УДК 349:681
DOI: 10.17223/22253513/23/15

**С.М. Трошина, А.В. Павловская**

# ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

*Высокие темпы информатизации современных технологий повышают риски уязвимостей в системах информационной безопасности организаций и используются нарушителями для несанкционированного получения персональных данных и интеллектуальной собственности. Для повышения защищенности информации предложена система комплексных мер организационно-правового характера. Внесены законодательные предложения по совершенствованию статей Уголовного и Уголовно-процессуального кодексов и приказа МВД России. Также внесены предложения по утверждению процедуры использования полицейскими органами ИТИСНТ в досудебном уголовном процессе. Кроме того, даны рекомендации в области издания локальных нормативных актов по защите персональных данных. Рекомендовано разработать процедуру предоставления всем пользователям бесплатной электронной подписи.*
Ключевые слова: *персональные данные, клевета, уязвимости, внутренний нарушитель, организованная преступная группа.*

В общественной жизни необходимость предоставления персональных данных является условием реализации прав и свобод граждан: права на труд и образование, права собственности, права передвижения и проч. При подписании договоров с банками, страховыми компаниями, поставщиками лицо дает согласие на передачу собственных персональных данных третьим лицам. При заполнении регистрационных форм на сайтах службы занятости или при поступлении на работу в организацию претендент на должность обязан заполнить все поля формы бланка организации.

Понятие персональных данных закреплено в Федеральном законе от 07.07.2006 № 152-ФЗ «О персональных данных». Согласно ст. 3 закона № 152-ФЗ персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и т.д. [1. Ст. 3]. Таким образом, при помощи персональных данных возможно идентифицировать конкретное физическое лицо. Поэтому доступ к подобной информации ограничен законом по кругу лиц.

В связи с широким использованием персональных данных встает вопрос о реальном состоянии защищенности правового поля личности. По статистическим данным американского центра исследования Pew Research Center эксперты прогнозируют следующие приватности Интернета: большинство американцев (64%) сами лично сталкивались с серьезной проблемой утечки информации, в связи с этим нарастает общественное недоверие в области защиты персональных данных в ключевых сайтах институтов государственной

власти, особенно в сайтах федерального правительства и социальных медиасайтов [2]. При этом формулируются выводы, что личная жизнь становится публичной по умолчанию, так как в современном мире невозможно существовать, не открывая персональную информацию государству и корпорациям; немногие физические лица или сообщества обладают ресурсами для противодействия «электронной слежке»; процесс обеспечения безопасности персональных данных осложняется из-за наличия Интернета; углубляются противоречия различных конфессий по поводу реализации гражданских свобод в интернет-пространстве.

Статья 5 закона «О персональных данных» устанавливает следующие принципы обработки персональных данных. Во-первых, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Во-вторых, не допускается обработка персональных данных, не отвечающих целям их обработки. И, наконец, содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, т.е. обрабатываемые персональные данные не должны быть избыточными [1. Ст. 5].

Исходя из вышеперечисленного, включение в гражданско-правовой или трудовой договор требования обязательности предоставления избыточных персональных данных является прямым нарушением закона. Однако законодательством не определен необходимый минимум персональных данных и, следовательно, не установлена юридическая ответственность [3]. Поэтому на практике имеет место злоупотребление операторами правом сбора и обработки персональных данных.

Также в п. 7 ст. 5 установлено, что персональные данные должны храниться не дольше времени, требующегося для достижения целей их обработки. Обрабатываемые персональные данные должны быть уничтожены либо обезличены после достижения целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом [1. Ст. 5]. Организации руководствуются собственными локальными нормативными актами. Например, ООО «ВЕКА Рус» в своем регламенте установило срок хранения персональных данных клиентов – 75 лет [4]. Возникают законные сомнения в необходимости хранения персональных данных клиентов в течение всей их жизни. Следует законодательно ограничить срок хранения персональных данных и ввести обязательную процедуру их уничтожения.

Обработка персональных данных осуществляется с письменного согласия субъекта на обработку его персональных данных в соответствии со ст. 6 закона «О персональных данных» [1. Ст. 6]. Однако субъекту персональных данных в организации не предоставляются гарантии защиты его персональных данных.

