращенный вариант определения представляется более удачным в целях выявления признаков инсайдерской информации, что абсолютно необходимо для осуществления качественного анализа рассматриваемого понятия. Всего можно выделить четыре признака инсайдерской информации: 1) это информация точная и конкретная; 2) это информация, которая не была распространена или предоставлена; 3) это информация, способная оказать существенное влияние на цены финансовых инструментов, иностранной валюты, товаров; 4) это информация, которая относится к сведениям, составляющим законодательно определенный перечень инсайдерской информации. Охарактеризуем каждый из этих признаков.

Инсайдерская информация – это точная и конкретная информация. Данный признак законодателем не раскрывается, поэтому для его пояснения считаем целесообразным обратиться к толковым словарям, что позволит определить значение категорий «точный» и «конкретный».

Точный: 1) показывающий, передающий что-нибудь в полном соответствии с действительностью, с образцом, совершенно верный[4]; 2) истинный, действительный, такой, как на самом деле; отражающий, воспроизводящий или постигающий что-нибудь в полном соответствии с действительностью, всецело совпадающий с образцом, совершенно верный[5]; 3) верный, безошибочный[6].

Конкретный: 1) реально существующий, вполне точный и вещественно определенный, в отличие от абстрактного, отвлеченного[7]; 2) воспринимаемый чувствами, реальный, определенный; противоположно абстрактный, общий, отвлеченный[8]; 3) реально существующий, предметно определенный, четко обозначенный (противоположно: абстрактный, отвлеченный)[9].

Соответственно, под точной информацией следует понимать информацию верную, безошибочную, подлинную, действительную, истинную (есть более подходящая категория, характеризующая указанные качества информации, – достоверность), а конкретную информацию можно охарактеризовать как определенную, отчетливую, однозначную, четко обозначенную информацию.

Относительно рассматриваемого признака инсайдерской информации в юридической доктрине нет однозначной позиции. Так, В. А. Федоров указывает, что «российские законодатели, стремясь сделать определение более четким, упускают серьезный момент: на фондовом рынке не всегда нужна точная и конкретная информация, так как порой достаточно намека»[10]. Схожую позицию занимает И. А. Клепицкий, отмечая, что «требование к “точности” информации представляется чрезмерным: инсайдерская информация может быть и не вполне точной»[11]. Обе этих позиции заслуживают внимания.

Инсайдерская информация всегда достоверна (или, выражаясь терминологией законодателя, точна), но не во всех случаях она является (и должна являться) конкретной. Совершенно очевидно, что вопрос о достоверности инсайдерской информации может возникнуть только в процессе передачи ее от инсайдера (обладателя инсайдерской информации) третьим лицам. В рамках инсайдерской торговли передаваться может только достоверная информация, ибо распространение заведомо ложных сведений будет квалифицироваться как: 1) манипулирование рынком (п. 1 ч. 1 ст. 5 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком»); 2) недобросовестная конкуренция (ст. 14.33 КоАП РФ, п. 1 ч. 1 ст. 14 ФЗ «О защите конкуренции»[12]); 3) мошенничество (при определенных обстоятельствах). Соответственно, инсайдерская информация характеризуется признаком достоверности. Однако ввиду своей очевидности и отсутствия особой концептуальной значимости этот признак в определении можно отдельно не выделять.

В целях достижения незаконного экономического преимущества не всегда требуется обретения конкретной (полной, точной, исчерпывающей) информации; порой участникам рынка для совершения выгодных для себя операций достаточно получить от инсайдера приблизительные сведения (или, как указал В. А. Федоров, – намеки), ограничиться лишь его рекомендациями, советами и указаниями. Указание в законодательном определении на конкретный характер инсайдерской информации является ошибкой, ибо наличие этого признака неоправданно и чрезмерно сильно ограничивает рассматриваемое понятие. В связи с последними замечаниями предлагаем внести в п. 1 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» изменения, исключив из него слова «точная и конкретная».

Инсайдерская информация – это информация, которая не была распространена или предоставлена. Для характеристики данного признака требуется определить понятия «распространение инсайдерской информации» и «предоставление инсайдерской информации».

Распространение инсайдерской информации. К распространению инсайдерской информации относятся действия: 1) направленные на получение информации неопределенным кругом лиц или на передачу информации неопределенному кругу лиц, в том числе путем ее раскрытия в соответствии с законодательством Российской Федерации о ценных бумагах; 2) связанные с опубликованием информации в средствах массовой информации, в том числе в электронных, информационно-телекоммуникационных сетях, доступ к которым не ограничен определенным кругом лиц (включая сеть Интернет); 3) связанные с распространением информации через электронные, информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц (включая сеть Интернет) (подпункты «а», «б», «в» п. 5 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком»).

Получается, распространение инсайдерской информации возможно в том числе и посредством ее раскрытия. П. 1 ст. 30 ФЗ «О рынке ценных бумаг»[13] поясняет, что под раскрытием информации на рынке ценных бумаг понимается обеспечение ее доступности всем заинтересованным в этом лицам независимо от целей получения данной информации в соответствии с процедурой, гарантирующей ее нахождение и получение. Раскрытой информацией признается информация, в отношении которой проведены действия по ее раскрытию.

Предоставление инсайдерской информации. Определение категории «предоставление инсайдерской информации» содержится в п. 4 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком», в соответствии с которым предоставление инсайдерской информации – это действия, направленные на получение информации определенным кругом лиц в соответствии с законодательством Российской Федерации о ценных бумагах. Процедура предоставления информации на рынке ценных бумаг определена федеральным законом «О рынке ценных бумаг» и рядом подзаконных нормативных правовых актов (а именно, соответствующими постановлениями ФСФР России[14]).

Итак, и распространение инсайдерской информации, и предоставление инсайдерской информации суть осуществляемый инсайдерами (владельцами инсайдерской информации) комплекс действий, направлен-

ный на передачу инсайдерской информации третьим лицам. Единственное, при распространении инсайдерской информации она передается неограниченному кругу лиц, а при предоставлении инсайдерской информации – строго определенному, конкретному кругу субъектов. До того момента, пока информация не была распространена или предоставлена, она согласно п. 1 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» считается инсайдерской информацией. Исходя из этого, можно заключить, что инсайдерская информация – это информация, которая не является общеизвестной, информация, к которой не обеспечен общий доступ, тайная информация.

Отсутствие общего доступа к экономически значимой информации порождает существенное информационное неравенство, дает располагающим этой информацией субъектам значительное конкурентное преимущество перед всеми прочими неосведомленными участниками рынка, что открывает широкие возможности для злоупотреблений. Во избежание этого законодатель наделил важные для рынка сведения, которые не являются общедоступными, статусом инсайдерской информации и запретил субъектам организованного рынка использовать ее в своей деятельности.

В свете последних пояснений актуализируется вопрос, по какой причине законодатель связал момент прекращения статуса инсайдерской информации с актом ее предоставления третьим лицам. Механизм предоставления инсайдерской информации обеспечивает передачу информации лишь ограниченному кругу субъектов. Соответственно, предоставленная инсайдерская информация не становится общедоступной, она не перестает быть тайной для всех неосведомленных остальных. Лишь распространение информации обеспечивает общий доступ к ней. Только после того, как инсайдерская информация была опубликована и стала общедоступной, исключается возможность инсайдерской торговли. В связи с этим считаем необходимым внести в пункт 1 статьи 2 федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» изменения, исключив из него слова «или предоставлена».

Более того, в законодательном определении инсайдерской информации сделано уточнение, что к последней может быть отнесена любая охраняемая законом тайна, в том числе коммерческая, служебная, банковская тайна, тайна связи (в части информации о почтовых переводах денежных средств). Однако постановка знака равенства между инсайдерской информацией и различными видами охраняемой законом тайны не совсем корректна. Дело в том, что коммерческая, служебная, банковская и прочие виды охраняемой законом тайны являются информацией секретной, скрытой, конфиденциальной, не подлежащей распространению, опубликованию. Выше было указано, что инсайдерская информация – это также тайная информация. Но есть одна очень важная особенность: сведения, составляющие инсайдерскую информацию, подлежат обязательному распространению (предоставлению). То есть инсайдерская информация – это не тайна в полном смысле этого слова, ибо режим конфиденциальности данной информации носит временный характер и сохраняется лишь до момента ее распространения.

Иными словами, инсайдерская информация – это тайна, подлежащая обязательному раскрытию. В данном случае акцент делается не на том, что инсайдерские сведения составляют тайну, секретную информацию, охраняемую законом, а на том, что до тех пор, пока эти сведения не будут раскрыты (то есть перестанут быть тайными), участники организованного рынка не вправе использовать их в своих личных целях при осуществлении операций с финансовыми инструментами (иностранной валютой, товарами). Указанное ни в коей мере не характерно для коммерческой, банковской, служебной (иных видов охраняемых законом) тайны. По этому поводу А. С. Погосова сделала абсолютно справедливое замечание, что режим инсайдерской информации не тождественен совокупности различных видов тайны и потому не вписывается в рамки классического понимания тайны, а сами инсайдерские сведения являются самостоятельным объектом правового регулирования[15].

Правомерно вести речь лишь о наличии связи между инсайдерской информацией и различными видами охраняемой законом тайны, даже о возможности перехода сведений из категории охраняемой законом тайны в категорию инсайдерской информации, но указывать на тождество рассматриваемых са-

мостоятельных правовых явлений неверно. Поэтому мы предлагаем в п. 1 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» внести изменения, исключив из нее следующие слова: «(в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну)».

Инсайдерская информация – это информация, способная оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров. Этот признак означает, что инсайдерская информация – это значимая для рынка информация, и к ней могут относиться лишь такие сведения, которые после их опубликования непосредственно воздействуют на процесс ценообразования на организованных рынках, существенно отклоняя цену на финансовые инструменты, иностранную валюту, товары от текущей рыночной цены. Критерии существенности отклонения цены на организованных рынках определяются методическими рекомендациями ФСФР[16].

Инсайдерская информация – это информация, которая относится к сведениям, составляющим законодательно определенный перечень инсайдерской информации. Список сведений, составляющих инсайдерскую информацию, для ряда субъектов определен в федеральном законе «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» (п. 2 ст. 3). Для остальных субъектов перечни сведений, относящиеся к инсайдерской информации, определены в приказе ФСФР России[17]. Следует также отметить, что в ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» (п. 5 ст. 3) прямо оговариваются категории сведений, не относящихся к инсайдерской информации: 1) сведения, ставшие доступными неограниченному кругу лиц, в том числе в результате их распространения; 2) осуществленные на основе общедоступной информации исследования, прогнозы и оценки в отношении финансовых инструментов, иностранной валюты и (или) товаров, а также рекомендации и (или) предложения об осуществлении операций с финансовыми инструментами, иностранной валютой и (или) товарами.

В юридической литературе сложилось неоднозначное отношение к рассматриваемому признаку инсайдерской информации. С одной стороны, законодательное установление исчерпывающего списка инсайдерской информации позволяет достичь четкости и однозначности в правовом регулировании, минимизировать вероятность произвольного толкования правоприменительными органами положений российского законодательства по этому вопросу, а значит, устранить возможность различных злоупотреблений. Во многом исходя из этих соображений еще до принятия федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» и введения законодательного перечня инсайдерской информации, в науке высказывались позиции о необходимости определения легального исчерпывающего списка сведений, относящихся к инсайдерской информации[18].

С другой стороны, сведение законодателем всего многообразия инсайдерской информации к ограниченному, конечному перечню сведений – не совсем оправданный шаг. Инсайдерская информация – это не являющаяся общедоступной информация, которая в случае своего распространения способна оказать значительное влияние на цены финансовых инструментов, иностранной валюты, товаров. Таких сведений, которые могут существенным образом воздействовать на процесс ценообразования на организованных рынках, бесчисленное множество. Информация, которую непосредственно учитывают рынки, чрезвычайно обширна, разнообразна и крайне изменчива, ибо зависит от сиюминутных потребностей рынка. В полной мере оправданной является позиция И. А. Клепицкого: «Подобный формально-бюрократический подход к определению инсайдерской информации в принципе исключает возможность эффективного применения рассматриваемого Закона. … Составить исчерпывающий перечень сведений, составляющих инсайдерскую информацию, невозможно. … Имеет место ошибка законодательной техники – казуистичность, влекущая пробельность закона»[19].

На основании вышеизложенного полагаем, что признак ограниченности сведений, составляющих инсайдерскую информацию, концептуально неверен. В связи с этим считаем необходимым внести изменения в п. 1 ст. 2

ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком», убрав из определения инсайдерской информации слова «(в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг (далее – эмитент), одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (далее – управляющая компания), одного или нескольких хозяйствующих субъектов, указанных в пункте 2 статьи 4 настоящего федерального закона, либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров) и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, указанный в статье 3 настоящего Федерального закона». Что касается самого перечня инсайдерской информации, то его следует оставить, сделав его при этом открытым.

Итак, нами было рассмотрено законодательное определение понятия «инсайдерская информация». Критический анализ данной правовой дефиниции позволяет заключить, что законодатель, стремясь дать максимально точное, исчерпывающее определение, создал очень громоздкую, перегруженную деталями и наполненную лишними характеристиками правовую конструкцию. Определение инсайдерской информации можно существенным образом сократить как в объеме, так и в содержательном плане (устранив из него лишние признаки). Для этого следует ч. 1 ст. 2 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» изложить в следующей редакции: «инсайдерская информация – недоступная для неограниченного круга лиц информация, распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров».

Примечания

[1] См.: Минбалеев, А. В. Понятие и признаки инсайдерской информации как особого вида информации ограниченного доступа // Вестник УрФО. Безопасность в информационной сфере. – 2011. – № 1. – С. 18–21.

[2] Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. – 2010. – № 31. – Ст. 4193.

[3] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

[4] Толковый словарь Ожегова онлайн. Точный: http://slovarozhegova.ru/word.php?wordid=32073 (дата обращения 20.11.2012).

[5] Толковый словарь Ушакова онлайн. Точный: http://ushakovdictionary.ru/word.php?wordid=77567 (дата обращения 20.11.2012).

[6] Толковый словарь Ефремовой On-Line. Значение слова «точный»: http://www.efremova.info/word/tochnyj.html (дата обращения 20.11.2012).

[7] Толковый словарь Ожегова онлайн. Конкретный: http://slovarozhegova.ru/word.php?wordid=11695 (дата обращения 20.11.2012).

[8] Толковый словарь Ушакова онлайн. Конкретный: http://ushakovdictionary.ru/word.php?wordid=24713 (дата обращения 20.11.2012).

[9] Толковый словарь Ефремовой On-Line. Значение слова «конкретный»: http://www.efremova.info/word/konkretnyj.html (дата обращения 20.11.2012).

[10] Федоров, В. А. Закон об инсайде: аналитический комментарий [Текст] / В. А. Федоров // Российское предпринимательство. – 2010. – № 11. – С. 90.

[11] Клепицкий, И. А. Инсайдерская информация и уголовный закон / И. А. Клепицкий // Закон. – № 9. – С. 76.

[12] Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3434.

[13] Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» // Собрание законодательства РФ. – № 17. – 1996. – Ст. 1918.

[14] К таковым, например, относятся приказ ФСФР России от 24.05.2012 № 12-32/пз-н «Об утверждении Положения о внутреннем контроле профессионального участника рынка ценных бумаг» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 24.12.2012. – № 52; приказ ФСФР России от 28.12.2011 № 11-68/пз-н «Об утверждении Порядка ведения реестра договоров, заключенных на условиях генерального соглашения (единого договора), предоставления информации, необходимой для ведения указанного реестра и информации из указанного реестра, а также представления реестра договоров, заключенных на условиях генерального соглашения (единого договора) в федеральный орган исполнительной власти по рынку ценных бумаг» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 15.10.2012. – № 42; приказ ФСФР России от 28.12.2010 № 10-78/пз-н «Об утверждении Положения о деятельности по организации торговли на рынке ценных бумаг» // Российская газета. – 2011, – 25 апр. – № 88.

[15] Погосова, А. С. Особенности правового режима инсайдерской информации на рынке ценных бумаг / А. С. Погосова // Современное право. – 2011. – № 1. (СПС «КонсультантПлюс»).

[16] Приказ ФСФР РФ от 08.11.2011 № 11-59/пз-н «Об утверждении Методических рекомендаций по установлению критериев существенного отклонения цены биржевых товаров» // Вестник ФСФР России. – 2011. – № 11; Приказ ФСФР РФ от 19.05.2011 № 11-21/пз-н «Об утверждении Методических рекомендаций по установлению критериев существенного отклонения цены ликвидных ценных бумаг» (в ред. от 07.07.2011) // Вестник ФСФР России. – 2011. – № 7; Приказ ФСФР РФ от 30.08.2011 № 11-38/пз-н «Об утверждении Методических рекомендаций по установлению критериев существенного отклонения цены низколиквидных ценных бумаг» // Вестник ФСФР России. – 2011. – № 10; Приказ ФСФР России от 24.01.2012 № 12-4/пз-н «Об утверждении Методических рекомендаций по установлению критериев существенного отклонения цены, спроса, предложения и объема торгов неликвидными ценными бумагами» // Вестник ФСФР России. – 2012. – № 4; Приказ ФСФР России от 12.07.2012 № 12-61/пз-н «Об утверждении Методических рекомендаций по установлению критериев существенного отклонения цены на иностранную валюту» // Вестник ФСФР России. – 2012. – № 8.

[17] Приказ ФСФР России от 12.05.2011 № 11-18/пз-н «Об утверждении Перечня информации, относящейся к инсайдерской информации лиц, указанных в пунктах 1–4, 11 и 12 статьи 4 Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», а также порядка и сроков раскрытия такой информации» // Российская газета. – 2011. – 05 авг. – № 171.

[18] Шевелев, Б. Страсти по инсайду / Б. Шевелев // Бухгалтерия и банки. – 2009. – № 10. – С. 37.

[19] Клепицкий, И. А. Указ. соч. – С. 76–77.

Майоров Владимир Иванович, доктор юридических наук, профессор, проректор по учебной работе Южно-Уральского государственного университета (национального исследовательского университета). E-mail: yakupov555@mail.ru

Mayiorov Vladimir Ivanovich, Doctor of Law, professor, vice rector of academic affairs in the South Ural State University (national research uni-versity). E-mail: yakupov555@mail.ru

Якупов Валерий Рамильевич, аспирант кафедры конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: yakupov555@mail.ru

Yakupov Valeriji Ramilevich, postgraduate student of Constitutional and Administrative Law Department of South Ural State University (national research university). E-mail: yakupov555@mail.ru

УДК 342.7 + 341.231.14 + 004.7.056
ББК Х400.323 + Х401.114

Волчинская Е. К.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СИСТЕМЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

В статье поднимается актуальная сегодня в теории и на практике проблема понимания сущности персональных данных. Автором дается анализ легального определения персональных данных. Исследуются сущностные признаки персональных данных как информации ограниченного доступа.

Ключевые слова: *персональные данные, информация ограниченного доступа, конфиденциальность.*

Volchinskaya E. K.

THE PERSONAL DATA ARE IN THE SYSTEM OF CONFIDENTIALITY OF INFORMATION

In the article rises actual today in a theory and in practice problem of understanding of essence of the personal data. An author is give the analysis of legal determination of the personal data. The signs of the personal data are investigated as to information of a limit access.

Keywords: *personal data, information limit access, confidentiality.*

Персональные данные, согласно международным[1] нормативным правовым актам, представляют собой любую информацию об определенном или поддающемся определению физическом лице (субъект данных).

Российское законодательство[2] предлагает похожее определение: «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

Таким образом, определение понятия «персональные данные» не содержит прямого указания на обязательную конфиденциальность соответствующей информации. Это не случайно, поскольку установление режима конфиденциальности и отмена этого режима осуществляются либо по воле субъекта персональных данных, либо в силу закона, в том числе на основании судебного решения.

Например, Закон Российской Федерации «О государственной тайне» и реализующие его подзаконные акты предусматривают ограничение права на неприкосновенность частной жизни, то есть лицо, получившее допуск к сведениям, составляющим государ-

ственную тайну, не вправе свободно распространять свои персональные данные. С другой стороны, российское законодательство (например, Федеральный закон от 08.05.1994 № 3-ФЗ (ред. от 21.11.2011 г.) «О статусе члена Совета Федерации и статусе депутата Государственной Думы Федерального Собрания Российской Федерации») обязывает члена Совета Федерации и депутата Государственной Думы ежегодно представлять в соответствующие комиссии Совета Федерации и Государственной Думы сведения о своих доходах, об имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей. Эти сведения должны размещаться на официальных сайтах палат Федерального Собрания и предоставляться общероссийским средствам массовой информации для опубликования.

К слову, утративший силу Федеральный закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003 г.) «Об информации, информатизации и защите информации» неправомерно относил персональные данные к категории конфиденциальной информации (п. 1 ст. 11), поскольку это не вытекало из определения этого понятия.

Аналогичное заблуждение продолжает сохраняться в Указе Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера», который безусловно относит персональные данные к таким сведениям, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. Указанное положение ограничивает права субъекта персональных данных на их распространение.

Тем не менее, сохраняет актуальность вопрос: можно ли по умолчанию устанавливать для персональных данных режим конфиденциальности? Полагаем, что можно, поскольку ситуации, когда субъект персональных данных заинтересован в распространении данных о себе или обязан предоставлять такие данные, представляют исключение. Правилом же является право человека на неприкосновенность частной жизни, личную и семейную тайну, которое обычно закрепляется конституцией. Соответственно, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается (ч. 1 ст. 24 Конституции Российской Федерации).

Следующий вопрос: в каком режиме конфиденциальности необходимо охранять персональные данные? Для России, где количество видов конфиденциальной информации (режимов конфиденциальности) превышает четыре десятка и продолжает множиться, это вопрос не праздный. Ведь что такое режим конфиденциальности? Это нормативно закрепленные обязанности различных субъектов в процессе обработки определенной информации (включая ее сбор и использование) по обеспечению конфиденциальности и безопасности охраняемой информации, ограничения прав на доступ к информации и ее использование, а также нормы ответственности за ее разглашение и неправомерное использование.

Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011 г.) «О персональных данных» (статья 7) определяет конфиденциальность персональных данных следующим образом: «Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом». Следовательно, в каждом конкретном случае должны быть законодательно определены как минимум «иные лица» и условия «раскрытия третьим лицам» или распространения персональных данных.

Кроме того, режим конфиденциальности тесно связан с мерами по обеспечению безопасности данных, призванных обеспечить их конфиденциальность. При этом необходимо иметь в виду, что, с одной стороны, требование конфиденциальности персональных данных не абсолютно. А с другой стороны, требование безопасности персональных данных относится и к открытым персональным данным, например, размещенным на официальных сайтах органов государственной власти, в профессиональных энциклопедиях и т. п.

В зависимости от режима конфиденциальности возникают права на применение мер обеспечения безопасности (например, обладателем информации, составляющей коммерческую тайну) или обязанности по применению необходимых мер (например, лицами, допущенными к сведениям, составляющим государственную тайну). Требования по обеспечению режима конфиденциально-

сти в отдельных сферах могут устанавливать регулятором (например, для банковской тайны). Следовательно, механизмы обеспечения режимов конфиденциальности различаются. Субъект права не может одни и те же сведения охранять одновременно в различных режимах конфиденциальности, поскольку это создает конкуренцию требований по обеспечению их безопасности.

Казалось бы, для того, чтобы избежать такой конкуренции, персональные данные должны охраняться самостоятельным режимом конфиденциальности. Этот подход, по существу, реализуется российским законодательством. Если Федеральный закон «О персональных данных» обходит молчанием вопрос о соотношении режимов конфиденциальности[3], то Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 28.07.2012 г.) «Об информации, информационных технологиях и о защите информации» в статье 9 «Ограничение доступа к информации» указывает категорию информации «персональные данные» наряду с иными категориями информации ограниченного доступа: информации, составляющей государственную, коммерческую, служебную или профессиональную тайну.

Следствием этого положения является позиция органов, регулирующих обработку персональных данных, которая предусматривает выделение персональных данных из информационных систем, содержащих информацию ограниченного доступа и защищаемых в режиме тайны, что во многих случаях просто нереализуемо. Выделение персональных данных из общего массива охраняемой информации создает для оператора проблему соотношения требований по технической защите информации, а также проблему соотношения прав и обязанностей субъектов в отношении защищаемой информации.

Интересно, что Федеральный закон от 27.07.2004 г. № 79-ФЗ (ред. от 21.11.2011 г., с изм. от 22.11.2011 г.) «О государственной гражданской службе Российской Федерации» реализует иную концепцию и предусматривает, что сведения о доходах, об имуществе и обязательствах имущественного характера, представляемые гражданским служащим, являются сведениями конфиденциального характера, если федеральным законом они не отнесены к сведениям, составляющим государственную тайну. Таким образом, предполагается, что персональные данные могут охраняться в режиме государственной тайны.

