ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(7) / 2013

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

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

КАДРОВАЯ БЕЗОПАСНОСТЬ

ПРАКТИЧЕСКИЙ АСПЕКТ

ORGANIZATIONAL AND TECHNICAL PROTECTION OF INFORMATION

PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT AND COMPUTER INFORMATION

ORGANIZATIONAL AND LEGAL PROTECTION OF INFORMATION

PERSONNEL SECURITY

THE PRACTICAL ASPECT

УДК 004.056 + 621.391 : 004.056 + 621.317.7 + 005.922.1
ББК 32.88 + 32.973 Х401.114

Антясов И.С., Петров И.С., Соколов А.Н.

АНАЛИЗ ТРЕБОВАНИЙ НОРМАТИВНО-ТЕХНИЧЕСКИХ ДОКУМЕНТОВ К АЛЬТЕРНАТИВНЫМ ИЗМЕРИТЕЛЬНЫМ ПЛОЩАДКАМ ДЛЯ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ

В статье рассмотрена модель возможного канала утечки информации и проанализированы требования ГОСТов к альтернативным измерительным площадкам для проведения специальных исследований технических средств.

Ключевые слова: *антенна; вспомогательные технические средства и системы (ВТСС); измерительная площадка; информационный сигнал; канал утечки информации; передатчик; побочные электромагнитные излучения и наводки (ПЭМИН); полубезэховая камера; приёмник; специальные исследования; технические средства хранения, обработки и передачи конфиденциальной информации (ТСПИ).*

Antyasov I.S., Petrov I.S., Sokolov A.N.

ANALYSIS OF TECHNICAL STANDARDS' REQUIREMENTS FOR ALTERNATIVE TECHNIC STUDY TEST SITES

The article contains a model of possible information leakage and analysis of Russian National Standard's (ГОСТ, or GOST) requirements for alternative technic study test sites.

Keywords: *antenna; support technology and systems; test site; data signal; covert channel; transmitter; side electromagnetic radiation and pickups; hemi-anechoic chamber; receiver; technic study; technology for storage, processing and transmission of confidential information.*

Специальные исследования (специсследования, СИ) — выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем, а также оценка соответствия защиты информации требованиям нормативных документов по защите информации[1]. Проведение специальных исследований технических средств хранения, обработки и передачи конфиденциальной информации (ТСПИ) регламентирует-

Рис. 1. Модель канала утечки

ся руководящими и нормативно-методическими документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ) России.

Задачей СИ является выявление и измерение так называемых «опасных» сигналов – информационных сигналов в каналах возможной утечки информации. Как правило, величины «опасных» сигналов малы по сравнению с присутствующими в эфире сигналами, поэтому задача их надёжной идентификации достаточно сложна. Идентификацию также затрудняют и помехи. Ошибка на этапе идентификации может привести либо к пропуску «опасного» сигнала, либо к завышению результатов.

Как и любой канал связи, канал утечки состоит из передатчика, собственно канала (с шумами) и приёмника (рис. 1).

В качестве передатчика может выступать любое техническое средство, являющееся источником «опасного» сигнала – сигнала с защищаемой информацией. Каналом утечки является среда распространения сигнала передатчика. Приёмник в данной модели – это технические средства перехвата информации потенциального противника.

Для обеспечения защиты информации от возможной утечки в рамках приведённой модели в точке размещения технических средств потенциального противника необходимо обеспечить такое соотношение сигнал – шум, которое не позволит противнику получить защищаемую информацию.

Задача СИ, как комплекса работ, позволяющего установить, возможна ли утечка информации в данном канале, сводится к измерению сигналов передатчика и пересчёту измеренных значений к величине, которая может поступить на вход оптимально адаптированного к данному виду информации приёмника потенциального противника.[2]

Наиболее важным этапом СИ является измерение сигналов передатчика. В зависимости от целей и задач специальных исследований, их целесообразно разделить на два вида по способу измерений:

- стендовые (лабораторные) специальные исследования;
- объектовые специальные исследования.

Основной целью стендовых специальных исследований ТСПИ является выявление и оценка опасности таких технических каналов утечки информации, как:

- побочные электромагнитные излучения и наводки (ПЭМИН) на оконечные устройства и линии вспомогательных технических средств и систем (ВТСС);
- наводки в сетях электропитания и заземления ТСПИ, обусловленные обработкой конфиденциальной информации в ТСПИ;
- акустоэлектрические преобразования в ТСПИ, обусловленные воздействием акустических сигналов, циркулирующих в помещении;
- паразитная генерация узлов и элементов ТСПИ, обусловленная обработкой конфиденциальной информации в ТСПИ.[3]

Основными задачами стендовых специальных исследований являются:

- выявление вышеперечисленных технических каналов утечки информации;
- расчёт показателей защищенности ТСПИ от утечки конфиденциальной информации по выявленным техническим каналам утечки информации;
- формирование так называемого «паспорта» ТСПИ, состоящего из протоколов проведенных специальных исследований, в которых приведены результаты измерений и расчётов, а также предписания на эксплуатацию ТСПИ, где изложены требования по защите информации.

Объектовые специальные исследования ТСПИ проводятся на конкретном объекте в условиях мешающего воздействия различных факторов и заключаются в оценке защищённости объекта информатизации в целом от перехвата информации в местах возможного размещения средств разведки.

Таким образом, сформированный в ходе стендовых исследований «паспорт» ТСПИ для неизменного комплекта ТСПИ является постоянным, в то время как результаты объек-

товых специальных исследований могут варьироваться в зависимости от места расположения объекта информатизации и способа размещения ТСПИ на объекте.

Для обеспечения постоянства результатов стендовых специальных исследований для одного и того же комплекта ТСПИ требуется эталонная измерительная площадка, на которой все мешающие воздействия сведены к минимуму или однозначным образом могут быть учтены при расчётах показателей защищенности ТСПИ. В противном случае, если стендовые специальные исследования проводятся в случайном или неизвестном с точки зрения мешающих воздействий месте, результаты исследований не совпадут с результатами специальных исследований при переносе ТСПИ на другой объект.

Измерительная площадка[4] – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней источника индустриальных радиопомех, излучаемых ТС в регламентированных условиях. Существует два типа измерительных площадок:

- открытые измерительные площадки, удовлетворяющие требованиям к затуханию;
- альтернативные измерительные площадки (АИП), физические характеристики которых отличны от характеристик открытых измерительных площадок, но при этом они удовлетворяют требованиям по затуханию и уровням промышленных радиошумов.

Открытые измерительные площадки устраивают вдали от городов, промышленных предприятий, загруженных автомобильных трасс и линий электропередач. С открытыми измерительными площадками возникает ряд проблем:

- недоступность мест вдали от индустриальных радиопомех;
- невозможность проведения специальных исследований круглогодично, так как исследуемое ТС должно находиться в своих рабочих условиях (комнатная температура, определенная относительная влажность);
- неудобство в электроснабжении.

Перечисленные проблемы приводят к необходимости проведения абсолютного большинства СИ на АИП, построение которых также приводит к необходимости решения ряда вопросов:

- экранирование от внешних электромагнитных излучений (ЭМИ);
- поглощение внутренних ЭМИ.

Решение обозначенных проблем условно можно разделить на три этапа:

- экранирование,
- радиопоглощение,
- применение радиочастотных фильтров.[5]

Экранирование (электромагнитное) – способ ослабления электромагнитной помехи с помощью экрана с высокой электрической и (или) магнитной проводимостями.[6] Экранирование зависит от поверхностного сопротивления материала, из которого выполнен экран, и волнового сопротивления (для падающей волны) пространства. Наиболее эффективно использовать материалы с хорошей проводимостью в качестве экрана, такие как медь и алюминий[7]. Наиболее сложным диапазоном в экранировании являются частоты до 30 МГц, а для экранирования частот свыше 300 МГц достаточно использование проводящих сетчатых материалов.

При оборудовании помещения необходимо обеспечить радиопоглощение электромагнитных волн для уменьшения переотражений от стен экрана (стоячие волны). Стоячая волна возникает при отражениях от преград и неоднородностей в результате наложения отраженной волны на падающую. Для решения данной проблемы используют специальные неметаллические материалы, состав и структура которых обеспечивают эффективное поглощение (при незначительном отражении) электромагнитной энергии в определённом диапазоне длин радиоволн.

В экранированное помещение вводятся сигнальные кабели и электропроводка. В результате их прокладки образуется связь с внешней средой и в экранированное помещение проникают помехи. Для ослабления помех по сетям электропитания устанавливают соответствующие фильтры.

Таким образом, необходимо устраивать АИП в помещениях, изначально имеющих высокую степень экранирования. Как правило, подбирают подвальные помещения с толстыми несущими стенами без окон и как можно дальше от торцевых стен. Само помещение представляет собой экранированную камеру с многослойной защитой, в которой каждый слой решает определенные функции. Так как на полу должен быть токопроводящий металлический лист, то АИП можно отнести к полубезэховой камере.

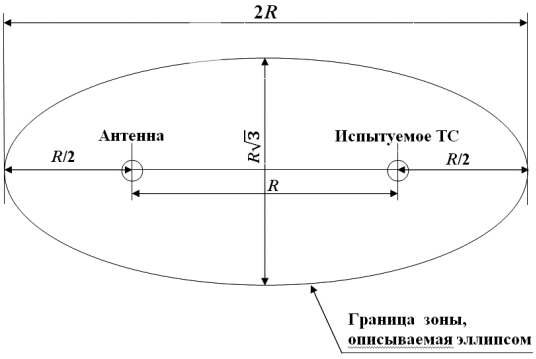

Рис. 2. Зона измерительной площадки с поворотной платформой

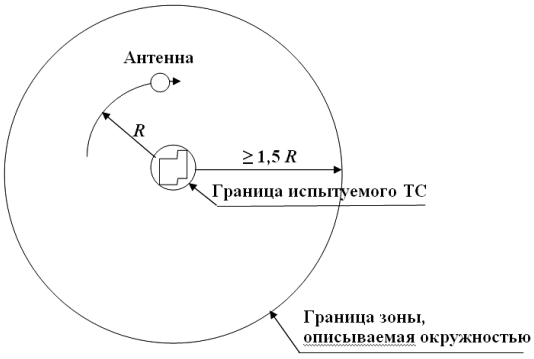

Рис. 3. Зона измерительной площадки со стационарным испытуемым ТС

Полубезэховая камера – это экранированное помещение, у которого стены и потолок покрыты радиопоглощающим материалом. Абсорбирующие материалы присутствуют только на стенах и потолке, а пол остается отражающим (для испытаний на излучения).[8]

В соответствии с требованиями ГОСТа[4], плоскость для АИП должна быть ровной и свободной от каких-либо предметов, отражающих электромагнитную энергию в пределах:

- эллипса (рис. 2), если площадка оборудована поворотной платформой для размещения испытуемого ТС;
- круга (рис. 3), если испытуемое ТС устанавливают стационарно и измерительную антенну перемещают вокруг него.

На представленных рисунках R – расстояние между антенной и испытуемым ТС.

Для АИП граница эллипса или круга означает площадь пола, за которой могут размещаться ограждающие конструкции камеры или помещения. При этом радиопоглощающее покрытие должно размещаться на расстоянии не менее 1 м от контура испытуемого ТС и антенны. Высота потолка должна быть не менее 3 – 4 м, чтобы обеспечить изменение высоты установки антенны от 1 до 4 м при измерительном расстоянии не более 10 м с учётом линейных размеров антенны и необходимостью изменения поляризации с горизонтальной линейной на вертикальную линейную путём разворота антенны в вертикальное положение.

Для открытой и альтернативной площадок измерительная аппаратура и обслуживающий персонал размещаются вне площадок. Электрические и радиочастотные кабели, подводимые к антенне и испытуемому ТС, прокладываются под проводящей поверхностью или на ней с обязательным жестким креплением их к поверхности. Провода прокладываются перпендикулярно к оси измерения. Кроме этого, антенные кабели должны быть ортогональны продольным осям элементов антенны, а расстояние между самым дальним краем антенны и вертикальным снижением кабеля – не менее 1 м.

При аттестации измерительных площадок для проведения стендовых СИ испытуемых ТС особое место занимает измерение параметров затухания электрической составляющей электромагнитной волны на открытой (альтернативной) измерительной площадке и проверка отсутствия сверхнормативных отражений в соответствии с требованиями ГОСТа[4].

Измерение параметров затуханий электромагнитных волн на измерительной площадке проводят следующим образом. Для заданного частотного ряда в диапазоне от 30 до 1000 МГц экспериментально определяют напряжение тестового сигнала генератора в различных участках некоторого испытуемого объёма, измеренное по полю. Для этого на заданном измерительном расстоянии устанавливают передающую и приёмную антенны одинакового типа. На тестовом генераторе устанавливают максимальный выходной уровень и отсчитывают уровень напряжения по индикатору измерительного прибора на каждой частоте из заданного ряда. Аналогичные измерения проводят слева, справа, спереди и сзади испытуемого объёма, а также при различных высотах расположения антенн – от 1 до 4 м и для двух видов поляризации: горизонтальной и вертикальной.

Оценка соответствия параметров затухания измерительной площадки проводится расчётным методом по формуле

$$\Delta = A_n - A_э,$$

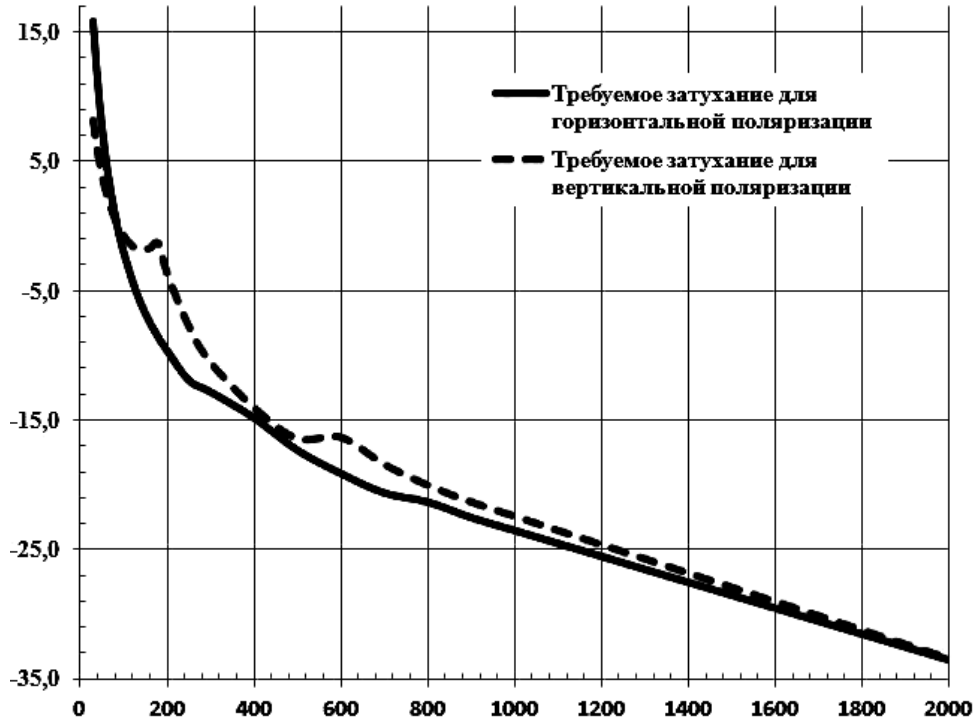

Рис. 4. Нормированные значения затуханий при горизонтальной и вертикальной поляризации

где Δ – отклонение экспериментального затухания от нормы, дБ,

$A_э$ – затухание электромагнитных волн, полученное по результатам экспериментальных исследований на измерительной площадке, дБ,

A_n – нормированное затухание электромагнитных волн на измерительной площадке, приведенное в ГОСТ4, дБ.

Затухание электрической составляющей электромагнитной волны, полученное по результатам экспериментальных исследований на измерительной площадке, рассчитывается по формуле

$$A_э = U_2 - U_1 - K_{пер} - K_{пр} - K_{вз},$$

где U_2 – уровень напряжения тестового сигнала на входе измерительного приёмника, измеренный по кабелю, дБ;

U_1 – уровень напряжения тестового сигнала на входе измерительного приёмника, измеренный по полю, дБ;

$K_{пер}$ – коэффициент калибровки передающей антенны, дБ;

$K_{пр}$ – коэффициент калибровки приёмной антенны, дБ;

$K_{вз}$ – поправочный коэффициент, учитывающий взаимный импеданс антенн, дБ.

Разности между A_n и $A_э$ не должны превышать допуск ±4 дБ. Стоит отметить, что при стендовых специальных исследованиях на ПЭМИН приходится выходить в частотном диапазоне за 1000 МГц, поэтому целесообразно расширить ряд значений частот измерений при проведении аттестации измерительной площадки, например до 2 ГГц. Несмотря на то, что ГОСТ4 не предусматривает проверку в диапазоне свыше 1000 МГц, то можно провести экстраполяцию нормированных затуханий электромагнитных волн (рис. 4).