В нормативном акте «Требованиях к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119) говорится о том, что безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы или лицо, осуществляющее обработку персональных данных по поручению оператора [5]. При этом под

информационной системой персональных данных понимается совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1]. Оператором может являться государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных [1].

Защита персональных данных законодательством возложена на оператора.

Механизм защиты оператором персональных данных субъектов позволяет определить три типа актуальных угроз [5. П. 6]:

– угрозы 1-го типа – актуальны при наличии недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

– угрозы 2-го типа – актуальны при наличии недокументированных (недекларированных) возможностей в прикладном обеспечении, используемом в информационной системе;

– угрозы 3-го типа – актуальны при отсутствии недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Информационные системы классифицируются по типу персональных данных и по типу субъектов персональных данных:

– обрабатывающие специальные категории персональных данных;

– обрабатывающие биометрические персональные данные;

– обрабатывающие общедоступные персональные данные;

– обрабатывающие иные категории персональных данных;

– обрабатывающие персональные данные сотрудников оператора.

Уровень защищенности определяется с учетом выбранного типа угроз, категории персональных данных и количества субъектов. Настоящие требования устанавливают четыре уровня защищенности персональных данных [5. Пп. 9–12], которыми устанавливаются условия обеспечения информационной безопасности каждого из уровней.

Таким образом, из вышеизложенного следует, что работодатель обязан ознакомить работника с уровнем защиты его персональных данных и условиями обеспечения информационной безопасности его персональных данных. Для этой цели на локальном уровне необходимо разработать нормативный акт информационной безопасности персональных данных.

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» устанавливается регулярный контроль за выполнением требований безопасности не реже 1 раза в 3 года, который организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации [5. П. 17].

Управлением по защите прав субъектов персональных данных подведены итоги осуществления государственного контроля (надзора) за период один-

надцать месяцев 2015 г. Уполномоченным органом по защите прав субъектов персональных данных в отношении операторов было проведено 805 проверок, из них 58 внеплановых (т.е. по жалобам). Было выявлено 1 188 нарушений в области защиты персональных данных по результатам 1 738 мероприятий систематического наблюдения, выдано 613 предписаний об устранении нарушений закона № 152-ФЗ, наложено штрафов на сумму более 8,2 млн руб. [18].

Можно сделать вывод, что деятельность по проверке выполнения законодательства ведется. Однако наблюдается высокий процент нарушений, что свидетельствует о недостаточном внимании операторов к состоянию защищенности информационных систем, обрабатывающих персональные данные внутренних и внешних субъектов.

Большое число правонарушений в области персональных данных имеет место в сети Интернет. Данный вид правоотношений подпадает под действие закона о персональных данных, поскольку закон № 152-ФЗ регулирует правоотношения, возникающие при обработке персональных данных, с помощью средств автоматизации [1. Ст. 3].

Для обработки информации необходимо согласие субъекта на обработку его персональных данных, при этом согласие должно быть дано в любой форме, позволяющей подтвердить факт его получения [1. Ст. 9]. Такой формой может быть согласие, представленное на бумажном носителе в письменной форме, собственноручно подписанное субъектом персональных данных либо представленное в виде электронного документа, подписанного электронной подписью [6. Ст. 6]. Пользователи Интернета в действительности не имеют электронной подписи, что осложняет защиту их персональных данных.

В случае несанкционированного использования злоумышленником персональных данных третьего лица, не подозревающего об использовании его персональных данных, ответственность будет нести оператор.

На большинстве сайтов в личном профиле сотрудника организации предлагается загрузить фотографию сотрудника. В п. 1 ст. 3 закона «О персональных данных» не указано, что фотография является объектом, на основании которого можно идентифицировать человека, хотя перечень не исчерпывающий. Однако использование фотографии без согласия субъекта не допускается в соответствии со ст. 152.1 Гражданского кодекса Российской Федерации [7. Ст. 152.1].