Законодательство о персональных данных не ограничивается базовым федеральным законом. В настоящее время на рассмотрении Государственной Думы находится проект федерального закона № 217355-4 «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона "О персональных данных"». Более 30 федеральных законов требуют уточнения в связи с особенностями работы с персональными данными в отдельных областях[4].

Обоснована ли концепция формирования самостоятельного режима конфиденциальности для персональных данных? Чтобы ответить на этот вопрос, следует разобраться в соотношении видов информации ограниченного доступа, ведь, по сути, персональные данные составляют большую часть информации, относимой к профессиональной тайне (врачебная, банковская тайна, тайна страхования, тайна усыновления и др.), и присутствуют в составе иных категорий информации ограниченного доступа. Например, в режиме государственной тайны охраняются персональные данные ряда лиц, имеющих доступ к государственным секретам. В режиме коммерческой тайны могут охраняться персональные данные авторов ноу-хау, используемых в производстве. В режиме коммерческой или профессиональной тайны охраняется информация персонального характера, характеризующая пользователей предоставляемых услуг. В режиме личной тайны – сведения об особенностях личности, ее пристрастиях, привычках, интересах.

Однако место этих данных в системе конфиденциальности четко не определено. Собственно, и самой системы конфиденциальности нет, по крайней мере, законодательно она не урегулирована. Это создает серьезные проблемы в правоприменении, о чем уже говорилось выше.

При подготовке проекта федерального закона «Об информации, информационных технологиях и о защите информации» планировалось такую систему выстроить. На тот момент, согласно Федеральному закону «Об информации, информатизации и защите информации» (ст. 10), весь массив информации

ограниченного доступа разделялся по условиям правового режима на две группы: сведения, составляющие государственную тайну, и конфиденциальная информация. Отнесение информации к конфиденциальной должно было осуществляться в порядке, установленном законодательством Российской Федерации.

Единственным нормативным правовым актом, содержащим перечень сведений конфиденциального характера, был в то время и остался упомянутый выше Указ Президента РФ. Представленный перечень носит спорный характер. Например, наряду со сведениями, связанными с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (профессиональная тайна), выделена категория сведений, составляющих тайну следствия и судопроизводства, а также сведений о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации. Критерий выделения этой категории не очевиден.

Также наряду со сведениями, связанными с коммерческой деятельностью (коммерческая тайна), в отдельную категорию выделены сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Эти сведения обычно составляют ноу-хау и охраняются режимом коммерческой тайны.

Но даже если абстрагироваться от этих противоречий, систему конфиденциальности данный указ не формирует, поскольку не устанавливает правовой режим сведений, конфиденциальность которых должна быть обеспечена, в том числе: права и обязанности субъектов (включая государство) в отношении сведений конфиденциального характера, требования по обеспечению безопасности соответствующих сведений и ответственность за нарушение режима конфиденциальности.

Кроме того, после принятия Федерального закона от 27.07.2006 г. № 149-ФЗ (ред. от 28.07.2012 г.) «Об информации, информационных технологиях и о защите информации» словосочетание «конфиденциальная информация» было из базового законодательства изъято, на смену ему пришла категория «конфиденциальность информации», определяемая как «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя». Исходя из концепции статьи 9, режим конфиденциальности распространяется как на сведения, составляющие государственную тайну, так и на иные виды информации ограниченного доступа. Наряду с этим в российском законодательстве появились смешанные категории информации, включающие информацию, охраняемую различными режимами конфиденциальности. Например, инсайдерская информация[5], в составе которой могут быть «сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну)» (ст. 2).

В ходе совершенствования базового законодательства об информации юридической наукой не была предложена концепция конфиденциальности информации, и ситуация запуталась еще больше. В 2005 году была предложена авторская концепция[6] классификации тайн по способу их образования:

«первичные» (естественные) тайны, которые непосредственно связаны с жизнедеятельностью субъекта,

«производные» тайны, которые связаны с защитой информации другого субъекта, получаемой в режиме тайны.

В состав «первичных» тайн входят: личная и семейная тайны (тайна физического лица; коммерческая тайна (тайна юридического лица), осуществляющего предпринимательскую деятельность; государственная и служебная (в части внутрисистемной информации) тайны (тайна государства, в том числе в лице органа государственной власти). Здесь и далее я говорю о служебной тайне в концепции законопроекта, внесенного в Государственную Думу и находящегося на рассмотрении вплоть до 2011 года, в соответствии с которой информация, составляющая служебную тайну, включает:

информацию, создаваемую (генерируемую) в органе государственной власти, доступ к которой временно ограничен в интересах государственного управления по решению руководителя;

информацию ограниченного доступа, представляемую в этот орган в режиме конфиденциальности.

В состав «производных» тайн входят:

профессиональные тайны, когда информация передается субъекту профессиональной деятельности от физических лиц в режиме личной или семейной тайны (врачебная тайна, тайна исповеди, тайна банковских вкладов, тайна усыновления, налоговая, нотариальная и др.) либо от юридических лиц в режиме коммерческой тайны (налоговая, банковская, нотариальная и др.);

служебная тайна в части переданной в органы власти от физических и юридических лиц информации ограниченного доступа.

Принципиальное различие этих категорий тайн состоит в том, что для «первичных» тайн у субъектов – обладателей соответствующей информации есть право на установление режима конфиденциальности, а для «производных» тайн у лица, которому доверена информация ограниченного доступа, возникает обязанность устанавливать соответствующий режим конфиденциальности.

Максимальный объем регулирования со стороны государства приходится на государственную и служебную тайны. Государство вправе установить требования по защите информации, составляющей государственную или служебную тайну, а также ответственность за нарушение конфиденциальности и безопасности этой информации.

В отношении других видов «первичных» тайн (личная и семейная тайны, коммерческая тайна) государство должно уступить право основного регулятора тем субъектам, которые образуют (устанавливают) эти режимы. Задача государства – обеспечить защиту их прав и интересов с учетом интересов других субъектов.

Таким образом, если, предположим, персональные данные составляют коммерческую тайну, то оператор вправе, в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне», самостоятельно применить меры защиты коммерческой тайны при условии соблюдения прав субъектов персональных данных, предусмотренных Федеральным законом «О персональных данных». С другой стороны, очевидно, что при обработке персональных данных в режиме государственной тайны приоритет получат требования по защите государственной тайны. Однако Федеральный закон «О персональных данных», и особенно подзаконные нормативные правовые акты, не позволяют это сделать.

Приведенные примеры, как нам представляется, свидетельствуют о том, что установление единых обязательных требований по обеспечению безопасности персональных данных не оправданно.

Участники упомянутых выше парламентских слушаний были, прежде всего, обеспокоены сложновыполнимыми требованиями по обеспечению безопасности персональных данных, установленными в ст. 19 Федерального закона «О персональных данных»[7].

Требования к операторам информационных систем персональных данных включали такие механизмы государственного регулирования, для реализации которых у большинства операторов не было достаточных материальных и трудовых ресурсов. Особенно это касалось бюджетных организаций в сфере образования, медицинского обслуживания, жилищно-коммунального комплекса.

В коммерческих организациях просчитывалось существенное увеличение затрат на подготовку информационной системы по требованиям безопасности персональных данных, что должно было неизбежно отразиться на стоимости услуг оператора.

Участники рынка услуг по защите персональных данных также не в силах были предоставить услуги всем заинтересованным операторам, число которых по экспертным оценкам составляет 5–7 миллионов.

Специалисты указывали на неадекватность требований по обработке данных возможным угрозам их утраты и конфликте требований, установленных разными законами.

В ряде отраслей реализация установленных требований требовала радикальных изменений бизнес-процессов (например, в банковской сфере, в сфере предоставления услуг связи), поскольку большинство коммерческих структур используют зарубежные программные продукты, при этом переход на отечественные сертифицированные продукты либо невозможен из-за отсутствия аналогов, либо несет огромные временные и материальные затраты, которые могут привести к остановке деятельности многих компаний.

В связи со сложившимся критическим положением в Рекомендации парламентских слушаний было включено предложение при доработке закона распространить обязательные требования по безопасности обработки

персональных данных, установленные Правительством Российской Федерации, на государственные информационные системы, содержащие персональные данные, определив в качестве критериев при разработке этих требований соразмерность затрат и возможности возникновения ущерба субъекту персональных данных, соответствие природе обрабатываемых данных и масштабам обработки.

Для негосударственных и муниципальных информационных систем определить общеобязательные минимальные требования к обеспечению безопасности персональных данных при их обработке, реализация которых не зависит от применения конкретного технического решения, и установить право оператора негосударственной и муниципальной информационной системы самостоятельно определять методы и средства обеспечения безопасности персональных данных при их автоматизированной обработке с учетом отраслевых (ведомственных) методических рекомендаций по обеспечению безопасности информационных систем персональных данных.

При подготовке этих Рекомендаций учитывались положения Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных, а также опыт защиты персональных данных в странах Европейского Союза.

Так, упомянутая Директива ЕС предусматривает (ст. 17), что контролер (оператор персональных данных) должен будет реализовать надлежащие технические и организационные меры для защиты персональных данных от случайного или незаконного уничтожения или случайной утраты, изменения, неправомерного раскрытия или доступа, а также от всех иных незаконных форм обработки. С учетом состояния и стоимости их реализации такие меры должны обеспечить надлежащий уровень безопасности для рисков, представленных обработкой и природой защищаемых данных.

В странах Европейского Союза, как правило, выбор средств и методов защиты персональных данных полностью оставлен на усмотрение оператора. Национальное законодательство ряда стран содержит рекомендации для оператора по выбору средств защиты (например, Ирландия, Великобритания, Нидерланды, Дания). В общем случае (за исключением особо чувствительных персональных данных) такие средства не отличаются от обычно используемых для защиты конфиденциальности.

Однако предложенная Рекомендациями парламентских слушаний концепция «демократизации» механизмов обеспечения безопасности персональных данных не была полностью реализована. В статье 19 Федерального закона «О персональных данных» закреплен определенный компромисс. Перечислены меры по обеспечению безопасности персональных данных. Правительство 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, в том числе, уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных (Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119, утвердившее Требования к защите персональных данных при их обработке в информационных системах персональных данных). Для каждого уровня защищенности устанавливаются требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание необходимых для выполнения этих требований организационных и технических мер по обеспечению безопасности персональных данных устанавливаются ФСБ России и ФСТЭК России в пределах их полномочий. Угрозы безопасности персональных данных, актуальные для информационных систем, эксплуатируемых при осуществлении соответствующих видов деятельности, определяют государственные органы с учетом содержания персональных данных, характера и способов их обработки. Это всё обязательные требования, а не рекомендации, как в европейских странах. Весь «демократизм» процедуры сосредоточился в праве негосударственных субъектов (ассоциаций, союзов и иных объединений операторов) своими решениями определить дополнительные угрозы безопасности персональных данных.

Таким образом, концепция рассмотрения персональных данных как самостоятельной

категории информации ограниченного доступа, для которой устанавливаются особые требования по обеспечению безопасности, не претерпела изменений и вряд ли изменится, пока не будут законодательно регламентированы принципы формирования в России системы конфиденциальности и требования к отдельным правовым режимам конфиденциальности. Базовые положения, обеспечивающие такую регламентацию, должны, по нашему мнению, содержаться в Федеральном законе «Об информации, информационных технологиях и о защите информации».

Примечания

[1] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года; Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных; Международный стандарт по защите персональных данных и частной жизни, принятый на 31-й Конференции уполномоченных органов по персональным данным (Мадрид, 2009).

[2] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011 г.) «О персональных данных».

[3] В Рекомендациях Парламентских слушаний на тему «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных» (20 октября 2009 г.) предлагалось при доработке закона предусмотреть возможности распространения на информационные системы персональных данных правовых режимов и способов защиты коммерческой, профессиональной и иной охраняемой законом тайны.

[4] В том числе: Трудовой кодекс Российской Федерации № 197-ФЗ от 30 декабря 2001 года (глава 14), Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30 декабря 2001 года (статья 13.11.), ФЗ «О государственной гражданской службе Российской Федерации» № 79-ФЗ от 27 июля 2004 года (глава 7), ФЗ «О муниципальной службе в Российской Федерации» № 25-ФЗ от 2 марта 2007 года (статья 29).

[5] Федеральный закон от 27.07.2010 № 224-ФЗ (ред. от 28.07.2012 г.) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».

[6] См. Волчинская Е. К. Коммерческая тайна в системе конфиденциальной информации // «Информационное право». – 2005. – № 3; Волчинская Е. К. Роль государства в обеспечении информационной безопасности // «Connect! Мир связи». – 2008 – Сент. Волчинская Е. К. Роль государства в обеспечении информационной безопасности // «Информационное право». – 2008. – №4.

[7] О недостатках предлагаемого подхода см.: Волчинская Е. К. Некоторые правовые проблемы применения Федерального закона «О персональных данных» // «Персональные данные». – 2009. – № 2. (электронный)

Волчинская Елена Константиновна, кандидат экономических наук, доцент кафедры теории права и сравнительного правоведения научно-исследовательского университета «Высшая школа экономики».

Volchinskaya Elena Konstantinovna, candidate of economic sciences, associate professor of department of theory of right and comparative jurisprudence of research university "Higher school of economy".

УДК 004.7:34.02
ББК Х401.114

Минбалеев А. В.

ОСНОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

В статье автор анализирует основы правового регулирования отношений в сети Интернет, исследуется зарубежный опыт. Дается характеристика современному состоянию законодательства, анализируются основные проблемы регулирования сети Интернет.

Ключевые слова: *правовое регулирование, сеть Интернет.*

Minbaleev A. V.

THE LEGAL GROUNDS TO REGULATE TELECOMMUNICATIONS NETWORK RELATIONS

In this article the author analyses the legal relations on the Internet and its legal regulation principles, foreign experience is being studied. A description to the modern state of legislation and the basic problems of regulating the Internet network is given.

Keywords: *legal regulation, the Internet network.*

Создание и развитие информационно-телекоммуникационной сети Интернет (далее – сети Интернет) способствовало формированию и развитию глобального информационного общества, объединило весь мир в системе бесчисленных информационных связей. Прежде чем исследовать особенности правовой природы массовых коммуникаций в сети Интернет, необходимо определить, что представляет собой сеть Интернет и как связана она с массовыми коммуникациями?

Согласно ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Исходя из ст. 16 Закона об информации, информационно-телекоммуникационные сети разграничиваются на информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, а также иные информационно-телекоммуникационные сети. Первую группу составляют открытые информационно-

телекоммуникационные сети. Под иными, соответственно, понимаются информационно-телекоммуникационные сети, доступ к которым ограничен и определяется их владельцем. Таким образом, критерием для разграничения информационно-телекоммуникационных сетей выступает возможность доступа к ним неопределенного круга лиц. Вторым критерием для разграничения законодатель называет механизм регулирования использования информационно-телекоммуникационных сетей. Регулирование использованияинформационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется Российской Федерацией с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок же использования иных информационно-телекоммуника-ционных сетей определяется их владельцами с учетом требований закона об информации. К таким требованиям, в первую очередь, относится необходимость соблюдения требований законодательства Российской Федерации в области связи, Закона об информации и иных нормативных правовых актов Российской Федерации, а также соблюдения принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации, на основе которых владельцы информационно-телекоммуникационных сетей устанавливают порядок доступа к ним и их использования.

Кроме того, в рамках информационно-телекоммуникационных сетей выделяют:

• локальные (в одном здании, в какой-либо организации);

• ведомственные (охватывающие пользователей одного ведомства);

• региональные (объединяющие пользователей субъекта федерации, муниципального образования и других территориальных единиц);

• специального назначения (например, защищенная сеть государственной автоматизированной системы ГАС «Правосудие», государственной автоматизированной системы ГАС «Выборы»);

• глобальными (сеть Интернет)[1].

Сеть Интернет относится к категории глобальных информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц. Согласно Указу Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» сеть Интернет представляет собой информационно-телекоммуникационную сеть международного информационного обмена[2]. Интернет в самом общем виде можно определить как уникальное объединение локальных, национальных и международных компьютерных сетей, организационно не являющихся чем-то единым целым. Интернет – явление неправовое, данное объединение сетей не может быть субъектом или объектом права, не может регулироваться как одно единое целое. В конце XX века в юридической науке сложилось мнение, что в отношении сети Интернет надо говорить лишь о правовом регулировании отдельных вопросов, а именно: порядка, условий использования сетей и защиты прав и законных интересов различных субъектов при циркулировании информации в сети[3]. Представляется, что сегодня мы можем говорить о возможности законодательного закрепления основ регулирования отношений в сети Интернет, а также регулирования определенных областей, сторон, вопросов.

На основе анализа действующего законодательства и особенностей сети Интернет П. У. Кузнецов определяет ее как «глобальную информационно-телекоммуникационную технологическую систему, состоящую из предназначенной для передачи по линиям связи и представленной на портале (сайте) совокупности (массива) информации, доступ к которой осуществляется с использованием организационных, программных и вычислительных средств, а также иных элементов сетевой инфраструктуры»[4]. Модельный закон Межпарламентской Ассамблеи государств – участников СНГ «Об основах регулирования Интернета» от 16 мая 2011 г. под Интернетом понимает глобальную информационно-телекоммуникационную сеть, связывающую информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанную на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющую возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц[5].

Таким образом, сеть Интернет, как и другие информационно-телекоммуникационные сети, нельзя рассматривать как форму массовых коммуникаций. Сеть Интернет представляет собой систему значительно более высокого уровня и порядка, это технологическая система, которая предоставляет возможность реализации различных форм коммуникации как массовой, так и индивидуальной направленности. В связи с этим применительно к массовым коммуникациям сеть Интернет мы можем рассматривать в широком и узком смыслах. В широком смысле – это виртуальная сфера, в которой массовые коммуникации находят свое реальное отображение и развитие в самых различных формах и проявлениях. В узком смысле сеть Интернет – это совокупность информационных технологий, с помощью которых происходит создание, размещение и распространение информации для неограниченного круга лиц.

Сеть Интернет обладает рядом признаков, которые необходимо учитывать при решении вопроса о необходимости регулирования отношений, складывающихся в ней по поводу массовых коммуникаций. К ним относятся следующие:

• массовость (так, по данным главы Международного телекоммуникационного союза при ООН Хамадун Туре, число пользователей Интернета в начале 2011 г. во всем мире достигло двух миллиардов, что составляет около 30 процентов населения Земли; число зарегистрированных мобильных телефонов достигло пяти миллиардов[6]; по данным главы Минкомсвязи РФ Игоря Щеголева число Интернет-пользователей в России в 2011 году выросло до 70 млн человек[7]);

• доступность сети. Сеть Интернет становится доступной практически любому пользователю. Этому способствует удешевление стоимости компьютерных устройств; развитие мобильного Интернета; обязательное подключение к Интернету образовательных заведений, библиотек, организаций связи; организация доступа к сети Интернет для реализации прав на получение государственных услуг через информационно-телекоммункиационные сети, в том числе сеть Интернет, и другие факторы;

• открытость (транспарентность) информации. Это общий принцип деятельности в сети Интернет и распространения в ней информации. По общему правилу, нахождение информации в сети Интернет предполагает ее открытость. Согласно ч. 5 ст. 16 Закона об информации передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

Наряду с указанными признаками позитивного характера в науке также выделяют признаки коммуникативности, универсальности, высокой скорости передачи, обмена и получения информации в сети Интернет, дистанционности и др. Кроме того, с сетью Интернет связывают и ряд свойств негативного характера, в том числе опасность несанкционированного доступа, повышенную доступность информации негативного характера, опасность использования как инструмента причинения вреда, подмену ценностей и зависимость общества от информационных технологий, виртуальность[8].

Правовое регулирование отношений в сети Интернет обусловлено рядом проблем: нарушение интеллектуальных прав на результаты интеллектуальной деятельности и средства индивидуализации; распространение ненадлежащей рекламы, оскорбительных и непристойных материалов и доступ к ним несовершеннолетних; несанкционированный доступ к информации ограниченного доступа; нарушение прав и законных интересов личности, общества и государства в процессе информационного обмена и другие.

Появление в сети Интернет ряда новых отношений, видов массовых коммуникаций, их активное развитие и проблемы функционирования обусловливают необходимость расширения сферы правового регулирования, увеличение ряда областей и сторон правового регулирования применительно к сети Интернет. Алексеев С. С. указывал, что расширение сферы правового регулирования состоит не в частичном усилении принудительных мер воздействия, вызванном подчас временными затруднениями, сложной обстановкой, а прежде всего в расширении таких областей и сторон правового регулирования, функционирование которых характеризует возрастание нравственных начал в жизни общества, усиление организованности обще-

ственных отношений, порядка ответственности во взаимоотношениях между людьми[9]. Идеи, высказанные ученым, несмотря на то, что они были сделаны более сорока лет назад, актуальны и для наших дней.

Функционирование ряда отношений в сети Интернет, в том числе в сфере массовых коммуникаций, свидетельствуют о необходимости включения данных отношений в предмет правового регулирования и увеличении ряда областей и сторон правового регулирования применительно к сети Интернет. В качестве факторов, закономерностей, обосновывающих данное заключение, можно привести следующие:

1. Распространение «вредной» информации в сети Интернет и проблемы защиты нравственности. Функционирование сети Интернет в режиме общедоступности на протяжении двух десятков лет свидетельствует о формировании значительного количества угроз информационной безопасности личности, общества и государства и, в первую очередь, угроз нравственным началам в жизни общества, а также порой бесконтрольное распространение порнографической информации, в том числе с изображением несовершеннолетних, диффамация, унижения, призывы к самоубийству, распространение экстремистской информации, дезинформация – это лишь часть «грязной» информации, которая приводит к общему падению нравственности человечества в целом и российского общества в частности. Подобная информация сегодня определяется как информация ограниченного распространения («вредная» информация).

Ст. 20 Международного пакта о гражданских и политических правах от 19.12.1966 г. исключает из сферы информационного обмена информацию, относящуюся к пропаганде войны, национальной, расовой или религиозной ненависти, представляющую собой подстрекательство к дискриминации, вражде или насилию. В резолюциях Генеральной Ассамблеи ООН закреплены запреты на распространение ложной или извращенной информации (резолюция от 15.11.1947 № 127), пропаганду ненависти и предвзятого отношения к другим народам (Декларация о воспитании народов в духе мира от 15.12.1947), подстрекательства к расизму, расовой дискриминации, ксенофобии и подобной нетерпимости (резолюция A/RES/51/79 от 25.02.1997)[10]. Ограничения подобной информации устанавливаются также в соответствии с целями и задачами государственной информационной политики[11] России, закрепленными в Доктрине информационной безопасности Российской Федерации[12], а также в Основных направлениях государственной семейной политики[13] и других документах, включающими защиту культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, духовное и нравственное воспитание населения, введение запрета на распространение посредством электронных средств массовой информации программ, пропагандирующих порнографию, насилие и жестокость, антиобщественное поведение, эксплуатирующих низменные проявления. Ограничения права на информацию на доступ и использование «вредной» информации опираются на общепризнанные принципы и нормы международного права, провозглашающие допустимость ограничения законом свободы получать и распространять информацию в случаях, если это необходимо в интересах национальной безопасности или общественного порядка, в целях предотвращения преступлений, а также для охраны здоровья и нравственности, защиты репутации или прав других лиц[14].

Наибольшую опасность «вредная» информация оказывает именно через Интернет. Связано это с такими обозначенными признаками сети Интернет, как массовость, доступность, коммуникативность, высокая скорость передачи, обмена и получения информации.

Угроза нравственности в связи с функционированием сети Интернет видится не только в связи с распространением «вредной» информации, но и обусловлена массовой подменой общественных ценностей и появлением зависимости общества от интернет-технологий. Постоянное использование сети Интернет приводит к замене реальных ценностей цивилизации знакомству с их виртуальными формами, причем часто низкого качества или недостоверного содержания; личное общение заменяется виртуальным, в том числе в интернет-сообществах. Как говорил М. Маклюэн, происходит качественное изменение системы человеческой деятельности и общественных ценностей[15].

Возрастание популярности сети Интернет способствовало развитию новой формы психологической и физиологической зависи-

мости – интернет-зависимости, проявляющейся в навязчивом желании подключиться к сети Интернет и болезненной неспособности вовремя отключиться от сети. Интернет-зависимость связывается с профессионально-технологической, предполагающей осуществление трудовой функции непосредственно в сети, и социально-психологической, являющейся наиболее опасной, поскольку способствует возможности манипулирования сознания зависимых, всецело доверяющих информации в сети Интернет и исключающих другие источники информации.