Сформулируем основные требования к АИП:

- помещение должно иметь размеры не менее 3 х 3 х 3 м;
- измерительная аппаратура и обслуживающий персонал размещаются вне площадок;
- заземление должно соответствовать нормам и требованиям нормативных документов;
- на полу должна располагаться пластина заземления не менее 2 х 2 м с зажимами для заземления;
- необходимо использование сетевого помехоподавляющего фильтра;
- АИП должна обеспечивать экранирование не менее 30 дБ;
- затухание не должно отличаться от нормированных значений более чем на ±4 дБ.

Примечания

[1] ГОСТ Р 51583 – 2000. Порядок создания автоматизированных систем в защищенном исполнении. – Введ. 2000-06-04. – М.: Госстандарт России, 2000. – 12 с.

[2] Бузов, Г.А. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

[3] Кондратюк, А.П. Правила устройства и аттестации измерительных площадок для проведения специальных исследований // Информационно-методический журнал «Защита информации. Инсайд». – 2008. – №1 – С. 37 – 41.

[4] ГОСТ Р 51320 – 99. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных помех. – Введ. 1999-22-12. – М.: Госстандарт России, 1999. – 27 с.

[5] Петров, И.С. Локализация и ослабление побочных электромагнитных излучений от средств вычислительной техники путем экранирования электромагнитных волн // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2012. – №23. – С. 189 – 191.

[6] ГОСТ Р 30372 – 95. Совместимость технических средств электромагнитная. Термины и определения. – Введ. 1997-01-01. – М.: Госстандарт России, 1996. – 11 с.

[7] ГОСТ Р 50414 – 92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний. – Введ. 1992-26-11. – М.: Госстандарт России, 1992. – 28 с.

[8] Зайцев, А.П. Технические средства и методы защиты информации / А.П. Зайцев, А.А. Шелупанов. – М.: Машиностроение, 2009. – 507 с.

Антясов Иван Сергеевич, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), E-mail:antyasov@gmail.com

Петров Игорь Сергеевич, преподаватель кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет) E-mail: petrov@unit74.ru

Соколов Александр Николаевич, кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), E-mail: ANSokolov@inbox.ru

Antyasov Ivan Sergeevich, student of Information Systems Security Department, South Ural State University (national research university), Email:antyasov@gmail.com

Petrov Igor Sergeevich, lecturer of Information Systems Security Department, South Ural State University (national research university), Email: petrov@unit74.ru

Sokolov Aleksandr Nikolaevich, candidate if engineering sciences, associate professor, head of Information Systems Security Department, South Ural State University (national research university), Email: ANSokolov@inbox.ru

УДК 004.056.5 + 342.7 : 004.056.5
ББК 32.973 Х 400.323

Мищенко Е.Ю., Соколов А.Н.

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Обезличивание – способ обработки персональных данных, целью которого является приведение этих данных в защищённое состояние, которое не позволяет злоумышленнику использовать их во вред физическому лицу. Фактически это способ защиты персональных данных, особенностью которого является изменение не среды обработки, а самого представления информации. В данной статье рассматривается терминология процесса обезличивания персональных данных.

Ключевые слова: *защита информации, персональные данные, обезличивание.*

Mishchenko E.Yu., Sokolov A.N.

DEPERSONALIZATION OF PERSONAL DATA: TERMS AND DEFINITIONS

Depersonalization is the way of personal data processing for the purpose of transforming data to protected status, in order to prevent disturber use it to damage the person. In fact depersonalization is the way to protect personal data, having feature to change not environment, but data performance. This article consider the terminology of personal data depersonalization.

Keywords: *information security, personal data, depersonalization.*

В соответствии со статьёй 3 Федерального закона «О персональных данных» (далее по тексту – Закон[1]) обезличивание персональных данных (ПД) – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту ПД.[1] Из определения термина «Обработка ПД» той же статьи Закона следует, что обезличивание ПД – это вид обработки ПД. Рассмотрим обезличивание как процесс обработки ПД.

Закон определяет следующие стороны любого процесса обработки ПД:

1) Человек (физическое лицо) – субъект обработки ПД;
2) ПД конкретного Человека;
3) Оператор (уполномоченный) – орган (или лицо), обрабатывающий или организующий обработку ПД;
4) Контролёр – федеральный орган исполнительной власти, контролирующий выполнение Закона.

Следовательно, определение обезличивания можно перефразировать так: обезличивание – это такие действия Оператора с ПД конкретного Человека, в результате которых Контролёр не сможет без помощи Оператора

доказать, что полученная им информация является ПД этого конкретного Человека. Рассмотрим, как различные стороны процесса обезличивания связаны друг с другом на модели связей сторон процесса обработки ПД (рис. 1).

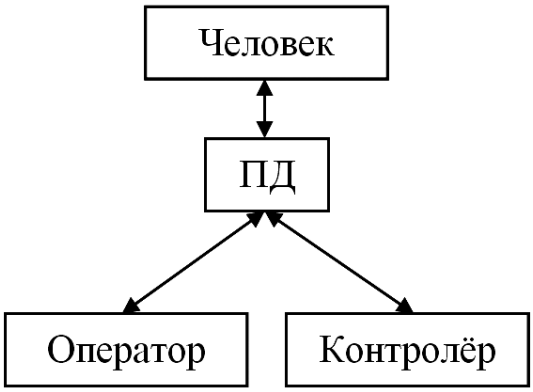

Рис. 1. Связи сторон процесса обработки ПД

1. Связь Человек – его ПД. Рассмотрим связь Человек – ПД. Согласно Закону, ПД – это любая информация, относящаяся к Человеку. Причем, к «прямо или косвенно определённому или определяемому»[1]. Слово «прямо» означает, что Человек сам подтверждает принадлежность своих ПД, а слово «косвенно» означает подтверждение принадлежности любым другим способом. Если связь устанавливается от Человека к ПД – то «определённому», если от ПД к Человеку – значит «определяемому».

В двух приведённых определениях мы столкнулись сразу с двумя формами связи Человека и его ПД: ПД «принадлежат» Человеку и «относятся» к нему. «Отношение» – термин скорее философский и отражает причинно-следственную связь: Человек является причиной существования своих ПД. «Принадлежность» – термин скорее юридический и отражает право собственности: Человек (а потом его наследники) является владельцем всех своих ПД. Закон говорит, что если информация «относится» к Человеку, то это ПД, и они этому Человеку «принадлежат». Следовательно, для обоснования «принадлежности» необходимо сначала прояснить значение термина «отношение».

Итак, Человек в процессе жизнедеятельности непрерывно порождает ПД. Причём происходит это чаще всего независимо от его воли и в совершенно необрабатываемом виде. Как и любые информационные сигналы, ПД сразу начинают распространяться во все стороны, причём только очень малую долю этой информации удаётся формализовать и приспособить для дальнейшей обработки, т.е. зафиксировать на каком-либо носителе (фотография, звукозапись, гораздо реже – читаемый текст).

В статье 1 Закона прямо сказано о том, что Закон регулирует обработку ПД именно на носителях. Но даже те ПД, которые хранятся на носителях, крайне редко сопровождаются подтверждением, к кому именно они относятся (нет подписи самого Человека или, скажем, решения суда). А пока подтверждения нет, эти ПД ни к кому не относятся и, строго говоря, не являются ПД.

С другой стороны, если подтверждение было, то оно распространяется на результаты любой Законной обработки ПД этого Человека. Однако есть один нюанс – Человек (или суд) даёт подтверждение исключительно на бумажном носителе, а ПД хранятся в электронном виде (к сожалению, электронной подписью в данном случае придётся пренебречь в связи с её малой распространённостью).

Значит ли это, что подтвердить «отношение» (и, следовательно, «принадлежность») ПД к конкретному Человеку автоматизированным путём невозможно?

По Закону ПД относятся к Человеку «прямо или косвенно определённому». И хотя можно перевести «прямую» подпись Человека в электронный вид (цифровое фото) или использовать электронный сертификат подлинности, на практике преимущественно используются косвенные методы. Методы обработки ПД определяются Оператором, т.е. относятся к связи Оператор – ПД.

2. Связь Оператор – ПД. В идеальном случае ПД должны относиться к единственному Человеку, и любая обработка ПД Оператором включает процесс проверки этого отношения, называемый идентификацией. Строго говоря, идентификация – это процесс сравнения двух различных наборов информации с целью удостовериться в их однозначном соответствии друг другу. Например, при личной проверке документов сотрудник охраны производит визуальное сравнение образа лица реального Человека с его изображением на фотографии, а системы контроля доступа производят автоматизированное сравнение образа отпечатка пальца с его математическим описанием в базе данных. Есть три варианта результатов сравнения:

1) положительный (все сравниваемые реквизиты совпадают) – значит, прочие (которые не сравнивались) данные (напечатанные в паспорте или хранящиеся в базе данных) являются ПД этого Человека;
2) отрицательный (не все сравниваемые реквизиты совпадают) – значит, прочие данные не являются ПД этого Человека;
3) ошибочный (технологически это возможно) – результат сравнения является сомнительным и не показывает ничего.

Во избежание ошибочного результата необходимо увеличивать количество сравниваемых реквизитов, а также совершенствовать технологию сравнения, например, применяя метод аутентификации – сравнение специальных трудно подделываемых реквизитов – хэш-функций, электронных ключей и т.д.

После обработки имеющегося объёма информации результат сравнения может измениться в любую сторону. Если в качестве процесса обработки применить обезличивание, то увидим следующую картину. Есть некий набор информации, принадлежащий конкретному Человеку (идентифицирующий его). Если в результате некоторых действий этот (точнее, уже изменившийся) объём уже не определяет (не идентифицирует) конкретного Человека, то эти некоторые действия в совокупности являются обезличиванием ПД. При этом ПД перестают быть ПД. То есть встречающийся местами термин «обезличенные ПД» – определяет не конечный вид ПД, а первоначальный источник информации. Выводы таковы:

4) имеющийся объём информации о Человеке только тогда является ПД этого Человека, когда данный объём однозначно определяет его (идентифицирует);
5) после любой обработки, кроме обезличивания, набор ПД должен идентифицировать Человека;
6) если имеющийся объём информации не определяет прямо или косвенно конкретного Человека, то этот объём информации не является ПД этого Человека.

Но, имея в распоряжении некий набор информации, нельзя понять точно – получился ли он в результате обезличивания или не имеет к ПД никакого отношения. Поэтому фактически в определении обезличивания заложено еще одно важное требование, следующее из словосочетания «…невозможно без использования дополнительной информации определить…»[1], а именно – обезличивание ПД должно быть обратимой операцией, иначе это будет просто потеря (уничтожение) ПД.

Оценка степени обезличивания не является обязательной для Оператора, это действие является функцией Контролёра.

3. Связь Контролёр – ПД. При попытке определить, является ли некий набор информации обезличенными ПД, Контролёр может столкнуться со следующими ситуациями:

1) в рамках данного набора информации можно идентифицировать Человека без дополнительной информации – это обычные ПД;
2) в рамках данного набора информации нельзя идентифицировать Человека, но при наличии некоторой дополнительной информации это можно сделать – либо ПД были обезличены, либо изначально набор был неполным (т.е. это были не ПД!);
3) даже при наличии некоторой информации, дополнительной к имеющемуся набору информации, Человека идентифицировать нельзя – либо ПД были уничтожены (частично), либо этот набор информации не был ПД.

Первый случай кажется простым, но это только на первый взгляд – ведь сравнивать-то информацию не с чем (других сведений об этом Человеке нет!). Поэтому мы идентифицируем Человека условно – по принципу уникальности (считается, что такой набор информации не может однозначно соответствовать различным людям). А если среди реквизитов будет штамп «копия верна» от миграционной службы – будет ли это достаточным условием идентификации? Однозначно решить сложно.

Второй случай сложнее, так как даже для условной идентификации данных не хватает, а термин «дополнительная информация» не очевиден по сути – то ли это дополнительные реквизиты Человека, то ли некий алгоритм обратной переработки информации. Оглядываясь на первый случай, хочется добавить уже упомянутый штамп и успокоиться. Только оснований для этого недостаточно.

Третий случай – самый сложный. Ведь оценивать обезличивание будет совсем не

Оператор, который обезличивал ПД. Оценивать будет либо Контролёр, либо Злоумышленник (раньше мы о нём не упоминали, но он есть!). И факт того, что им никак не удалось идентифицировать Человека, может говорить о том, что их средства были недостаточными, а не о том, что ПД принципиально не восстанавливаются.

Из выше сказанного следует, что процессы обезличивания и идентификации не могут быть описаны исключительно на качественном уровне. Кроме качественных критериев необходимо ввести количественные, такие как, например, вероятность идентификации и степень обезличивания, но рассмотрение этих параметров выходит за рамки данной статьи.

Примечания

[1] Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» (в редакции 2011 года) [электронный ресурс]. URL: http://www.garant.ru

Мищенко Евгений Юрьевич, старший преподаватель кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), E-mail: Eug6303@mail.ru

Соколов Александр Николаевич, кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), E-mail: ANSokolov@inbox.ru

Mishchenko Evgeny Yurievich, senior lecturer of Information Systems Security Department, South Ural State University (national research university), Email: Eug6303@mail.ru

Sokolov Aleksandr Nikolaevich, candidate of engineering sciences, associate professor, head of Information Systems Security Department, South Ural State University (national research university), Email: ANSokolov@inbox.ru

ББК Х 401.114(2)
УДК 34 : 004 + 347.77 : 004

ВОЛКОВ Ю. В.

ОБ ИСПОЛЬЗОВАНИИ В РОССИИ ЭЛЕКТРОННОЙ ПОДПИСИ, ПОЛУЧЕННОЙ В ЕВРОПЕ

Экономические факторы свидетельствуют о том, что европейские электронные подписи могут получить широкое применение в России. Вопросы трансграничного использования и правовой режим электронной подписи, полученной в Европе, рассмотрены в настоящей работе.

Ключевые слова: *электронная подпись, иностранная электронная подпись.*

VOLKOV Y. V.

ABOUT THE USE IN RUSSIA OF ELECTRONIC SIGNATURE, GOT IN EUROPE

Economic factors suggest that the European electronic signatures can be widely used in Russia. Questions of cross-border use and legal regime of the digital signature received in Europe, are considered in the real work.

Keywords: *digital signature, foreign digital signature.*

Вопрос об использовании в России электронной подписи, полученной в Европе, может показаться надуманным. Тем не менее, его рассмотрение весьма актуально в связи с тем, что Россия вступила в ВТО, растут международные связи и, вероятно, российских участников информационного обмена интересуют и экономические аспекты электронной коммерции. Рассмотрим стоимость отдельных услуг связанных с электронной подписью. Данные[1] получены группой исследователей Междисциплинарного центра права и информационных технологий университета города Лёвен (Бельгия) и представлены в полном варианте отчета Правовые и рыночные аспекты электронной подписи[2]. Согласно названному отчету данным в Бельгии квалифицированная электронная подпись выдается любому гражданину старше 18 лет на 5 лет по стоимости 400 рублей. Для общения с налоговым ведомством электронная подпись бесплатна для граждан Бельгии, Германии, Франции, Дании. В Ирландии все сервисы с электронной подписью «почти бесплатно». В Австрии электронная подпись – 48 рублей, регистрация – 48 рублей. Для электронного взаимодействия граждан, предпринимателей электронная подпись стоит – 240 рублей в год. В Швеции (3 миллиона пользователей) электронная подпись для работы с банком –

от 0 до 80 рублей, электронная подпись для получения электронных государственных услуг – от 0-200 рублей. В Словении – 400 рублей. Наиболее высокая европейская цена электронной подписи в Италии – до 600 рублей. Количество пользователей в отдельных странах доходит до 30–40 % населения (Дания, Швеция). В России большинство цен на электронную подпись в зависимости от удостоверяющего центра и сферы применения сосредоточены в диапазоне от 2000 до 8000 рублей на год. Количество пользователей электронной подписи в России оценивается экспертами в пределах не более 0,2% от общего числа населения. Приведённые данные позволяют представить весьма вероятным, что многие участники международного информационного обмена предпочтут получить электронную подпись европейского образца.

В этой связи возникает второй вопрос насколько это правомерно и безопасно. Вопрос о признании и применимости электронной подписи можно формулировать в общем контексте проблемы признания российским правом объектов, созданных и признанных нормами иностранного права и международными стандартами. Согласно пункту 4 статьи 15 Конституции Российской Федерации[3], общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законодательством, то применяются правила международного договора. Пленум Верховного Суда пояснил, что судам при осуществлении правосудия надлежит исходить из того, что общепризнанные принципы и нормы международного права, закрепленные в международных пактах, конвенциях и иных документах (в частности, во Всеобщей декларации прав человека, Международном пакте о гражданских и политических правах, Международном пакте об экономических, социальных и культурных правах) и международные договоры Российской Федерации являются в соответствии с ч. 4 ст. 15 Конституции Российской Федерации составной частью ее правовой системы[4]. В том же постановлении подчеркивается, что если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора. Учитывая это, суд при рассмотрении дела не вправе применять нормы закона, регулирующего возникшие правоотношения, если вступившим в силу для Российской Федерации международным договором, решение о согласии, на обязательность которого для Российской Федерации было принято в форме федерального закона, установлены иные правила, чем предусмотренные законом. В этих случаях применяются правила международного договора Российской Федерации. Таким образом, общий теоретический принцип права и судебной практики применительно к вопросу о применимости электронной подписи и электронного документа, созданных на основе международных соглашений, должен обозначать автоматическое их признание в России. Однако это не совсем так. Федеральный закон Российской Федерации «Об электронной подписи»[5] (далее – Закон) содержит в статье 7 специальные положения о признании электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами. Согласно положениям Закона электронные подписи «не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права»[6].