Изображение сотрудника, размещеное на корпоративном сайте организации, является общедоступной информацией. Однако изображение гражданина защищается законом, и использование данного изображения возможно только с письменного согласия лица, изображенного на фотографии. Очевидно, что изображение гражданина, размещенное на корпоративном сайте, не может быть использовано с целью опорочить его доброе имя и деловую репутацию. Как, например, в фильме «Розыгрыш» злоумышленник, имея профессиональную квалификацию по работе с электронными изображениями, используя «фотошоп» или другое программное обеспечение, подставляет изображение сотрудника органиации в рекламу порносайтов, экстремистских и террористических организаций, а

также для создания посредством пластической хирургии двойников и поддельных документов. В фильме справедливость восторжествовала.

Однако в правоприменительной практике имеются в настоящее время значительные сложности организационно-технического, кадрово-профессионального и правового характера.

Во-первых, отсутствуют программное обеспечение, организационно-техническая база и профессиональные кадры, имеющие компетенцию «информационная безопасность в телекоммуникационных системах». Соответствующим оборудованием для сбора доказательств в совершении компьютерных преступлений оснащен только один отдел «К» в структуре Главного управления МВД по Свердловской области. При этом возбуждение уголовного дела производится по территориальному принципу, т.е. отделением полиции того района города, где было совершено преступление. В территориальных районных отделениях полиции отсутствуют организационные средства и кадровый состав полицейских, специализированный на информационной безопасности телекоммуникационных систем. Кроме того, как правило, не представляется возможным достоверно определить территорию, на которой было совершено компьютерное преступление, так как злоумышленник может пользоваться удаленным доступом.

В отношении заявления о возбуждении уголовного дела, поступившего в отдел «К» ГУ МВД по Свердловской области, выносится постановление о передаче его по территориальному признаку в отделение полиции соответствующего района города, где выносится постановление об отказе в возбуждении уголовного дела в связи с отсутствием события (п. 1 ч. 1 ст. 24 УПК РФ) или отсутствия в деяниях состава преступления (п. 2 ч. 1 ст. 24 УПК РФ) [8. Ст. 24]. Очевидно, отделы «К», оснащенные оргтехникой и профессионалами в области информационной безопасности в телекоммуникационных системах, должны быть в каждом отделении полиции. Требованиям всех перемен в информационном обществе должен соответствовать высоко информатизированный уголовный процесс досудебного производства.

Во-вторых, имеется сложность с определением предмета и объекта преступления, его квалификации и сбора доказательств, подтверждающих сам факт совершения преступления – клевета и виновность лиц, его совершивших. Потерпевшее от клеветы в Интернете лицо, как правило, не имеет в собственом ведении клеветнической информации: порноизображение с вставленной в него головой потерпевшего, поскольку злоумышленники распространяют клеветнические измышления третьим лицам – сослуживцам и знакомым потерпевшего [9. Ст. 128.1]. Последние из опасения предъявления им обвинения в распространении клеветнических измышлений уклоняются от сотрудничества с правоохранительными органами. Кроме того, злоумышленники распространяют вместе с клеветой в электронной форме легенду о том, что якобы потерпевший собственноручно выкладывает приватные сведения в социальную сеть.

Клевета – уголовный состав, относящийся к делам частного обвинения, т.е. возбуждается по заявлению потерпевшего. Потерпевший должен

подтвердить факт распространения сведений, т.е. передачу клеветнических измышлений третьим лицам. Существует множество сайтов и операторов, разнообразные способы передачи информации с мобильных и стационарных устройств. Злоумышленники часто меняют операторов и сим-карты. У потерпевшего, в отличие от спецслужб, отсутствуют специальные устройства, улавливающие потоки исходящей информации. При таких обстоятельствах очевидно, что в эпоху стремительной информатизации необходимо состав преступления, предусмотренный ст. 128.1 УК РФ, перевести в категорию уголовных дел частно-публичного обвинения.