2. Необходимость усиления организованности общественных отношений. Виртуальность сети Интернет и возможность создания искаженной реальности, возможность практически бесконтрольного функционирования большого количества сегментов сети приводит к ряду нарушающих права и свободы физических и юридических лиц, государства, наносит вред интересам личности, общества и государства. Дезорганизованность ряда отношений в сети Интернет приводит к появлению угроз информационной безопасности, в том числе несанкционированного доступа к охраняемой законом информации, распространения и использования компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Отсутствие стандартов и законодательных требований в сфере массовых коммуникаций приводит к неограниченному появлению и использованию различных видов массовых коммуникаций, которые маскируются под легальные формы или открыто распространяют массовую информацию, но при этом к ним не применяются требования, установленные к традиционным средствам массовых коммуникаций.

3. Необходимость установления порядка ответственности во взаимоотношениях между субъектами. П. У. Кузнецов совершенно справедливо замечает, что, несмотря на прогрессивность сети Интернет, данный технологический инструмент «постепенно становится и бременем для общества, поскольку соотношение между свободой распространения информации и ответственностью ее распространителя находится в глубоком кризисе»[16]. В качестве субъектов отношений, складывающихся в сети Интернет можно отнести:

• государство в лице его органов власти, уполномоченных на осуществление регулирования сети Интернет;

• пользователи сети Интернет – юридические и физические лица, которым предоставляются услуги сети Интернет;

• операторы услуг сети Интернет;

• саморегулируемые организации, участвующие в процессе регулирования сети Интернет.

При функционировании сети Интернет сегодня решается целый ряд вопросов ответственности пользователей за распространение «вредной» информации; ответственности органов государственной власти за неоказание или ненадлежащее оказание государственных услуг через сеть Интернет, непредставление информации; ответственности операторов услуг сети Интернет за нарушение требований, устанавливаемых к ним государством. В то же время остается огромное количество нерешенных проблем:

• проблемы юрисдикции. При разрешении споров, связанных с правонарушением в сети Интернет, возникают коллизии иностранного и национального законодательства. Возникает вопрос о том, правовые нормы какого государства должны применяться в том или ином случае? Учитывая экстерриториальный характер использования сети Интернет, данная проблема должна быть разрешена, в первую очередь, на международном или межгосударственном уровне, что пока вызывает определенные сложности. В качестве положительного опыта решения такого вопроса можно найти в модельном законе Межпарламентской Ассамблеи государств – участников СНГ «Об основах регулирования Интернета», согласно которому юридически значимые действия, осуществленные с использованием Интернета, признаются совершенными на территории государства, если действие, породившее юридические последствия, было совершено лицом во время его нахождения на территории этого государства. Временем совершения юридически значимых действий признается время совершения первого действия, породившего юридические последствия. А в случае если при разрешении споров, связанных с использованием Интернета, возникает коллизия иностранного и национального законодательства, то действует норма национального законода-

тельства государства, на территории которого считается совершенным юридически значимое действие;

• проблема необходимости принятия государством политики по противодействию использованию сети Интернет в противоправных целях и регулирования вопросов ответственности за неправомерное использование сети Интернет, совершение правонарушений в сети. К сожалению, сегодня в Российской Федерации устанавливаются лишь отдельные меры и направления в этой области. Полагаем, что в данном направлении необходимо:

1) разработать отдельную Концепцию противодействия использованию сети Интернет в противоправных целях, в которой должно содержаться описание современного состояния использования сети Интернет в противоправных целях, системы угроз, комплекс принимаемых и необходимых к принятию мер по противодействию, основные направления совершенствования законодательства в данном направлении;

2) закрепление на уровне базового закона «Об основах регулирования отношений в сети Интернет норм о разграничении между государством, саморегулируемыми организациями и операторами услуг сети Интернет компетенции по определению правонарушений, связанных с незаконным использованием сети Интернет, и оснований для привлечения к ответственности; полномочия данных субъектов по привлечению к ответственности; общий порядок и виды ответственности; основные положения о взаимодействии с зарубежными государствами, международными организациями по вопросам ответственности. Также необходимо в данном законе закрепить общие подходы к ответственности операторов услуг сети Интернет за распространение и хранение информации, разграничению ответственности операторов и пользователей; обязанность операторов услуг Интернета хранить информацию о пользователях и об оказанных им услугах не менее установленного периода времени и предоставлять данные сведения по запросу судебных и (или) правоохранительных органов в порядке и в целях, устанавливаемых законом.

Так, согласно европейскому опыту, провайдеры несут ответственность, если они были осведомлены о наличии такой информации и блокирование ее было технически возможно[17]. Данное положение не является столь однозначным, так как «не всегда представляется возможным определить, имеет ли место нарушение закона»[18]. Российская судебная практика по данному вопросу неоднозначна даже в рамках одного дела. Ее позиция по ответственности интернет-провайдеров подчас меняется от отрицания возможности привлечения провайдера к ответственности до признания его полной ответственности с определением условий ее возложения на провайдера[19]. Так, рассматривалось дело, в котором ООО «Контент и право» обратилось в Арбитражный суд города Москвы с иском к ООО «МетКом» и ЗАО «Мастерхост» о взыскании с каждого из ответчиков компенсации в размере 100 000 рублей за нарушение исключительных прав истца на музыкальные произведения. Истец, как обладатель исключительных прав на произведение, требовал защиты своих прав от незаконного воспроизведения данных произведений и их доведения до всеобщего сведения на сайте ответчика, размещенном на сервере хостинг-провайдера – ЗАО «Мастерхост». Отказывая в удовлетворении требования правообладателя, суд первой инстанции исходил из того, что поскольку ЗАО «Мастерхост» является оператором связи, оказывающим услуги передачи данных сети связи общего пользования на территории Москвы, оно не может нести ответственность за содержание хранимой и распространяемой абонентом информации[20].

Суд апелляционной инстанции не согласился с выводами суда первой инстанции. В решении суда было указано, что представление ответчиком доказательства принадлежности сайта www.zaycev.net другому лицу не доказывает факта размещения данного сайта на сервере хостинг-провайдера третьим лицом, а не самим ответчиком. ЗАО «Мастерхост» было признано нарушителем исключительных прав истца[21]. При рассмотрении дела в кассационной инстанции решение суда апелляционной инстанции было оставлено без изменения.

Затем дело поступило в Президиум ВАС РФ, который отменил все вышеуказанные акты и отправил дело на новое рассмотрение в Арбитражный суд г. Москвы. Президиум ВАС РФ указал, что суды кассационной и апелляционной инстанций не установили, знал или мог ли знать ответчик о незаконных распространениях названных произведений, и,

следовательно, неправомерно возложили на него бремя доказывания отсутствия факта использования им этих произведений. Факт несанкционированного использования произведений путем доведения до всеобщего сведения должен быть доказан правообладателем, требующим защиту своих исключительных прав. Материалами дела было подтверждено, что ЗАО «Мастерхост» является компанией, предоставляющей услуги по размещению интернет-сайтов на своих серверах либо по размещению оборудования абонента на своей площадке, т. е. является хостинг-провайдером, осуществляющим исключительно технические функции: размещение оборудования абонента и его техническое обслуживание. Предоставляя услуги такого рода, провайдер, как правило, не имеет доступа к оборудованию абонента[22]. Таким образом, провайдер не несет ответственности за передаваемую информацию, если не он инициирует ее передачу, не выбирает получателя информации, не влияет на целостность передаваемой информации. Такой подход, может, и не всегда устраивает правообладателей, но он на сегодняшний день действительно, оказывается единственно возможным в условиях отсутствия государственной политики по вопросам ответственности за незаконное использование сети Интернет.

Интернет с его высочайшей скоростью распространения информации и анонимностью пользователей может стать эффективным инструментом общественной самоорганизации в борьбе с бюрократами и производителями некачественной продукции. Однако, как и многие другие инструменты и технические новинки, его можно использовать как на благо людей, так и во вред им.

Сегодня очень сложно сказать, как сочетать всеобщий свободный доступ к сети Интернет с запретами и ограничениями в отношении ряда противозаконных действий в сети (призывы к убийствам, террору, описание подготовки к ним, педофилия) или распространения вредного контента (порнография, диффамация и т. п.). Эта проблема стоит перед всеми государствами и пока не имеет эффективного решения ни в одной стране мира. Общественно-государственную систему этических ограничений в сети Интернет, которая придет на смену цензуре и запретам, во многих странах быстро создать не удастся. Многие государства используют систему жесткого контроля и ограничения к Интернету, разрешая лишь допуск к отдельным сайтам (Китай). В других государствах, наоборот, обеспечивается достаточно свободный доступ к информации в сети Интернет, что является основанием для широкого распространения вредной информации. Поскольку Интернет является общедоступной сетью в мире, то естественно, что вредная информация, разрешаемая к распространению во многих государствах, становится доступной всем пользователям. В этой связи возникает дилемма: нужно ли обеспечивать доступ к сети Интернет, или необходимо ужесточать контроль над доступом?

В некоторых экономически развитых государствах доступ в сеть Интернет был признан в качестве права. Например, парламент Эстонии принял закон, объявив в 2000 году доступ в Интернет как основное право человека. Конституционный совет Франции фактически объявил доступ в Интернет одним из основных прав в 2009 году. Конституционный суд Коста-Рики пришел к аналогичному решению в 2010 году. Финляндия приняла постановление в 2009 году о том, что каждое интернет-соединение должно иметь скорость хотя бы в размере одного мегабита в секунду (быстрый уровень). Согласно результатам опроса, проведенного британской вещательной корпорацией в марте 2010 года, 79% опрошенных в 26 странах считают, что Интернет является основополагающим правом человека[23].

Интернет как средство, через которое может быть осуществлено право на свободу выражения мнений, может выполнять данную цель только при условии, что государства возьмут на себя обязательства разработать эффективную политику для достижения всеобщего доступа к Интернету. Данная политика должна обеспечивать защиту прав, свобод человека и гражданина, не допускать возможность распространения вредной информации, противоречащей международным требованиям. Без конкретных стратегий и планов действий Интернет станет технологическим инструментом, который доступен только для определенной элиты в условиях «цифрового разрыва». Политика любого государства должна осуществляться в двух направлениях:

1) с одной стороны, государство должно обеспечивать общий доступ в Интернет. В этой связи должна осуществляться политика невмешательства в личную жизнь граждан,

обеспечиваться возможность получения ими разной информации;

2) с другой стороны, государство должно устанавливать запрет на распространение отдельных видов информации, устанавливать некоторые пределы доступа в Интернет в отношении вредной информации. Эти ограничения могут быть сделаны только на законных основаниях. Государство должно обеспечить получение гражданами необходимой информации, должно установить, какие сведения являются запрещенными к распространению, и научить граждан противодействовать их распространению.

Право на доступ в сеть Интернет – это право человека искать, получать и передавать информацию и мысли, убеждения посредством сети Интернет. Согласно данным Международного союза электросвязи, на данный момент в целом число интернет-пользователей по всему миру составляет свыше 2 миллиардов. Число активных пользователей Facebook, онлайн-платформы социальной сети, возросло со 150 миллионов до 600 миллионов (2009–2011 гг.). Сеть Интернет играет огромную роль и в мобилизации населения и призвании к справедливости, равноправию, ответственности и к большему уважению прав и свобод человека. Благодаря сети Интернет осуществляются реализация ряда прав человека, борьба с неравенством и развитие прогресса. В рамках ООН сейчас ведется активная работа по отнесению права на доступ в Интернет к числу фундаментальных прав человека. Поводом принятия такого решения стало и событие 3 июня 2011 г., когда власти Сирии отключили интернет-доступ по всей стране с целью не дать оппозиции координировать свои действия.

В этой связи возникает вопрос о природе права на доступ в Интернет и четкого оформления его названия. Представляется, что данное право необходимо обозначить как «право на доступ к сети Интернет и размещенной в ней информации». Полагаем, что в отношении данного права необходимо говорить не только о доступе к подключению к сети Интернет, но и о доступе к информации, размещаемой в ней. Связано это с многочисленными случаями ограничения доступа к отдельным сайтам и порталам, веб-сервисам в сети Интернет при наличии возможности подключения к ней и доступности других сайтов. Ряд государств устанавливают запреты на доступ к некоторым сайтам исходя из различных оснований. В ряде случаев это обоснованные ограничения доступа к сайтам с порнографической информацией, информации экстремистской направленности. Во многих случаях государство руководствуется политической, экономической или иной целесообразностью неполучения гражданами информации, негативно отражающей те или иные процессы, происходящие в государстве.

Обозначенное право является разновидностью права на информацию, поскольку основная цель реализации данного права – получить доступ (ознакомление и использование) к информации, а сеть Интернет выступает как средство для ее осуществления. Обособление данного права в системе права на информацию играет огромную роль в обеспечении доступа к наиболее важным видам общественной информации, размещаемым в сети Интернет. Данное право предоставляет возможность реализации других личных, социальных, экономических, политических и иных прав человека и гражданина.

Полагаем, что право на доступ к сети Интернет и размещенной в ней информации необходимо законодательно закрепить на уровне базового Закона об информации.

Таким образом, руководствуясь системным подходом, на основе анализа природы сети Интернет, закономерностей ее функционирования, можно заключить о наличии необходимости законодательного закрепления основ регулирования отношений в сети Интернет, а также ряда областей, сторон и видов отношений в сети Интернет. Выявленные факторы, обусловливающие необходимость правового регулирования отношений в сети Интернет. Здесь также актуальными являются необходимость обеспечения ряда прав и свобод человека и гражданина, в первую очередь свободы массовой информации, свободы слов, мнений, а также важного их проявления – права на доступ в сеть Интернет; необходимость введения ограничений на распространение отдельных видов информации; необходимость организации и упорядочивания функционирования средств массовых коммуникаций и необходимость определения ответственности между субъектами по поводу ряда их действий.

Примечания

[1] Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П. У. Кузнецова. – М.: Издательство Юрайт, 2011. – С. 73.

[2] Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 // СЗ РФ. – 2008. – № 12. – Ст. 1110.

[3] См.: Терещенко Л. К. Правовые проблемы использования Интернета в России // Журнал российского права. – 1999. – № 7/8. – С. 3.

[4] Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П. У. Кузнецова. – С. 81.

[5] Модельный закон Межпарламентской Ассамблеи государств – участников СНГ «Об основах регулирования Интернета». Принят на тридцать шестом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление № 36-9 от 16 мая 2011 года) [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.iacis.ru/html/?id=22&pag=792&nid=1, свободный. – Загл. с экрана. – Яз. рус.

[6] См.: В мире – 2 миллиарда пользователей Интернета. 27.01.2011 [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.svobodanews.ru/content/news/2288315.html, свободный. – Загл. с экрана. – Яз. рус.

[7] См.: Подсчитано число пользователей Интернета в России в 2011 году. 27.12.2011 [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://vz.ru/news/2011/12/27/550090.html, свободный. – Загл. с экрана. – Яз. рус.

[8] См. : Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П. У. Кузнецова. – С. 75-76.

[9] См.: Алексеев С. С. Социальная ценность права в советском обществе. – М.: Юрид. литература, 1971. – С. 29.

[10] См.: Талимончик В. П. Международно-правовое регулирование отношений информационного обмена в Интернете : дис. на соискание ученой степени к.ю.н. – СПб., 1999. – С. 125.

[11] Об информационной политике государства подробнее см.: Информационная политика : учебник / Под общ. ред. В. Д. Попова. – М.: Изд-во РАГС, 2003. – 463 с.

[12] Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации от 09.09.2000 № ПР-1895 // Российская газета. – 2000. – 28 сент.

[13] Основные направления государственной семейной политики. Утверждены Указом Президента Российской Федерации от 14.05.1996 № 712 // СЗ РФ. –1996. – № 21. – Ст. 2460.

[14] См.: п. 2 ст. 29 Всеобщей декларации прав человека. Принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10.12.1948; п. 3 ст. 19 и ст. 20 Международного пакта о гражданских и политических правах от 19.12.1966; ст. 10 Международного пакта об экономических, социальных и культурных правах от 19.12.1966 // Ведомости ВС СССР. – 1976. – № 17 (1831). – Ст. 292; Ст. 10 Конвенции о защите прав человека и основных свобод от 04.11.1950; ст. 10 Конвенции СНГ о правах и основных свободах человека от 26.05.1995 // СЗ РФ. – 1999. – № 13. – Ст. 1489; Европейские конвенции: о совместном кинопроизводстве (1992 г.), о трансграничном телевидении (1989 г.), о компьютерных преступлениях (2001 г.); Декларация Совета Европы о средствах массовой информации и правах человека (1970 г.); Рекомендации Комитета Министров государств – членов Совета Европы: № R (89)7 относительно принципов распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание от 22.04.1989 г. и № R (97)19 «О демонстрации насилия в электронных средствах массовой информации» от 30.10.1997 г.

[15] Маклюэн М. Галактика Гуттенберга: становление Человека печатающего. – М., 2005. – С. 288–295.

[16] Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П. У. Кузнецова. – С. 76.

[17] См.: Охрана интеллектуальной собственности в электронной торговле. Составитель и автор аналитического обзора Л. Г. Кравец. – М., 2001. – С. 57.

[18] Терещенко Л. К. Правовые проблемы использования Интернета в России. – С. 35.

[19] Паферова О., Соколова Е. Защита авторского права, нарушенного в Интернете. Практика российских арбитражных судов // Интеллектуальная собственность. Авторское право и смежные права. – 2009. – № 7. – С. 55.

[20] Постановление Федерального арбитражного суда Московского округа от 13.05.2008 по делу № А40-6440/07-5-68 // СПС «Гарант».

[21] Постановление Девятого арбитражного апелляционного суда от 05.02.2008 по делу № А40-6440/07-5-68 // СПС «Гарант».

[22] Постановление Президиума Высшего арбитражного суда Российской Федерации от 23.12.2008 по делу № 10962/08 // СПС «Гарант».

[23] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. Distr.: General 16 May 2011.

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

Minbaleev Aleksey Vladimirovich, Associate professor in the Department of Constitutional and Administrative Law at the South Ural State University, Associate professor in the Department of Information Law at the Ural State Law Academy, Doctor of Law. E-mail: alexmin@bk.ru

УДК 342.7.03 + 004.7.056:342.7
ББК Х401.114 + Х400.323

Кафтанникова В. М.

ОСНОВНЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБНОВЛЕННОМУ ЗАКОНОДАТЕЛЬСТВУ

В статье поднимается актуальная сегодня на практике проблема защиты персональных данных в информационных системах. Автором исследуются изменения в законодательстве в области требований к защите персональных данных.

Ключевые слова: *информационные системы, персональные данные.*

Kaftannikova V. M.

THE BASIC REQUIREMENTS TO THE PROTECTION OF THE PERSONAL DATA ON THE RENEWED LEGISLATION

In the article the actual rises today in practice problem of protection of the personal data in the informative systems. An author is investigate changes in a legislation in area of requirements to the protection of the personal data.

Keywords: *informative systems, personal data.*

Законодательная база, регламентирующая деятельность в сфере персональных данных в Российской Федерации, с каждым годом претерпевает изменения. В качестве примера можно взять главный документ о персональных данных – одноименный Федеральный закон «О персональных данных» (далее – ФЗ «О персональных данных»), в частности – последние изменения от 25 июля 2011 г. В рамках исследования изменений законодательства особый интерес представляет ст. 19 ФЗ «О персональных данных», п. 5 которой гласит, что «федеральные органы исполнительной власти … иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки»[1]. Можно заметить, что данный пункт (а также предыдущие пункты ст. 19 ФЗ «О персональных данных») стал основополагающим для утверждения новых требований к защите персональных данных при их обработке в ин-

формационных системах персональных данных[2] (далее – требования к защите персональных данных).

Сменилось и постановление Правительства Российской Федерации, устанавливающее требования к защите персональных данных (на смену постановления Правительства Российской Федерации № 781 от 17 ноября 2007 г[3]. принято новое – постановление Правительства № 1119, вступившее в силу 15 ноября 2012 г.).

Во-первых, сразу встает вопрос о документах, которые создавались в соответствии с тем или иным пунктом постановления № 781:

• Приказ ФСТЭК России № 55, ФСБ России № 86, Мининформсвязи Российской Федерации № 20 от 13.02.2008 «Об утверждении Порядка классификации информационных систем персональных данных» (зарегистрировано в Минюсте РФ 03.04.2008 № 11462)[4];

• Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»[5] (в соответствии с пунктом 3);

• «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»[6] от 14 февраля 2008 года (ФСТЭК России);

• Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»[7] от 21 февраля 2008 года (ФСБ России);

• 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» от 21 февраля 2008 года (ФСБ России).

Для многих специалистов в области защиты персональных данных открыто стоит вопрос о том, имеют ли силу данные документы, или они утратили ее с выходом в свет нового постановления Правительства РФ. Действительно, данная ситуация ввела в заблуждение работников, но, с юридической точки зрения, данные документы официально не утратили силу и должны применяться в части, не противоречащей новому акту.

Например, приказ ФСТЭК России от 05.02.2010 № 58 противоречит постановлению Правительства № 1119 в следующих пунктах:

– п. 1.4 полностью теряет смысл, поскольку ссылается на классификацию информационных систем; в пунктах 2.2, 2.11, 2.12, 3.1–3.4 упоминается класс информационной системы; классификация согласно Постановлению № 781 утратила силу; а также «методы и способы защиты информации от несанкционированного доступа в зависимости от класса информационной системы» – противоречит уже исходя из названия. Таким образом, документ, не потеряв своей юридической силы, потерял свойство полезности. Общественность ждет новых нормативно-правовых актов, которые придут на смену таким документам с отсутствием конкретики.

В рамках данного вопроса можно рассмотреть соответствие нового постановления ФЗ «О персональных данных», а именно п. 3 ст. 19, который гласит о том, что «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, требования к защите ПДН при их обработке в ИСПДН, требования к материальным носителям…». Ознакомившись с постановлением № 1119, можно заметить, что основными критериями для обеспечения защиты являются:

• объем персональных данных и их содержание;

• актуальность угроз;

• признак того, что сотрудник оператора или нет.

Вред субъекту и вид деятельности оператора во внимание не принимается.

Весьма актуальным, но не понятным со стороны непосредственного применения явилось нововведение в виде следующих дефиниций: информационная система, обрабатывающая специальные категории персональных данных; информационная система, обрабатывающая биометрические персональные данные; информационная система, обрабатывающая общедоступные персо-

нальные данные; информационная система, обрабатывающая иные категории персональных данных; информационная система, обрабатывающая персональные данные сотрудников оператора.

Что дает такая классификация информационных систем персональных данных? Специальные, биометрические и общедоступные ИСПДН закреплены в ФЗ «О персональных данных». Теперь защите подлежат общедоступные персональные данные. Конечно, можно предположить, что защита таких данных нужна во избежание их изменения или удаления, но тогда логичен вопрос о защите общедоступных источников персональных данных.

Другой момент, который вводит в заблуждение работающих с информационными системами, – наличие данных сотрудников и иные категории персональных данных (наиболее часто встречающийся пример в практике). Неужели после изменений в законодательстве оператор будет обязан разделять существующую информационную систему на 2 разных, согласно вышеуказанной классификации? Согласно принципам обработки персональных данных (п. 2 ст. 5 ФЗ «О персональных данных») «не допускается обработка персональных данных, несовместимая с целями сбора персональных данных», но в законе указано, что оператор (т. е. лицо, ответственное за законный и легитимный сбор данных) сам устанавливает цель. В данном случае простор для творчества оператора безграничен: оператор вправе установить настолько общую цель сбора данных, насколько это будет требовать экономия средств и времени. В таком случае данная классификация не будет иметь смысла.

Возвращаясь к вопросу об ИСПДН, обрабатывающей общедоступные персональные данные, стоит заметить, что, согласно законодательству, общедоступные персональные данные – полученные из общедоступных источников, либо с разрешения субъекта персональных данных. В настоящее время в Российской Федерации существует достаточно большой перечень различных реестров, содержащих персональные данные, которые можно считать общедоступными в силу законодательства – ЕГРЮЛ или ЕГРИП. Ответ на вопрос о том, будет ли законным сбор данных из таких источников, остается неоднозначным.