Таким образом, нет автоматического признания, имеет место правило запрещающее автоматический запрет использования иностранной электронной подписи.

Очередной вопрос, который возникает в процессе использования электронной подписи, – совместимость зарубежной и российской подписей.

Данный вопрос интересует многих исследователей, например, М. Дутов, проводя сравнительное исследование вопроса применения электронной подписи и электронного документа в Европе и в Украине, констатирует, что использование электронной подписи и электронный документооборот базируются на двух правовых основаниях и практически каждая страна сталкивается с вопросом какой правовой режим применять[7]. Директива об электронной коммерции 2000 года (ДЭК)[8], и Директива об электронных подписях 1999 года (ДЭП)[9]. Вопросы, возникающие в процессе формирования практики использования электронной подписи, отражают специфику конкретного государства. Для

стран общего права, например, Соединенного Королевства, – характерен подход ограничения вмешательства государства в частные дела. Для Германии же характерен государственный подход к регулированию многих сфер деятельности, вследствие чего и электронный документооборот оказался под жестким контролем государства. Единый подход даже в отдельных странах ещё не сформировался.

Другой исследователь, И. В. Зимин, который представляет интересы Министерства юстиции России, поднимает вопрос о значимости электронных документов и признания их юридической значимости. Он акцентирует проблему восприятия человеком электронного документа. Основной вывод автора по широкому кругу вопросов заключается в целесообразном закреплении правового режима электронного документа как совокупности правовых норм, методов правового регулирования, обеспечивающих комплексное воздействие на отношения субъектов, участвующих в электронном документообороте, на основе юридических, организационных, технических и иных средств[10].

С. Кирюшкин, изучая вопрос о придании юридической силы документам, подписанным электронной подписью, созданной на основе зарубежного законодательства приходит к следующим выводам: юридически значимое трансграничное информационное взаимодействие – уже реальность; специальных норм о процедурах признания юридического значения иностранных документов в настоящее время не выработано; . основой могут служить проекты, которые реализуются сейчас в России и в рамках стран-участников Таможенного союза, эти решения универсальны и могут быть применены за рамками таможенного информационного взаимодействия[11].

Понятие электронной подписи введено Директивой 1999/93/ЕС Европейским парламентом в документе под наименование Общие правила регулирования электронной подписи[12]. Электронная (базовая) подпись это – любые данные в электронном формате, которые прилагаются или логически связаны с другими электронными данными и которые служат способом проверки подлинности. Основной целью этот вид электронной подписи можно считать определение происхождения подписанного документа или сообщения. «Усиленная» (дословно продвинутая) электронная подпись отвечает следующим требованиям:

а) однозначно связаны с подписавшим;

б) позволяет идентифицировать подписавшего;

с) создается с использованием средств находящихся под полным единоличным контролем подписавшего лица;

г) она связана с данными, к которым она относится, таким образом, что любое последующее изменение данных может быть обнаружено.

По сравнению с первым базовым типом электронной подписи, усовершенствованная электронная подпись служит кроме проверки подлинности трем другим дополнительным целям. А именно, идентификация подписавшего, связь (едино происхождение) источника подписи, подписанного содержимого и подлинности содержания подписанного подписью. Усовершенствованная электронная подпись, кроме того, должна соответствовать требованиям конфиденциальности и уникальности при её использовании. Данное требование означает, – все, что может быть создано, подписавшим, создано под его единоличным контролем. Также введено понятие длительности срока действия свидетельства, представленного в современной электронной подписи.

«Квалифицированная» электронная подписи однозначно не определена в Директиве 1999/93/ЕС. Тем не менее, это третий вид электронной подписи, которая соответствует более высоким требованиям к безопасности чем, требования, предусмотренные законом для усиленных (продвинутых) электронных подписей. «Квалифицированная» подпись на самом деле является наиболее защищённой (передовой) электронной подписью. Она обеспечивается квалифицированным сертификатом и создается при помощи защищенного устройства для создания подписей. По сравнению с усиленной электронной подписью при создании «квалифицированной» электронной подписи должны быть удовлетворены дополнительные требования. Названные требования изложены в приложении директивы в отношении: содержание сертификата удостоверяющего личность подписавшего; качество эмитентов сертификатов; требования по обеспечению безопасности устройств, используемых для генерации квалифицированных электронных подписей. Именно последний вид соответствует элек-

тронной цифровой подписи, использование которой ещё имеет место в России.

Кроме упомянутого документа, который постоянно является объектом пристального внимания исследователей, регулирование отдельных направлений деятельности с использованием электронной подписи осуществляется и другими документами. Например, Директива 2001/115/ЕС об условиях упрощения, модернизации и согласования условий, предусмотренных для выставления счета, в отношении налога на добавленную стоимость[13], приобретает большое значение, поскольку страны участники Евросоюза имеют не только разные ставки по налогу на добавленную стоимость, но и разные условия реализации данного налога. Унификация процесса может повысить скорость обменных операций, их прозрачность. Другие документы, например, Директива 2004/17/ЕС о координации процедур закупок субъектов, действующих в сфере водоснабжения, энергетике, на транспорте и в отрасли почтовой связи[14] и Директива 2004/18/ЕС о координации процедур рассмотрения и подписания государственных заказов, контрактов на поставку общественных и государственных контрактов на оказание услуг[15], обладают определенной спецификой, связанной с применением определенного вида электронной подписи, а не всех видов сразу.

Предлагается обратить внимание на оценку, которую дала Специальная комиссия Европейского парламента[16]. Комиссия считает, что цели Директивы (правовая определенность по поводу электронных подписей, необходимость юридического признания электронных подписей) в основном выполнены и что нет острой необходимости ее пересмотра на данном этапе. Тем не менее, учитывая проблемы взаимного признания электронных подписей, Комиссия запланировала ряд встреч с государствами-членами для решения отдельных вопросов: использование квалифицированной электронной подписи; рынок недостаточно развит; пользователи не имеют единого, электронного сертификата для подписи.

Вопросы использования электронной подписи в рамках Европейского Союза являются предметом современных международных исследований. Так, например участники конференции XII Европейский Форум по электронной подписи - EFPE 2012 отметили следующее. Действия Европейской Комиссии по замене Директивы 1999/93/ЕС об электронной подписи Положением с более сильной формой государственного регулирования, оцениваются положительно. Обозначение перечня услуг и определение их квалифицированных форм на уровне ЕС признано важным шагом по направлению к строительству европейского пространства доверия. Признано, что новые правовые режимы должны вводиться во всех странах ЕС для обеспечения непрерывности оказания услуг. Разделение электронных подписей физических и юридических лиц. Отмечена потребность уточнения критериев признания сертификатов за пределами Евросоюза и т.д.[17].

Оценивая в комплексе вопрос о юридическом признании иностранной электронной подписи, следует отметить следующее. Европа продвинулась в данном вопросе значительно дальше России, но это вовсе не значит, что следует автоматически признавать юридически значимой любую электронную подпись из Европы. В каждом случае установления международного электронного взаимодействия следует комплексно оценить как российское законодательство, так и законодательство страны контрагента.

Примечания

[1] Европейские цены переведены в российскую валюту из расчета 1 Евро = 40 рублей.

[2] См.: Legal and market aspects of electronic signatures /Jos Dumortier, StefanKelm, Hans Nilsson, Georgia Skouma, Patrik van Eecke / The Legal and Market Aspects of Electronic Signatury // Interdisciplinary centre for Law & Information Technology.– Katholiek Universiteit LEUVEN. Service Contract C 28.400. 2003.– 345 p. См. также краткий вариант – Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma, Patrick van Eecke // Datenschutz und Datensicherheit 28 (2004) 3 P.141-146.

[3] См.: Конституция Российской Федерации [электронный ресурс] // Официальное электронное издание http://www.constitution.ru.

[4] См.: Пункт 5 Постановления Пленума Верховного Суда РФ от 31 октября 1995 года № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» (с изменениями от 6 февраля 2007 г.) // http://constitution.garant.ru/act/right/10103328/#5.

[5] См.: Федеральный закон Российской Федерации от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» // Российская Газета, 2011. 8 апрель.

[6] Там же.

[7] См.: Дутов М. Сравнительный анализ европейского законодательства в области электронного документооборота // Підприємництво, господарство і право. - 2002. - № 8. - С. 25-28.

[8] См.: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) // Official Journal of the European Communities. L 178, 17.7.2000, P. 1–16.

[9] См.: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures // Official Journal of the European Communities. L 13, 19.1.2000, P.12.

[10] Зимин И.В. Юридическая значимость электронных документов как важнейший элемент в формировании единого информационного пространства в Российской Федерации // Вестник Самарского государственного университета. 2012 № 1 (92). С. 137-144.

[11] Кирюшкин С. Трансграничный юридически значимый документооборот: нюансы решений актуального вопроса // CONNECT 2011. № 4. С. 120-123.

[12] См.: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures // OJ L 13, 19.1.2000, p.12.

[13] См.: Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax, OJ L 15, 17.1.2002, p.24.

[14] См.: Directive 2004/17/EC of the European Parliament and of the Council of 31 march 2004 coordinating the procurement procedures of entities operating in the water, energy, transports and postal services sectors, OJ L 134, 30.4.2004, p.1.

[15] См.: Directive 2004/18/EC of the European Parliament and of the Council of 31 march 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, OJ L 134, 30.4.2004, p.114.

[16] См.: Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures // Report from the Commission to the European Parliament and the Council/ Brussels, 15.3.2006 COM (2006) 120 final.–10 p.

[17] См.: Меморандум XII Европейского Форума по электронной подписи - EFPE 2012 // XII Европейский Форум по электронной подписи - EFPE 2012 (4-6 июня 2012 г. Мендзыздрое, Польша).: Мендзыздрое.– 2012. Программный Комитет EFPE 2012. URL= https://www.efpe.ru/efpe/main.xml

---

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, associate professor in the Department of Information Law at the Ural State Law Academy, Candidate of law. E-mail: yuriivolkov@yandex.ru; volkov@usla.ru

УДК 004.45 : 339.1 + 347.75 : 004.45
ББК Х911.221.1

Ю.П. Сигута

АСПЕКТЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРАНСГРАНИЧНОЙ ТОРГОВЛИ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Статья посвящена некоторым способам таможенного и налогового оптимизирования международной торговли программным обеспечением с помощью международно-правовых стандартов.

Ключевые слова: *программное обеспечение, международная торговля, правовое регулирование, файлообменный сервис.*

Siguta Iuliia

INTERNATIONAL LEGAL REGULATION ASPECTS OF CROSS-BORDER SOFTWARE TRADE

The article is devoted to some methods of custom and tax optimization of the international software trade using international legal standards.

Keywords: *software, international trade, regulation, file sharing service.*

В современном информационном обществе значение программного обеспечения для успешной работы субъектов хозяйствования невозможно переоценить. Хранение файлов и персональных данных, бухгалтерские, складские и юридические системы, системы планирования деятельности предприятия и системы связи подразделений между собой, шифровка и защита от вирусов, программное обеспечение для аппаратов и механизмов – вот далеко неполный перечень задач, решаемых покупкой подходящего компьютерного программного продукта.

Покупка предприятием-резидентом одной страны программного обеспечения в другой стране имеет существенные правовые особенности своего регулирования и оформления.

Так, если разработчик или продавец программного обеспечения имеет сертифицированные дилерские центры на территории страны покупателя, задача упрощается, т.к. в таком случае перемещением программного продукта через таможенную территорию и всеми сопутствующими проблемами занимается дилер, покупателю остается только подписать соответствующее соглашение, получить определенные права на программное обеспечение и перечислить дилеру согласованную его стоимость.

Однако в случае, если дилеров нет, перед юрисконсультами обеих компаний встают непростые задачи выбора и надлежащего оформления путей трансграничной передачи прав на данное программное обеспечение. Разумеется, обеим сторонам хочется из-

бежать передачи программного обеспечения в качестве товара, при которой необходимо прохождение процедур таможенной очистки, оформления таможенной декларации и т.д.

Самый простой способ избежать таможенных процедур – после надлежащего оформления лицензионного соглашения и, возможно, даже предварительной оплаты, предприятие-лицензиар загружает продукт на собственным или арендуемый файлообменный сервис и передает лицензиату доступ к цифровой ячейке памяти, пользуясь которой лицензиат может записать программное обеспечение непосредственно на оборудование в стране покупателя. Таким образом, перемещение программного продукта происходит не через таможенную границу в физическом мире, а в виртуальном пространстве с помощью средств телекоммуникаций. Согласно методическим рекомендациям ООН «Статистика международной торговли товарами – концепции и определения», 2010 г. доставка электронным способом (загрузка, использование электронной почты, потоковая передача данных и т.д.) из одной страны в другую любого контента (например, электронных книг, газет и периодических изданий, справочников и списков рассылки, загрузка музыкальных аудиопрограмм, потоковый аудиоконтент, загрузка фильмов и других видеоматериалов, загрузка системного программного обеспечения, загрузка прикладного программного обеспечения, онлайновых игр и т.д.) исключена из сферы охвата статистики международной торговли товарами [1, п.1.55]. Будучи современным, безопасным и удобным, данный способ имеет один существенный недостаток. Замечено, что продавцы программного обеспечения часто не желают прибегать к нему из-за боязни потерять контроль над тем, у кого конкретно во владении окажется программное обеспечение и на скольких компьютерах оно будет установлено. По нашему мнению, данные опасения могут быть сочтены несостоятельными и скорее объяснимы не действительными причинами, а недостаточной технической квалификацией специалистов предприятия-продавца и плохо налаженной коммуникацией между техническим, юридическим и коммерческим отделами компании-лицензиата. Ведь, по сути, с точки зрения защиты данных, нет разницы, производится ли установка программного обеспечения с помощью каналов связи Интернет или непосредственно с лазерного диска.

Другим способом избегания оформления таможенных процедур при покупке программного обеспечения у иностранного предприятия может стать представление программного обеспечения не в качестве товара, но в качестве работы или услуги. Так, согласно обновленным рекомендациям в п.1.18 ООН «Статистика международной торговли товарами – концепции и определения», 2010 г. носители информации, являющихся носителями специального программного обеспечения или программного обеспечения, разработанного для конкретного клиента, или исходных материалов любого вида, как правило, не подлежат включению в статистику международной торговли товарами. Такой подход к определению понятий уже стал традиционным, ведь еще в соответствии с методическими рекомендациями ООН «Статистика международной торговли товарами: концепции и определения», 1998 г., дискеты и лазерные диски CD ROM с записанными на них программами и/или данными, разработанными на заказ, аудио- и видео пленки с оригинальными записями, индивидуально выполненные чертежи (технико-экономические обоснования, проектно-конструкторские и дизайнерские разработки) и так далее рассматриваются как выполнение работ или оказание услуг [2]. При такой передаче произведений таможенные органы не осуществляют таможенный контроль за экспортом и импортом вышеописанных работ и услуг и не проводять их таможенное оформление, т.к. суть процедуры декларирования товаров таможенными органами состоит в возможности осуществления контроля за соответствием внесенных в декларации сведений про товары путем физического осмотра и оценки этих товаров. В случае же разработки специального компьютерного программного обеспечения или разработки программного продукта на заказ для отельного клиента осуществить подобный осмотр с определением соответствия фактически не представляется возможным, потому как программное обеспечение, скорее всего, будет записано на немаркированный промышленным образом для серийного производства CD или флешнакопитель.

Вышеописанный поход полностью соответствует принципам взимания налогов при

импорте и экспорте товаров (работ, услуг), принятым Соглашением о принципах оформления непрямых налогов во время экспорта и импорта товаров (работ, услуг) между государствами-участниками Содружества Независимых Государств. В соответствии с вышеупомянутым Соглашением к услугам, которые при импорте-экспорте не декларируются таможенными органами, а как правило передаются заказчику по акту сдачи-приемки выполненных работ (предоставленных услуг), например, относятся: переуступка патентов, лицензий, торговых марок, авторских и аналогичных прав, консультационные, юридические, инженерные (предпроектные и проектные услуги, бизнес-планы, технико-экономические обоснования проектно-конструкторские разработки), рекламные и услуги по обработке информации [3, п.2.5]. При этом взимание непрямых налогов при экспорте и импорте таких работ и услуг осуществляется налоговыми органами.

Подчеркнем, что именно запакованные дискеты и лазерные диски CD ROM с записанными на них компьютерными программами или данными, разработанными для общего использования или в коммерческих целях (не на заказ для отельного клиента и не специальными) к которым, как правило, прилагается инструкция по использованию, аудио- и видеопродукция, записанная для общего и коммерческого использования, сборнкики типових проектов и чертежей, относятся к товарам. При таможенном оформлении таких товаров, которые содержат объекты интеллектуальной собственности, подается грузовая таможенная декларация, а определение их таможенной стоимости осуществляется в соответствии с законодательством страны покупателя. Необходимо отметить, что определение таможенной стоимости программного обеспечения на магнитных носителях информации осуществляется, как правило, на общих основаних, т.е. именно стоимость носителя не отделяется стоимости програмного обеспечения.