В-третьих, для того чтобы сотрудники правоохранительных органов могли получить доказательства о распространении при помощи Интернета сфабрикованной злоумышленниками информации, составляющей квалифицированный состав клеветы, необходимо преодолеть ограничения ст. 13 Уголовного процессуального кодекса Российской Федерации на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений. Для достижения цели следователю или дознавателю надо получить судебное решение, удовлетворяющее ходатайство (ч. 1 ст. 13 УПК РФ) [8. Ст. 13], поскольку контроль и запись телефонных и иных переговоров, получение информации о соединениях между абонентами и (или) абонентскими устройствами могут производиться только на основании судебного решения (ч. 2 ст. 13 УПК РФ) [8. Ст. 13]. Для внесения судом в мотивировочную часть постановления об удовлетворении ходатайства на разрешение получать информацию о соединениях между абонентами и (или) абонентскими устройствами (п. 12 ч. 2 ст. 29 УПК РФ) [8. Ст. 29] следователю или дознавателю необходимо представить допустимые доказательства причастности подозреваемых лиц в совершении преступлений, которые, как правило, отсутствуют в материалах уголовного дела в связи с ограничением доступа к сведениям в соответствии с ч. 1 ст. 13 УПК РФ.

В соответствии с ч. 1 ст. 165 УПК РФ в случаях, предусмотренных п. 12 ч. 2 ст. 29 УПК РФ, следователь с согласия руководителя следственного органа, а дознаватель с согласия прокурора возбуждают перед судом ходатайство о производстве следственного действия, о чем выносится постановление. Рассмотрев указанное ходатайство, судья выносит постановление о разрешении производства следственного действия или об отказе в его производстве с указанием мотивов отказа (ч. 4 ст. 165 УПК РФ) [8. Ст. 165]. Громоздкость процессуальных действий очевидна и вряд ли целесообразна.

В исключительных случаях, предусмотренных ч. 5 ст. 165 УК РФ, когда проведение следственных действий не терпит отлагательства, указанные следственные действия могут быть произведены на основании постановления следователя или дознавателя без получения судебного решения. В этом случае следователь или дознаватель не позднее 3 суток с момента начала производства следственного действия уведомляет судью и прокурора о производстве следственного действия. К уведомлению прилагаются копии постановления о производстве следственного действия и протокола следственного действия для проверки законности решения о его

производстве. Получив указанное уведомление, судья в срок, предусмотренный ч. 2 ст. 165 УК РФ, проверяет законность произведенного следственного действия и выносит постановление о его законности или незаконности [8. Ст. 165]. Однако данное правило не распространяется на случаи получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Очевидно, данный законодательный пробел необходимо восполнить, расширив процессуальные права следователя и дознавателя, поскольку основной задачей МВД России является обеспечение защиты жизни, здоровья, прав и свобод граждан Российской Федерации, иностранных граждан, лиц без гражданства, противодействие преступности, охрана общественного порядка и собственности, обеспечение общественной безопасности, предоставление государственных услуг в сфере внутренних дел (пп. 4 п. 2 Положения о Министерстве внутренних дел Российской Федерации) [10. П. 2]. При этом отсутствуют опасения, сравнимые с публикациями в США, освещающие в печати факты допущения обращения, связанного с насилием полицейских сотрудников, в которых формируется общественное мнение о нелегитимности правоохранительных органов [11. P. 38–40]. Печатные издания США свидетельствуют о том, что напряженность отношений между полицией и обществом возрастает [12].

Проблема в России состоит в отсутствии достаточной полноты полномочий у полицейских для раскрытия и пресечения преступлений (пп. 12, 17, п. 11 Положения) [10], что отражается в статистических данных: возрастает количество отказных материалов. Права потерпевшей стороны не восстанавливаются в уголовном процессе, в связи с этим основная задача органов МВД – обеспечение в пределах своих полномочий защиты прав и свобод человека и гражданина (пп. 4 п. 2 Положения о Министерстве внутренних дел Российской Федерации) – остается не выполненной [10. П. 2]. Очевидно, нормоположения, перечисленные в Приложении № 1 к Приказу МВД России от 17.01.2006 № 19 «Инструкция о деятельности органов внутренних дел по предупреждению преступлений», должны быть изменены в строну расширения полномочий полицейских органов в процессе осуществления профилактической деятельности. Сотрудникам полиции в информационном обществе должно быть предоставлено право широкого использования всех инноваций информатизации для защиты правопорядка с целью обеспечения информационого преимущества над нарушителями. В настоящее время уделяется большое внимание развитию информационо-технологической инфраструктуры сферы науки и технологий в России и за рубежом [13]. В связи с подготовкой новой редакции приказа МВД о профилактике преступлений актуально внесение в его содержание нормоположения, направленного на практическое решение задачи по развитию доступа полицейских органов к ИТИСНТ, что в значительной мере расширит поле правоохранительной деятельности и разнообразит перечень превентивных мер. В противном случае меры по предупреждению преступлений останутся декларацией. Бездействие правозащитников может привести к нелегитимности полицейских органов и к серьезным общественным беспорядкам.