Вопросами, касающимися непосредственно технической терминологии, задаются многие эксперты в сфере защиты персональных данных. Например, М. Емельяненко в своем блоге[8] поднимает вопрос о законных обоснованиях таких дефиниций, как «сотрудники оператора» (мотивируя тем, что термин «работники оператора» будет более приемлемым) и «электронный журнал сообщений» и чем он отличается от «электронного журнала безопасности». Не совсем ясно, как оценка возможного вреда может сказаться на признании или непризнании наличия НДВ в системном или прикладном программном обеспечении ИСПДН. Вероятно, следует ожидать, что ответ на данный вопрос будет получен в обновленных методических документах ФСТЭК и ФСБ России[9]. Кроме того, в документе нет определения терминов системного и прикладного программного обеспечения. Необходимо определить данные дефиниции именно в исследуемом документе либо кореллирующих с ним нормативно-правовых актах. Оператор должен знать и четко понимать, чем нужно руководствоваться при выявлении недекларированных возможностей в прикладном либо системном программном обеспечении; а также осознавать, насколько широк круг вышеуказанных дефиниций.

Одним из главных нововведений постановления № 1119 является изменение принципа обеспечения соответствующего уровня защищенности персональных данных в зависимости от актуальных угроз, объема данных (убран критерий по численности в 1000 субъектов ПДН) и принадлежности данных к информационной системе персональных данных, обрабатывающих данные сотрудников оператора.

Если сравнивать два постановления по требованиям к защите персональных данных и мероприятиям по обеспечению безопасности персональных данных, то можно заметить тенденцию к сокращению таких требований.

Согласно новому постановлению, контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей не реже 1 раза в 3 года.

В постановлении № 781 устанавливалось, что безопасность персональных данных достигается путем исключения несанкционированного доступа. В постановлении № 1119 не говорится про мероприятия, касающиеся не-

санкционированного доступа, а в ст. 19 ФЗ «О персональных данных» обеспечение безопасности определяется уже совершенным действием, а именно «обнаружением фактов несанкционированного доступа к персональным данным и принятием мер».

Кроме того, в постановлении № 1119 появились требования об автоматической регистрации в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе. Также стоит заметить, что ст. 19 ФЗ «О персональных данных» в последней редакции содержит определение угроз безопасности персональных данных при их обработке.

В общем, многие требования остались прежними: методы и способы защиты информации в информационных системах устанавливаются ФСТЭК и ФСБ в пределах их полномочий; средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных; содержание электронного журнала обращений периодически.

Конечно, большой резонанс вызвала отмена многих требований в сравнении с постановлением № 781. Прекратили действовать такие требования, как: защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе; порядок проведения классификации информационных систем устанавливается совместно ФСТЭК, ФСБ и Минкомсвязи; возможные каналы утечки информации при обработке персональных данных в информационных системах определяются ФСТЭК и ФСБ в пределах их полномочий; многие другие требования, связанные с конкретными действиями по защите безопасности информационных систем персональных данных, перестали быть актуальными. Вероятно, с одной стороны, можно увидеть в этом позитивную сторону, но, в противном случае, на сегодняшний день вся ответственность по защите лежит на операторе ПДН, кроме того, отсутствует сама методология защиты данных.

Как отмечают специалисты по защите персональных данных, новый документ не привнес в их деятельность ничего нового и конкретного: «та же оценка соответствия, тот же непонятный электронный журнал, то же требование утверждения списка допущенных лиц, то же требование установления режима безопасности в помещениях, та же отсылка к нормативным документам ФСТЭК и ФСБ»[10].

Таким образом, можно сделать вывод, что постановление Правительства № 1119 вступит в полную силу при наличии соответствующих документов регуляторов в сфере персональных данных – ФСТЭК и ФСБ по поводу методики определения актуальных угроз безопасности для информационных систем персональных данных.

Примечания

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

[2] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. – 2012. – № 45. – Ст. 6257.

[3] Постановление Правительства РФ от 17.11.2007 № 781 ««Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. – 2007. – № 48 – (2 ч.). – Ст. 6001.

[4] Приказ ФСТЭК России № 55, ФСБ России № 86, Мининформсвязи Российской Федерации № 20 от 13.02.2008 «Об утверждении Порядка классификации информационных систем персональных данных» // Российская газета. – 2008. – 12 апр. – № 80.

[5] Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» // Российская газета. – 2010. – 05 март. – № 46.

[6] «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утв. ФСТЭК РФ 14.02.2008 // Документ опубликован не был.

[7] «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 // Документ опубликован не был.

[8] Емельяненко М. – http://dlp-expert.ru/blog/50/24521

[9] НТЦ Вулкан. – http://www.ntc-vulkan.ru/netcat_files/File/Vulkan_1119_nov_2012.pdf

[10] Лукацкий А. – http://lukatsky.blogspot.ru/2012/11/781-1119.html

---

Кафтанникова В. М., аспирант кафедры конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: irinakuldybaeva@mail.ru

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

УДК 004.056 + 342.518:004.7.056
ББК Х401.114 + Х401.011.2

Кулдыбаева И. У.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В статье поднимается актуальная сегодня на практике проблема обеспечения информационной безопасности электронного правительства. Автором исследуются угрозы безопасности информации, обрабатываемой в органах государственной власти, исследуются меры защиты и направления государственной политики в области обеспечения информационной безопасности электронного правительства.

Ключевые слова: *информационная безопасность, электронное правительство, защита.*

Kuldybaeva I. U.

PROVIDING OF INFORMATIVE SAFETY OF ELECTRONIC GOVERNMENT

In the article the actual rises today in practice problem of providing of informative safety of electronic government. An author is investigate the threats of safety to the information processed in public authorities , the measures of defence and direction of public policy are investigated in area of providing of informative safety of electronic government.

Keywords: *informative safety, e-Government, protection.*

Концепция формирования в Российской Федерации электронного правительства[1] предусматривает оказание государственных услуг населению с использованием современных информационно-коммуникационных технологий, что подразумевает создание специализированной телекоммуникационной инфраструктуры на базе единого оператора.

Целью построения технологической платформы электронного правительства является создание защищенной телекоммуникационной сети, обеспечивающей автоматическое информационное взаимодействие между функциональными компонентами инфраструктуры электронного правительства. Телекоммуникационная инфраструктура должна обеспечить равный и безопасный доступ к функциям электронного правительства для всех абонентов.

Обеспечение требуемого уровня информационной безопасности электронного правительства при его функционировании определено в качестве одной из целей создания электронного правительства. Ст. 14 ч. 9 Федерального закона от 27 июля 2006 № 149-ФЗ «Об информации, информационных техноло-

гиях и о защите информации»[2] определена обязанность государственных органов, определенных в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обеспечить защиту информации, содержащейся в данной информационной системе, от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Система обеспечения информационной безопасности выступает в качестве инженерного вспомогательного элемента единого комплекса в составе инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг[3].

Защита персональных данных граждан, конфиденциальных сведений юридических лиц, служебной информации ограниченного распространения государственных и муниципальных органов должна иметь первостепенное значение при проектировании и реализации инфраструктурных элементов и информационных систем электронного правительства[4]. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» система обеспечения информационной безопасности состоит из правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

Таким образом, должна быть сформирована как инфраструктура, обеспечивающая информационную безопасность электронных форм взаимодействия органов государственной власти между собой, с населением и организациями, обеспечения доверия к электронной подписи, так и правовое обеспечение информационной безопасности в данной области правоотношений.

Предоставление государственных услуг в электронном виде, имеющих правовые последствия, требует создания системы юридически значимого электронного документооборота между заявителем и органами государственной власти. Существенным требованием является необходимость обеспечения юридической значимости передаваемой информации, в том числе за счет идентификации и аутентификации пользователей при доступе к информационным ресурсам и автоматизированным рабочим местам.

Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» должна обеспечивать санкционированный доступ участников информационного взаимодействия в единой системе идентификации и аутентификации к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах[5].

В рамках реализации постановления Правительства РФ от 28.11.2011 г. № 977 о федеральной государственной информационной системе ЕСИА Минкомсвязью России был разработан ряд нормативно-технологических документов, касающихся ее функционирования: положение о ЕСИА, утвержденное приказом Минкомсвязи России от 13.04.2012 г. № 107, методические рекомендации по использованию ЕСИА, регламент взаимодействия при использовании ЕСИА.

ЕСИА предназначена:

• для обеспечения доступа заявителей к электронным ресурсам и услугам, предоставляемым на всех государственных порталах, без необходимости повторной регистрации на основе единых идентификационных параметров с использованием различных носителей: СНИЛС и пароль, электронная подпись, SIM-карта или смарт-карта;

• для обеспечения доступа уполномоченных лиц органов исполнительной власти ЕСИА к государственным информационным ресурсам;

• для обеспечения авторизации ведомственных информационных систем при межведомственном электронном взаимодействии с использованием системы межведомственного электронного взаимодействия.

Основными принципами межведомственного электронного документооборота в том числе являются обеспечение целостности передаваемой информации и обеспечение конфиденциальности информации[6].

В целях исполнения своих функций система межведомственного электронного взаимодействия обеспечивает[7]:

• получение, обработку и доставку электронных сообщений в рамках информационного взаимодействия органов и организаций с обеспечением фиксации времени передачи, целостности и подлинности электронных сообщений, указания их авторства и возможности предоставления сведений, позволяющих проследить историю движения электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме;

• защиту передаваемой информации от несанкционированного доступа, ее искажения или блокирования с момента поступления указанной информации в систему взаимодействия до момента передачи ее в подключенную к системе взаимодействия информационную систему.

Информационная безопасность при осуществлении межведомственного электронного документооборота обеспечивается комплексом технических и организационных мероприятий. Технические мероприятия предусматривают использование сертифицированных по требованиям безопасности средств защиты информации и обеспечение целостности обрабатываемых данных.

К организационным мероприятиям относятся:

• контроль выполнения требований нормативных документов, регламентирующих обеспечение защиты информации;

• определение должностных лиц, ответственных за обеспечение информационной безопасности;

• установление порядка резервного копирования, восстановления и архивирования баз данных, а также порядка обновления антивирусных баз;

• установление порядка допуска для проведения ремонтно-восстановительных работ программно-технических средств;

• организация режимных мероприятий в отношении помещений, в которых размещены технические средства этих узлов межведомственного электронного документооборота.

Организация защищенного канала передачи данных должна быть осуществлена с использованием сертифицированных по требованиям безопасности шифровальных (криптографических) средств защиты информации.

Доступ должностных лиц органов и организаций к информационным ресурсам информационных систем иных органов и организаций и элементам инфраструктуры взаимодействия, а также доступ заявителей к информационным ресурсам предоставляется при условии прохождения идентификации, аутентификации и авторизации в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

В единой системе идентификации и аутентификации санкционированный доступ к информации должен осуществляться посредством использования простых электронных подписей и усиленных квалифицированных электронных подписей в порядке, устанавливаемом Правительством Российской Федерации, должностными лицами органов власти и иных организаций и заявителями.

Технология электронной подписи позволяет обеспечить:

• Аутентификацию граждан, подключающихся к ресурсам;

• Проверку подлинности ресурсов, к которым подключаются граждане;

• конфиденциальность данных, передаваемых по общедоступным сетям;

• Аутентификацию отправителя и обеспечение гарантии;

• Авторство и подлинность сообщения.

Защита информации должна осуществляться в соответствии с требованиями, установленными Правительством РФ и компетентными органами, в частности, Федеральной службой безопасности РФ, Федеральной службой по техническому и экспортному контролю, Министерством связи и массовых коммуникаций и другими уполномоченными органами.

При этом необходимо учитывать, что угрозы безопасности инфраструктуры «электронного правительства», как крупнейшей в России государственной информационной системы, имеют широчайший спектр. Это могут быть внутренние угрозы (со стороны людей, имеющих доступ к инфраструктуре «электронного правительства»), внешние (со стороны внешних по отношению к системе пользователей, киберпреступников, кибер-

спецслужб), а также угрозы стихийного характера (потеря информации вследствие техногенных катастроф, природных катаклизмов). Поэтому при проектировании системы обеспечения информационной безопасности для инфраструктуры «электронного правительства» упор был сделан на комплексный подход. Система интегрирует разнородные средства защиты информации, необходимые для нейтрализации угроз безопасности для всех ее компонент, в единую взаимосвязанную среду, обеспечивающую выполнение целевых задач по информационной безопасности.

Основную платформу инфраструктуры электронного правительства составляет телекоммуникационная инфраструктура ОАО «Ростелеком» – защищенная сертифицированная корпоративная система передачи данных. Все внутренние каналы связи в рамках инфраструктуры «электронного правительства» защищены средствами криптографической защиты; каждая система «электронного правительства» имеет свою подсистему обеспечения информационной безопасности; вместе с внедрением этих систем создается подсистема мониторинга и управления информационной безопасностью.

Примечания

[1] Концепция формирования в Российской Федерации электронного правительства до 2010 года. Утв. распоряжением Правительства Российской Федерации от 6 мая 2008 г. № 632-р // Собр. законодательства Рос. Федерации. – 2008. – № 20. – Ст. 2372.

[2] Собр. законодательства Рос. Федерации. – 2006. – № 31 (1 ч.). – Ст. 3448.

[3] Положение «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Утв. постановлением Правительства РФ от 8 июня 2011 г. № 451 // Собр. законодательства Рос. Федерации. – 2011. – № 24. – Ст. 3503.

[4] Более подробнее о защите персональных данных см.: Кулдыбаева И. У. Обеспечение безопасности персональных данных в условиях развития электронного правительства // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (4). – С. 20–24.

[5] Требования к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Утв. постановлением Правительства РФ от 28 ноября 2011 г. № 977 // Собр. законодательства Рос. Федерации. – 2011.. – №49 (ч. 5). – Ст. 7284.

[6] Положение о системе межведомственного электронного документооборота. Утв. постановлением Правительства РФ от 22 сентября 2009 г. № 754 // Собр. законодательства Рос. Федерации. – 2009. – № 39. – Ст. 4614.

[7] Положение «О единой системе межведомственного электронного взаимодействия». Утв. постановлением Правительства РФ от 8 сентября 2010 г. № 697. // Собр. законодательства Рос. Федерации. – 2010. – № 38. – Ст. 4823.

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

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

УДК 349.22 + 342.7:349.22 + 004.7.056
ББК Х400.7 + Х405.11:Х401.114

Станскова У. М.

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ТРУДОВЫХ ОТНОШЕНИЯХ

В статье поднимается актуальная сегодня на практике проблема защиты персональных данных в трудовых отношениях. Автором дается анализ норм трудового права, регулирующих обработку персональных данных. Исследуются отдельные проблемы защиты персональных данных.

Ключевые слова: *персональные данные, информация ограниченного доступа, трудовые отношения, персональные данные работника.*

Stanskova U. M.

PROBLEMS OF PROTECTION OF THE PERSONAL DATA ARE IN LABOUR RELATIONS

In the article the actual rises today in practice problem of protection of the personal data in labour relations. An author is give the analysis of norms of labour right, regulative treatment personal data. The separate problems of protection of the personal data are investigated.

Keywords: *personal data, information limit access, labour relations, personal data of worker.*

Необходимость применения в трудовых отношениях Федерального закона «О персональных данных»[1] и иных нормативных правовых актов в этой сфере обусловливает ряд трудностей для работодателей. Наличие в Трудовом кодексе РФ[2] главы 14, посвященной защите персональных данных, не устраняет проблем правового регулирования данного вида информации.

Во-первых, ТК РФ и Закон № 152-ФЗ используют различный понятийный аппарат. В частности, возникает вопрос о соотношении специальных категорий персональных данных (Закон № 152-ФЗ) и сведений о частной жизни работника (ч. 4 ст. 86 ТК РФ). Очевидно, что персональные данные включают в себя информацию о частной жизни работника.

Определяя специальные категории персональных данных, законодатель пошел по пути казуистического перечисления: это персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной

жизни (п. 1 ст. 10 Закона № 152-ФЗ). Признаки указанной категории персональных данных в Законе не выделены. Из анализа содержания специальных категорий персональных данных следует, что они касаются интимных сторон жизни субъекта данных, зоны особой чувствительности и зоны эмоционального комфорта их субъекта. Действия с этими персональными данными без должных гарантий обеспечения прав субъектов персональных данных могут нанести ему повышенный ущерб[3]. В связи с чем напрашивается вывод об отнесении к специальным категориям персональных данных информации о частной жизни субъекта. В. П. Иванский пишет, что именно эта категория получила название «персональные данные» и была квалифицирована как информация, несанкционированный доступ или ненадлежащее использование которой приводит к посягательствам на права частной жизни субъекта данных[4]. Очевидно, что данные специальной категории составляют информацию о частной жизни субъекта. На первый взгляд несколько иначе обстоит дело с информацией о судимости, так как судимость представляет собой последствие осуждения и назначения наказания со стороны государства и может повлечь ряд неблагоприятных последствий, а потому должна быть публичной. Однако действия, направленные на совершение преступления, являются внутренним выбором субъекта, а значит, относятся к его частной жизни. В п. 1 ст. 10 Закона № 152-ФЗ сведения о судимости прямо не названы как специальные категории, но на возможность их обработки указано в п. 3 статьи. Из чего следует, что такие сведения относятся к специальным категориям.

Согласно новой редакции п. 2 ст. 10 Закона № 152-ФЗ работодатель вправе обрабатывать специальные категории данных в соответствии с трудовым законодательством. Однако в ТК РФ термин «специальные категории» не употребляется, следовательно, отсутствует запрет на их обработку. В п. 4 и 5 ст. 86 ТК РФ предусмотрен запрет обработки отдельных сведений работника: о частной жизни, о политических, религиозных и иных убеждениях; о членстве в общественных объединениях или профсоюзной деятельности работника. Очевидно, что перечень сведений специальной категории шире, чем тех сведений, обработка которых запрещена по ТК РФ. Кроме того, сведения, составляющие частную жизнь, требуют дополнительного уточнения. На необходимость закрепления в ТК РФ развернутого перечня сведений, которые не могут быть истребованы от работника, указывает А. М. Лушников[5].

В целях приведения трудового законодательства в соответствие с Законом № 152-ФЗ считаем необходимым предусмотреть в ст. 86 ТК РФ запрет на обработку специальных категорий персональных данных, предусмотренных федеральными законами, в том числе сведений о частной жизни работника.

В силу ст.ст. 65, 331 и ст. 351.1 ТК РФ при поступлении на работу предоставляются сведения о наличии судимости или факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям. И. Н. Басаргин рассматривает сведения о наличии судимости как тесно связанные с публичной сферой и подлежащие передаче работодателю по его требованию[6]. Однако, на наш взгляд, по вопросу получения информации о судимости работника ситуация не столь однозначна, как с другими публичными сведениями. Для их обработки работодателем необходимо, чтобы такие сведения относились к вопросу о возможности выполнения работником его трудовой функции (ст. 88 ТК РФ) в силу федерального закона, которым предусмотрен запрет на допуск к работе лиц, имеющих или имевших судимость, подвергающихся или подвергавшихся уголовному преследованию (ч. 1 ст. 65 ТК РФ). К информации, которая также может потребоваться в трудовых отношениях, относятся сведения о наличии (отсутствии) запретов на занятие определенной должности или на осуществление определенных видов деятельности при применении ст.ст. 65, 331, 351.1, п. 4, 8 и 9 части первой ст. 83 и ст. 84 ТК РФ. Однако получить подобного рода информацию для работодателя в силу законодательства о персональных данных от третьих лиц невозможно, за исключением сведений о дисквалификации. Порядок предоставления информации, содержащейся в реестре дисквалифицированных лиц, осуществляется в соответствии с Постановлением Правительства РФ 11 ноября 2002 г. № 805 «О формировании и ведении реестра дисквалифицированных лиц»[7]. В других случаях решение о сообщении или несообщении таких сведений зависит от желания работника. На практике у работодателей нередко возникают проблемы с получением информации о наличии в отношении работника обвинительного при-

говора суда о назначении наказания, исключающего продолжение прежней работы или поступления на работу. Наличие данной информации связывается с возможностью прекращения трудового договора по п. 4 ст. 83 и ст. 84 ТК РФ. Невозможность получения работодателем соответствующей информации ставит под сомнение реализацию уголовных наказаний в виде лишения права занимать определенные должности или права заниматься определенной деятельностью. Поэтому считаем необходимым вести реестр лиц, осужденных к наказанию в виде лишения права занимать определенные должности или заниматься определенной деятельностью, по аналогии с реестром дисквалифицированных лиц.

Следовательно, специальные категории персональных данных работника – это информация о частной жизни работника, касающаяся его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, факта уголовного преследования и судимости, в отношении которых устанавливается режим ограниченного доступа, получение и обработка которой не допускается, за исключением случаев, предусмотренных федеральным законом.

Во-вторых, Закон № 152-ФЗ закрепляет дихотомическое деление персональных данных по доступу на общедоступные персональные данные (пп. 10 части 1 ст. 6) и персональные данные, обеспеченные в режиме конфиденциальности (ст. 7). Однако в ТК РФ подобное деление не прослеживается. В связи с чем возникает проблема с определением тех персональных данных работника, в отношении которых не требуется или невозможно установление режима конфиденциальности. На практике имел место следующий случай: работодатель поздравил работницу с юбилеем, организовал публичное поздравление, а работница расценила действия работодателя как разглашение ее персональных данных и обратилась в суд.

По смыслу ст. 7 Закона № 152-ФЗ все персональные данные должны обеспечиваться в режиме конфиденциальности, в том числе паспортные данные, фамилия, имя, отчество, возраст, место регистрации и жительства, пол, образование, профессия и др. В трудовых отношениях такое правило порождает ряд трудностей. Например, работник требует обеспечения конфиденциальности сведений о его профессии, специальности, квалификации, занимаемой должности. Данные сведения необходимы для осуществления трудовой функции, а потому не могут быть скрыты от других работников и носят публичный (общеизвестный) характер. В п. 10 части 3 ст. 6 Закона № 152-ФЗ допускается обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных или по его просьбе (общедоступных персональных данных). В прежней редакции Закона № 152-ФЗ предусматривалось также, что данные являются общедоступными в силу федерального закона. В новой редакции такого указания нет[8]. Конкретный список общедоступных персональных данных содержит Закон Испании «О защите персональных данных»[9] в котором в качестве общедоступных источников данных названы списки лиц по профессиям, содержащие только информацию об именах, званиях, профессии, роду деятельности, ученой степени, адресе и указание на принадлежность к этим группам. С. Ю. Головина выделяет в составе персональных данных две составляющие: публичную и частную. Публичная составляющая подлежит передаче работодателю по его просьбе, частная составляющая может быть разглашена лишь с волеизъявления работника[10]. Осуществление трудовых отношений связано с обработкой определенной публичной информации о работнике, поэтому в ТК РФ должен быть предусмотрен перечень общедоступных (публичных) персональных данных работника. В качестве таковых предлагается закрепить в ТК РФ фамилию, имя, отчество, пол, сведения о месте регистрации, образовании, профессии, квалификации работника, если федеральным законом не требуется установления режима ограниченного доступа таких сведений. Наличие такой нормы в ТК РФ позволит избежать появления на практике следующих вопросов: можно ли указывать в трудовом договоре работника, принимаемого на время отсутствия другого работника, фамилию, имя и отчество работника, которого он заменяет? В силу действующего законодательства необходимо получить письменное согласие. Такая же проблема возникает с размещением в общедоступных местах табличек с указанием ответственных за технику безопасности и охрану труда, при размещении информации на бейджах работников и т.д.

Приведем пример судебной практики. Т. был уволен по пп. «в» п. 6 части первой ст. 81 ТК РФ за направление истцом по электронной почте объяснительных записок работников на свой электронный адрес. В судебном заседании было определено, что действия Т. не были направлены на передачу персональных данных другим лицам или на ознакомление с персональными данными неограниченного круга лиц. Судом установлено, что объяснительные записки работников К., К., А., П. и Т. содержат фамилии работников, их инициалы и должности. Поскольку данные работники, находясь на рабочем месте, носят бейджи, на которых открыто размещены вышеуказанные сведения, персональные данные, содержащиеся в вышеуказанных объяснительных записках, следует считать общедоступными. Суд приходит к выводу об отсутствии у ответчика оснований для увольнения истца[11]. В приведенном случае отсутствовал сам факт разглашения – сведения, содержащиеся в объяснительных записках, не были сообщены неуполномоченным лицам. Однако в объяснительных записках могла содержаться и другая информация, составляющая конфиденциальные персональные данные.

В-третьих, ТК РФ предоставляет защиту только части персональных данных – персональным данным работника. Отсюда увольнение работника по пп. «в» п. 6 части первой ст. 81 ТК РФ возможно только за разглашение персональных данных другого работника. Так, в прессе обсуждалось распространение работниками отеля «Мариотт Гранд» информации о поведении футболистов, проживавших в этом отеле, перед ответственным матчем со Словенией, в результате служащий был уволен администрацией отеля[12]. Очевидно, что подобного рода информация касается частной жизни и может быть отнесена к персональным данным, а работники отеля не вправе были распространять подобного рода информацию без согласия ее субъекта. Однако указанные персональные данные не являются персональными данными другого работника, поэтому увольнение такого работника по пп. «в» п. 6 части первой ст. 81 ТК РФ не представляется возможным.