Исходя из вышеизложенного, можно сделать вывод, что именно международно-правовые документы и соглашения в большей степени определяют регулирование современного глобального рынка торговли программным обеспечением, служат платформой для внедрения инноваций в этой отрясли и являются основой национального законодательства различных стран.

Список литературы

1. Рекомендации ООН «Статистика международной торговли товарами: концепции и определения», 2010 г.

2. Рекомендации ООН «Статистика международной торговли товарами: концепции и определения», 1998 г.

3. Соглашение о принципах взимания косвенных налогов при экспорте и импорте товаров (работ, услуг) между государствами - участниками Содружества Независимых Государств" от 25 ноября 1998 г.

Сигута Ю.П., аспирантка кафедры общеправовых дисциплин и международного права Одесского национального университета им. И. И. Мечникова (Украина). E-mail: syp@ukr.net.

Siguta Iuliia, postgraduate student common law disciplines and international law department of Odessa National University named after I.I. Mechnikov (Ukraine). E-mail: syp@ukr.net.

УДК 343.91.018 + 343.3/. 7 : 004.056.53 + 004 : 343
ББК Х 408.135 + Х512

И.И. Сухих

ВЗАИМОСВЯЗЬ ЛИЧНОСТИ ПРЕСТУПНИКА И СОВЕРШЕННОГО ИМ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В статье дается характеристика личности преступника, совершившего преступление в сфере компьютерной информации. Дается классификация лиц, совершивших компьютерные преступления, на основе их личностных особенностей.

Ключевые слова: *безопасность в сфере компьютерной информации, компьютерные преступления, личность преступника.*

I.I. Sukhikh

INTERCOMMUNICATION OF PERSONALITY OF CRIMINAL AND COMMITTED CRIME BY HIM IN THE FIELD OF COMPUTER INFORMATION

In the article description is given of personality of criminal, committing crime in the field of computer information. Classification of persons accomplishing computer crimes is given, on the basis of their personality features.

Keywords: *Safety and security in the field of computer information, computer crimes, personality of criminal.*

Рассматривая данную взаимосвязь, следует разобраться с основополагающими определениями в данной сфере. К компьютерным преступникам относятся лица, совершившие хотя бы одно из перечисленных в уголовном кодексе преступлений в сфере компьютерной информации. К преступлениям в сфере компьютерной информации относятся преступления, совершаемые людьми, использующими информационные для преступных целей[1].

Рассматривая уголовное законодательство Российской Федерации, можно выделить три вида компьютерных преступлений.

Первым преступлением в сфере компьютерной информации уголовный закон рассматривает «неправомерный доступ к компьютерной информации» (ст. 272 УК РФ). Под неправомерным доступом следует понимать получение, в обход определённых запретов и ограничений, возможности тем или иным способом овладеть информацией и/или ознакомиться с ней «воочию». Следующим типом является «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273 УК РФ). Под данным видом дея-

ния понимается создание, использование и распространение специальных программ, причиняющих вред ЭВМ, созданных с помощью языков программирования для различных аппаратных платформ. Данные типы преступлений в сфере компьютерной информации имеют наибольшее распространение, как в мире, так и нашей стране. Они включают в себя множество модификаций и форм, вследствие этого большая часть компьютерных преступников, которые совершают компьютерные преступления, привлекается ответственности по данным статьям.

Преступление и лицо, его совершившее, неразделимо связаны между собой, поэтому для более успешного расследования и раскрытия данного вида преступных деяний следует рассмотреть взаимосвязь личности преступника и того состава преступления, которое он совершил. Получение лицом неправомерного доступа к информации и создание вредоносных программ, подразумевает под собой определённую, а учитывая современное развитие компьютерной техники и информационных технологий, и специальную подготовку в сфере компьютерных технологий.

Лиц, совершивших компьютерные преступления, указанные в гл. 28 УК РФ, на основе их личностных особенностей, можно разделить на 3 подвида:

1) «Начинающие». Возрастные границы: 15–25 лет. Пол: в подавляющем большинстве случаев мужской. Образование: среднее, среднее специальное или высшее, в некоторых случаях неоконченное. На всех ступенях образования есть связь с технологией, в основном, компьютерной. Происхождение – из семей среднего достатка. Приобщение к компьютерной технике произошло в большинстве случаев в старших классах школы. Имеют дома 1 или более персональную ЭВМ, с постоянным и зачастую неограниченным доступом к глобальной сети Интернет.

Знания компьютерных технологий включают в себя языки программирования низкого и высокого уровней (Assembler, C++, Java, PHP, HTML) и знание аппаратной части компьютерных платформ. Они нигде не работают, либо работают системными администраторами приходящего или постоянного типа в организациях с малой или средней компьютерной инфраструктурой.

Это, как правило, увлеченные компьютерными технологиями личности, поддерживающе скупые связи с внешним – некомпьютерным миром. В сети Интернет, скрывают подлинные имена за так называемыми «никами» (от английского слова «nickname» - кличка, прозвище, вымышленное имя), используют «ники» в повседневном открытом общении[2].

Преступную деятельность начинают достаточно рано и, неосознанно, т.е. еще не понимая, что их действия подпадают под квалификации по соответствующим статьям УК РФ. Формирование установок на преступное поведение у данных лиц, осуществляется стихийно. Закрепление происходит путем влияния «авторитетного мнения старших товарищей», высказанное ими после общения с «новичком» в сетевых ресурсах. Несколько раз в месяц совершают деяния, подпадающие под ст. 272 (п. 1) и ст. 273 (п. 1) УК РФ. В основном это получение паролей других пользователей сети Интернет для подключения к этой сети за чужой счёт, доступ к информации о кредитных картах в Интернет-магазинах в России и за рубежом. В более крупных компьютерных преступлениях, в основном по ст. 272 (п. 2) УК РФ, участвуют как соисполнители.

б) «Закрепившиеся». Возраст: 20–25 лет. Отличие от «начинающих» заключается в следующих аспектах. Обладают знаниями языков программирования и аппаратной части на более осмысленном и систематизированном уровне. Совершая компьютерные преступления, пользуются наборами заблаговременно подготовленных «программ-инструментов», разработанных 1-ой группой или другими людьми своей группы, либо являются организаторами хакерских атак с исполнителями из 1-ой группы. Лица достаточно уравновешенные, со сформировавшейся системой взглядов и ценностей, не высоко-амбициозные. Имеют постоянную работу в IT-фирмах. Преступная «карьера» берет свое начало из «карьеры» «начинающего», либо формируется сразу в устоявшейся форме за счет общения и протекции со стороны профессиональных преступников. Во внешности – отличительных особенностей не наблюдается. Основные виды преступных деяний, совершаемых данными лицами, заключаются: в сетевом взломе, отдельных действиях и операциях по получению сильно защищённой информации (в том числе и шпионаж). Более «мелкие» дела практически не совершают.

в) «Профессионалы». Возраст: 25–45 лет. Пол: мужской. Отличительными чертами являются: Социальное происхождение - из семьи с достатком выше среднего, которые могли позволить приобретение ЭВМ и доступ в сеть Интернет в середине 80-ых, начале 90-ых. Наличие высшего технического образования (иногда более 1-го высшего образования). Знания в области компьютерных технологий являются строго систематизированными и исчерпывающими. Совершаемые ими деяния подпадают под ст. 272 (оба пункта) и некоторые дополнительные статьи (в том числе, шпионаж - военный и промышленный). Личностный психотип данных лиц крайне уравновешенный, стойкий к внешним воздействиям, с устоявшимися взглядами и системой ценностей. Личности крайне амбициозные, но знающие себе цену. Мотивация преступного поведения формируется обычно на стадии освоения «просторов киберпространства». Практически недосягаемы для органов правосудия, ввиду поручения всей «грязной» работы лицам 1-ой и 2-ой групп. Процент лиц женского пола в данной среде на порядок выше, чем для первых двух типов.

В качестве вывода о лицах, совершающих подпадающие под ст. 272, 273 УК РФ деяния, можно сказать, что высокая техническая подготовленность - их основная черта, высокая латентность преступлений - основа их мотивации, внутренняя предрасположенность - основное условие вступления на преступный путь, и социально-экономическая ситуация в стране – основная причина окончательного выбора. После изменений в УК РФ, внесенных 7.12.2011 г., в ст. 273 УК РФ появились положения, которые добавляют сюда в качестве субъекта преступления любого пользователи, который с помощью программы обходит защиту файлов с целью их дальнейшего беспрепятственного использования. Данная обширная группа лиц стоит особняком от подвидов компьютерных преступников, ввиду отсутствия специальных знаний в области компьютерных технологий.

Особняком стоит ст. 274 УК РФ, которая устанавливает уголовную ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние, причинило существенный вред (ч.1) или повлекло по неосторожности тяжкие последствия (ч. 2) ст. 274 УК РФ.

Среди преступлений, предусмотренных гл. 28 УК РФ, данное преступление является наименее распространенным. Ввиду чего составление отдельного портрета личности преступника является невозможным, ввиду слабой практической разработанности.

Примечания

[1] URL: http://ru.wikipedia.org/wiki/Информационные _технологии

[2] URL: http://ru.wikipedia.org/wiki/%D0%9D%D0%B8%D0%BA

Сухих Иван Иванович, аспирант кафедры уголовного права, криминологии и уголовно-исполнительного права Южно-Уральского государственного университета (национального исследовательского университета). E-mail: suhihivan@gmail.com.

Sukhikh Ivan Ivanovich, graduate student of department of criminal law, criminology and criminally-executive right for the South Ural State University (national research university). E-mail: suhihivan@gmail.com.

УДК 347.61/.64.03 + 342.7.03 (094.5.072)
ББК Х 404.5

Минбалеев А.В., Кулдыбаева И.У.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНСТИТУТА ЛИЧНОЙ И СЕМЕЙНОЙ ТАЙНЫ

В статье анализируются основы правового регулирования личной и семейной тайны в Российской Федерации, обозначается ее связь с категорией «персональные данные». Исследуются меры юридической ответственности за нарушение личной и семейной тайны, дается характеристика современного состояния законодательства.

Ключевые слова: *личная тайна и семейная тайна, персональные данные, правовое регулирование.*

Minbaleev A. V., Kuldybaeva I.U.

THE LEGAL REGULATION OF THE INSTITUTION OF PERSONAL AND FAMILY SECRETS

The article analyzes the legal regulation of personal and family secrets in the Russian Federation, indicates its relationship with the «personal data» category. In the article investigated a measure of legal liability for infringement of personal and family secrets, described the current state of legislation.

Keywords: *the personal and family secrets, the personal data, the legal regulation.*

Информатизация общества и развитие информационных технологий неизбежно ведет к появлению новых ограничений права на неприкосновенность частной жизни. Возрастает возможность контроля над личностью, манипулирования человеком, вмешательства в частную жизнь, покушения со стороны государства, общества, средств массовой информации, отдельных граждан на личную и семейную тайну. В настоящее время остро стоит вопрос о правовом регулировании и обеспечении безопасности информации о частной и семейной жизни человека, защите субъектов таких данных.

Правовое исследование личной и семейной тайны рассматривается в рамках неприкосновенности частной жизни. Имеется ряд диссертационных исследований, в которых право на частную жизнь рассматривается с точки зрения уголовного процесса, конституционного права. По мнению многих исследователей в этой области, в том числе Т.О. Пра-

ницкой, Н.И. Шахова, М.А. Ступаловой, личная и семейная тайна представляет собой элемент структуры конституционного права на неприкосновенность частной жизни, наряду с правом на личную неприкосновенность человека, включая его физическую неприкосновенность; право на свободу передвижения; право на защиту чести и доброго имени; право на творческую деятельность, правом на тайну любых коммуникаций и другими правами. Конституция РФ[1] относит к частной жизни личную и семейную тайну, защиту чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Право на частную жизнь означает предоставленную человеку и гарантированную государством возможность контролировать информацию о себе, препятствовать разглашению сведений личного, интимного характера[2].

Это конституционное право граждан на информационную неприкосновенность частной жизни, защиты общественных интересов, а также интересов лиц, использующих конфиденциальную информацию о физических лицах в своей деятельности. Предметом правового исследования являются информационные отношения в связи с использованием информации, которая составляет личную или семейную тайну одного или нескольких лиц. Ю.А. Говенко[3] в своем диссертационном исследовании отмечает, что понятия личной и семейной тайны взаимосвязаны и во многом совпадают. Различия между ними заключаются в принадлежности интересов одному или нескольким лицам – членам семьи. В законодательстве нигде не содержится точное определение сведений, которые могут составлять «личную или семейную тайну», а также, какая информация считается «информацией о частной жизни». Согласно п. 1 ст. 23 Конституции РФ, каждый имеет право на личную и семейную тайну. Они относятся к личным неимущественным правам гражданина и охраняются различными отраслями права. Предметом личной и семейной тайны является информация о лице, определенная законом в качестве конфиденциальных сведений, в том числе биографические сведения; сведения о состоянии здоровья, о совершенных правонарушениях, философских, религиозных, политических взглядах и убеждениях, имущественном положении, профессиональных занятиях, об отношениях в семье. Ю.А. Шахов в общее понятие личной тайны включает:

- тайну индивидуальности (без специального предоставления сведений правообладателем для третьих лиц нет способа индивидуализации личности кроме внешнего облика);
- тайну прошлого (к ней относятся сведения о происхождении лица, о его времяпрепровождении в прошлом – разглашение информации не порочащего, с точки зрения права, характера (например, сведения о том, что лицо имеет снятую судимость) может быть чревато серьезными неудобствами для правообладателя);
- тайну социального обособления (социальные координаты лица, в том числе место работы, жительства, традиционно посещаемые места проведения досуга, уровень образования и т.п.).

К семейной тайне Ю.А. Шахов относит тайну семейных взаимодействий (состояние в открытом, реальном или гражданском браке) и тайна усыновления, а именно: тайна факта усыновления; тайна подлинных имени, места рождения ребенка, если таковые были изменены, а также сведения о его кровных родителях[4].

Семейная тайна – это сведения о лицах, фактах, событиях, существующих в сфере отношений, регулируемых семейным правом. Семейную тайну составляют следующие сведения: тайна усыновления, тайна частной жизни супругов, тайна частной жизни детей, личные неимущественные и имущественные отношения, существующие между супругами, и другие. Предметом семейной тайны могут быть сведения: о фактах биографии лица; о состоянии его здоровья; об имущественном положении; о роде занятий и совершенных поступках; о взглядах, оценках, убеждениях; об отношениях в семье или об отношениях человека с другими людьми.

Для целей правового регулирования к личной и семейной тайне относится информация, в отношении которой физические лица в соответствии с законом имеют исключительное право установить режим конфиденциальности в момент ее возникновения. К личной тайне не относится информация, которая становится общедоступной по воле обладателя. Итак, к информации составляющей личную и семейную тайну относится следующая: о внутрисемейных отношениях; об интимной жизни; об истинных обстоятельствах рождения и усыновления в случае, когда офи-

циальные данные о рождении были изменены по просьбе усыновителя; об обстоятельствах брака и развода; о событиях, произошедших в жилище гражданина; об обстоятельствах преступных деяний, объектом которых стал гражданин.

Сбор и хранение такой информации о лицах без согласия самих лиц, а также ее распространение запрещается. Граждане имеют право самостоятельно охранять любую информацию, исключительными обладателями которой они являются, кроме обязательной к предоставлению или раскрытию в соответствии с законодательством.

Законодательство, регулирующее личную и семейную тайну, стало появляться только в XIX веке. Нормы, касающиеся охраны личной и семейной тайны впервые были закреплены на международном уровне. Ст. 12 Всеобщей декларации прав человека 1948 г. устанавливает, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию[5]. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

Ст. 8 Конвенции о защите прав человека и основных свобод 1950 г. закрепляет право каждого на уважение частной и семейной жизни. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц[6].

Ст. 24 Конституции Российской Федерации устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Это конституционное положение о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица является одной из гарантий закрепленного в ст. 23 Конституции РФ права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Ст. 150 Гражданского кодекса Российской Федерации относит личную и семейную тайну к нематериальным благам, охраняемым гражданским законодательством[7]. Федеральный закон «Об информации, информационных технологиях и о защите информации» в качестве одного из принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации провозглашает неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия[8].

Информация о частной жизни лица представляет собой категорию персональных данных, которые впервые были отнесены к конфиденциальной информации Федеральным законом «Об информации, информатизации и защите информации». Последующее развитие правового регулирования отразилось в Федеральном законе «О персональных данных»[9], который является базовым в сфере защиты персональных данных и регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

Нормы о защите персональных данных присутствуют в различных отраслях законодательства, в Федеральном законе «Об актах гражданского состояния» (ст. 12), «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования» (ст. 17), в законах, связанных с профессиональными тайнами: «О банках и банковской деятельности», «О государственной гражданской службе Российской Федерации», Семейном кодексе РФ, Налоговом кодексе РФ и других. Требования к защите персональных данных и права работников в этой сфере изложены в Трудовом кодексе РФ. Но-

вые нормы защиты персональных данных учитывают международные требования к защите данных и являются на сегодняшний момент наиболее подробными и прогрессивными в этой сфере.