Как правило, злоумышленником, несанкционированно использующим персональные данные, является внутренний нарушитель, т.е. лицо, состоящее с организацией в трудовых отношениях, имеющее доступ к персональным данным других работников. Внутри организации режим информационной безопасности зачастую имеет множество уязвимостей, которые использует внутренний нарушитель для достижения преступной цели. Мотивы могут быть различные: от личной неприязни до организованно спланированных действий по устранению сотрудников, профессиональная компетенция которых может быть помехой для реализации преступных планов хищения интеллектуальной собственности работников и организации.

В настоящее время такого рода внутренние диверсии имеют широкое распространение. Действуют организованные преступные группировки, специализирующиеся на промышленном шпионаже. Состоящий в трудовых правоотношениях внутренний нарушитель оказывает помощь по трудоустройству соучастнику, которому впоследствии передаются ключевые функции организационно-управленческого процесса, сосредотачивая в области ведения ОПГ все рычаги планово-финансовой и хозяйственной деятельности (ст. 210 УК РФ) [9. Ст. 210].

Как правило, продвигается по служебной лестнице член ОПГ – молодая привлекательная женщина, поскольку само присутствие красавицы является отвлекающим маневром. Члены преступной группы заведомо вводят в управленческий процесс и хозяйственную деятельность ошибочные решения, дезинформируют личный состав организации и создают для себя информационное преимущество в обладании ключевой информацией. Последствия таких действий имеют результатом дезорганизацию производственного процесса, несанкционированное получение и передачу внешним нарушителям интеллектуальной собственности и устранение сотрудников, противодействующих реализации преступных планов ОПГ.

Вопрос о соразмерности тяжести совершенного преступления и мере наказания, предусмотренного за него, сохраняет свою актуальность как для России, так и для США [14. P. 431, 450]. Позиция, осуждающая длительность сроков тюремного заключения, ошибочна. Продолжительное тюремное заключение в одиночной камере лиц, осужденных за тяжкие и особо тяжкие преступления, имеет правовое, социальное и психологическое обоснование, поскольку наказание должно быть соразмерно тяжести совершенного лицом преступления. Наказание, предусмотренное ст. 128.1 УК РФ, безусловно, является необоснованно мягким. Клевета – это лишь результат, как правило, продолжаемого или длящегося преступления в отношении потерпевшего, сопряженного с рядом других преступлений, совершенных против общества и личности. Последствия распространения клеветнических измышлений для потерпевшего трагичны: ухудшение состояния здоровья, потеря работы, утрата родственных и социальных связей, опороченность доброго имени и деловой репутации. Безусловно, ст. 128.1 УК РФ должна инкриминироваться злоумышленникам по совокупности со ст. 117 УК РФ (истязание). В некоторых случаях клевета перерастает в смежный состав преступления против личности, предусмотренный ст. 110 УК РФ – доведение до

самоубийства. Однако доказать наличие данного состава сложно вследствие причинения смерти.

Ужесточение наказания в виде лишения свободы на длительные сроки не противоречит практике применения уголовного наказания зарубежных стран. Россия не лидирует по статистическим данным, отражающим численность лиц, содержащихся под стражей и в местах лишения свободы. В США 716 человек из 100 тыс. жителей содержатся под стражей, эта доля в 5 раз превышает статистические показатели большинства стран мира [15].

Недобросовестное использование чужих персональных данных является основным видом уязвимости организации. Человеческий фактор служит основной угрозой информационной безопасности организации [16]. Субъекты персональных данных, пользователи сайта, размещая в социальных сетях избыток личной информации, неосознанно предоставляют свободный доступ к собственным персональным данным внешним нарушителям. Злоумышленники, воспользовавшись информацией с сервиса, могут получить интересующие их данные о сотрудниках организации и впоследствии использовать их для достижения преступных целей.