Приведем пример судебной практики. Р. была уволена по подп. «в» п. 6 части первой ст. 81 ТК РФ за разглашение персональных данных: предоставление своей дочери для обращения в суд копий рабочих ведомостей, содержащих сведения о вознаграждении лицам, заключившим договоры подряда. Суд принял во внимание доводы истца о том, что те сведения, которые содержались в предоставленных Р. ведомостях, не являются персональными данными работников предприятия. Однако в Положении МУП об обработке и защите персональных данных, с которым была ознакомлена под роспись Р., под работниками подразумеваются лица, заключившие трудовой договор с МУП «ССС». По мнению суда, лица, заключившие договоры подряда с МУП «ССС», его работниками в смысле трудового законодательства не являются, так как трудового договора с ними не заключалось. Таким образом, данные лица не относятся к тем, чьи персональные данные подлежат защите в соответствии с Трудовым кодексом и Положением об обработке и защите персональных данных работников. Следовательно, к дисциплинарной ответственности в виде увольнения Р. привлечена неправомерно[13].

Выходом из сложившейся ситуации могло бы быть отнесение персональных данных лиц, не являющихся работниками, к иным видам охраняемой законом тайны, например, служебной. Однако в данном случае возможно отнесение к тайне сведений, потенциальная ценность которых незначительна, например, фамилия, имя и отчество. Представляется, что при доказанности действительной или потенциальной коммерческой ценности обеспечения конфиденциальности персональных данных клиентов, контрагентов они могут быть отнесены к режиму коммерческой тайны. Однако при отсутствии таковой персональные данные других лиц должны обеспечиваться в режиме конфиденциальности в соответствии с Законом № 152-ФЗ. Нарушение данного требования является основанием для привлечения работодателя к ответственности. Поэтому видится необходимость расширения объекта, защищаемого трудовым правом на информацию ограниченного доступа, в состав которой войдут как охраняемые законом тайны, так и иные виды информации, в том числе персональные данные, без конкретизации их субъекта.

В-четвертых, в пп. «в» п. 6 части первой ст. 81 ТК РФ использована не совсем ясная формулировка «охраняемая законом тайна … в том числе персональные данные другого работника», что ставит вопрос о том, за разглашение каких персональных данных возможно увольнение. Верховный Суд РФ указывает только на «относимость» разглашенных пер-

сональных данных к персональным данным другого работника. Очевидно, что сообщение общедоступных сведений не может быть расценено в качестве разглашения, так как такие сведения фактически не могут сохраняться в режиме конфиденциальности в трудовых отношениях. Представляется, что серьезные правовые последствия должны влечь разглашение или неправомерное использование только тех персональных данных, которые подпадают под состав охраняемой законом тайны и специальных категорий персональных данных, в отношении которых обладателем установлен режим конфиденциальности, что должно найти свое отражение в ТК РФ.

За нарушение законодательства о персональных данных по нормам ТК РФ применение полной материальной ответственности не предусмотрено. Пункт 7 части первой ст. 243 ТК РФ применяется только в отношении охраняемой законом тайны. Такое положение также не способствует эффективной защите персональных данных в трудовых отношениях и требует уточнения формулировки данной нормы по аналогии с предложенной ранее редакцией пп. «в» п.6 части первой ст. 81 ТК РФ.

Также следует поставить вопрос об изменении традиционного подхода к дисциплинарной ответственности работника, наступление которой возможно только за проступки, совершенные в рабочее время. Принимая во внимание особенность охраняемого объекта – информации ограниченного доступа, ответственность к работнику должна быть применена вне зависимости от времени разглашения – до или после рабочего времени. Такой подход позволит обеспечить эффективное правовое регулирование и защиту информации ограниченного доступа, в том числе персональным данным, так как их разглашение часто совершается во внерабочее время.

В-пятых, внесение изменений в ст. 6 Закона № 152-ФЗ[14] обусловило проблему получения согласия работника на обработку его персональных данных в трудовых отношениях. В прежней редакции данной статьи четко разграничивались случаи, когда допускается обработка персональных данных без согласия их субъекта. В частности, к таковым относилась обработка в целях осуществления договора, стороной которого является субъект персональных данных. Поэтому при заключении трудового договора согласия на обработку персональных данных работника не требовалось. Неопределенность новой редакции ст. 6 требует получения согласия на обработку персональных данных работника в трудовых отношениях. Отсюда на практике возникают ситуации, когда работники такого согласия не дают, что делает невозможным исполнение работодателем его обязанностей по заключению трудового договора, оформлению трудовых отношений, по оплате труда работника и т. д. Поэтому норма об обработке персональных данных по договору без дополнительного письменного согласия субъекта должна быть возвращена в законодательство.

В силу ст. 88 ТК РФ предоставление персональных данных работника третьей стороне возможно только с письменного согласия работника. При проведении аттестации работника в состав комиссии могут входить приглашенные работодателем эксперты, которые и выступают в качестве третьей стороны. Следовательно, предоставление таким экспертам персональных данных аттестуемого работника возможно только с его письменного согласия. На практике работник может злоупотребить своим правом и отказаться от дачи согласия, что сделает невозможным проведение аттестации. В ст. 88 ТК РФ обозначены исключения из правила о предоставлении персональных данных работника третьей стороне с письменного согласия работника: 1) когда их обработка необходима в целях предупреждения угрозы жизни и здоровью работника; 2) в других случаях, предусмотренных ТК РФ и иными федеральными законами. Рассмотренный нами случай не подпадает под данные исключения. Следовательно, в ТК РФ должно быть сделано соответствующее исключение.

В-шестых, следует отметить отсутствие в ТК РФ такого важного условия, как необходимость обеспечить режим ограниченного доступа персональных данных. Указанное условие должно быть предусмотрено в ст. 86 ТК РФ в числе требований к их обработке и защите, а также в ст. 89 в виде права работника на обеспечение конфиденциальности его персональных данных.

В трудовых отношениях для работодателя интерес представляют данные о состоянии здоровья работника, которые относятся к частной жизни и специальным категориям. Ст. 88 Трудового кодекса РФ запрещает работодателю запрашивать информацию о состо-

янии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником своей трудовой функции. Работник должен проходить обязательные предварительные, периодические и внеочередные медицинские осмотры по нормам ст. 69 и 213 ТК РФ. Согласие на прохождение таких медицинских осмотров выражается в самом факте поступления на работу, предусматривающую их прохождение. При прохождении медицинского обследования работодателю не должна быть предоставлена информация о конкретных заболеваниях работника, так как решается вопрос только о возможности выполнения работы или наличии противопоказаний для ее выполнения. Иначе будет нарушено требование законодательства о сохранении врачебной тайны. Отсюда следует, что прохождение обязательных и периодических медицинских осмотров нельзя рассматривать как обязанность предоставить сведения о состоянии здоровья, а только как обязанность предоставить сведения об отсутствии противопоказаний для допуска к работе. При оформлении листков нетрудоспособности конфиденциальность диагноза обеспечивается следующими нормами: 1) в строке «причина нетрудоспособности» указывается двузначный код; 2) в некоторых медицинских организациях могут быть использованы специальные печати или штампы без указания профиля организации[15].

По вопросу защиты информации о здоровье работника представляет интерес Кодекс практики МОТ по защите персональных данных работников[16]. В соответствии с п. 6.7 персональные данные медицинского характера не должны собираться работодателем за исключением тех случаев, когда это не противоречит национальному законодательству, сохранению врачебной тайны и общим принципам профессионального здравоохранения и безопасности, и только тогда, когда необходимо: a) определить, подходит ли данный работник для выполнения конкретной работы; b) выполнять требования профессионального здравоохранения и безопасности; и c) определять право на пособия по социальному страхованию и их предоставление.

Системное толкование норм ТК РФ и Закона № 152-ФЗ позволяет выделить условия, при которых в трудовых отношениях допускается обработка персональных данных о состоянии здоровья работника: 1) сведения обрабатываются в соответствии с трудовым законодательством (пп. 2.3. п. 2 ст. 10 Закона); 2) сведения относятся к вопросу о возможности выполнения трудовой функции и осуществления прав и гарантий работников (ст. 88 ТК РФ); 3) работник дал согласие в письменной форме на обработку информации о состоянии здоровья (пп. 1 п. 2 ст. 10 Закона и п. 4 ст. 86 ТК РФ); 4) если обработка данных сведений необходима работодателю для защиты жизни и здоровья работника и защиты жизненно важных интересов других лиц, а получение согласия субъекта невозможно (пп. 3 п. 2 ст. 10 Закона).

Согласно ст. 241 ТК РФ работник обязан немедленно сообщить работодателю об ухудшении состояния своего здоровья, в том числе проявлении признаков острого профессионального заболевания (отравления). В связи с чем многие работодатели закрепляют в своих локальных актах обязанность работника известить о невыходе на работу по состоянию здоровья. Например, Челябгортранс предусматривал соответствующее правило в правилах внутреннего трудового распорядка, но государственная инспекция труда определила данное требование как неправомерное. Приведем противоположное решение в аналогичной ситуации. Г. обратилась в суд с иском к ОАО в части отмены дисциплинарного взыскания – замечания за нарушение Должностной инструкции инженера-технологу цеха дезактивации и Правил внутреннего распорядка работников, выразившееся в неизвещении непосредственного руководителя о причинах отсутствия на рабочем месте по причине болезни. Суд не нашел оснований для удовлетворения исковых требований и полагает, что требование правил внутреннего трудового распорядка не нарушает индивидуальные права работника, поскольку обеспечивает реализацию контрольной функции работодателя за соблюдением работником трудовой дисциплины и исполнения трудового договора[17].

Согласно пп. 1 и 2.3 части 2 ст. 10 Закона и п. 4 ст. 86 ТК РФ обработка специальных категорий персональных данных допускается при наличии письменного согласия их субъекта. Однако в трудовых отношениях должны быть предусмотрены случаи, когда обработка специальных категорий персональных данных возможна без такого согласия. В частности, при обработке их персональных данных о состоянии здоровья в ст. 86.1. ТК РФ следует

предусмотреть закрытый перечень случаев, когда допускается получение и обработка таких сведений без письменного согласия работника, а именно: 1) для прохождения обязательных предварительных, периодических и внеочередных медицинских осмотров и психиатрических освидетельствований; 2) при необходимости перевода и прекращения трудового договора по медицинскому заключению, а также при отстранении от работы; 3) при получении увечья или профессионального заболевания, при несчастном случае на производстве; 4) о периодах временной нетрудоспособности (для выплаты пособия по временной нетрудоспособности). В иных случаях обработка персональных данных о состоянии здоровья работника и членов его семьи, а также других специальных категорий персональных данных допускается только с согласия (или по заявлению) работника в целях предоставления гарантий и льгот, предусмотренных действующим законодательством.

На практике часто возникает необходимость получения работодателем информации об инвалидности работника, подтверждения его больничного листа. Например, ФГУ ДЭП № 246 обратилось в суд с иском к ФГУ «Главное бюро медико-социальной экспертизы по Магаданской области» об обязании предоставления сведений об инвалидности работника предприятия В. В. длительное время болела, вследствие чего ей был предоставлен листок нетрудоспособности, по которому В. с 13 ноября 2008 года является инвалидом 2 группы. В. отказалась предоставить администрации предприятия соответствующие документы, определяющие возможность выполнения ею трудовых функций. Суд первой инстанции пришел к выводу о том, что требования истца удовлетворению не подлежат: гражданин, признанный инвалидом, самостоятельно решает, предоставлять работодателю разработанную для него программу реабилитации или не предоставлять. Соответствующую информацию работодателю следует запрашивать у такого гражданина. Судебная коллегия оставила кассационную жалобу без удовлетворения[18].

В зарубежной практике управления персоналом распространение получило генетическое тестирование. Генетические тесты призваны сделать гипотетический прогноз будущих болезней и врожденных пороков испытуемого лица[19]. Так, 39-летняя Памела Финк сейчас судится со своим бывшим работодателем, уволившим ее на основании генетических тестов. Ее понизили в должности, а затем и вовсе указали на дверь после того, как генетические исследования показали предрасположенность к раку молочной железы. Она является носительницей гена BRCA2, и шанс, что она заболеет раком, составлял 80%[20]. В США вступает в силу новый Закон о недопущении дискриминации в связи с генетической информацией. Один из эпизодов, способствовавших принятию закона, произошел в железнодорожной компании, которая без разрешения работников проводила генетическое тестирование. Выяснилось, что руководство компании проводило генетическое тестирование на предрасположенность работников к различным заболеваниям (включая запястный синдром) с целью оправдать снижение компенсационных выплат работникам, получившим производственные травмы[21]. Новый Закон США запрещает работодателю требовать от работника прохождения генетических тестов, кроме установленных законом случаев[22]. В Австрии применение таких тестов должно быть предметом переговоров руководства предприятия с производственным советом; во Франции по решению заводского врача; в Финляндии законодательство требует от работодателей учет риска повреждения генов при приеме на работу[23]. Кодекс практики МОТ по защите персональных данных рекомендует запретить или ограничить проведение генетических тестирований работников. В России соответствующие запреты отсутствуют, поэтому их проведение возможно, в том числе, в рамках прохождения медицинских осмотров. Аргумент за проведение таких тестирований – сохранение здоровья работника. Против проведения генетических тестирований выступает то, что наличие генетической предрасположенности к болезни не означает реальное наступление заболевания. В конечном счете, работник должен сам решать, подвергать свое здоровье риску, связанному с работой в определенных условиях, или нет. На наш взгляд данный вопрос должен найти свое правовое регулирование с установлением общего запрета на проведение таких тестирований и определения исчерпывающего перечня случаев их проведения.

В заключение рассмотрим еще один пример нарушения работодателем требований к обработке персональных данных. Г. обратил-

ся в суд с иском о признании незаконными действий СТУ в части порядка сбора (получения) сведений, относящихся к персональным данным государственного гражданского служащего. Г. является государственным гражданским служащим ИФНС г. Магнитогорска Челябинской области. Он узнал, что в ИФНС поступило письмо СТУ (прежнего работодателя) о предоставлении в отношении него копий приказа о назначении на должность и копии трудовой книжки. Данные сведения были инспекцией направлены в адрес СТУ без его согласия. Суд признал действия ИФНС о передаче Сибирскому таможенному управлению персональных данных государственного гражданского служащего Г. без его согласия незаконными и взыскал компенсацию морального вреда 800 рублей. В иске о признании действий и бездействия Сибирского таможенного управления незаконными, взыскании с Сибирского таможенного управления компенсации морального вреда Г. отказал[24]. При оценке данного решения следует указать на норму ст. 64.1 ТК РФ, предписывающую работодателю сообщить бывшему нанимателю государственного и муниципального служащего о заключении с таковым трудового договора. Поэтому, если соответствующий запрос был сделан в рамках данной нормы, то действия правомерны.

Таким образом, анализ правового регулирования защиты персональных данных в трудовых отношениях выявил ряд проблем, препятствующих эффективной защите данного вида информации. В целях совершенствования механизма защиты персональных данных необходимо расширить объект, охраняемый трудовым правом, и ввести в ТК РФ категорию «информация ограниченного доступа», в состав которой войдут любые персональные данные (не только персональные данные работника). Следует привести понятийный аппарат ТК РФ в соответствие с Законом №152-ФЗ и включить в ТК РФ понятие «специальные категории персональных данных работника», а также закрепить правила по обработке сведений о состоянии здоровья работника. Требуется уточнение норм, предусматривающих дисциплинарную и материальную ответственность работников за разглашение персональных данных (пп. «в» п. 6 части первой ст. 81 и п. 7 части первой ст. 243 ТК РФ). Также следует предусмотреть возможность применения трудоправовой ответственности за разглашение информации ограниченного доступа, совершенное как в рабочее, так и во внерабочее время.

Примечания

[1] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (ч.1) (далее – Закон № 152-ФЗ).

[2] Трудовой кодекс РФ от 30 декабря 2001 г. № 197-ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 3. (далее – ТК РФ).

[3] Петров М. И. Комментарий к Федеральному закону «О персональных данных» (постатейный). – М.: ЗАО Юстицинформ, 2007. – С. 68.

[4] Иванский В. П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования : монография. – М.: Изд-во РУДН, 1999. – С. 8.

[5] Лушников А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. – 2009. – № 10. – С. 78.

[6] Басаргин И.Н. Личные неимущественные права в трудовом правоотношении: автореферат дис. … канд.юрид.наук. – Екатеринбург, 2002. – С. 20.

[7] Собрание законодательства РФ. – 2002. – № 46. – Ст. 4584.

[8] В пп. 11 части 1 ст. 6 Закона есть указание на персональные данные, подлежащие опубликованию на основании федерального закона. Однако требования об общедоступности и опубликовании сведений не расцениваются нами как равнозначные.

[9] Ley Oranica 15/1999, de deciembre, De Protection de Datos de Caracter Personal.

[10] Трудовое право России : учебник / под ред. С. Ю. Головиной, М. В. Молодцова. – М.: Норма, 2008. – С. 241.

[11] Решение Фрунзенского районного суда г. Владивостока от 14.01.2010 г. – http://frunzensky.prm.sudrf.ru/modules.php?name=docum_sud&id=557&cl=1

[12] Из отеля «Мариотт Гранд» уволен «изобличитель» сборной РФ по футболу. – http://www.progressor.uz/2009/12/11/iz-otelya-mariott-granduvolen-izoblichitelsbornoj-rf-po-futbolu/ (дата доступа – 11.12.2009 г.).

[13] Решение Ломоносовского районного суда г. Архангельска от 3 июня 2009 г. Дело 2-1880/09. – http://files.sudrf.ru/&sort=0&pagelen=10

[14] Федеральный закон от 25 ноября 2011 г. № 266-ФЗ «О внесении изменений в Федеральный закон "О персональных данных" по вопросам реализации международных договоров Российской Федерации о реадмиссии» // Собрание законодательства РФ. – 2009. – № 48. – Ст. 5716.

[15] Приказ Минздравсоцразвития РФ от 29 июня 2011 г. № 624н «Об утверждении Порядка выдачи листков нетрудоспособности» // Российская газета. – 2011. – 11 июля. – № 148.

[16] Кодекс практики МОТ по защите личных данных работника. МБТ, 1997. – http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

[17] Решение Удомельского городского суда Тверской области от 11 февраля 2011 г. – http://sudoved.ru/ru/docs/1875233/?query=% (дата доступа – 15.03.2012 г.)

[18] Определение Магаданского областного суда от 01 сентября 2009 г. - http://files.sudrf.ru/1533/user/33-953.doc (дата доступа - 12.12.2009 г.)

[19] Киселев И. Я. Сравнительное трудовое право : учебник. – М.: ТК Велби; Изд-во «Проспект», 2005. – С. 131.

[20] Кадровые агентства будут привлекать работников по составу ДНК . – http://hrm.by/novosti/kadrovyie-agentstva-budut-privlekat-rabotnikov-po-sostavu-dnk.html. (дата доступа – 18.03.2012 г.).

[21] Имеет ли право работодатель все знать о ваших болезнях. - http://www.zakonia.ru/news/76/50845 (дата доступа – 18.03.2012 г.)

[22] The Genetic Information Nondiscrimination Act of 2008. - http://www.eeoc.gov/laws/statutes/gina.cfm. (дата доступа - 18.03.2012 г.)

[23] См.: Киселев И. Я. Указ. соч. – С. 131–132.

[24] Решение Заельцовского районного суда г. Новосибирска Новосибирской области. - http://sudoved.ru/ru/docs/962578/?query=% (дата доступа – 15.03.2012 г.)

Станскова Ульяна Михайловна, старший преподаватель кафедры трудового и социального права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: uljana-st@yandex.ru

Stanskova Ulyana Mikhajlovna, senior teacher of department of the Labour and social right for the South-Ural state university (national research university). E-mail: uljana-st@yandex.ru

УДК 343.151.037 + 347.951.037 + 342.7.037
ББК Х400.323 + Х410.114:Х400.323

Денисова Ю. И.

РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СУДЕБНЫХ РЕШЕНИЯХ

В статье исследуется актуальная сегодня на практике проблема защиты персональных данных при распространении судебных решений. Автором исследуются угрозы безопасности персональных данных, распространяемых в правоприменительных судебных актах.

Ключевые слова: *информационная безопасность, суд, судебные решения, персональные данные.*

Denisova Y. I.

DISTRIBUTION OF THE PERSONAL DATA IS IN COURT DECISIONS

In the article the actual is investigated today in practice problem of protection of the personal data at distribution of court decisions. An author is investigate the threats of safety of the personal data expandable in judicial acts.

Keywords: *informative safety, court, court decisions, personal data.*

Гласность правосудия – один из фундаментальных принципов функционирования судебной системы. Основным элементом принципа гласности является доступ к информации. В нашей стране продолжительное время отсутствовало законодательство, регламентирующее право на доступ к информации, что невыгодно выделяло Россию среди других демократических стран. В 2008 году была заложена правовая база реализации права на доступ к информации о деятельности судов. 22 декабря 2008 года был принят Федеральный закон № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Среди множества положений закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» одним из ключевых является требование о размещении судебных актов в информационно-телекоммуникационной сети «Интернет» (пп. «г» п. 2 ч. 1 ст. 14). Данное положение, несомненно, является революционным в вопросе обеспечения доступа к информации о деятельности судов. Возможность доступа к судебной практике позволяет гражданам, профессиональному и научному сообществам знакомиться с правоприменительной практикой в режиме on-line. Основной же проблемой, возникающей в связи с размещением судебных актов, является вопрос исключения из них персональных данных. Стоит отметить, что в системе арбитражных судов доступ к судебным актам открыт практически полностью, следовательно, рассмотрим данный вопрос в системе судов общей юрисдикции.

В п. 5 ч. 2 ст. 1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» указано, что его положения не распространяются на отношения, возникающие при предоставлении уполномоченными ор-

ганами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Согласно ст. 1 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» к информации о деятельности судов относится информация, подготовленная в пределах своих полномочий судами. Отсюда следует, что тексты судебных актов не требуют исключения персональных данных. Оценка допустимости или недопустимости размещения судебного акта в сети Интернет должна основываться либо на типе судебного разбирательства (открытое или закрытое), либо на закрытом перечне дел, которые закреплены в законе как не подлежащие размещению на сайте (п. 5 ст. 15).

В п. 3 ст. 15 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» выдвигается иное требование, а именно исключение персональных данных из судебных актов, кроме фамилий и инициалов истца, ответчика, третьего лица, гражданского истца, гражданского ответчика, осужденного, оправданного, лица, в отношении которого ведется производство по делу об административном правонарушении, секретаря судебного заседания, рассматривавших (рассматривавшего) дело судей (судьи), а также прокурора, адвоката и представителя, если они участвовали в судебном разбирательстве. Кроме того, данное требование конкретизируется в Регламенте организации размещения сведений о находящихся в суде делах и текстов судебных актов в информационно-телекоммуникационной сети Интернет на официальном сайте суда общей юрисдикции (утв. Постановлением Президиума Совета судей РФ от 27 января 2011 г. № 253). Данный Регламент устанавливает открытый перечень персональных данных участников судебного процесса, подлежащих исключению из объема сведений о находящихся в суде делах и текстов судебных актов, размещаемых на сайте суда.

Таким образом, возникает коллизия: согласно закону «О персональных данных» суды обязаны размещать судебные акты, вынесенные в рамках открытого судебного разбирательства, без изменений, но на основании Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» и Регламента их обязывают выполнять процедуру деперсонификации.

Согласно исследованию, проведенному Институтом проблем правоприменения, подавляющее большинство судов в той или иной мере выполняет требование об удалении персональных данных. Это производится по-разному и иногда действительно никак не затрагивает существо дела. Но в связи с отсутствием единого понимания о пределах и критериях деперсонализации эта работа порой приобретает абсурдные формы. Согласно результатам исследования, проведенного в декабре 2011 г., значимые для дела данные в гражданских делах удалены почти в половине случаев (46%), меньше всего пострадали административные дела (10%), из уголовных дел удалены значимые для понимая существа дела данные в 26% случаев.