Субъектами личной и семейной тайны являются физические, юридические лица, органы власти и местного самоуправления, осуществляющих действия с конфиденциальной информацией о физических лицах. Обладателем личной и семейной тайны всегда является физическое лицо или неопределенный круг лиц, связанных между собой отношениями родства, супружества, в соответствии с законом обладающие исключительными правами на конфиденциальную информацию, в том числе правом передавать эту информацию другим лицам на условиях конфиденциальности. Распорядителями личных и семейных тайн являются лица, обладающие правом распоряжаться конфиденциальной информацией в силу свое профессиональной деятельности с согласия обладателей, ими могут быть как физические, так и юридические лица, органы власти и местного самоуправления.

В рамках отношений в области персональных данных выделяется такой субъект персональных данных как оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Содержание права на семейную тайну составляют правомочия члена семьи требовать неразглашения соответствующих сведений и правомочия распоряжаться этой информацией по своему усмотрению с согласия всех других членов семьи. По мнению М.Н. Малеиной, если нельзя обособить, «вырвать» сведения, касающиеся только одного члена семьи, то согласие всех других членов семьи, имеющих право на тайну семейной жизни, должно испрашиваться. Следует отметить, что при этом вопрос не может и не должен решаться количеством голосов. Даже наличие одного «против» должно привести к отказу от раскрытия тайны семейной жизни. Следовательно, члены семьи обладают не только правом на семейную тайну, но также обязанностью сохранять семейную тайну[10].

Правомочие члена семьи раскрыть семейную тайну состоит в возможности распорядиться имеющейся у него информацией только с согласия всех иных членов семьи, интересы которых эта тайна затрагивает.

Основная функция обеспечения неприкосновенности частной жизни лица, в частности личной и семейной тайны, возлагается на государство: оно и само должно воздерживаться от вмешательства, и гарантировать воздержание от такого вмешательства со стороны физических и юридических лиц. Законодательно обладателям личной и семейной тайны предоставлена возможность самим определять меры и средства защиты конфиденциальной информации. Но в случае попадания информации к другим субъектам, осуществляющим обработку информации о частной жизни гражданина, законодатель определяет конкретные требования к обеспечению безопасности полученной информации.

Например, ст. 18.1 Федерального закона «О персональных данных» закреплены обязанности оператора принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных. К таким мерам могут, в частности, относиться:

- назначение ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику оператора в отношении обработки персональных данных;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных»;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона;
- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в от-

ношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- обеспечение неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

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[11]:
- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке в информационных системах персональных данных осуществляются уполномоченными на то федеральными органами исполнительной власти:
- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, — Федеральная служба безопасности (ФСБ);
- федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации — Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, — Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Право на неприкосновенность частной жизни, прежде всего, это запрет для государства на вмешательство в частную жизнь граждан. Кроме того, необходимо наличие соответствующих правовых механизмов и гарантий защиты от посягательств на данное благо, что предполагает определение ответственности для его нарушителей.

Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

Уголовный кодекс Российской Федерации в ст. 137 «Нарушение неприкосновенности частной жизни» содержит наказание за «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации; если эти деяния совершенны лицом с использованием своего служебного положения»[12]. Закон не связывает ответственность за незаконное распространение сведений о частной жизни лица с конкретным способом распространения. Под распространением понимается любая незаконная передача указанных сведений третьим лицам. Незаконным распространением является разглашение личной или семейной тайны лицом, обязанным ее хранить в силу своей профессии (адвокатская, врачебная тайна и т.д.). В некоторых случаях разглашение сведений о частной жизни по Уголовному кодексу Российской Федерации образует одновременно состав другого преступления: разглашение тайны усыновления (ст. 155), разглашение данных предварительного расследования (ст. 310), разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311), разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст. 320).

Административная ответственность за нарушение режима конфиденциальности личной и семейной тайны предусмотрена ст. 13.11 Кодекса Российской Федерации об административных правонарушениях за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персо-

нальных данных)[13]. Статья 13.12. КоАП РФ устанавливает ответственность за нарушение правил защиты информации. Статьей 13.14 КоАП РФ предусмотрена административная ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), гражданами и должностными лицами, получившими доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

В виде дисциплинарной ответственности работнику, совершившему какой-либо дисциплинарный проступок в связи с обработкой персональных данных, не повлекший за собой административную, гражданскую или уголовную ответственность, может быть вынесено замечание, выговор, или он может быть уволен по соответствующим основаниям, предусмотренным ст. 81 Трудового кодекса Российской Федерации (далее – ТК РФ)[14]. В ТК РФ четко не установлен вид дисциплинарной ответственности за нарушение порядка обработки персональных данных, а лишь указано, что лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном тк рф и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. Согласно ст. 192 ТК РФ за совершение дисциплинарного проступка работодатель имеет право применить по отношению к работнику следующие дисциплинарные взыскания: (замечание; выговор; увольнение по соответствующим основаниям). Работодатель может по своей инициативе расторгнуть трудовой договор, подпункт «в» п. 6 ст. 81 ТК РФ предусматривает расторжение трудового договора за разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

Гражданско-правовая ответственность в связи с нарушением норм о защите персональных данных работника наступает в случаях, когда работнику причинен имущественный ущерб и моральный вред. ГК РФ предусматривает защиту нематериальных благ граждан, включая неприкосновенность частной жизни, личную и семейную тайну, деловую репутацию и др. Соответственно устанавливаются формы гражданско-правовой ответственности в виде денежной компенсации за причиненный моральный вред, обязанности опровержения сведений, порочащих честь, достоинство или деловую репутацию гражданина (работника)[15].

В ст. 24 Федерального закона «О персональных данных» помимо административной, дисциплинарной, уголовной ответственности предусмотрено возмещение морального вреда, причиненного субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Непроработанность понятийного аппарата затрудняет реализацию конституционного права на неприкосновенность частной жизни. Закрепляя уголовную ответственность в ст. 137 Уголовного кодекса Российской Федерации за незаконный сбор и распространение сведений, составляющих личную и семейную тайну, законодатель не дает определения понятий личная и семейная тайна, а также какие сведения, в том числе персональные данные, могут быть отнесены к такой тайне. Таким образом, привлечь к уголовной ответственности человека, разгласившего чьи-то персональные данные или собирающего их незаконным путем, практически невозможно.

В случаях вмешательства физического или юридического лица в неприкосновенность частной жизни другого лица дело обстоит не так просто. Во многих случаях оказывается, что измерить нанесенный ущерб просто невозможно; более того, ситуация складывается таким образом, что иногда невозможно и привести стороны в первоначальное состояние. Нарушения частной жизни могут иметь очень разные последствия, поскольку концепция частной жизни охватывает широкий круг интересов.

Несмотря на положительные изменения, которые в последнее время произошли в России, уровень реальной защищенности личной и семейной тайны остается невысо-

ким. Юридические гарантии реализации и защиты этого права в должной мере не обеспечиваются. Значимость защиты данного права полностью не осознается ни обладателем, ни распорядителем личной и семейной тайны. Развитие новых информационных технологий подчеркивает необходимость создания действенного механизма, обеспечивающего неприкосновенность сферы частной жизни человека.

Примечания

[1] См.: Статья 23 Конституции Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // СЗ РФ. 2009. № 4. Ст. 445

[2] Шахов, Ю.А. Уголовно-правовая охрана тайны частного характера: автореферат дис. …канд. юрид. наук / Ю.А. Шахов. Краснодар, 2010. 29 с.

[3] См.: Говенко Ю.А. Уголовно-правовая охрана тайны частного характера : автореф. дис. ... канд. юрид. наук. Краснодар., 2010. С. 11.

[4] Шахов, Ю.А. Уголовно-правовая охрана тайны частного характера: автореферат дис. …канд. юрид. наук / Ю.А. Шахов. Краснодар, 2010. 29 с.

[5] Всеобщая декларация прав человека. Принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г. // СПС «Гарант».

[6] Конвенция о защите прав человека и основных свобод. Заключена в г. Риме 04 ноября 1950 (с изм. от 13.05.2004) // СЗ РФ. 2001. №2. Ст. 163.

[7] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 № 51-ФЗ (в ред. от 11 февраля 2013 г.) // СПС «Гарант».

[8] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. Федерального закона от 5 апреля 2013 г. № 50-ФЗ) // СПС «Гарант».

[9] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в ред. Федерального закона от 5 апреля 2013 г. № 43-ФЗ) // СПС «Консультант Плюс».

[10] См.: Малеина М.Н. Личные неимущественные права граждан: Понятие, осуществление, защита. М.: МЗ-Пресс, 2000.

[11] См.: Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01 ноября 2012 № 1119 // СЗ РФ. 2012. № 45. Ст. 6257.

[12] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. Федерального закона от 5 апреля 2013 № 59-ФЗ) // СПС «Консультант Плюс».

[13] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. Федерального закона от 5 апреля 2013 г. № 33-ФЗ) // СПС «Гарант».

[14] Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (в ред. Федерального закона от 5 апреля 2013 г. № 60-ФЗ и от 5 апреля 2013 г. № 58-ФЗ) // СПС «Гарант».

[15] См.: Ст. 150, 151, 152 Гражданского кодекса Российской Федерации (часть первая) от 30 ноября 1994 № 51-ФЗ (в ред. от 11 февраля 2013 г.) // СПС «Гарант».

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 (national research university). Associate professor in the Department of Information Law at the Ural State Law Academy, Doctor of Law. E-mail: alexmin@bk.ru.

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.

ББК Х 400. 323 + Х 401. 114
УДК 342.7 : 004.056 + 340.11 : 004.056

Астахова Л.В., Рублёв Е.Л.

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПЕРИОД СМЕНЫ НОРМАТИВНОЙ БАЗЫ И ПУТИ ИХ РЕШЕНИЯ

В статье представлены результаты сравнительного анализа требований Постановления Правительства Российской Федерации 17.11.2007 № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и Постановления Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Для нейтрализации обнаруженных противоречий разработан «Алгоритм действий оператора персональных данных в период смены нормативной базы», который может быть использован в практической деятельности операторов до момента приведения государственными регуляторами системы нормативно-правового регулирования защиты персональных данных в оптимальное состояние.

Ключевые слова: *персональные данные, защита, нормативные правовые акты, проблемы, алгоритм.*

Astakhova L.V., Rublev E.L.

PROBLEMS OF PERSONAL DATA PROTECTION IN THE PERIOD OF REGULATORY SYSTEM CHANGES AND WAYS OF THEIR DECISIONS

The article presents the results of a comparative analysis of requirements of Decree of the Russian Federation Government dated 17.11.2007 No. 781 "On approval of Regulation on ensuring personal data protection while being processed in personal data information systems" and Decree of the Russian Federation Government dated 01.11.2012 No. 1119 "On approval of requirements for personal data protection while being processed in personal data information systems". In order to neutralize the found out contradictions, the authors developed "A plan of actions of personal data controller in the period of regulatory system changes", which can be used in practical activity of a controller till the moment of bringing the normative legal regulation system of personal data protection in an optimal state.

Keywords: *personal data, protection, regulatory legal acts, problems, plan.*

Периодическое внесение изменений в законодательство обусловлено стремительно меняющимися реалиями времени. В этом отношении не является исключением и сфера регулирования защиты персональных данных - сравнительно новая сфера деятельности для России, находящаяся на стадии накопления опыта и построения адекватных отечественной практике технологий. В связи с утратой силы Постановления Правительства от 17 но-

ября 2007 года №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и принятием Постановления Правительства от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - Постановление №1119) проблема защиты персональных данных существенно актуализировалась.

Цель настоящей работы - выявление проблем, возникших в связи с вступлением в силу новых требований к защите персональных данных, и определение путей их решения. Для реализации цели исследования нами был предпринят сравнительный анализ требований Постановления Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановления Правительства Российской Федерации от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Анализ требований названных постановлений показал, что в новом документе появилось 4 новых требования, а 28 требований, которые существовали на протяжении пяти последних лет, утратили силу. Результаты сравнительного анализа представлены в Таблице 1.

Таблица 1. Сравнительный анализ требований к защите персональных данных в Постановлениях Правительства Российской Федерации №781 и №1119.

Требование	ПП-781	ПП-1119
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.	+	–
Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора	+	–
Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по ТЗКИ	–	+
Контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом)	–	+
Порядок проведения классификации информационных систем устанавливается совместно ФСТЭК, ФСБ И Минкомсвязи	+	–
Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих мер и (или) путем применения технических средств	+	–
Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются ФСТЭК и ФСБ в пределах их полномочий	+	–
Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации	+	–
Своевременное обнаружение фактов несанкционированного доступа к персональным данным	+	–
Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование	+	–

Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	+	–
Постоянный контроль за обеспечением уровня защищенности персональных данных	+	–
Формирование модели угроз	+	–
Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации	+	–
Установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией	+	–
Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними	+	–
Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных	+	–
Учет лиц, допущенных к работе с персональными данными в информационной системе	+	–
Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией	+	–
Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений	+	–
Описание системы защиты персональных данных	+	–
Возложение на одно из структурных подразделений функций по обеспечению такой безопасности	–	+
Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений	+	–
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	–	+
При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин	+	–
Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков	+	–
В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации	+	–

Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой ФСТЭК и ФСБ в пределах их полномочий	+	–
К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с ФСТЭК и ФСБ в пределах их полномочий	+	–
Изменение условий применения средств защиты информации, предусмотренных правилами, согласовывается с ФСТЭК и ФСБ в пределах их полномочий	+	–
Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется ФСТЭК и ФСБ в пределах их полномочий	+	–
Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах	+	–

Логично предположить, что для операторов процесс защиты персональных данных теперь должен значительно упроститься. Однако, вопреки логике, процесс стал более сложным и противоречивым.

Дело в том, что Постановление Правительства Российской Федерации №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» отменяет только предыдущее Постановление № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Это значит, что с 15 ноября 2012 года должны были утратить силу еще несколько, уже привычных для нас, документов, принятых «во исполнение» старого постановления. Такими документами являются:

- 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);
- Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» 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» 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).

Постановление Правительства от 15 сентября 2008г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и Постановление Правительства от 06 июля 2008г. №512 «Об утверждении требований к материальным носителям биометрических персональ-

ных данных и технологиям хранения таких данных вне информационных систем персональных данных», а также «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008г. остаются действующими документами и не претерпели никаких изменений.

Сейчас сложилась противоречивая ситуация: вышеназванные документы, логически не имея юридической силы, фактически являются действующими нормативно-правовыми актами, за неимением чего-либо другого. Прошло более полугода, однако не принято ни одного документа государственных регуляторов, не внесены изменения и в уже существующие нормативные правовые акты. Принятие Постановления №1119, а также отсутствие координации нормотворческой деятельности государственных регуляторов защиты персональных данных дестабилизировали практику защиты персональных данных. В настоящее время существует множество вопросов относительно оформления и составления организационно – распорядительных документов по защите персональных данных, ответы на которые смогут дать только новые нормативные акты.

Полагаем, что любые нормативные изменения должны быть целостными и комплексными, для чего необходима координация действий Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности России и др. заинтересованных министерств и ведомств. Для предупреждения противоречивых ситуаций целесообразно принимать документы полным пакетом.

Для нейтрализации уже возникших негативных последствий описанных противоречий нами разработан «Алгоритм действий оператора персональных данных в период смены нормативной базы». Рассмотрим наиболее сложный вариант - создание системы защиты персональных данных с нуля.

Таблица 2. Алгоритм действий оператора персональных данных в период смены нормативной базы.