Таким образом, основной проблемой информационной безопасности персональных данных является субъективный фактор: добропорядочность операторов, их заинтересованность в выполнении нормативных требований, с одной стороны, и с другой – внимательность самих обладателей персональных данных. Напоминание пользователям о необходимости соблюдения правил информационной безопасности должно быть основным правилом работы каждого оператора и работодателя. Пренебрежение к принципам безопасности может привести к значительным экономическим потерям [17].

Обучение пользователей сайтов процедурам ограничения предоставления информации, повышая уровень их грамотности в вопросах освоения возможностей информационных технологий, необходимо начинать со школьного возраста [19]. В литературе предложена заслуживающая внимания система мер обеспечения безопасности персональных данных при работе в Интернете [20].

Одной из мер защиты собственных персональных данных является электронная подпись. Процедура получения электронной подписи для подтверждения своей личности в сети Интернет доступна, однако не каждый пользователь имеет возможность внести плату за ее предоставление. Все вышеизложенное дает основание полагать, что необходимо разработать систему безвозмездного предоставления всем пользователям доступной электронной подписи, гарантирующей ее целостность и подлинность.

В целях совершенствования действующего законодательства в области защиты персональных данных на основании проведенных исследований вносим следующие предложения:

Статью 128.1 Уголовного кодекса Российской Федерации перевести в категорию уголовных составов частно-публичного обвинения с ужесточением санкции.

Предусмотреть возможность наложения судом наказания за квалифицированный состав клеветы в виде тюремного заключения на длительный срок.

Расширить полномочия следователя и дознавателя в ч. 5 ст. 165 Уголовно-процессуального кодекса Российской Федерации, предусмотрев возможность проведения неотложных следственных действий по контролю и записи телефонных и иных переговоров и получению информации о соединениях между абонентами и (или) абонентскими устройствами с последующим уведомлением в течение 3 суток судьи и прокурора.

Разработать систему безвозмездного предоставления каждому пользователю доступной электронной подписи, гарантирующей ее целостность и подлинность.

Создать условия для организации высоко информатизированного досудебного производства уголовного процесса.

Создать отделы «К», оснащенные оргтехникой и профессионалами в области информационной безопасности телекоммуникационных систем, в каждом районном отделении полиции муниципального образования.

Законодательно ограничить срок хранения персональных данных в организации и ввести обязательную процедуру их уничтожения после истечения срока хранения.

Обязать работодателей вести процедуру ознакомления сотрудников с уровнем защиты и условиями обеспечения информационной безопасности персональных данных. Для этой цели на локальном уровне необходимо разработать нормативный акт, предусматривающий методы и способы обеспечения информационной безопасности персональных данных на локальном уровне.

Предоставить полицейским право широкого использования всех инноваций информатизации для защиты правопорядка с целью обеспечения информационного преимущества над нарушителями.

В связи с подготовкой новой редакции приказа МВД о профилактике преступлений ввести процедуру, обеспечивающую доступ полицейских органов к ИТИСНТ.

Расширить объекты правоохранительной деятельности и перечень превентивных мер противодействия преступности в приказе МВД России о профилактической деятельности органов полиции.

Таким образом, совершенствование системы организационно-нормативных мер повышения информационной безопасности личности, общества и государства с использованием инноваций информатизации автоматизированных систем станет гарантом профилактики компьютерных преступлений и соблюдения прав человека и гражданина в Российской Федерации.

***Литература***

1. *О персональных* данных: федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 03.07.2016) [Электронный ресурс]. URL: http:// http://www.consultant.ru/ cons/ cgi/online.cgi?req=doc;base=LAW;n=137356#02.