Яркой иллюстрацией потери смысла части судебного акта является текст решения, вынесенного 27 апреля 2011 г. Лобненским городским судом (Московская область):

«Истцы обратились в суд с иском к ООО «иные данные» о взыскании денежных средств, указав, что они заключили с ООО «иные данные» договоры об участии в инвестировании строительства жилого дома в иные данные, предметом которых являлось участие истцов в инвестировании строительства указанного жилого дома и приобретение права на получение в собственность квартир. Так, Т.А.А. заключил с ООО «иные данные» договор №№ от 00.00.0000, С.С.А. – договор №№ от 00.00.0000, С.О.В. – договор №№ от 00.00.0000, К.Т.А. – договор №№ от 00.00.0000 В счет исполнения договора Т.А.А. оплатил ООО «иные данные» иные данные руб., К.Т.А. – иные данные руб., С.О.В. – иные данные руб., С.С.А. – иные данные руб. Ранее 00.00.0000 между ООО «иные данные» и ООО «иные данные» были заключены договоры №, №, согласно которым ООО «иные данные» обязался участвовать в инвестировании строительства квартир по адресу».

Таким образом, чтобы разобраться в возникшей коллизии, необходимо проанализировать нормы федерального законодательства. В противоречии между Федеральным законом «О персональных данных» и Федеральным законом «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» очевидно, что более высо-

кой юридической силой обладают положения первого (как общей нормы, закрепляющей само понятие «персональные данные»). Следовательно, нормы, закрепленные в Федеральном законе «О персональных данных», не могут быть скорректированы положениями Регламента.

Решением возникшей коллизии мы считаем то, что все ограничения на публикацию информации, имеющейся в судебных актах, должны определяться видом судебного разбирательства (открытое, закрытое) и положениями ч. 5 ст. 15 ФЗ-262. В случае же если судебный акт не подпадает под эти ограничения, он подлежит размещению на сайте полностью и без изъятий. Такое решение позволит не только разгрузить лиц, ответственных за подготовку и размещение информации на сайтах судов, но и расширить доступ граждан к информации о деятельности судов.

Денисова Юлия Игоревна, аспирант кафедры конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: yla190588@mail.ru

Denisova Yulia Igorevna, postgraduate student of Constitutional and Administrative Law Department of South Ural State University (national research university). E-mail: yla190588@mail.ru

УДК 342.7:004.056 + 004.7.056
ББК Х400.323 + Х401.114

Волков Ю. В.

ЗАЩИЩЕННОСТЬ СУБЪЕКТА ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье рассмотрены вопросы защищенности персональных данных в условиях современной глобализации. Предложено авторское толкование понятий «автоматизированная обработка персональных данных» и «способы правовой защиты персональных данных».

Ключевые слова: *автоматизированная обработка, персональные данные, правовая защита.*

Volkov Y. V.

SECURITY OF SUBJECT AT THE AUTOMATED PROCESSING OF HISPERSONAL DATA

The questions of protection of data personal are discussed in the article on the conditions of contemporary globalization. The author proposed another concept automated processing of data personal, and the legal protection of personal data.

Keywords: *the automated processing, the data personal, a legal protection.*

В условиях современной глобализации многих граждан волнуют вопросы защищенности в информационной сфере. Объективные основания для такого беспокойства действительно имеют место. Комментарии специалистов о возможностях преступников в киберпространстве создают дополнительное напряжение в обществе. В таких условиях весьма актуальными будут разъяснения норм действующего законодательства. Права субъектов персональных данных и обязанности операторов, предусмотренные статьей 16 Федерального закона «О персональных данных»[1] (далее – Закона). Особо следует подчеркнуть, что не всегда понимание, и особенно толкование законодательства, осуществляется техническими специалистами и правоведами одинаково. Принципиальным в нашем комментарии является толкование 1 и 2 частей названной статьи 16 Закона. Именно они формируют норму материального права о том, что юридические последствия, которые формируются в результате автоматизированной обработки персональных данных, возможны только при письменном согласии субъекта, которое дается субъектом исключительно для данной конкретной обработки. Остальные части названной статьи описывают процедурные вопросы.

1. Ключевое понятие статьи именно – автоматизированная обработка. Для того что-

бы понять причины, побудившие выделить автоматизированную обработку в отдельную категорию, необходимо выяснить: как она возникла, что из себя представляет. И чем, собственно, отличается автоматизированная обработка от неавтоматизированной, ручной обработки для правовых целей (законодательных, правоприменительных и охранительных). Понятие автоматизированной обработки тесно связано с теорией автоматов и относится к научным терминам, категориям математики и информатики. Вопросы автоматизации привлекали исследователей во все времена. В современной истории наиболее активные исследования начались в конце 20-х годов XX века. В период Второй мировой войны основные усилия были направлены на расчеты и обработку разведывательных данных (расшифровку сообщений). По существу, эти исследования и привели к созданию первых электронно-вычислительных машин. Одновременно с практическими вопросами разрабатывалась и теория автоматов. Часть исследований после Второй мировой войны были оформлены в виде Общей и логической теории автоматов (Д Нейман - А. Тьюринг, 1960, в США) и в виде Абстрактной теории автоматов (В. М. Глушков, 1961, в СССР), а также в огромном количестве других работ на эту тему. Посещение в 1961 году СССР основателем кибернетики Н. Винером активизировало интерес к автоматизированной обработке данных в правовой сфере. В некоторых вузах Москвы, Киева были открыты курсы правовой кибернетики. В период 60–70-х годов XX века сформировались и основные понятия, которые используются и в настоящее время. Так, например, automatic data processing (ADP) – автоматическая обработка данных – включает несколько контекстов: «1) обработка данных выполненная в основном автоматическими средствами; 2) в широком смысле дисциплина, изучающая методы и технику обработки данных автоматическими средствами; 3) относится к оборудованию для обработки данных, такому, как электрические бухгалтерские машины и электронное оборудование для обработки данных»[2].

Более современные источники определяют автоматическую обработку данных – automatic data processing (ADP) – как манипуляцию данными с помощью автоматизированных устройств[3]. В основном большинство источников содержат близкие по смыслу определения ключевого термина в данном словосочетании. Automatic – автоматический, как правило, определяется как процесс или устройство, способные (при заданных условиях) функционировать без вмешательства человека[4]. В этой связи имеются основания полагать, что именно отсутствие вмешательства человека и заданные условия обработки являются основными признаками автоматизации применительно к обработке персональных данных.

Необходимо также учитывать, что правовое понятие, введенное Конвенцией о защите физических лиц при автоматизированной обработке персональных данных, незначительно отличается от технического толкования термина, а именно «автоматическая обработка» включает 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»[5].

Введенное задолго до эпохи Интернета понятие автоматизации обозначало действия по облегчению труда человека. Изначально автоматизация как явление не создавало угроз в части перехвата юридически значимых действий. Дальнейшее использование термина, по сути, впитало и компьютеризацию, и интернетизацию и глобализацию. Семантический объем термина «автоматизация» вырос значительно. Это обстоятельство обусловило в современных условиях широкий спектр мнений по данному вопросу. Например, о том, что «…на уровне определений достаточно трудно провести четкую линию раздела между автоматизированной и неавтоматизированной обработкой данных»[7].

Действительно, считывание штрихкода с квитанции за оплату коммунальных услуг – это автоматизированная обработка или нет? Другой пример содержится в нормативном правовом акте. Пункт 2 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: «2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее»[8].

Вместе с тем анализ текста упомянутого

Положения позволяет выявить следующие обстоятельства. Классификация видов обработки данных и вывод осуществляются на основе применяемых при обработке предметов. Обработка персональных данных, осуществляемая без использования средств автоматизации, характеризуется использованием ручного труда, ручных пометок и записей в соответствующих документах, бланках, карточках, реестрах, журналах, книгах, иных материальные (не электронных) носителях. Применительно к юридическим последствиям классификации не проводится.

Практически полностью цитирует положения 2 пункта названного Постановления одно из авторитетных экспертных изданий и приводит следующий комментарий. «К примеру, если пользователь внес данные в персональный компьютер только для того, чтобы их распечатать, и не сохранял данные на компьютере, то эту обработку можно считать неавтоматизированной»[9]. Полагаем, что данное толкование является ошибочным.

Другой аспект этого вопроса – предмет специальной научной дисциплины – защита информации. Ввод информации в память компьютера и распечатка файла представляют собой действия, сопряженные с функционированием процессора – вычислителя, технические параметры которого характеризуются определенной тактовой частотой. Постоянные ввод и распечатка формируют устойчивый **автоматизированный** канал утечки информации, которая содержит и персональные данные. Радиоизлучение может быть зафиксировано, считано, сохранено и расшифровано, т. е. прочитано специальной техникой, если в компьютере нет специальной защиты. Естественно, такой вариант утечки данных невозможен при рукописном оформлении документа. В описанном варианте невозможно признать обработку персональных данных в форме ввода и распечатки с помощью компьютера, а также с помощью отдельных электронных печатных машин, как неавтоматизированную обработку персональных данных. К аналогичному мнению склоняются практические специалисты и авторы публикаций в специализированных изданиях по защите информации. Современные научные исследования и достижения в этом направлении позволяют отслеживать активность пользователей по клавиатурному почерку, распознавать личность по фотографии, иные объекты по заданным признакам. Традиционными во многих странах стали камеры слежения за дорожным (автомобильным) трафиком и управления им без постоянного участия, но под контролем человека. Процесс управления в таком случае весьма часто включает фиксацию нарушений, наложение штрафных санкций, рассылку квитанций и т. д.

Вопрос отнесения обработки к автоматизированной и неавтоматизированной имеет глубокое практическое значение и требует пристального изучения. Следствием признания обработки персональных данных автоматизированной является обязанность оператора изготовить и сертифицировать программные продукты для их защиты, либо приобрести лицензированные продукты. А в случае автоматизированной обработки персональных данных по договору для других лиц получить лицензию на деятельность по защите информации.

Автоматизированная обработка предполагает участие «автомата» на любой его стадии. В этом смысле невозможно утверждать, что, скажем, компьютер был использован только как устройство для набора текста, а всё остальное было ручной обработкой. Подобного рода утверждения весьма часто имеют место в административной практике со стороны операторов и, в отдельных случаях, становятся объектом судебного спора.

До настоящего времени судебная практика не нашла единого подхода к точному и однозначному пониманию автоматизированного процесса обработки данных, общее представление в различных решениях концептуально не отличается. И только конкретные обстоятельства в каждом конкретном случае позволяют принять то или иное решение.

2. Другой аспект проблемы – признание за автоматизированной обработкой исключительности. Вопрос заключается в том, что многие авторы при рассмотрении фразы «…принятие решений на основании исключительно автоматизированной обработки…» переставляют акцент. В цитированной фразе внимание переключается с «**исключительно** автоматизированной» обработки на «исключительно **автоматизированную**» обработку. Юридическая конструкция, которая предполагает ограничение исключительности, но не запрет, ориентирует нас на обдуманное принятия решения, порождающего юридические последствия, на основе автома-

тизированной обработки, т. е. без участия человека. При смещении акцента в сторону **автоматизированной** обработки и все дальнейшие вопросы рассматриваются в контексте, что есть автоматизированная и что есть ручная обработка. Одно из решений вопроса предложено в форме теста CAPTCHA [Ка́пча, ка́птча][10].

Другим решением является обязательная подпись субъекта персональных данных, которая подтверждает факт принятия волевого решения субъектом, а не автоматом. Поэтому запрет на использование автоматической обработки фактически следует рассматривать не как общее правило, а как исключение из правила, сформулированного во 2-м пункте комментируемой статьи. В противном случае придется повсеместно отказываться от автоматизированной обработки данных и переходить на ручную обработку.

Пункт 2 статьи 16 Закона содержит общую норму об обязательном уведомлении субъекта об автоматизированной обработке его персональных данных и возможных последствиях такой обработки. Данное положение размещено во 2-м пункте статьи 16, но по смыслу это общее правило статьи. Исходный смысл данной юридической конструкции, по нашему убеждению, заключается в следующем. Обработанные автоматизированным способом персональные данные должны быть понятны и, в идеальном варианте, представлены субъекту до принятия решения, которое влечет юридические последствия. Субъект в начале отработки должен быть уведомлен о том, что обработка будет производиться в автоматическом режиме, что вмешательства человека в процесс не будет. Соответственно, никто не сможет исправить его, субъекта, ошибки (если таковые допущены) и только он несет ответственность за последствия представления данных (если сведения ошибочные). Предварительное уведомление субъекта имеет цель предупредить о возможном наступлении юридических последствий. Соответственно любая распечатка персональных данных (по мнению названных экспертов – ручная операция) без его уведомления и согласия фактически будет нарушать его права.

Судебная практика по вопросу, должен ли быть ознакомлен под роспись субъект персональных данных, свидетельствует о том, что и подпись под данной фразой, и специальное место для подписи должны быть. Так, Федеральный арбитражный суд Северо-Кавказского округа, рассмотрев в кассационном порядке дело № А63-11458/2010, пояснил следующее.

Субъект персональных данных согласился на использование его данных в системе информационно-справочного обслуживания, заполнив и подписав стандартный бланк договора оказания услуг связи. Названная форма не содержит отдельное поле для получения согласия абонента на обработку его персональных данных, что является нарушением. Дальнейшие действия надзорного органа, предписавшего устранить нарушение, признаны законными[10].

Суммируя все перечисленные аргументы, следует отметить, что обеспечить защищенность субъекта персональных данных невозможно без его участия. Оператор обязан во всех спорных, пограничных случаях предусмотреть в бланках, формах соответствующее место или объяснить, каким образом будут обработаны персональные данные. Кроме того, он обязан рассмотреть все возражения субъекта и дать аргументированный ответ.

Примечания

[1] См.: Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» [электронный ресурс]. URL: http://www.garant.ru

[2] См.: Вычислительная техника и обработка данных. Терминологический толковый словарь фирмы IBM / пер. с англ. Т. Тер-Микаэляна. – М.: Статистика, 1978. – С. 20.

[3] См.: Англо-русский энциклопедический словарь по современной электронной технике и программированию: компьютеры, Интернет, телекоммуникации, аудио,- видео-, теле- и радиотехника и пр. / И. Л. Мостицкий. – М.: Изд. Триумф, 2004. – С. 73.

[4] Там же.

[5] См.: Конвенция о защите физических лиц при автоматизированной обработке персональных данных Страсбург, 28 января 1981 г. с изменениями от 15 июня 1999 г.

[6] См.: Петров М. И. Комментарий к Федеральному закону «О персональных данных» (постатейный). – М.: ЗАО Юстицинформ, 2007. – С. 109.

[7] См.: Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [электронный ресурс] // ИПС Гарант. Доступ свободный URL: http://www.garant.ru.

[8] См.: Jet info информационный бюллетень – 2009. – № 5 (192). – С. 11.

[9] CAPTCHA, Completely Automatic Public Turing Test to Tell Computers and Humans Apart – полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей. Пользователю предлагается ввести в специальное поле формы автоматически осознанное выражение на картинке из цифр и/или букв разного регистра, разного цвета, прочтение которого требует логического (человеческого) восприятия, недоступного автомату.

[10] См.: Постановление Федерального арбитражного суда Северо-Кавказского округа от 03.10.2011 по делу № А63-11458/2010, рассмотренному в кассационном порядке [электронный ресурс] // ИПС Гарант. Доступ свободный URL: http://www.garant.ru.

Волков Юрий Викторович, кандидат юридических наук, доцент, доцент кафедры информационного права Уральской государственной юридической академии. E-mail: yuriivolkov@yandex.ru, volkov@usla.ru

Volkov Yuriy Victorovich, candidate of legal sciences,associate professor, associate professor of department ofinformative right for the Ural state legal academy. E-mail: yuriivolkov@yandex.ru, volkov@usla.ru

УДК 004.056:378 + 378.1:004.056 + 004.7.056
ББК Ч448.027

Южаков А. А., Шабуров А. С., Рашевский Р. Б.

О РАЗРАБОТКЕ УЧЕБНО-ЛАБОРАТОРНОГО КОМПЛЕКСА ДЛЯ ИССЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

В статье анализируется проблема информационной безопасности критически важных объектов, а также предлагается описание функциональных возможностей учебно-лабораторного комплекса для подготовки специалистов по защите информации на критически важных объектах.

Ключевые слова: *информационная безопасность, критически важный объект, вредоносная программа, кибератака, кибероружие, лабораторный комплекс, администратор информационной безопасности, злоумышленник, программируемый логический контроллер, угроза информационной безопасности, локальная вычислительная сеть, межсетевой экран.*

Yuzhakov A., Shaburov A., Rashevskiy R.

ON THE DEVELOPMENT OF EDUCATIONAL RESEARCH LABORATORY COMPLEX FOR IMMUNITY CRITICAL FACILITIES

This article analyzes the problem of security of critical facilities, and offers a description of the functionality of teaching and laboratory complex for the training of information security at critical facilities.

Keywords: *information security, a critical facility, a malicious pro-gram, cyber attacks, cyber weapons, la-boratory, information security administrator, the attacker, a programmable logic controller, the threat of information security, local area network, a firewall.*

Развитие лабораторной базы для подготовки специалистов по защите информации является одной из актуальных задач совершенствования системы их профессионального обучения[1]. Создание новых учебно-лабораторных комплексов для исследования защищенности информационных систем позволит сформировать необходимые практические навыки и выработать требуемые компетенции для будущей

профессиональной деятельности студентов.

Особенно важной составляющей подготовки специалистов по защите информации является их готовность к обеспечению информационной безопасности в системах управления экологически опасными производствами и критически важными объектами (КВО)[2].

Примерами подобных объектов, наиболее приближенными по своему функциональному предназначению к вопросам обеспечения жизни и здоровья людей, являются объекты систем энергообеспечения и водоснабжения, системы управления транспортом и т. п.[3] Интенсивное развитие и внедрение информационных технологий в системы государственного и муниципального управления, в управление производством, транспортом, финансовые системы, системы образования и здравоохранения обусловливают значительное расширение уже сформировавшегося подобного класса объектов и систем в ближайшей перспективе.

В настоящее время для защиты КВО от вредоносных программ применяются различные разновидности метода сигнатурного детектирования, такие как: сигнатурные базы, эвристика и эмулятор процессора операционной системы. Однако в данном случае традиционные решения по защите информации не способны обеспечить должный уровень безопасности, что убедительно доказывается результатами динамических тестирований антивирусных продуктов.

За последние годы было зафиксировано несколько инцидентов с участием вредоносных программ, направленных исключительно на КВО[4]. Наиболее известной программой данного класса является «червь» «Stuxnet», обнаруженный в июле 2010 на секретном заводе по обогащению урана в г. Натанзе (Иран). По мнению экспертов, основной целью «Stuxnet» являлся вывод из строя центрифуг ядерных реакторов для обогащения урана посредством вредоносного воздействия на управляющий технологическим процессом промышленный логический контроллер (ПЛК) Siemens Simatic.

В сентябре 2011 г. на крупном промышленном объекте в Венгрии обнаружен второй представитель подобного класса программ – «Duqu». Данный вредоносный продукт был создан на платформе «Stuxnet» и функционировал, предположительно, с 2009 г., обладая явно выраженным шпионским функционалом. По одной из версий, он был разработан непосредственно для кражи сертификатов цифровых подписей у корневых доверенных центров сертификации и дальнейшего использования этих подписей для других образцов вредоносных программ.

Не менее серьезный по последствиям инцидент с применением вредоносных программ произошел в 2012 г. в Иране. Организации различного профиля деятельности (в том числе нефтяные компании, кредитно-финансовые учреждения и др.) были атакованы «червем» «Wiper», основной целью которого является уничтожение баз данных различных форматов.

Приведенные примеры подтверждают неэффективность классических антивирусных технологий против узконаправленных информационных угроз, поскольку для современных вредоносных программ типа «Stuxnet», «Wiper», «Duqu» и т. п. характерно применение таких технологий как полиморфизм, обфускация, шифрование[5]. В данном случае анализ вредоносного кода для выделения сигнатуры максимально затруднен и может занимать достаточно продолжительное время, что является особенно критичным фактором в контексте атаки на КВО.

Более того, по мнению ведущих лабораторий по информационной безопасности, количество инцидентов на КВО с применением стратегического кибероружия за последние годы значительно возросло, а в 2013 году удвоится по сравнению с 2012 годом[6].

Существование подобного типа угроз ставит новые задачи по обучению специалистов по защите информации и совершенствованию учебно-лабораторной базы, соответствующей требованиям как сегодняшнего дня, так и перспективы. В целях подготовки и переподготовки специалистов по защите информации по вопросам противодействия кибератакам на информационно-управляющие системы КВО на базе Пермского национального исследовательского политехнического университета (ПНИПУ) планируется создание специализированного лабораторного комплекса.

Оснащение данного лабораторного комплекса предполагает его оборудование современными компонентами программно-

аппаратного обеспечения, а функциональные возможности позволят решать следующие научно-исследовательские и практические задачи по изучению защищенности КВО в целом и промышленных автоматизированных систем, в частности:

1. Изучение механизмов атак и отработка способов защиты промышленных автоматизированных систем.

2. Моделирование воздействий угроз информационной безопасности КВО на основе применения кибероружия.

3. Изучение и отработка методов защиты информационных управляющих систем КВО.

4. Исследование защищенности процессов обмена информацией.

5. Исследование стойкости криптографических протоколов информационного взаимодействия.

6. Исследование безопасности баз данных (БД).

7. Исследование механизмов авторизации в различных операционных системах (ОС).

Для решения данных задач в составе лабораторного комплекса оборудуется стенд ПЛК с использованием образцов контроллеров крупнейших мировых производителей, применяемых для автоматизации различных промышленных процессов (Siemens Simatic S7), в системах «умный дом» (Echelon i-Lon SmartServer), а также в системах контроля и управления доступом (Apollo AAN-100).

Развертывание специализированных SCADA-систем для управления ПЛК в рамках лабораторного комплекса позволит воссоздать условия, аналогичные реальным промышленным объектам и информационным системам, реализованным на действующих системах.

Использование при построении локальной вычислительной сети (ЛВС) лаборатории современного сетевого оборудования (управляемый коммутатор Cisco, межсетевой экран (МЭ) нового поколения ССПТ-2, криптографическое программное обеспечение, используемое в банковской сфере) даст возможность проводить подготовку студентов по защите процессов обмена информацией на качественно новом уровне.

Установка на сервере ЛВС сетевой версии базы данных Oracle 11g, являющейся наиболее распространенной системой управления базами данных в мире, позволит проводить теоретические и практические (лабораторные) занятия по исследованию защищенности баз данных.

Использование в лабораторном комплексе различных операционных систем (ОС) (Microsoft Windows, Linux, Mac OS X) будет способствовать исследованию механизмов авторизации в различных ОС и выработке рекомендаций по улучшению их защищенности от несанкционированного доступа (НСД).

Применение аппаратной виртуализации на базе технологии VMWare на сервере ЛВС учебно-лабораторного комплекса позволит освоить различные операционные системы (Microsoft Windows Server 2012, Oracle Enterprise Linux, RedHat Enterprise Linux) и встроенные в них инструменты обеспечения безопасности с точки зрения администрирования информационной безопасности.

Рассмотрим пример использования лабораторно-учебного комплекса для отработки навыков защиты КВО от информационных атак вероятного злоумышленника.

В качестве объекта атаки выбрана виртуальная локальная сеть (созданная с помощью инструментов управления управляемого коммутатора Cisco), в которой присутствует ПЛК Siemens Simatic, предназначенный для автоматизации различных промышленных задач. Данный ПЛК подключен через коммутатор к персональному компьютеру (ПК), с которого выполняются управление и мониторинг.

Для обеспечения защиты процесса управления в сети установлено рабочее место администратора информационной безопасности (студента-«защитника»). Рабочее место администратора информационной безопасности и рабочее место управления ПЛК подключены к МЭ и к управляемому сетевому коммутатору.

Рабочее место злоумышленника (студента-«нападающего») находится за пределами атакуемой виртуальной локальной сети. В целях мониторинга действий обучаемых рабочее место преподавателя подключено непосредственно к МЭ ССПТ-2, что позволяет преподавателю в режиме реального времени отслеживать и оценивать все действия как со стороны злоумышленника, так и администратора информационной безопасности. Схематично данный пример проиллюстрирован на рис. 1.