№ п/п	Действие оператора	Документы, в соответствии с которыми шаг должен быть сделан	Документы, на основе которых шаг должен быть реализован
1	Создание комиссии по защите персональных данных (председатель комиссии – лицо, которое будет ответственным за обработку ПДн в организации, а так же 2-3 члена комиссии – например, системный администратор, юрист, главный бухгалтер, руководитель отдела кадров и т.д.).	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ	Приказ о назначении ответственного за организацию обработки ПДн, администратора безопасности ИСПДн, комиссии по классификации ИСПДн
2	Разработка плана мероприятий по организации защиты персональных данных	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ	План мероприятий по защите ПДн

3	Разработка инструкций, регламентирующие деятельность ответственного за организацию обработки ПДн, администратора безопасности ИСПДн, пользователей ИСПДн.	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2.Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58 Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 N 687 4. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211	-Инструкция ответственного за организацию обработки ПДн -Инструкция администратора безопасности ИСПДн -Инструкция пользователя ИСПДн -Инструкция о порядке работы с ПДн
4	Проведение инвентаризации ИСПДн.	Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58	-Перечень ИСПДн -Перечень автоматизированных рабочих мест -Перечень серверного, коммутационного и сетевого оборудования -Перечень общесистемного и прикладного программного обеспечения -Перечень средств защиты информации -Схема расположения основных технических средств и систем
5	Формирование перечня сведений, составляющих ПДн.	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ	Перечень сведений, содержащих ПДн с указанием сроков их обработки и правовых оснований обработки ПДн
6	Пересмотр договоров с сотрудниками в поисках пунктов, касающихся обработки ПДн.	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ	Договоры с работниками, другими физ. лицами в части обработки ПД, их распространения (передачи) и использования

7	Получение согласий субъектов на обработку их ПДн.	1. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211 2.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ	-Согласие субъекта на обработку ПДн -Обязательство о неразглашении информации ограниченного доступа
8	Документально регламентировать работу с ПДн (политика обработки и защиты ПДн, положение об обработки ПДн с использованием средств автоматизации и т.д.).	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2.Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211 3.Постановление Правительства РФ «Положение об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. N 1119 4.Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 N 687 5.Приложение к Приказу ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58	-Положение об обеспечении безопасности ПДн при их обработке в ИСПДн -Положение об обработке ПДн без использования средств автоматизации -Политика обработки и защиты ПДн
9	Определение списка должностных лиц, допущенных к обработке ПДн.	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 N 687 Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58 4. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211	Приказ об утверждении списка лиц допущенных к ПДн (с указанием способа обработки)

10	Определение мест хранения материальных носителей ПДн.	Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 N 687	Приказ об утверждении мест хранения материальных носителей ПДн
11	Классификация ИПСДн. Присвоение уровня защищенности ИСПДн.	1.Приказ ФСТЭК России, ФСБ России, Мининформсвязи России «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 13.02.2008 г. N 55/86/20 2.Постановление Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	-Акт проведения классификации ИСПДн -Акт присвоения уровня защищенности ИСПДн
12	Формирование модели угроз ИСПДн и частного технического задания на создание системы защиты ПДн.	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2.Приказ ФСТЭК России, ФСБ России, Мининформсвязи России «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 13.02.2008 г. N 55/86/20 3. Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58	-Частная модель угроз безопасности ПДн -Частное техническое задание на создание системы защиты ПДн
13	Составление и направление в Роскомнадзор «Уведомление об обработке ПДн».	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211	Уведомление об обработке (о намерении осуществлять обработку) ПДн
14	Разработка инструкций, регламентирующие работу с персональными данными и их защиту.	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2.Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58	-Инструкция о порядке работы с персональными данными -Инструкция по организации антивирусной защиты -Инструкция по организации парольной защиты -Инструкция по физической охране ИСПДн, контролю доступа в помещение

15	Введение в действие данных документов и составление плана внутренних проверок состояния защиты ИСПДн.	Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 N 687 3.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 21.02.08 №149/6/6-622 4. Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 20.03.2012г. N 211	-Приказ о введении в действие ОРиЭД по защите ПДн -План внутренних проверок состояния защиты ИСПДн -Акт уничтожения ПДн (электронные и бумажные носители)
16	Составление и ведение журналов (журнал учета паролей пользователей ИСПДн, журнал учета машинных носителей информации и т.п.).	1.Федеральный закон «О персональных данных» от 27.07.2006 г. N 152-ФЗ 2.Приказ ФСТЭК России «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» от 05.03.2010 г. N 58	-Журнал учета паролей пользователей ИСПДн -Журнал учета машинных носителей информации -Журнал учета средств защиты информации, эксплуатационной и технической документации к ним -Журнал учета ключей от помещений и сейфов -Журнал учета обращений субъектов персональных данных -Журнал учета проверок юридического лица -Журнал учета работ в информационных системах персональных данных

Таким образом, в ходе сравнительного анализа требований Постановления Правительства Российской Федерации № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановления Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» выявлены противоречия. Для нейтрализации обнаруженных противоречий был разработан «Алгоритм действий оператора персональных данных в период смены нормативной базы», который может быть использован в практической деятельности операторов до момента приведения государственными регуляторами системы нормативно-правового регулирования защиты персональных данных в оптимальное состояние.

Список использованной литературы

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» [электронный ресурс] - Режим доступа: http://base.consultant.ru

2. Бизнес без опасности [электронный ресурс] - Режим доступа: http://lukatsky.blogspot.ru/

3. Постановление Правительства Российской Федерации от 01 ноября 2012г. №1119 г.Москва «Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных» [электронный ресурс] - Режим доступа: http://www.rg.ru/2012/11/07/pers-dannye-dok.html

4. Постановление Правительства Российской Федерации от 17 ноября 2007г. №781 г.Москва «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [электронный ресурс] - Режим доступа: http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html

5. Рецепты безопасности от Емельянникова [электронный ресурс] - Режим доступа: http://emeliyannikov.blogspot.ru/

6. Прозоров А. Жизнь 80 на 20. [электронный ресурс] - Режим доступа: http://80na20.blogspot.ru/

Астахова Людмила Викторовна, Рублёв Р.Л.

Astakhova Lyudmila Viktorovna, Rublev R.L.

УДК 336.763 : 004.056 + 336.763 : 342.951.03
ББК Х401.041 + У 9(2) 262.29 : Х 401.041

В. Р. Якупов

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ ЮРИДИЧЕСКИХ ЛИЦ ЗА НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

В статье делается анализ инсайдерской информации, обозначены признаки инсайдерской информации, исследуется административная ответственность за незаконное использование инсайдерской информации.

Ключевые слова: *инсайдерская информация, неправомерное использование инсайдерской информации, административная ответственность.*

V.R. Yakupov

ADMINISTRATIVE LIABILITY OF LEGAL PERSONS FOR THE MISUSE OF INSIDER INFORMATION

In the article an analysis of insider information indicated signs of insider information, investigate the administrative responsibility for the illegal use of insider information.

Keywords: *insider information, misuse of inside information, the administrative responsibility.*

Административная ответственность за неправомерное использование инсайдерской информации была введена в связи с принятием Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее по тексту – Закон об инсайдерской информации). До этого момента административно-деликтным законодательством устанавливался запрет на использование служебной информации на рынке ценных бумаг (статья 15.21 КоАП РФ). Во многом понятия «служебная информация» и «инсайдерская информация» (в ее современной интерпретации) являются родственными, схожими.

Многие страны уже установили ограничения на использование инсайдерской информации при совершении операций с финансовыми инструментами. Так, в США законодательный запрет на инсайд был наложен еще в 1934 году (Securities Exchange Act 1934 г.), в Австралии – в 1961 году (Companies Act), во Франции – в 1967 году (Ordonnance Number 67-833), в Великобритании – в 1980 году (Companies Act), в Японии – в

1989 году (Shoken Torihikiho), в Германии – в 1994 году (Securities Trading Act)[1]. Соответственно, запрет инсайдерской торговли – не просто прихоть законодателя, обусловленная стремлением приблизить российское законодательство к праву наиболее развитых стран, а разумный ответ на поразившую отечественный финансовый рынок практику недобросовестной конкуренции. Установление правовой ответственности за неправомерное использование инсайдерской информации обусловлено необходимостью обеспечения защиты прав и законных интересов участников финансового рынка.

Административная ответственность за инсайд предусмотрена ст. 15.21 КоАП РФ («Неправомерное использование инсайдерской информации»). Диспозиция этой статьи выглядит следующим образом: «Неправомерное использование инсайдерской информации, если это действие не содержит уголовно наказуемого деяния». Санкция данной правовой нормы имеет следующий вид: «влечет наложение административного штрафа на юридических лиц – в размере суммы излишнего дохода либо суммы убытков, которых гражданин, должностное лицо или юридическое лицо избежали в результате неправомерного использования инсайдерской информации, но не менее семисот тысяч рублей». Рассмотрим подробнее данный состав правонарушения, раскрыв его элементы.

Объект правонарушения – общественные отношения, обеспечивающие справедливое ценообразование на финансовые инструменты, иностранную валюту и (или) товары, равенство инвесторов и укрепление их доверия (п.1 ст. 1 Закона об инсайдерской информации). Предмет правонарушения – инсайдерская информация. Можно выделить четыре признака инсайдерской информации: 1) это информация точная и конкретная; 2) это информация, которая не была распространена или предоставлена; 3) эта информация, способная оказать существенное влияние на цены финансовых инструментов, иностранной валюты, товаров; 4) эта информация, которая относится к сведениям, составляющим законодательно определенный перечень инсайдерской информации.

Субъект правонарушения – любое лицо, неправомерно использовавшее инсайдерскую информацию (п. 1 ст. 7 Закона об инсайдерской информации). Субъект неправомерного использования инсайдерской информации общий: юридическое лицо любой организационно-правовой формы и формы собственности. Однако из категории «любое юридическое лицо» необходимо осуществить несколько изъятий:

1) публичные субъекты, осуществляющие операции с финансовыми инструментами в целях управления государственным и муниципальным долгом (Правительство Российской Федерации либо уполномоченный им федеральный орган исполнительной власти; высшие исполнительные органы государственной власти субъектов Российской Федерации либо соответствующие финансовые органы субъектов Российской Федерации; исполнительно-распорядительные органы муниципальных образований (местные администрации)[2];

2) публичные субъекты, осуществляющие операции с финансовыми инструментами, иностранной валютой в целях реализации Банком России функций по осуществлению единой государственной денежно-кредитной политики, защите и обеспечению устойчивости рубля (Центральный банк Российской Федерации и иные лица, действующие от его имени);

3) средства массовой информации, опубликовавшие переданную им инсайдерскую информацию;

4) профессиональные участники рынка ценных бумаг и иные лица, совершившие операции, сопровождающиеся неправомерным использованием инсайдерской информации, если указанные операции совершены по поручению (распоряжению) лица, владеющего инсайдерской информацией.

Таким образом, по российскому законодательству совершить правонарушение, предусмотренное статьей 15.21 КоАП РФ, может любое лицо, владеющее инсайдерской информацией. При этом из числа субъектов рассматриваемого состава правонарушения законодатель выделил исчерпывающий перечень лиц, которые правомерно располагают инсайдерской информацией в силу служебного положения, должностных или профессиональных обязанностей, заключенного трудового или гражданско-правового договора, – инсайдеров. Соответственно, в России за неправомерное использование инсайдерской информации к административной ответственности могут быть привлечены в равной степени как инсайдеры, так и не относящиеся к инсайдерам лица. Каким образом подобный

вопрос решается в зарубежных государствах? Проведем сравнительный анализ.

Объективная сторона правонарушения – неправомерное использование инсайдерской информации, если это действие не содержит уголовно наказуемого деяния. Для уяснения содержания объективной стороны необходимо определить категорию «неправомерное использование инсайдерской информации».

К неправомерному использованию инсайдерской информации относится следующее: 1) совершение операций с финансовыми инструментами, иностранной валютой, товарами на основе инсайдерской информации; 2) неправомерная передача инсайдерской информации третьим лицам; 3) дача рекомендаций на совершение сделок с финансовыми инструментами, иностранной валютой, товарами или склонение к совершению этих сделок любым способом.

В ряде зарубежных правопорядков юридическая ответственность за незаконное использование инсайдерской информации устанавливается не только для инсайдеров, но и для вторичных инсайдеров (или квазиинсайдеров, то есть лиц, располагающих инсайдерской информацией). При этом в законах этих стран делается разграничение относительно способов осуществления неправомерного использования инсайдерской информации в зависимости от субъекта правонарушения. Как правило, вторичные инсайдеры (квазиинсайдеры) не подлежат ответственности за передачу инсайдерской информации или за дачу рекомендаций третьим лицам; для них установлен запрет лишь на использование инсайдерской информации при совершении операций с финансовыми инструментами. Для российского законодательства подобное разделение нехарактерно: запрет на неправомерное использование инсайдерской информации (независимо от способа его совершения) является универсальным и распространяется абсолютно на всех лиц, располагающих инсайдерской информацией (безотносительно к тому, является ли это лицо инсайдером или нет). Единственное, в пункте 2 статьи 7 федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» сделано уточнение, что использование инсайдерской информации считается неправомерным, а лицо, ее использовавшее, подлежит юридической ответственности только в том случае, если это лицо осознавало, что информация является инсайдерской.

Полагаем, широко представленный в зарубежном законодательстве дифференцированный подход к ответственности за инсайд, учитывающий особенности субъекта правонарушения, является более предпочтительным. На лиц, на относящихся к инсайдерам, не должна распространяться ответственность за передачу полученной ими инсайдерской информации другим субъектам, а также за дачу рекомендаций третьим лицам по совершению операций на организованных рынках, если в основе этих рекомендаций лежит инсайдерская информация. Связано это с тем, что у не являющего инсайдером субъекта ввиду отсутствия у него должностных, трудовых, договорных отношений (то есть каких-либо правовых связей) с организацией никаких юридических обязательств перед этой компанией относительно использования ее внутренних сведений (инсайдерской информации) нет и не может быть. Негативные юридические последствия за нарушение режима конфиденциальности инсайдерской информации должны наступать лишь для тех, кто этот режим обязан был соблюдать, то есть для тех, кому эта информация была на легальных основаниях вверена – для инсайдеров. Для всех же прочих правовой запрет на инсайдерскую торговлю может распространяться лишь на случаи непосредственного использования полученной инсайдерской информации в целях совершения операций на организованных рынках.

Итак, для лиц, не относящихся к инсайдерам, следует исключить административную ответственность за передачу инсайдерской информации другим лицам и за дачу третьим лицам основанных на инсайдерской информации рекомендаций относительно совершения сделок на организованных торгах. Для этого необходимо в статью 6 федерального закона «О противодействии неправомерному использованию инсайдерской информации» ввести часть 1.1. следующего содержания: «Запрет, установленный пунктами 2 и 3 части 1 настоящей статьи, распространяется только на лиц, указанных в статье 4 настоящего Федерального закона».

Важно также отметить следующее:

1) при осуществлении действий по неправомерной передаче инсайдерской информации, а также по даче рекомендаций на

совершение операций с финансовыми инструментами (иностранной валютой, товарами) факт получения лицом, располагающим инсайдерской информацией, вознаграждения не имеет юридического значения;

2) при передаче инсайдерской информации ответственность наступает независимо от осознания лицом, владеющим инсайдерской информацией, того факта, что переданная инсайдерская информация будет использована третьими лицами при совершении сделок на организованном рынке.

Еще следует обратить внимание на то обстоятельство, что диспозиция статьи 15.21 КоАП РФ не предусматривает общественно вредных последствий. Соответственно, состав неправомерного использования инсайдерской информации по конструкции объективной стороны является формальным. То есть независимо от того, причинила ли инсайдерская торговля ущерб участникам рынка либо принесла лицу, использовавшему инсайдерскую информацию, доход или позволила последнему избежать убытков, само по себе неправомерное использование инсайдерской информации является противозаконным и наказуемым деянием.

Субъективная сторона правонарушения – непринятие юридическим лицом всех зависящих от него мер по соблюдению установленных законодательством правил и норм, за нарушение которых статьей 15.21 КоАП РФ предусмотрена административная ответственность, при условии, что у него имелась возможность для их соблюдения. Таким образом, законодатель связывает административную ответственность организации с непринятием ею всех необходимых для предотвращения неправомерного использования инсайдерской информации мер. Но в чем эти меры должны заключаться?

Законодатель частично ответил на этот вопрос, установив в статье 11 федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» минимальный круг обязанностей юридических лиц по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации. К этим обязанностям относятся:

1) разработка и утверждение порядка доступа к инсайдерской информации, правил охраны ее конфиденциальности и контроля за соблюдением требований федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» и принятых в соответствии с ним нормативных правовых актов;

2) создание (определение, назначение) структурного подразделения (должностного лица), в обязанности которого входит осуществление контроля за соблюдением требований федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» и принятых в соответствии с ним нормативных правовых актов и которое подотчетно совету директоров (наблюдательному совету), а в случае его отсутствия высшему органу управления юридического лица;

3) обеспечение условий для беспрепятственного и эффективного осуществления структурным подразделением (должностным лицом), указанным в пункте 2 настоящего перечня, своих функций.

Однако принятие юридическим лицом всего комплекса обозначенных законодателем мер по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации не дает этой организации абсолютно никаких гарантий от привлечения ее к административной ответственности за противоправные действия работников этой компании. Очевидно несовершенство законодательного подхода к определению вины юридического лица (в связи с тем, что этот вопрос был исследован в первой главе настоящей работы, более подробно данная проблема рассматриваться не будет).

Также необходимо остановиться отдельно в рамках анализа состава неправомерного использования инсайдерской информации, – практика применения ст. 15.21 КоАП РФ. Реализация правовой нормы – важнейший аспект ее существования. Вне правоотношений право вообще не имеет смысла. Поэтому правоприменительная практика – один из центральных моментов характеристики любого состава правонарушения. Однако ст. 15.21 КоАП РФ в практике не применялась ни разу.

До настоящего момента ни одна организация не была привлечена к административной ответственности за неправомерное использование инсайдерской информации. Означает ли этот факт, что на российских финансовых рынках отсутствует такое явление

как инсайдерская торговля? Напротив, на рынке имеется немало примеров, однозначно свидетельствующих об обратном. Приведем некоторые из них.

Так, например, акции ОАО Концерн «Калина» за сентябрь – октябрь 2011 года выросли на 75% как раз за две недели до того, как стало известно о покупке компании (82%) со стороны Unilever.[3] В августе 2011 года акции ОАО «НК «Роснефть» подскочили почти на 10% за два дня до объявления о партнерстве с ExxonMobil. Управляющий директор УК «Финам Менеджмент» Элвис Марламов обращает внимание на сделку по выкупу акций Казанского вертолетного завода (КВЗ) холдингом «Вертолеты России». По его словам, бумаги долго шли вверх перед неожиданно объявленным выкупом акций. Эта сделка стала очень успешной для клиентов Газпромбанка, которые в ноябре 2011 года уверенно купили 13,25% акций КВЗ по цене около 90 руб. за штуку. В следующем году «Вертолеты России» выкупили бумаги по 108,2 руб. за бумагу.[4] Одним из ярчайших случаев инсайда, причем на высшем уровне, было повышение кредитного рейтинга России агентством Standard & Poor's в 2004 году. За 33 минуты до официального объявления этой новости цены на российские еврооблигации стали расти, увеличившись на 1%. А за 15 минут до обнародования информации стоимость многих акций, а вместе с ней и фондовые индексы бирж РТС и ММВБ, поднялась примерно на 2%.[5]

Таким образом, ст. 15.21 КоАП РФ в настоящее время на практике не применяется. При этом в реальности на российских организованных торгах инсайд процветает. Подобная ситуация, с одной стороны, объясняется несовершенством действующего законодательства (о чем было сказано выше), а с другой, является однозначным показателем существенных изъянов в деятельности правоприменительных органов.