2. *Americans* and Cybersecurity: Pew Research Center, january 26, 2017 [Электронный ресурс]. URL: www.pewresearch.org

3. *Шередин Р.В*. Защита персональных данных: новые требования: интернет-интервью 10.01.2012 [Электронный ресурс]. URL: http://oblteleset.ru/2012/10-01-2012-zashhita-personalnyx-dannyx-novye-trebovaniya/

4. *Регламент* о защите персональных данных клиентов ООО «ВЕКА Рус»: локальный нормативный акт [Электронный ресурс]. URL: http://www.veka.ru/reglament_ o_zashhite_personalnyh_dannyh.html

5. *Об утверждении* требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Российской Федерации от 01.11.2012 № 1119 [Электронный ресурс]. URL: http://http://www.consultant.ru/ cons/ cgi/online.cgi?req=doc;base=LAW;n=137356#0

6. *Об электронной* подписи: федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) [Электронный ресурс.]. URL: http:// http://www.consultant.ru/cons/cgi/ online.cgi?req=doc; base= LAW; n=137356#0

7. *Гражданский* кодекс Российской Федерации. Часть Первая. Федеральный закон от 30.11.1994 № 51 (ред. от 28.12.2016) [Электронный ресурс]. URL: http:// http://www. consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137356#0

8. *Уголовно*-процессуальный кодекс Российской Федерации. Федеральный закон от 18.12.2001 № 174-ФЗ (в ред. от 19.12.2016) [Электронный ресурс]. URL: http://www. consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137356#0

9. *Уголовный* кодекс Российской Федерации. Федеральный закон от 13.06.1996 № 63 (в ред. 19.12.2016) [Электронный ресурс]. URL: http://www.consultant.ru/cons/ cgi/online.cgi?req= doc;base=LAW;n=137356#0

10. *Об утверждении* Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации: указ Президента Российской Федерации от 21.12.2016 № 699 [Электронный ресурс]. URL: http://www.consultant.ru/cons/ cgi/ online. cgi?req=doc;base=LAW;n=137356#0

11. *Westley W.* Violence and the Police // American Journal of Sociology. 1953. Vol. 59. P. 34–41.

12. *Weitzer R.* Incidents of police misconduct and public opinion // Journal of Criminal Justice. 2002. Vol. 30, iss. 5. P. 397–408.

13. *Ижванов Ю.Л., Куракин Д.В.* О концепции развития информационно-технологической инфраструктуры сферы науки и технологии // Информатизация образования и науки. 2016. № 2(30). С. 92–105.

14. *Conley A.* Torture in US Jails and Prisons: An Analysis of Solitary Confinement Under International Law // Vienna Journal on International Constitutional Law. 2013. Vol. 7, № 4. P. 415–453.

15. *Walmsley R.* World Prison Population List [Electronic resource] / R. Walmsley.10th ed. Mode of access: https://www. prisonstudies.org/sites/prisonstudies.org/ files/resources/ downloads/ wppl_10.pdf.

16. *Трошина С.М., Рязанова Т.П.* Человеческий фактор как угроза информационной безопасности // Вестн. Урал. финансово-юридического ин-та. 2016. № 2(4). С. 93–97.

17. *Петров Ю.И.* Защищенность как одна из наиболее актуальных характеристик современного программного обеспечения // Информатизация образования и науки. 2016. № 2(30). С. 106–116.

18. *Контеримов Ю.Е.* Особенности государственного контроля за деятельностью операторов, осуществляющих обработку персональных данных. Применение риск-ориентированного подхода и обеспечение взаимодействия регулятора и отрасли: доклад // Междунар. конф. защиты персональных данных. М.: Ренесанс Москва Монарх Центр, 08.11.2016 [Электронный ресурс]. URL: http://zpd-forum.com/programm.html

19. *Солдатова Г.В.* Российские школьники: приватность и безопасность в Сети: доклад // Междунар. конф. защиты персональных данных. М.: Ренесанс Москва Монарх Центр, 08.11.2016 [Электронный ресурс]. URL: http:://zpd-forum.com/

20. *Емельянников М.* Как защищать персональные данные в интернете// infosec.ru [Электронный ресурс.]. URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/kak-zaschischat-personalnye-dannye-v-internete

*Troshina Svetlana M., Pavlovskaya Ann V.* Department radio-electronics and communication IRIT-RTF Ural Federal University First President of Russia B.N. Yeltsin (Yekaterinburg, Russian Federation)

**PROBLEMS OF IMPROVEMENT OF PERSONAL DATA PROTECTION MEASURES**

Key words: personal data, slander, vulnerabilities, internal violator, organized criminal group.