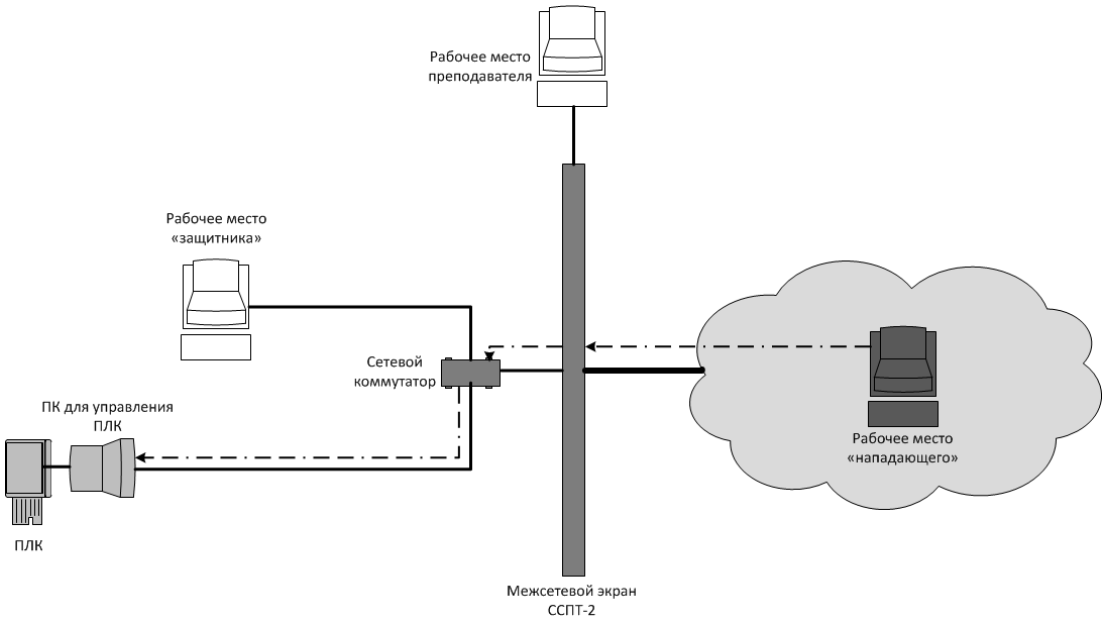

Рис. 1. Схема блокирования кибератаки на ПЛК Siemens Simatic

Сценарий развития кибератаки может быть следующим. В первую очередь злоумышленник выполняет сетевую разведку с помощью программного обеспечения NMAP. Данное программное обеспечение позволяет получить информацию об устройствах, используемых в атакуемой вычислительной сети, а также определить используемые сетевые сервисы и открытые сетевые порты на различных устройствах.

После успешно проведенной сетевой разведки и выявления сетевого устройства (ПК для управления ПЛК), на котором развернуты база данных MS SQL и программное обеспечение для управления ПЛК Siemens Simatic, злоумышленник выполняет «взлом» базы данных с помощью утилиты SQLMap. Также со стороны нападения в целях сокрытия сетевой атаки могут применяться методы подмены MAC-адреса и перехвата сетевого трафика атакуемой сети с помощью ПО Ettercat. В результате проведенных действий злоумышленник получает возможность скопировать содержимое базы данных, а также изменять содержимое таблиц.

Администратор информационной безопасности для предотвращения атаки использует функциональные возможности аппаратного МЭ ССПТ-2, который позволяет проводить мониторинг сетевого трафика.

При обнаружении сканирования защищаемой сети администратор должен своевременно заблокировать доступ злоумышленника к защищаемой сети с помощью МЭ, а также, задействовав дополнительный функционал предотвратить повторные атаки с измененным MAC-адресом или с использованием методов перехвата сетевого трафика.

Несмотря на ограниченное количество участников одного примерного сценария информационной атаки, учебно-лабораторный комплекс предусматривает проведение групповых занятий, предполагающих одновременное задействование большего количества обучаемых (до шести) с каждой стороны.

Решение подобного рода задач возможно в ходе проведения лабораторных работ и практических занятий по дисциплинам: «Разработка и эксплуатация защищенных автоматизированных систем», «Безопасность сетей ЭВМ», «Безопасность сетей баз данных», «Безопасность операционных систем», «Информационная безопасность распределенных информационных систем» и др., а также в процессе проведения научно-исследовательских работ.

Кроме того, лабораторный комплекс позволит расширить возможности по реализуемым программам дополнительного профессионального образования: «Техническая защита конфиденциальной информации», «Комплексное обеспечение информацион-

ной безопасности автоматизированных систем» в рамках функционирующего регионального научно-исследовательского центра (РУНЦ) по информационной безопасности.

Таким образом, развитие учебно-лабораторной базы по исследованию защищенности КВО в целом и промышленных объектов, в частности, будет способствовать повышению уровня их защищенности от различных угроз информационной безопасности, позволит качественно повысить подготовку специалистов по защите информации.

Примечания.

[1] Данилов А. Н., Кон Е. Л., Кон Е. М., Южаков А. А. Модель многоканального управления учебным процессом высшей школы // Открытое образование – 2012. – № 2. – с. 7–11.

[2] ГОСТ Р 53113.1-2008. Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

[3] Федеральный закон Российской Федерации от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»// Российская газета. – 2011. – 26 июля.

[4] http://www.securelist.com/ru/analysis/208050779/Kaspersky_Security_Bulletin_2012_Kiberoruzhie

[5] http://www.securelist.com/ru/analysis?pubid=204007553

[6] http://digit.ru/internet/20121212/397387470.html

Южаков Александр Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Автоматика и телемеханика», директор РУНЦ по информационной безопасности ПНИПУ. E-mail: uz@at.pstu.ru

Шабуров Андрей Сергеевич, кандидат технических наук, доцент кафедры «Автоматика и телемеханика», сотрудник РУНЦ по информационной безопасности ПНИПУ. E-mail: shans@dom.raid.ru

УДК 004.056 + 004.934.2
ББК 32.973

Гуляев В. П., Шушарин А. С.

АНАЛИЗ АЛГОРИТМОВ ШУМООЧИСТКИ РЕЧЕВЫХ СИГНАЛОВ

В доступных литературных источниках не обнаружены работы по анализу надежности защиты речевой информации при пространственно-многоканальном ведении акустической речевой разведки (АРР) с применением различных алгоритмов шумоочистки. Такая тактика ведения АРР требует иных подходов к активной маскировке речевых сигналов. В статье приводятся результаты анализа пяти алгоритмов шумоочистки при пространственно-многоканальном ведении АРР и активной маскировке речевых сигналов.

Ключевые слова: *адаптивные алгоритмы, отношение сигнал/шум (С/Ш), фильтрация, словесная разборчивость.*

Gulyaev V. P., Shusharin A. S.

ANALYSIS OF ALGORITHMS FOR NOISE REDUCTION OF SPEECH SIGNALS

In the available literature did not detect any analysis reliable protection of verbal information with spatial-multichannel acoustic voice operated exploration (RDA) using various algorithms for noise reduction. The tactics of the RDA requires other approaches to active disguise voice signals. This article provides an analysis of five algorithms for noise reduction in spatial-multichannel run by RDA and actively disguise voice signals.

Keywords: *adaptive algorithms, signal to noise ratio (s/w), filtering, verbal intelligibility.*

Под пространственно-многоканальным ведении АРР следует понимать ведение технической разведки одновременно с разных разведнаправлений (в пределах зон разведдоступности) с использованием аппаратуры различного назначения (акустическая, виброакустическая, оптико-электронная, ПЭМИН и т. д.).

В процессе анализа алгоритмов шумоочистки проведен ряд исследований.

1. Произведены обзор и классификация более 70 систем активной защиты речевой информации, представленных на отечественном рынке.

2. При помощи пакета прикладных программ MatLab 7 разработаны модели шумовой маскировки речевых сигналов, такие как: *"белый" шум, "розовый" шум, "речеподобная" помеха и "микшированная" помеха* (полученная с помощью нормирования и суммирования трех музыкальных файлов).

3. На основе информационного критерия оценки защищенности акустического и виброакустического каналов (словесной раз-

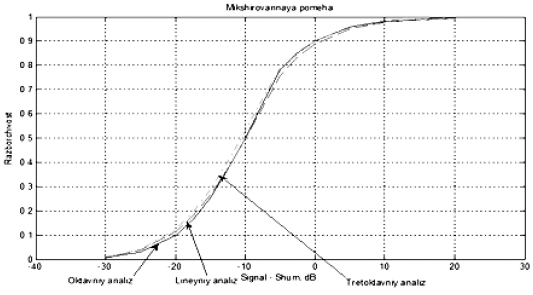

Рис. 1. Зависимости словесной разборчивости от отношения С/Ш, для "микшированной" помехи

борчивости) проведен *сравнительный анализ маскировки речи данными типами помех* [2]. Наилучшие результаты были показаны "микшированной" помехой, для которой достаточно задания сравнимо меньшего значения отношения сигнал/шум (в среднем менее 2,5 дБ). Полученные зависимости словесной разборчивости от отношения С/Ш приведены на рис. 1.

4. Экспериментальные исследования и анализ алгоритмов шумоочистки.

4.1. Суммарная обработка зашумленных речевых сигналов.

Суть данного метода состоит в суммировании сигналов, принимаемых с нескольких разведнаправлений:

$$sn_{\Sigma} = sn_1 + sn_2 + ... + sn_N = N \cdot s + (n_1 + n_2 + ... + n_N), \quad (1)$$

где: sn_{Σ} – суммарная смесь сигнала и шумов; $sn_1, sn_2, ..., sn_N$ – зашумленные речевые сигналы; s – чистый речевой сигнал; $n_1, n_2, ..., n_N$ – маскирующие взаимнонекоррелированные шумы; N – количество разведнаправлений АРР.

При сложении мощность когерентно суммируемого речевого сигнала увеличивается в N^2 раз. Мощность суммируемого шума, у которого межсигнальная корреляция отсутствует, увеличивается в N раз (аналогично дисперсии суммы независимых слагаемых). За счет этого отношение сигнал/шум в суммарном сигнале возрастает по сравнению с начальным.

Рассмотрено последовательное увеличение количества направлений ведения разведки с одного до четырех. Так, для одного направления при приеме зашумленного речевого сигнала с начальной величиной словесной разборчивости, равной 20% (рис. 2), после обработки сглаживающим фильтром Савицкого – Голея словесная разборчивость стала 35%. После увеличения количества направлений разведки до четырех анализируемая величина повысилась до уровня 84% (рис. 3а). Также обработка производилась для

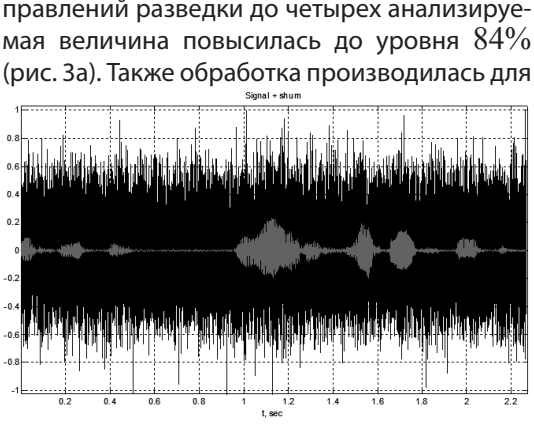

Рис. 2. Смесь сигнала и шума (W_1=20%)

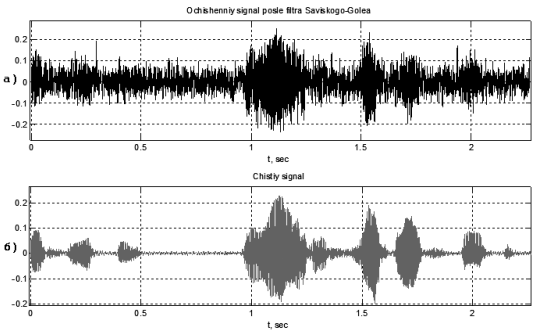

Рис. 3:
а) очищенный сигнал после фильтра Савицкого – Голея (W_{SG}=84%);
б) чистый речевой сигнал

меньшей начальной величины словесной разборчивости 10%. В результате для четырехканального приема словесная разборчивость повысилась до 72%.

4.2. Алгоритм вычитания амплитудных спектров.

В качестве обоснования этого алгоритма приводятся следующие соображения. Если стационарный сигнал $s(t)$ искажен аддитивным стационарным шумом $n(t)$, который предполагается некоррелированным с $s(t)$, следовательно, спектральная плотность мощности полезного сигнала может быть оценена как разность спектральных плотностей мощности зашумленного сигнала и шума:

$$G_s(iw) = G_{sn}(iw) - G_n(iw). \quad (2)$$

Так как речевые сигналы являются нестационарными, использовать это соотношение нельзя. На практике при обработке речи на достаточно коротких участках, например,

квазистационарных участках гласных звуков, данные величины аппроксимируют с помощью усредненных квадратов кратковременных амплитудных спектров сигнала и шума. Спектр шума при этом должен оцениваться в моменты пауз речи [3]:

$$|S(t,i\cdot w)|^2 = \begin{cases} |X(t,i\cdot w)|^2 - A(t)\cdot|N(t,i\cdot w)|^2 \\ B\cdot|N(t,i\cdot w)| \end{cases}, \quad (3)$$

где: $S(t,i\cdot w)^2$ – оценка квадрата амплитудного спектра сигнала; $X(t,iw)^2$ – кратковременный амплитудный спектр зашумленного сигнала; $N(t,iw)^2$ – оценка кратковременного амплитудного спектра шума; $A(t)$ – фактор переоценивания, зависит от соотношения сигнал/шум на сегменте анализа; B – спектральный порог, выбирается в диапазоне 0,01 – 0,1.

Для определения пауз в зашумленном речевом сигнале производится деление каждой смеси сигнала и шума на сегменты и вычисляются коэффициенты корреляции между ними. Если коэффициент корреляции меньше определенного порога, то считается, что речевой сигнал отсутствует и сегмент является шумом. В результате строится шумовой вектор, собранный поинтервально, значения которого на каждом из интервалов могут быть либо нулевыми (если принято решение о наличии речевого сигнала), либо равными значениям зашумленного сигнала. Полученный шумовой вектор изображен на рис. 4.

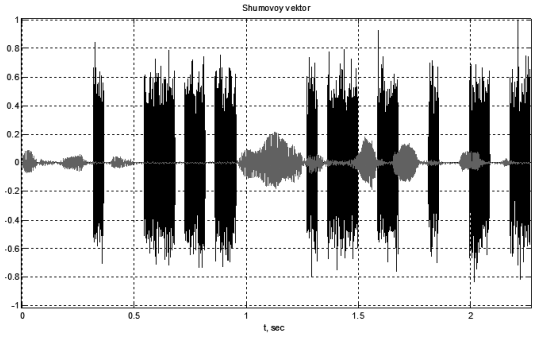

Рис. 4. Шумовой вектор (синим) и речевой сигнал (красным)

Далее берется один сегмент с шумом и дополняет пустые места вектора шума. Тем самым создается оценка шума, не имеющего в себе речевого сигнала, но коррелированного со смесью сигнал+шум. Дополненный шумовой вектор изображен на рис. 5.

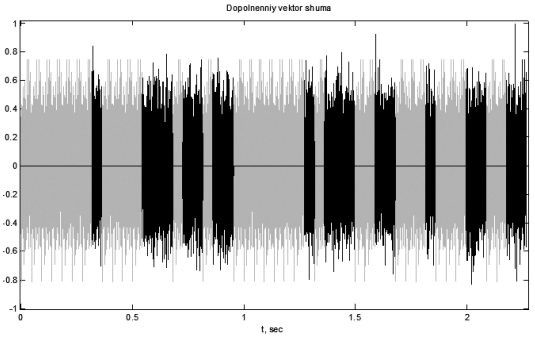

Рис. 5. Дополненный шумовой вектор

Используя полученный шумовой вектор, производится очистка речевого сигнала в соответствии с данным алгоритмом. В итоге словесная разборчивость повысилась с 20% до 53% (рис. 6а), либо для меньшей начальной величины с 10% до 32%.

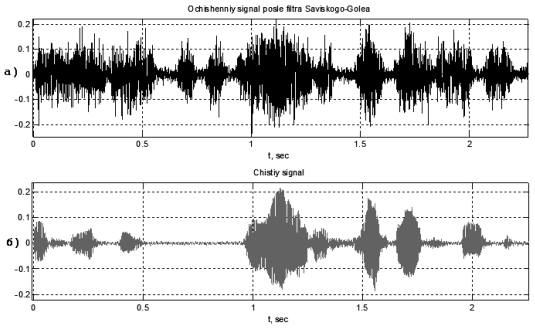

Рис. 6:
а) очищенный сигнал после фильтра Савицкого – Голея (W_{SG}=53%);
б) чистый речевой сигнал

4.3. Алгоритм оценивания минимальной среднеквадратической ошибки.

Как и вычитание спектров, алгоритм основан на оценке амплитудного спектра сигнала, для которого дополнительно определяются два – апостериорное и априорное – локальные отношения сигнал/шум [3]:

$$q_{POST}(f) = \frac{G_{sn}(iw)^2}{\sum G_n(iw)^2}, \quad (4)$$

$$q_{PRI}(f) = \frac{\sum G_s(iw)^2}{\sum G_n(iw)^2}. \quad (5)$$

Далее по аналогии с предыдущим алгоритмом определяются участки в смеси сигнала и шума, которые соответствуют моментам пауз в речевом сообщении, и строится шумовой вектор. В результате словесная разборчивость по-

высилась с 20% до 75% (рис. 7а), либо для меньшей начальной величины с 10% до 58%.

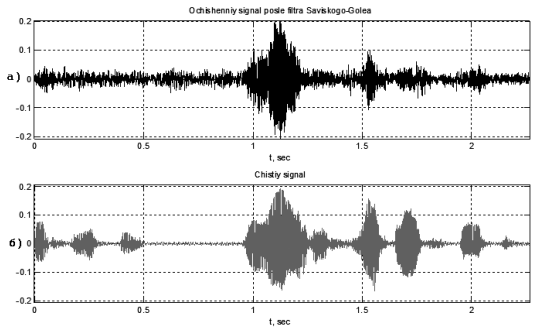

Рис. 7:
а) очищенный сигнал после фильтра Савицкого – Голея (W_{SG}=75%);
б) чистый речевой сигнал

4.4. Адаптивная фильтрация зашумленных речевых сигналов.

Свойства адаптивных фильтров в некотором смысле напоминают определенные свойства живых организмов. Биологическое значение слова «адаптация» имеет следующую трактовку: любое изменение в структуре или функции организма или любой из его частей в результате естественного отбора, с помощью которого организм становится более приспособленным для выживания и размножения в окружающей его среде. Такое же определение в некоторой степени подходит и для «искусственных», или созданных человеком, адаптивных систем.

Адаптивный фильтр представляет собой систему, структура которой изменяется таким образом, чтобы его функционирование улучшалось в результате взаимодействия с окружающей его средой [4].

Рассматривается схема адаптивного подавления помех, изображенная на рис. 8. В ней присутствуют два входа. На первый вход подается первая смесь сигнала и шума 1, а на второй вход вторая смесь сигнала и шума 2. На представленном рисунке шумовые сигналы n_1 и n_2 некоррелированны. Так же, как и речевой сигнал s некоррелирован с этими шумами.

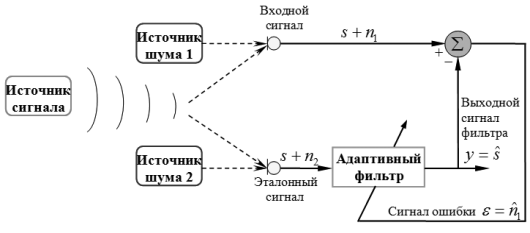

Рис. 8. Адаптивная фильтрация зашумленных речевых сигналов

Адаптивный фильтр, изменяя свои весовые коэффициенты, стремится преобразовать второй входной сигнал так, чтобы на выходе была оценка чистого речевого сигнала. Затем выходной сигнал адаптивного фильтра вычитается из первого входного сигнала, таким образом, получается сигнал ошибки. Процесс изменения весовых коэффициентов адаптивного фильтра будет продолжаться до тех пор, пока в сигнале ошибки кроме шума будет проходить часть речевого сигнала. Если же сигнал ошибки будет состоять только из шума, тогда корреляции между вторым входным сигналом фильтра и сигналом ошибки не будет, следовательно, весовые коэффициенты фильтра изменяться не будут. В качестве алгоритма адаптивной фильтрации рассматривается алгоритм наименьших квадратов (Least Mean Squares, LMS).

В результате пропускания двух зашумленных речевых сигналов через адаптивный фильтр в выходном сигнале словесная разборчивость повысилась с 20% до 78% или с 10% до 68%.

Так же адаптивная фильтрация применима при использовании более двух каналов съема информации. Основываясь на методе суммарной обработки сигналов, на первый вход адаптивного фильтра подается первый зашумленный сигнал, а на второй вход суммарная смесь, содержащая все зашумленные сигналы кроме первого. При обработке четырех зашумленных сигналов словесная разборчивость повысилась: с 20% до 91% (рис. 9а), либо с 10% до 83%.

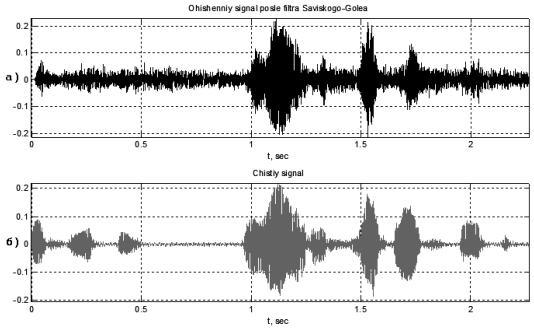

Рис. 9
а) очищенный сигнал после фильтра Савицкого – Голея (W_{SG}=75%);
б) чистый речевой сигнал

4.5. Фильтрация на основе нейронных сетей.

Нейронные сети или, точнее, искусственные нейронные сети, представляют собой технологию, которая находит свое применение в разнообразных областях благодаря

одному важному свойству — способности обучаться на основе данных при участии учителя или без его вмешательства. В общем случае нейронная сеть представляет собой машину, моделирующую способ обработки мозгом конкретной задачи.

Для того чтобы добиться высокой производительности, нейронные сети используют множество взаимосвязей между элементарными ячейками вычислений — нейронами [5].

Работа искусственной нейронной сети по шумоочистке речевого сигнала происходит следующим образом. Используются два подмассива – первый, в котором содержится исключительно шум, и второй, в котором присутствует смесь сигнала и шума. Процесс функционирования нейронной сети состоит из двух основных этапов – этапа обучения и этапа непосредственной работы.

На *этапе обучения* используется подмассив, содержащий исключительно шум. Вводится два окна – окно с входными данными длиной k отсчетов и окно с целевыми данными длиной m отсчетов, как это показано на рис. 10.

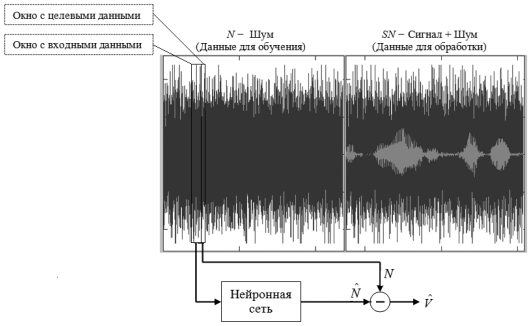

Рис. 10. Этап обучения нейронной сети

Таким образом, например, для ряда вида $\{0.3\ \ 0.5\ \ 0.2\ \ 0.4\ \ 0.3\ \ 0.7\ \ 0.1\ \ 0.9\ \ 0.1\ \ 0.5\ \ \ldots\}$ и $k = 4$, $m = 1$ будем иметь такие вектора:

$$0.3\ \ 0.5\ \ 0.2\ \ 0.4 \Rightarrow 0.3$$
$$0.5\ \ 0.2\ \ 0.4\ \ 0.3 \Rightarrow 0.7$$
$$0.2\ \ 0.4\ \ 0.3\ \ 0.7 \Rightarrow 0.1.$$

Во входное окно войдут первые 4 значения, а в целевое окно пятое значение, далее выполняется сдвиг на один отсчет, и так далее. На выходе нейронной сети формируется сигнал N'. Таким образом, сеть учится предсказывать значение точки за пределами входного окна на основе тех точек, которые в него попали. Вводится величина V, которая равна разности значений целевого окна и выходных значений нейронной сети [6].

Если нейронная сеть обучилась точно предсказывать поведение шума, тогда $N=N'$, следовательно, $V=0$, но так как шум представляет собой случайный процесс, значения которого распределены по нормальному закону, то в этом случае сеть не сможет свести ошибку к нулю. Единственное, что может сделать сеть на основе полученных статистических данных, указать, какое значение сейчас наступит с большей вероятностью. В результате выходная величина V, будет представлять собой шум, являющийся ошибкой экстраполяции (прогнозирования).

На *этапе работы,* согласно рис. 11, используется подмассив, содержащий как шум, так и полезный сигнал. Но на данном этапе используется только одно окно с входными данными. Так как в процессе обучения сеть научилась предсказывать только случайную составляющую, исходный квазигармонический речевой сигнал будет претерпевать незначительные изменения. В результате на выходе нейронной сети будет смесь речевого сигнала и ошибки экстраполяции входного вектора шума.