Примечания

[1] Ширинян, И. Мировой опыт использования инсайдерской информации на рынке ценных бумаг / И. Ширинян // Рынок ценных бумаг. 2004. № 10. С. 51-76.

[2] Выведение указанных публичных лиц за пределы сферы действия статьи 15.21 КоАП РФ, является частным подтверждением общего вывода, сделанного в первом параграфе первой главы настоящей работы, о непринадлежности государственных и муниципальных органов к числу субъектов административно-деликтного права.

[3] ФСФР не выявила ни одного случая манипулирования или инсайдерской торговли // Ведомости. – http://www.vedomosti.ru/finance/news/3272521/rost_bez_viny (дата обращения 04.02.13).

[4] Кто и как манипулирует на российском финансовом рынке // РБК daily – http://www.rbcdaily.ru/2012/10/17/finance/562949984941415 (дата обращения – 04.02.13).

[5] Вержбицкий, А. Инсайдеров будут сажать через три года / А. Вержбицкий // Аудит. 2010. № 7-8. С. 37.

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 (094.5.072) + 347.1 : 004.056
ББК Х 400.323 + Х 401.114

Н.Е. Циулина

ФОРМИРОВАНИЕ И РАЗВИТИЕ ПРАВОВОЙ КАТЕГОРИИ «ПЕРСОНАЛЬНЫЕ ДАННЫЕ»

В статье автор анализирует содержание понятия «персональные данные». Исследуется зарубежный опыт определения персональных данных в законодательстве. Дается характеристика современному определению персональных данных, закрепленному в российском законодательстве.

Ключевые слова: *Федеральный закон, персональные данные, иностранное законодательство.*

N. E. Tsiulina

FORMATION AND DEVELOPMENT LEGAL CATEGORY OF «PERSONAL DATA»

The author analyzes the concept of "personal data". Study the international experience of the definition of personal data in the legislation. A characteristic of the modern definition of personal data, in Russian law.

Keywords: *Federal Law, personal data, foreign legislation.*

Исследование проблемы персональных данных требует выявления содержания используемых понятий. Ключевой в данной работе является дефиниция «персональные данные», прошедшая достаточно длительный путь формирования и развития.

В 1980 г. Организация экономического сотрудничества и развития разработала рекомендации по защите личной тайны и трансграничной передаче персональных данных, включив в понятие персональной информации следующие виды данных : первичные данные: имя, дата и место рождения, гражданство; семейное положение: брак, родственники, дети, иждивенцы; образование и навыки: информация о пройденном обучении, полученных степенях, званиях и достижениях; стиль жизни и личные предпочтения, потребительские предпочтения, увлечения, спорт, личное поведение в быту; финансовые ресурсы: доход, собственность недвижимость; финансовые идентификаторы: детали банковских счетов и пароли доступа к ним[1].

Конвенция Совета Европы № 108 от 28 января 1981 г. «О защите физических лиц при автоматизированной обработке персональных данных»[2], на наш взгляд, стала объединяющим началом для соответствующего национального законодательства большинства европейских стран. Она установила категорию «персональные данные» как любую информацию об определенном или поддающемся определению физическом лице.

Дальнейшее развитие понятие «персональные данные» получило в Директиве Европейского Парламента и Совета Европы

95/46/ЕС от 24 октября 1995г. «О защите личности в отношениях обработки персональных данных и свободном обращении этих данных» [3], которая, по сути, является правовым стандартом как для стран-членов Европейского Союза, так и для неевропейских стран, определяет **персональные данные,** как «любую информацию, относящуюся к определенному или определяемому физическому лицу («субъекту данных»); определяемым является лицо, которое может быть определено, прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности». Особая значимость этого документа в том, что он закрепил несколько правовых понятий. Во-первых, «персональные данные» определены как любая информация, связанная с идентифицированным лицом (субъектом данных), и подразумевает информацию, зафиксированную на любом носителе. Вводится понятие «контролеры данных» - лица или организации, которые определяют цели и способы обработки персональных данных. Под «обработкой персональных данных» Директива ЕС понимает любые операции с персональными данными или их совокупность, включая сбор, запись, систематизацию, хранение, изменение, передачу или раскрытие.

В России начало разработки категории «персональные данные», определение ее содержания приходится на конец XX – начало XXI вв. и хронологически совпадает с широким внедрением информационных технологий в повседневную жизнь, превращением информации в самый дорогой товар, т.е. переходом на ступень информационного общества.

Основные права и свободы человека и гражданина, в том числе, права и свободы в области информации, были закреплены в Конституции РФ 1993 года[4], именно Конституционные нормы положили начало определению содержания дефиниции «персональные данные».

Следующей вехой стал Указ Президента РФ от 06 марта 1997 года № 188[5], которым утвержден перечень сведений конфиденциального характера. К персональным данным, а, следовательно, прав и свобод граждан России гарант Конституции РФ, относит «персональные данные» - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность» к сведениям конфиденциального характера, т.е. к информации, которая подлежит защите от незаконного распространения (разглашения) и охраняется законом.

В Российском законодательстве впервые легальное определение персональных данных было установлено Федеральным законом «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ, как «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»[6]. Данная формулировка могла быть оправдана только при расширительном толковании термина «жизнь»[7].

Одновременно проблему содержания персональных данных стремилось решать отраслевое законодательство с учетом специфики регулируемой сферы общественных отношений.

Исследование нормативных актов выявляет различие в подходах к содержанию персональных данных. Так, понятие «персональные данные работника», приведенное в ТК РФ, свидетельствует, что оно рассматривается как информация, получение которой необходимо работодателю в отношении каждого конкретного работника в связи с трудовыми отношениями. Иными словами, речь идет не обо всех сведениях (фактах, событиях, обстоятельствах частной жизни граждан), а лишь о таких обстоятельствах, которые могут характеризовать гражданина как работника, поэтому понятие «персональные данные» в трудовом законодательстве сужается[8].

Федеральный закон «О государственной автоматизированной системе Федерации «Выборы»[9] трактует «персональные данные», как сведения, которые содержатся в государственной автоматизированной системе «Выборы», позволяющие идентифицировать личность гражданина .

В соответствии со статьей 17 Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»[10] к «персональным данным» относятся: страховой номер; фамилия, имя отчество; фамилия, которая была у застрахованного лица при рождении; дата рождения; место рождения; пол; адрес постоянного места жительства; серия и номер паспорта или удостоверения личности, дата выдачи указанных

документов; наименование выдавшего их органа; гражданство; номер телефона; периоды трудовой и иной общественно полезной деятельности, включаемые в общий стаж для назначения государственной трудовой пенсии, а также специальный стаж, связанный с особыми условиями труда, работой в районах Крайнего Севера и приравненных к ним местностях, выслугой лет, работой на территориях, подвергшихся радиоактивному загрязнению; заработная плата или доход (за каждый месяц страхового стажа), на которые начислены страховые взносы в Пенсионный фонд Российской Федерации в соответствии с законодательством Российской Федерации; сумма заработка (за каждый месяц страхового стажа), который учитывается при назначении трудовой пенсии; сумма начисленных данному застрахованному лицу страховых взносов (за каждый месяц страхового стажа), включая страховые взносы за счет работодателя и страховые взносы самого застрахованного лица; периоды выплаты пособия по безработице; периоды военной службы и другой приравненной к ней службы, включаемые в общий трудовой стаж; сведения о назначении (перерасчете), индексации и начислении пенсии.

Согласно Указу Президента РФ от 23.10.2008 № 1517, «под персональными данными гражданского служащего понимаются сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего либо подлежащие включению в его личное дело»[11].

Персональные данные муниципального служащего – «информация, необходимая представителю нанимателя (работодателю) в связи с исполнением муниципальным служащим обязанностей по замещаемой должности муниципальной службы и касающаяся конкретного муниципального служащего»12. Стоит подчеркнуть, что в силу указанной нормы персональные данные муниципального служащего подлежат обработке в соответствии с общими требованиями трудового законодательства (в отличие, например, от персональных данных государственных гражданских служащих). Такое различие в подходах к определению персональных данных государственных и муниципальных служащих обусловлено, в частности, разницей в концепциях указанных видов деятельности. Так, государственная гражданская служба базируется на «концепции служебного права», законодательную основу которой составляет административное законодательство, а муниципальная служба явно основана на трудоправовом подходе[13].

Проведенный анализ российского законодательства по избранной проблеме свидетельствует об отсутствии у законодателя единой согласованной трактовки понятия «персональные данные».

Определенный вклад в разработку дефиниции «персональные данные» внесли и ученые – юристы. По мнению И.Л. Бачило, «персональные данные» - это такие сведения о личности, которые включаются в информационную систему государственных, общественных и частных, корпоративных организаций по инициативе индивида или в силу закона в целях реализации его прав и обязанностей при участии в самых разных социальных процессах и отношениях. Это та часть частной жизни, которая определенным образом представлена и присутствует в публичном и гражданском секторах правовых отношений индивида с другими субъектами права[14]. Персональные данные не только обеспечивают социализацию личности, но и обязывают общественные структуры выстраивать отношения с гражданином в рамках закона и с учетом его правового статуса, материализованной основой, доказательством которого являются его персональные данные[15].

Ю. В. Травкин утверждает, что «к персональным данным относятся также мнения о данном человеке, объективные или субъективные, если они зафиксированы и соотнесены с данным человеком»[16].

Накопленный опыт и стремление законодателя не только преодолеть отставание от Европы, ликвидировать пробелы в праве в связи с возросшей значимостью информации, но и практически обеспечить реализацию конституционных прав граждан, способствовали разработке и принятию Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»[17]. Уточнение и развитие положений Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» отражено в Федеральном законе от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»[18] (далее - Новый закон). В соответствии со ст. 3 Нового закона «персональные данные – любая информация, относящаяся к

прямо или косвенно определенному или определяемому физическому лицу»[19].

В основном определении персональных данных Старый закон содержит перечень сведений, которые относятся к персональным данным человека (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация), данный перечень не является исчерпывающим, поскольку, исходя из самой природы персональных данных, полностью их перечислить достаточно сложно. На наш взгляд, в Старом законе нарушается главное требование к юридическому термину, а именно, каждый применяемый в праве термин в идеале должен иметь свое, и только свое, оригинальное и притом единственное значение[20].

Действительно, в Старом законе содержание категории персональных данных неоправданно сужено, потому что не указывает на понятия персональных данных, которые приведены в следующих ст. 10 и ст. 11[21]. В указанных статьях закон дает косвенное определение специальной категории персональных данных, как сведений, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни биометрические персональные данные, и биометрических персональных данных, как сведений которые характеризуют физиологические особенности человека на основании которых можно установить его личность, становится не понятно и законом это не устанавливается к какой категории относятся персональные данные, которые даны в основном понятии, а именно фамилия, имя, отчество и др. Ключевой в формулировке в Старом законе, на наш взгляд, является оговорка «другая информация», под которой понимается любая информация, позволяющая идентифицировать человека.

В Новом законе налицо явное расширение понятия «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу», т.к. в оно включает в себя и специальную категорию персональных данных и биометрические. Это может быть любая личная информация, которая относится к тому или иному человеку. Существенное расширение понятия «персональные данные» увеличивает круг операторов, их обрабатывающих, что требует дополнительных мер по защите. Понятие однозначно связывается с личностью и информацией прямо или косвенно касающейся этой личности, при этом не закрепляет объем сведений, которые могут к такой информации относиться, потому что объем этих сведений не однозначен и зависит от особенностей правовой системы отрасли права.

Но, на наш взгляд, такая трактовка понятия «персональные данные» содержит и некоторое логическое противоречие. С одной стороны, определение, данное таким образом, обеспечивает однозначное понимание природы персональных данных и является базовым для комплекса правовых дефиниций во всех отраслях права Российского законодательства. А с другой – закон не содержит четких критериев, позволяющих разграничить информацию персонального характера, которая затрагивает аспекты частной жизни лица и сведения, которые могут понадобиться оператору для осуществления заявленной цели. Это затрудняет установление степени допустимого вмешательства в частную жизнь.

Данный подход подтверждает и зарубежный опыт. Так, в Латвии – «персональные данные» – это «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу». По закону Австрии «О защите персональных данных» 2000 г. Персональные данные - это «сведения, которые идентифицируют определенного или определяемого лица». Данный подход характерен для большинства европейских государств, а именно: для Германии «Закон об охране данных 1990 г.), Великобритании (Законы о защите данных 1984 и 1998 гг.), Дании (законодательные акты о регистрах публичных органов власти и о частных регистрах 1979 г.), Франции (Закон об обработке данных, файлах данных и индивидуальных свободах 1978 г.) и многих других стран[22].

С момента появления первых нормативных актов по данной проблеме защита персональных данных рассматривалась в контексте права на неприкосновенность частной жизни. Реалии времени, стремительное развитие информационных технологий, активный сбор и обработка персональных данных как в сфере частной жизни, так и в публичных отношениях индивидов с организациями и властными структурами заметно меняют содержание правовой категории.

Для граждан основным способом защиты их персональных данных будет проявление бдительности при предоставлении кому-либо информации личного характера, а также знание прав и обязанностей, которыми наделяет Федеральный закон операторов и субъектов персональных данных.

Таким образом, конец XX – начало XXI вв. характеризуются в России достаточно активной разработкой (законодательной и научной) понятия «персональные данные». Более позднее вступление России на ступень информационного общества, технологического отставания предопределили значительное влияние европейского законодательства на формирование понятийного аппарата института персональных данных.

Примечания

[1] Вельдер И. А. Система правовой защиты персональных данных в Европейском Союзе: Автореф. дисс. … канд. юрид.наук. Казань, 2006. с. 21

[2] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. (ETS N 108) [Электронный ресурс] // КонсультантПлюс.

[3] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года) [Электронный ресурс] // http://pd.rsoc.ru/law/

[4] Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // СЗ РФ. 2009. № 4. Ст. 445

[5] Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изм., внесенными Указом Президента РФ от 23 сентября 2005г. №1111) // Российская газета. №51. 14.03.1997.

[6] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 28.07.2012) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // КонсультантПлюс.

[7] Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2(4). – С.4-9.

[8] Новичкова Ю.В. Персональные данные – без права передачи, или особенности расторжения трудового договора за разглашение персональных данных / Ю.В.Новичкова // Справочник кадровика. 2007. № 1. С. 14-23.

[9] Федеральный закон «О государственной автоматизированной системе РФ «Выборы» принят Госдумой 20.12.2002 г. [Электронный ресурс] // http://www.consultant.ru

[10] Федеральный закон от 01.04.1996 № 27-ФЗ (ред. от 23.07.2008) «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (принят ГД ФС РФ 08.12.1995) [Электронный ресурс] // http://www.consultant.ru

[11] Указ Президента РФ от 23.10.2008 № 1517 «О внесении изменений в некоторые акты Президента Российской Федерации» [Электронный ресурс] // http://www.consultant.ru

[12] Ст.29 Федерального закона от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» // Российская газета. № 47. 07.03.2007

[13] Чаннов С.Е. Правовой режим персональных данных на государственной и муниципальной службе // Российская юстиция. 2008. № 1. С. 22-23.

[14] Бачило И. Персональные данные в сфере бизнеса // Закон. – 2002. - № 12 .- С.52-58.

[15] Бачило И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования / И.Л. Бачило, Л.А. Сергиенко, Б.В. Кристальный и др. – Минск, 2006. – С. 86.

[16] Травкин Ю. В. Персональные данные. М.: Амалданик, 2007. С. 33.

[17] Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» // Российская газета. № 165. 29.07.2006.

[18] Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» [Электронный ресурс] // http://base.consultant.ru/

[19] Там же

[20] Шугрина Е.С. Техника юридического письма. М.: Дело, 2001. С. 62. Электронный ресурс http://www.lawmix.ru/comm.php?id=9120

[21] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 04.06.2011) "О персональных данных" [Электронный ресурс] // {КонсультантПлюс}

[22] Минбалеев А.В. Понятие и признаки персональных данных // Актуальные проблемы права России и стран СНГ-2005: Материалы VII междунар. науч.-практ. конф., 7-8 апр. 2005 г. Челябинск: Издательство ЮУрГУ, 2005. Ч. 2. С. 162-164.

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

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

ББК У9(2)240 : Х401.114
УДК 331.108.3 + 005.953 : 005.841 : 343 + 004.056.5 : 331.108.3

Л.В. Астахова, О.О. Землянская

МЕТОДИКА ОЦЕНКИ КАДРОВЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ЭТАПЕ ПРИЕМА СОТРУДНИКА НА РАБОТУ

В статье представлена методика оценки кадровых уязвимостей информационной безопасности на этапе приема сотрудника на работу, разработанная на основе анализа нормативных документов, классификации причин дестабилизирующих воздействий на информацию ограниченного доступа и психологических тестов.

Ключевые слова: *методика, оценка, информационная безопасность, кадровая уязвимость.*

L.V. Astakhova, O.O. Zemlyanskay

ASSESSMENT METHOD OF COMPANY'S INFORMATION SECURITY PERSONNEL VULNERABILITIES AT THE STAGE OF RECRUITMENT

The article presents an assessment method of company's information security personnel vulnerabilities at the stage of recruitment, developed on the basis of analysis of regulatory documents, classification of reasons destabilizing effects on confidential information and psychological tests.

Keywords: *method, assessment, information security, personnel vulnerability.*

Преступления, в том числе в информационной сфере, совершаются людьми. Большинство систем не может нормально функционировать без участия человека. Пользователь системы, с одной стороны, — ее необходимый элемент, а с другой - причина и движущая сила нарушения или преступления. Вопросы безопасности систем большей частью есть вопросы человеческих отношений и человеческого поведения. Особенно это актуально в сфере информационной безопасности, т. к. утечка информации в подавляющем большинстве случаев происходит по вине сотрудников. В связи с этим существует необходимость в оценке угроз и уязвимостей персонала.

Анализ международных и национальных стандартов, методик государственных регуляторов и Центрального Банка России, предпринятый в наших публикациях [2,3], показал, что ни в одном из них в качестве уязвимостей ин-

формационной безопасности не названы личностные качества персонала и не определены методы их оценки. Между тем, личностные качества входят в структуру профессиональных компетенций специалиста любого профиля, и именно они составляют сущность понятия «человеческий фактор», являющийся зачастую причиной утраты и утечки защищаемой информации.

Для определения требуемых личностных качеств специалиста, чья деятельность в организации связана с защитой информации, рассмотрим причины, вызывающие дестабилизирующие воздействия на состояние информационной безопасности, предложенные авторитетным экспертом в области информационной безопасности А.И. Алексенцевым [1].

К преднамеренным причинам ученый отнес: стремление нанести вред (отомстить) руководству или коллеге по работе; стремление обезопасить себя, родных и близких от угроз, шантажа, насилия; воздействие со стороны злоумышленника. К непреднамеренным причинам, по его мнению, относятся: неквалифицированное выполнение операций; халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе; небрежность, неосторожность, неаккуратность.

Обстоятельствами появления этих причин являются: склонность к развлечениям, пьянству, наркотикам; зависть, обида; тщеславие, самомнение, завышенная самооценка, хвастовство; низкий уровень профессиональной подготовки; излишняя болтливость, привычка делиться опытом, давать советы [1].

Исходя из перечисленных причин и обстоятельств дестабилизирующих воздействий на защищаемую информацию, в данной работе смоделирована методика по оценке персонала в контексте информационной безопасности, в которой в качестве критериев для оценки выбраны личностные качества человека.

Созданная методика предназначена для использования при приеме сотрудника на работу, оценка кандидата совмещается с собеседованием. В ходе собеседования сотрудник отдела кадров заполняет ответы кандидата на вопросы Анкеты, представленной в Таблице 1.Поставить ее на Следующую страницу! Результатом является процентный показатель уязвимости: от 0% (кандидат уязвим с точки зрения безопасности, и представляет угрозу информационной безопасности предприятия) до 100% (кандидат неуязвим и не представляет угрозы). На усмотрение руководства и службы информационной безопасности могут быть выставлены минимальные проходные пороги для различных категорий сотрудников.

Категорирование сотрудников необходимо для определения сценария оценки кандидата и заполнения таблицы ответов. Критерии могут быть разными. Например, можно выделить категории, учитывая такие факторы, как ценность информации, с которой необходимо работать сотруднику (аналогично формам допуска к государственной тайне); частота обращения к конфиденциальной информации (КИ): постоянно, периодически, обращение редкое или отсутствует.

Категории сотрудников могут выглядеть следующим образом:

1. Сотрудники постоянно работают с КИ высокой степени важности.
2. Сотрудники периодически работают с КИ высокой степени важности.
3. Сотрудники постоянно работают с КИ средней степени важности.
4. Сотрудники периодически работают с КИ средней степени важности.
5. Сотрудники редко работают с КИ средней степени важности.
6. Сотрудники периодически работают с КИ низкой степени важности.
7. Сотрудники редко работают с КИ низкой степени важности.

Категории могут быть объединены. Например:

I категория включает в себя 1,2,3 позиции;

II категория – 4,5 позиции;

III категория – 6 и 7 позиции.

Оценивать уязвимость кандидата необходимо по факторам, которые представлены в виде блоков: болтливость, злопамятность, хобби, темперамент, наличие вредных привычек, внимательность, стрессоустойчивость, подверженность влиянию, общие представления о необходимости защиты информации.

Излишняя болтливость опасна с точки зрения информационной безопасности, так как сотрудник может раскрыть информацию ограниченного доступа посторонним людям. Болтливость можно оценить в ходе собеседования или попросить рассказать историю на определенную тему, например, о том, как прошел вчерашний день.

Стремление сотрудника отомстить руководству или коллеге может привести к утечке информации во время работы или после

увольнения недовольного сотрудника. Оценить риск злого умысла можно, спросив мнение о прошлом месте работы (руководстве, взаимоотношениях в коллективе).

Некоторые увлечения характерны частым взаимодействием с людьми, это увеличивает риск утечки информации. Такими хобби могут быть походы в ночные клубы, групповые спортивные, танцевальные клубы, туризм. Спокойные домашние хобби более безопасны с точки зрения информационной безопасности, например, рукоделие, изучение науки, кулинария.

Наличие вредных привычек повышает риск утечки информации в неформальной обстановке, например, в курилке во время перерывов, в компании, находясь при нахождении в состоянии алкогольного опьянения.

Внимательность так же может послужить показателем в процессе оценки персонала. Рассеянный сотрудник может потерять носители с конфиденциальной информацией, а значит, представляет угрозу компании. Внимательность можно оценить с помощью специальных тестов.

Стрессоустойчивого сотрудника сложнее выбить из колеи, а значит, злоумышленнику сложнее добиться информации ограниченного доступа. Слабо устойчивый к стрессам сотрудник плохо контролирует себя в нестабильном состоянии, что может привести к разглашению конфиденциальной информации. Стойкость в стрессовых ситуациях можно выявить методом стресс-интервью. Можно предложить нестандартную ситуацию и узнать о действиях сотрудника в ней.

Подверженный манипуляциям сотрудник может допустить несанкционированный доступ злоумышленника к конфиденциальной информации. Оценить устойчивость к манипуляциям можно с помощью психологического теста «Подвержены ли вы манипуляции?» К. Бурениной [5].

Важнейшим показателем личностных качеств субъекта является наличие у него общих представлений о необходимости защиты конфиденциальной информации. Кандидата необходимо спровоцировать на выдачу тайной информации по профилю предыдущего места работы. Исходя из ответа, необходимо сделать соответствующий вывод об уязвимости претендента на вакансию.

В дополнение к оценке личностных качеств претендента во время собеседования следует использовать недавно появившийся способ - сбор и анализ информации о субъекте с помощью социальных сетей. Личная страничка в сети может многое поведать о жизни человека, его интересах и моральных принципах, а потому ее анализ страницы дополняет оценивание вышеуказанных блоков личностных качеств.

Факторами для оценки сотрудника могут являться:

- список интересуемых групп, страниц, на которые подписан пользователь (дополнение к блоку о хобби);
- содержание анкеты, сообщений, фото- и видеоматериала (дополнение к блоку о хобби);
- уровень конфиденциальности страницы, т.е. степени ограничения для разных категорий пользователей (дополнение к блоку о наличии общих представлений о необходимости защиты конфиденциальной информации).

Запросы по фамилии, имени и отчеству в поисковых системах могут дать любую информацию о человеке. Выявленную информацию необходимо интерпретировать индивидуально в каждом случае.

Оценивание происходит по 4-балльной шкале по каждому показателю:

0 – кандидат представляет чрезвычайно высокую угрозу информационной безопасности (чрезмерно болтлив, злопамятен, вспыльчив, в свободное время часто находится в окружении больших компаний, рассеян, легко подвергается манипуляциям, без раздумий сообщает тайны);

1 – кандидат представляет большую угрозу информационной безопасности (отвечает развернуто, иногда допускает лишнюю информацию, склонен к злопамятности, вспыльчивости, в свободное время больше склонен находиться в окружении больших компаний, больше склонен к рассеянности, с трудом подвергается манипуляциям, без раздумий сообщает некоторые детали тайной информации);

2 – кандидат представляет небольшую угрозу информационной безопасности (речь лаконична, редко допускает лишнюю информацию, склонен к злопамятности, вспыльчивости, в свободное время больше склонен находиться в кругу семьи, иногда находится в окружении большого количества людей, скорее внимателен, с большим трудом подвергается манипуляциям, на просьбу сообщить тайную информацию раздумывает, отвечает неконкретно);

Таблица 1. Анкета для оценки кандидата.

Категория сотрудника			Исследуемый блок	Вопрос. Иной показатель оценки
I	II	III		
V	V	V	Излишняя болтливость	Просьба рассказать о вчерашнем дне
V	V			«Вы общительный человек?»
V				В ходе собеседования
V	V	V	Стремление отомстить руководству или коллеге по работе	«Вы легко прощаете людей?»
V	V			Мнение о предыдущем месте работы
V	V	V	Склонность к развлечениям, пьянству, наркотикам	«Чем Вы увлекаетесь?»
V	V			«Как Вы относитесь к проведению свободного времени в большой шумной компании?»
V	V	V	Наличие вредных привычек	«Есть ли у Вас вредные привычки?»
V	V	V	Внимательность	Психологическое тестирование "Корректурная проба" (Тест Бурдона)
V	V	V	Стрессоустойчивость	Применение провокационного интервью
V	V			«Насколько легко Вас вывести из себя?»
V	V	V	Подверженность манипуляциям (воздействие со стороны злоумышленника)	«Насколько сложно изменить Ваше мнение?»
V	V			Тест «Подвержены ли мы манипуляции?» из книги Киры Бурениной
V				(попытка манипулировать)
V	V	V	Неквалифицированное выполнение операций	Провокация на разглашение КИ (Сценарий для каждой должности продумывается индивидуально)
V	V	V		«Есть ли в вашей работе информация, распространение которой ограничено?»
V	V	V	Страница в социальной сети	Анализ содержания анкеты, сообщений, фото- и видеоматериала
V	V			Список интересуемых групп, страниц, на которые подписан пользователь
V				Уровень конфиденциальности страницы
V	V		Обращение на предыдущее место работы	Беседа с руководителем, сотрудниками, которые имеют возможность дать характеристику сотрудникам (секретарь, вахтер)
V			Запрос по личным данным в поисковых системах	Выявленная информация интерпретируется индивидуально в каждом случае

Количество баллов за ответ				Сумма баллов в блоке
3	2	1	0	
контролирует свою речь, отвечает кратко	речь лаконична, редко допускает лишнюю информацию	отвечает развернуто, иногда допускает лишнюю информацию	чрезмерно много информации	
Нет	Скорее нет	Скорее да	Да	
контролирует свою речь, отвечает кратко	речь лаконична, редко допускает лишнюю информацию	отвечает развернуто, иногда допускает лишнюю информацию	чрезмерно болтлив	
Нет	Скорее нет	Скорее да	Да	
Позитивное	«Обиженный» сотрудник. Не склонен к мести	Невозможно оценить. Отказывается отвечать.	«Обиженный» сотрудник. Склонен к мести	
Предполагает постоянное взаимодействие с людьми	Предполагает периодическое взаимодействие с людьми	Предполагает редкое взаимодействие с людьми	Не предполагает взаимодействия с людьми	
Отрицательно	Скорее отрицательно	Скорее положительно	Положительно	
Отсутствуют	Только курение	Только употребление алкоголя	Курение и алкоголь	
76 – 100% – отличное внимание	51 – 75% – хорошее внимание	26 – 50% – среднее внимание	0 – 25% – плохое внимание	
Не стрессоустойчив	Скорее не стрессоустойчив	Скорее стрессоустойчив	Стрессоустойчив	
Сложно	Скорее сложно	Скорее легко	Легко	
Сложно	Скорее сложно	Скорее легко	Легко	
Не подвержен (24-32 балла)	Скорее не подвержен (16-24 балла)	Скорее подвержен (9-16 баллов)	Подвержен (0-8 баллов)	
Не подвержен	Скорее не подвержен	Скорее подвержен	Подвержен	
Не разглашает	Абстрактно ответил	Разглашает детали	Разглашает	
Присутствует	Скорее присутствует	Не знает	Отсутствует	
Содержание анкеты позитивно характеризует ее владельца	Содержание анкеты скорее позитивно характеризует ее владельца	Содержание анкеты скорее негативно характеризует ее владельца	Содержание анкеты негативно характеризует ее владельца	
Список групп не доступен	Групп и страниц мало (до 10), содержание которых позитивно характеризует ее владельца	Групп и страниц немного (10-20), содержание некоторых негативно характеризует ее владельца	Групп и страниц много (более 20), содержание которых негативно характеризует ее владельца	
Страница под псевдонимом с минимальным количеством информации	На странице указана информация, которая не дает полного представления о ее владельце	Страница доступна всем пользователям. Анкета достаточно заполнена.	Доступно очень много информации, страница открыта для всех пользователей	
Отзывы о кандидате позитивные	Отзывы о кандидате скорее позитивные	Отзывы о кандидате скорее негативные	Отзывы о кандидате негативные	
кандидат неуязвим	кандидат скорее неуязвим	кандидат скорее уязвим	кандидат уязвим	

3 – кандидат не представляет угрозы информационной безопасности (контролирует свою речь, отвечает кратко, совершенно не злопамятен, эмоционально устойчив, в свободное время проводит в семейном кругу, внимателен, устойчив к манипуляциям, не сообщает тайны).

После собеседования происходит расчет коэффициента уязвимости кандидата – P , выраженный в процентах, по формуле:

$$P = \frac{\sum_{i=1}^{N} p_i}{N*4} * 100\% \quad (1)$$

где N – количество выставленных оценок (в том числе оценки «0 баллов»);

p_i – количество баллов за i-ый ответ;

i – порядковый номер ответа.

Допустим, кандидат относится ко второй категории, по которой, как правило, оцениваются 2 критерия по каждому блоку. Оценены 10 блоков, в каждом блоке по 2 оценки. Значит N=20. Баллы выставлены следующим образом:

1 – 2; 2 – 1; 3 – 2; 4 – 3; 5 – 1; 6 – 2; 7 – 0; 8 – 1; 9 – 0; 10 – 3; 11 – 3; 12 – 2; 13 – 1; 14 – 0; 15 – 1; 16 – 0; 17 – 3; 18 – 2; 19 – 1; 20 – 1.

Посчитаем сумму баллов (числитель дроби)

$$\sum_{i=1}^{N} p_i = 2 + 1 + 2 + 3 + 1 + 2 + 0 + 1 + 0 + 3 + 3 + 2 + 1 + 0 + 1 + 0 + 3 + 2 + 1 + 1 = 29$$

Рассчитаем коэффициент уязвимости кандидата – P по формуле 1.

$$P = \frac{29}{20 * 4} * 100\% = 0{,}3625 * 100\% = 36{,}25\ \%$$

Интерпретация результата может быть такой:

«Коэффициент равен 36,25%. Показатель ниже 50%, значит, что кандидат представляет угрозу информационной безопасности организации».

Таким образом, уникальность разработанной методики заключается, во-первых, в числовом результате оценки сотрудника, которая составляется по различным критериям для оценивания; во-вторых, в возможности проводить оценку в зависимости от градации кандидата, что влияет на глубину проверки; в-третьих, в экономичности, т.к. методика не требует больших финансовых, материальных и трудовых затрат. Результатом является числовой показатель в интервале от 0 до 100%: результат 0% означает, что «кандидат уязвим, представляет угрозу информационной безопасности предприятия», 100% - «кандидат неуязвим, не представляет угрозы информационной безопасности». В дополнение к оценкам личностных качеств, полученным в процессе собеседования, необходим анализ информации о кандидате в открытом доступе в интернете: в социальных сетях, с помощью запросов по фамилии, имени и отчеству в поисковых системах.

Список использованной литературы:

1. Алексенцев, А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. – М., 2000.– № 3.

2. Астахова, Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – М., 2013.– № 1. –С.79-83.

3. Астахова, Л.В. Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. – М., 2011.– № 1. –С.26-33.

4. Бруннер Е.Ю. Лучше, чем супервнимание: Методики диагностики и психокоррекции: Психология внимания; Оценочные тесты; Развивающие игровые упражнения. Серия: Психологический практикум.— Ростов-на-Дону: Феникс, 2006.— 317 с.

5. Буренина К. Офис. Стратегия выживания. – М.: Эксмо, 2007. – 112 с.

Астахова Людмила Викторовна, Землянская Ольга Олеговна

Astakhova Lyudmila Viktorovna, Zemlyanskaya Olga Olegovna

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 № 1(7) / 2013

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.