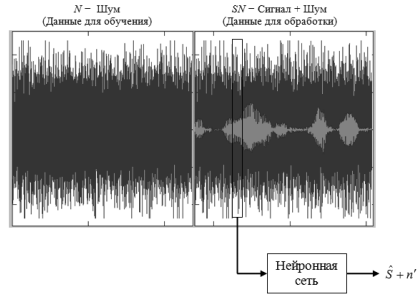

Рис. 11. Этап работы нейронной сети

В результате после фильтрации словесная разборчивость повысилась с 20% до 80% (рис. 12а), либо для меньшей начальной величины с 10% до 65%.

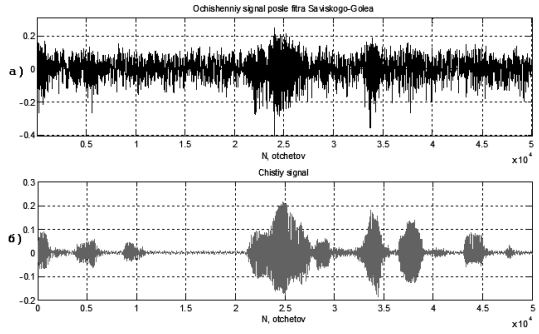

Рис. 12
а) выходной сигнал фильтра Савицкого – Голея (W_{SG}=80%);
б) чистый речевой сигнал

5. Также исследован метод компенсации помеховых сигналов – *метод синхронной обработки зашумленных речевых сигналов*.

Суть данного метода шумоочистки заключается в синхронной регистрации сигнала двумя радиозакладками с вибродатчиками, размещенными на внешней поверхности стены помещения, защита которой производится одним вибропреобразователем средств защиты речевой информации.

Данный способ основывается на том, что скорости распространения звука в строительных конструкциях на порядок превышают скорость его распространения в воздухе (в кирпичной или бетонной стене этот показатель составляет около 3500–4000 м/с, в воздухе – около 340 м/с). Так, в случае расположения источника информации в произвольной точке выделенного помещения, а излучающего шум вибропреобразователя – в центральной части стены, и снимающих информацию вибродатчиков – на взаимном расстоянии около 3 м, сигнал на выходе каждого вибродатчика будет представлять собой смесь шума и речевого сигнала с различным временным смещением. Пример подобного канала утечки информации приведен на рис. 13.

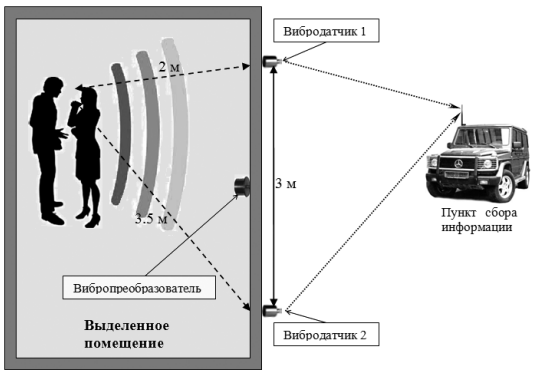

Рис. 13. Схема канала утечки речевой информации

Переданные в пункт сбора информации зарегистрированные сигналы в последующем могут быть обработаны по простейшему алгоритму, заключающемуся в нормировке по уровню и получении разностного сигнала. В результате обеспечивается практически полная очистка полезного речевого сигнала от шума [1].

Проведен эксперимент, в котором воспроизводилась модель данного канала утечки информации (рис. 14). Использовались: два персональных компьютера, два одинаковых микрофона и три колонки. К каждому компьютеру подключено по одному микрофону для записи акустических сигналов. Две колонки, подключенные к первому компьютеру, предназначены для воспроизведения шумовых помех. Третья колонка необходима для воспроизведения речевого сигнала.

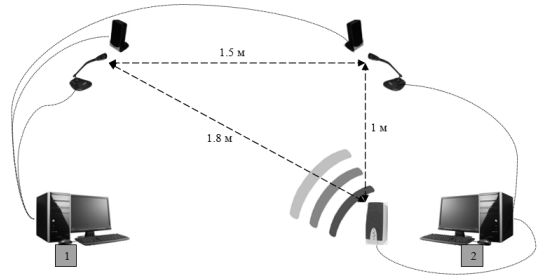

Рис. 14. Модель канала утечки речевой информации

Эксперимент производился следующим образом: на каждом персональном компьютере включались на запись акустические сигналы. В процессе записи первые две колонки, расположенные в непосредственной близости от микрофонов, воспроизводили шумовые сигналы длительностью 15 секунд. В этом интервале времени 15-ти секунд запускался на воспроизведение речевой сигнал длительностью 10 секунд с помощью третьей колонки.

Так как одновременное включение программы записи, установленной на каждом компьютере, маловероятно в силу человеческого фактора, дополнительно использовались импульсы синхронизации, которые представляли из себя три синусоидальных колебания. Данные импульсы синхронизации воспроизводились вместе с шумовым сигналом одним файлом. При обработке принятых сигналов выделяется часть сигнала, началом которого служат импульсы синхронизации. На рис. 15, изображены два принятых сигнала, синхронизированных по времени и нормированных по амплитуде.

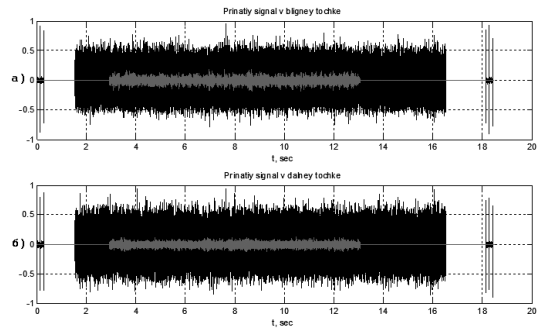

Рис. 15:
а) принятый сигнал в ближней точке;
б) принятый сигнал в дальней точке

В результате шумоочистки по данному методу в выделенном речевом сигнале значительно повысилась словесная разборчивость. Точное значение величины словесной разборчивости получить не удалось. Тем не менее, при воспроизведении и прослушивании выделенного речевого сигнала и очищенного с помощью фильтра Савицкого – Голея аудиосигнала можно объективно утверждать, что сообщение содержит достаточное количество правильно понятых слов, что позволяет уверенно понимать смысл разговора. Это говорит о том, что словесная разборчивость лежит в пределах 80–95%.

Все предыдущие результаты величин словесной разборчивости при анализе различных алгоритмов шумоочистки приводились для маскировки сигналов "белым" шумом, который является самым распространенным типом помехи, используемым в средствах защиты речевой информации. Также проведено сравнение результатов шумоочистки речевых сигналов для двух других типов маскирующих помех: *"розового" шума и "микшированной" помехи.* Так, наиболее надежную маскировку речевой информации из трех типов помех показал "розовый" шум. Практически такие же высокие результаты показала "микшированная" помеха, преимущество которой еще заключается в задании сравнимо меньшего значения отношения сигнал/шум (в среднем менее 2,5 дБ).

Анализ надежности шумовой маскировки речевой информации показывает, что использование различных алгоритмов шумоочистки и ведение многоканальной виброакустической разведки позволяют повысить величины словесной разборчивости и отношения сигнал/шум до уровня, достаточного для составления злоумышленником подробной справки о содержании перехваченного разговора.

В связи с этим появляется необходимость в создании наиболее эффективных средств и методов активной защиты речевой информации, учитывающих возможности шумоочистки речевых сигналов и ведения многоканальной речевой разведки. Для этого необходимо проанализировать, какие слабые и сильные стороны присутствуют в способах защиты от перехвата речевой информации.

Результаты экспериментальных исследований по сравнению маскирующих свойств трех различных типов помех показали, что наименее надежную маскировку речевой информации обеспечивает "белый" шум, при этом являясь самым распространенным типом помехи, используемым в сертифицированных средствах виброакустической защиты.

Далее необходимо проанализировать особенности работы различных алгоритмов шумоочистки речевых сигналов. Три из пяти алгоритмов: алгоритм вычитания амплитудных спектров, алгоритм оценивания минимальной среднеквадратической ошибки и нейросетевые алгоритмы – основываются на получении дополнительной статистической информации во время пауз разговора. Таким образом, у злоумышленника появляется возможность взятия образца чистого шумового сигнала. Это говорит о том, что непрерывный источник маскирующего шума является избыточным.

Предложен более эффективный метод маскировки речевых сигналов, который основывается на синхронном выключении источника шума на моменты пауз разговора.

Для этого необходимо задание порога срабатывания, который учитывает особенности пассивной защиты на основе звукоизоляции различных строительных материалов. Таким образом, если речевой сигнал имеет слабую интенсивность, то в этом случае сигнал защищается только пассивным способом, так как необходимость в активной защите отсутствует. На рис. 16 показана модель синхронной маскирующей помехи.

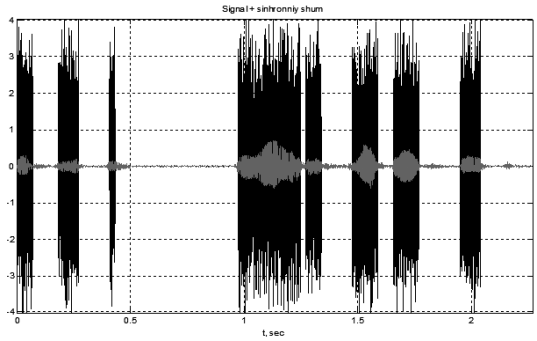

Рис.16. Синхронный шум

Также в алгоритме работы синхронного генератора шума должен производиться анализ частотного диапазона принимаемых сигналов.

В качестве альтернативы можно использовать неравномерный синхронный шум, уровень которого зависит от уровня анализируемого речевого сигнала. Модель такого шумового сигнала показана на рис. 17.

Таким образом, для каждого интервала речи обеспечивается минимально необходимая для защиты интенсивность помехового сигнала.

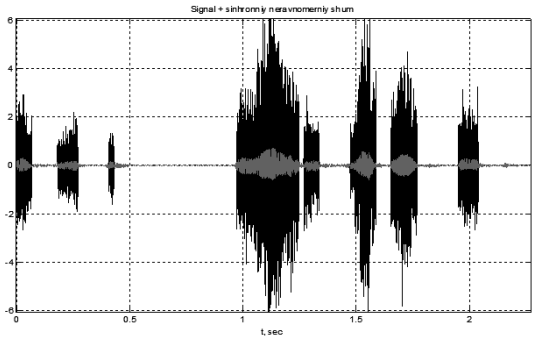

Рис. 17. Синхронный неравномерный шум

Из сертифицированных ФСТЭК России нет ни одной, обладающей подобной функцией выключения в моменты пауз разговора. Среди несертифицированных средств есть похожие системы, но при этом большая часть из них относится к мобильным средствам, использующим наушники, микрофоны и сильношумящие колонки, что неприемлемо при проведении закрытых совещаний.

В заключение необходимо отметить, что синхронный генератор шума имеет еще одно положительное свойство, связанное с минимизацией влияния на нервную систему человека, что в конечном итоге приводит к уменьшению дискомфорта при проведении переговоров.

Примечания

[1] Бортников А. Н. Совершенствование технологий информационной безопасности речи // Защита информации. Конфидент. – 2001. – №4. – С. 34–37.

[2] Покровский Н. Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962.

[3] Чучупал В. Я., Чичагов А. С., Маковкин К. А. Цифровая фильтрация зашумленных речевых сигналов. – Вычислительный центр РАН Москва, 1998. – 52 с.

[4] Уидроу Б., Стирнз С. Д. Адаптивная обработка сигналов. – М.: Радио и связь, 1989. – 440 с.

[5] Хайкин С. Нейронные сети: полный курс. М.: Издательский дом "Вильямс", 2006. – 1104 с.

[6] Валюх А. А., Хандецкий В. С. Адаптивный цифровой фильтр на основе нейронной сети // Нейроинформатика. – 2010. – №1. – С. 174–182.

Гуляев Владимир Павлович, кандидат технических наук, доцент каф. ТОР ИРИТ-РТФ ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина». E-mail: gulyaev-vp@ya.ru

Шушарин Александр Сергеевич, студент ИРИТ-РТФ ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина». E-mail: Shusharin-alex@mail.ru

ЦЕНТР ПО ЭКСПОРТНОМУ КОНТРОЛЮ ЮУрГУ

В соответствии с решением Комиссии по экспортному контролю Российской Федерации Южно-Уральский госуниверситет получил Свидетельство о специальном разрешении № 027 на осуществление деятельности по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля.

В настоящее время ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ) располагает научно-педагогическим персоналом с высоким профессиональным и интеллектуальным уровнем, а также развитой лабораторной базой, это позволяет профессионально и качественно осуществлять деятельность по проведению независимой идентификационной экспертизы товаров и технологий, проводимой в целях экспортного контроля.

В соответствии с номенклатурой продукции, в отношении которой планируется осуществлять экспертизу, подобрано 107 экспертов, из них докторов наук 35, кандидатов наук 57 и 15 специалистов, не имеющих ученой степени. Все эксперты являются сотрудниками университета и способны квалифицированно и качественно провести экспертизу.

Если Вы являетесь поставщиками оборудования, машин, материалов, запасных частей и комплектующих для них, выпускаете сложную технику, научно-техническую продукцию и Вам приходится сталкиваться с терминами **«экспортный контроль»** и **«товары двойного назначения»**, то мы можем быть Вам полезны.

В соответствии с российским законодательством экспертизу товаров и технологий для целей экспортного контроля могут проводить только экспертные организации, получившие специальное разрешение Комиссии экспортного контроля Российской Федерации.

Центр по экспортному контролю ЮУрГУ осуществляет деятельность по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля в отношении **продукции по всей номенклатуре действующих контрольных списков, утвержденных указами Президента Российской Федерации.**

Директор Центра:
Анатолий Григорьевич Мещеряков.
Тел. (351) 267-95-49.

Заключения нашей экспертизы действуют на всей территории России и являются официальным документом, подтверждающим принадлежность или непринадлежность объекта экспертизы к продукции, включенной в списки контролируемых товаров и технологий.

Наши услуги:

1. Оформление заключений идентификационной экспертизы для целей экспортного контроля и таможенного оформления.
2. Консультация по экспортному контролю товаров (технологии).

Перечень документов, необходимых для проведения экспертизы:

1. Заявка.
2. Контракт (договор, соглашение).
3. Спецификация (перечень поставляемой продукции) и иные приложения.
4. Техническая документация (паспорта, сертификаты качества, руководства по эксплуатации, технические описания, этикетки и пр.).
5. Доверенность.

Наши координаты

Адрес: 454080, пр. им. В. И. Ленина, 85, корпус 3А, ауд. 502.
Телефон (351) 267-95-49
E-mail: exp-174@mail.ru
Транспорт (автобус, троллейбус, маршрутное такси): остановка «ЮУрГУ»

ФИРМЕННЫЙ БЛАНК ОРГАНИЗАЦИИ

Исх. № _____
от «___» _____ 201__ г.

Директору Центра по экспортному
контролю ГОУ ВПО «ЮУрГУ»
А. Г. Мещерякову
454080, пр. им. В. И. Ленина, 85,
корпус 3А, ауд. 502

ЗАЯВКА
на проведение работ

Прошу Вас провести независимую идентификационную экспертизу товаров (технологий) в целях экспортного контроля и таможенного оформления.

Грузоотправитель: _____
_____

Грузополучатель: _____
_____

Перечень поставляемой продукции:

№ п/п	Наименование продукции	Единица измерения	Количество	Код ТН ВЭД

Оплату работ по выставлении счета гарантирую.

Уполномоченный по техническим вопросам: _____
_____

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Полезная информация

1. Экспертиза проводится в течение 3-х рабочих дней. По просьбе заказчика экспертиза может быть проведена в более короткие сроки.

2. Стоимость проведения экспертизы зависит от:

- объема рассматриваемого материала, продукции, информации, представленных согласно заявке;
- количества наименований товаров;
- количества кодов ТН ВЭД;
- сроков исполнения заявки;
- степени секретности материала, представленного на экспертизу.

3. Готовое заключение выдается на бумажном носителе (по просьбе заказчика — в электронном варианте).

4. Договор на оказание услуг заключается каждый раз в соответствии с заявкой.

Федеральные органы исполнительной власти

ФСТЭК России: http://www.fstec.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 организации, 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

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

AUT VIAM INVENIAM AUT FACIAM

Приглашаем на программу повышения квалификации

«СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННО-ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ»

(в рамках указанной образовательной программы предоставляются дополнительные консультационные услуги)

Занятия проводят ведущие специалисты в области делопроизводства и информационных сетевых технологий Южно-Уральского государственного университета

Участникам выдается удостоверение о повышении квалификации государственного образца
Лицензия на образовательную деятельность № 0816 от 03.03.2011 г.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПРОГРАММЫ

Документационное обеспечение управления (ДОУ):

- Классификация документов;
- Особенности составления и оформления распорядительных, организационно-правовых, информационно-справочных документов;
- Требования к реквизитам бланков документа;
- Организация документооборота;
- Порядок движения документов в организации;
- Обработка документов (регистрация документов, контроль за исполнением документов) с помощью программы Excel;
- Номенклатура дел, порядок составления;
- Определение сроков хранения документов;
- Применение нового «Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения»;
- Формирование и оформление дел постоянного, временного (свыше 10 лет) хранения;
- Экспертиза ценности документов (ЭЦД);
- Порядок проведения ЭЦД;
- Подготовка документов к уничтожению;
- Правила оформления акта о выделении к уничтожению документов;
- Составление и оформление описей на дела постоянного, временного (свыше 10 лет) хранения.

Правовые основы:

• Современная нормативно-методическая база по делопроизводству;

• Правила выдачи и свидетельствования предприятиями, учреждениями и организациями копий документов;

• Организационно-правовые основы документирования управленческой деятельности.

Органы управления ДОУ:

• Службы документационного обеспечения управления;

• Положение о службе документационного обеспечения управления и должностные инструкции работников.

IT-технологии:

• Типы компьютерных сетей;

• Основные сведения о сети Интернет и локальной сети;

• Семейство протоколов TCP/IP и адресация компьютеров;

• Online-справочники;

• Поисковые системы;

• Принцип работы поисковых серверов;

• Web-каталоги и web-индексы;

• Электронная почта;

• Правила работы с электронным сообщением;

• Безопасность и защита информации при работе в Интернете.

Стоимость участия одного слушателя составляет 6480 руб.

(шесть тысяч четыреста восемьдесят) рублей 00 коп., НДС не облагается

При участии пяти и более человек от одной организации предоставляется скидка 10%

Оплата производится на расчетный счет

454080, г. Челябинск, пр. В. И. Ленина, 76.
ИНН 7453019764/КПП 745301001
УФК по Челябинской области (ФГБОУ ВПО «ЮУрГУ» (НИУ)
л/с 20696X28730)
р/с 40501810600002000002
БИК 047501001, ОКПО 02066724
ОКАТО 75401000000, ОГРН 1027403857568
ГРКЦ ГУ Банка России по Челябинской области,
г. Челябинск, КБК 00000000000000000130
В платежном поручении в графе «назначение платежа» указать:
«За обучение Ф.И.О. по «Современным технологиям информационно-документационного обеспечения управления».
Копию платежного поручения иметь при себе.

Продолжительность программы составляет 72 часа

Предлагаем повысить Ваш квалификационный уровень по программе, содержащей курс лекций и практические занятия

Занятия проводятся по мере комплектования групп

Желаем успеха Вам и Вашему бизнесу!

Заявки на участие по программе повышения квалификации принимаются по телефонам:
(351) 267-90-51; 267-99-00 (факс)

E-mail: admin@susu.ac.ru / bov@susu.ac.ru
Сайт: www.susu.ac.ru
г. Челябинск

ЗАЯВКА

на обучение по программе повышения квалификации в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

ФИО участника: _____

Должность: _____

Наименование организации: _____
(полное и сокращенное)

_____

Руководитель организации: _____

Прошу внести меня в список обучающихся по программе повышения квалификации «Современные технологии информационно-документационного обеспечения управления».

_____/_____
(расшифровка подписи)

Реквизиты организации:

юр. адрес: _____ БИК: _____

_____ ОГРН: _____

р/с: _____ ОКПО: _____

в _____ телефон: (_____)_____

к/с: _____ тел. (факс): _____

ИНН/КПП: _____ e-mail: _____

Оплату услуг по настоящей заявке согласно выставленному Исполнителем счету гарантируем.

Руководитель организации _____/_____
М.П. (расшифровка подписи)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

AUT VIAM INVENIAM AUT FACIAM

Приглашаем на программу повышения квалификации

«КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ»

Приглашаются должностные лица,
ответственные за организацию и обеспечение защиты персональных данных

Занятия проводят ведущие специалисты в области документационного обеспечения управления и защиты информации Южно-Уральского государственного университета

Участникам выдается удостоверение установленного образца
Лицензия на образовательную деятельность № 0816 от 03.03.2011 г.

В связи с подписанием Президентом РФ новой редакции Федерального закона «О персональных данных» от 25.07.2011 года организации, предприятия и учреждения обязаны разработать комплекс мер, обеспечивающих конфиденциальность персональных данных работников и клиентов, таким образом создать систему защиты персональных данных на предприятии и в его структурных подразделениях.

В соответствии с требованиями настоящей редакции закона Оператор обязан издать документы, определяющие политику оператора в отношении обработки персональных данных (ПДн) и устанавливающие процедуры, направленные на предотвращение нарушений законодательства.

Предлагаем повысить Ваш квалификационный уровень по программе, содержащей курс лекций и практические занятия.

По окончании обучения слушателю предоставляется раздаточный материал, включающий подборку нормативных правовых актов, документов, перечень web-порталов и иных полезных ресурсов сети Internet.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПРОГРАММЫ

• Классификация и правовые основы защиты сведений конфиденциального характера;

• Правовые основы защиты ПДн в организации;

• Внутренние документы организации, регламентирующие обработку (автоматизированную, неавтоматизированную) персональных данных;

• Организация работы со сведениями, составляющими служебную тайну;

• Организация работы по обеспечению безопасности ПДн;

• Правила осуществления допуска должностных лиц к обработке ПДн;

• Порядок осуществления внутреннего контроля обработки ПДн;

• Практикум «Разработка Положения о защите ПДн в организации».

Стоимость участия одного слушателя составляет 12 960 руб.
(двенадцать тысяч девятьсот шестьдесят) рублей 00 коп., НДС не облагается
При участии четырех и более человек от одной организации предоставляется скидка 10%

Иногородним участникам программы предлагается проживание в одно- и двухместных номерах различной степени комфортности гостиницы университета

Продолжительность программы составляет 72 часа

Оплата производится на расчетный счет
454080, г. Челябинск, пр. В. И. Ленина,76.
ИНН 7453019764/КПП 745301001
УФК по Челябинской области (ФГБОУ ВПО «ЮУрГУ» (НИУ)
л/с 20696Х28730)
р/с 40501810600002000002
БИК 047501001, ОКПО 02066724
ОКАТО 75401000000, ОГРН 1027403857568
ГРКЦ ГУ Банка России по Челябинской области,
г. Челябинск, КБК 00000000000000000130
В платежном поручении в графе «назначение платежа» указать:
«За обучение Ф.И.О. по «Конфиденциальному делопроизводству и организации работы с персональными данными».
Копию платежного поручения иметь при себе.

Занятия проводятся по мере комплектования групп
Желаем успеха Вам и Вашему бизнесу!

Заявки на участие по программе повышения квалификации принимаются по телефонам:
(351) 267-90-51; 267-99-00 (факс)
E-mail: admin@susu.ac.ru / bov@susu.ac.ru. Сайт: www.susu.ac.ru
г. Челябинск

ЗАЯВКА

на обучение по программе повышения квалификации в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

ФИО участника: _____

Должность: _____

Наименование организации: _____
(полное и сокращенное)

_____

Руководитель организации: _____

Прошу внести меня в список обучающихся по программе повышения квалификации «Конфиденциальное делопроизводство и организация работы с персональными данными».

_____/_____
(расшифровка подписи)

Реквизиты организации:

юр. адрес: _____ БИК: _____

_____ ОГРН: _____

р/с: _____ ОКПО: _____

в _____ телефон: (_____)_____

к/с: _____ тел. (факс): _____

ИНН/КПП: _____ e-mail: _____

Оплату услуг по настоящей заявке согласно выставленному Исполнителем счету гарантируем.

Руководитель организации _____/_____
М.П. (расшифровка подписи)

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.

ОБРАЗЕЦ

УДК
ББК

А. А. Первый, Б. Б. Второй, В. В.Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 3–4(5–6)/2012

Подписано в печать 25.12.2012. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 6,45. Тираж 300 экз. Заказ 28/159.
Цена свободная.

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