High rates of informatization of modern technologies increase the risks of vulnerabilities in information security systems of organizations and are used by violators for unauthorized receiving of personal data and intellectual property. This determines the urgency of the present research.

The concept of personal data is enshrined in the Federal law 152-FZ "On personal data" 07.07.2006. According to Article 3 of the law personal data is any information relating to the person (the subject of personal data) including his surname, name, middle name; date and place of birth; address; marital, social and property status; education; profession; income etc. Thus, it is possible to identify a concrete person by means of personal data. Therefore, according to law the access to such information is limited by the scope of persons. Due to the wide use of personal data, there is a question of protection of the legal framework of a person. Article 5 of the law "On personal data" establishes the following principles of processing personal data. Firstly, processing of personal data has to be limited by achieving concrete, predetermined and lawful purposes. Secondly, processing of personal data, which do not serve the purpose of their processing, is not allowed. Moreover, the content and volume of the personal data under procession have to correspond to the stated purposes of processing, that is the processed personal data should not be superfluous.

Subjective circumstances are the main reason for the leakage of key information. The internal violator uses a human factor for establishing the organized criminal group and reports information to the external violator. To increase the protection of information, the system of complex organizational and legal measures is offered. Legislative suggestions for improving the articles of criminal and criminal procedure codes and the order of the RF Ministry of Internal Affairs have been made. Suggestions on the approval of the procedure for application of ITISNT by police in the course of pre-trial criminal proceedings have been made. Moreover, the authors make recommendations in the field of publication of local regulations on the protection of personal data. It is recommended to develop the procedure for providing the free digital signature to all users.

***References***

1. Russian Federation. (2006) *O personal'nykh dannykh: federal'nyy zakon ot 27.07.2006 № 152-FZ (red. ot 03.07.2016)* [On personal data: Federal Law No. 152-FZ of July 27, 2006 (as amended on July 3, 2016)]. [Online] Available from: http:// http://www.consultant.ru/ cons/ cgi/online.cgi?req= doc;base=LAW;n=137356#02.

2. Olmstead, K. & Smith, A. (2017) *Americans and Cybersecurity*. [Online] Available from: www.pewresearch.org.

3. Sheredin, R.V. (2012) *Zashchita personal'nykh dannykh: novye trebovaniya: internet-interv'yu 10.01.2012* [Protection of personal data: new requirements: Online interview January 10, 2012]. [Online] Available from: http://oblteleset.ru/2012/10-01-2012-zashhita-personalnyx-dannyx-novye-trebovaniya/.

4. LLC Veka Rus. (n.d.) *Reglament o zashchite personal'nykh dannykh klientov OOO "VEKA Rus": lokal'nyy normativnyy akt* [Regulation on the protection of personal data of customers LLC VEKA Rus: a local regulatory act]. [Online] Available from: http://www.veka.ru/reglament_ o_zashhite_personalnyh_dannyh.html.

5. Russian Federation. (2012) *Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: postanovlenie Pravitel'stva Rossiyskoy Federatsii ot 01.11.2012 № 1119* [On the approval of the requirements for the protection of personal data when processing them in personal information systems: Resolution of the Government of the Russian Federation No. 1119 of January 11, 2012]. [Online] Available from: http://http://www.consultant.ru/ cons/ cgi/online.cgi?req=doc;base=LAW;n=137356#0.

6. Russian Federation. (2011) *Ob elektronnoy podpisi: federal'nyy zakon ot 06.04.2011 N 63-FZ (red. ot 23.06.2016)* [About the electronic signature: Federal law N 63-FZ of April 6, 2011 (as of June 23, 2016)]. [Online] Available from: http:// http://www.consultant.ru/cons/cgi/ online.cgi?req=doc; base= LAW; n=137356#0.

7. Russian Federation. (1994) *Grazhdanskiy kodeks Rossiyskoy Federatsii. Chast' Pervaya. Federal'nyy zakon ot 30.11.1994 № 51 (red. ot 28.12.2016)* [Civil Code of the Russian Federation. Part one. Federal Law No. 51 of November 30, 1994 (as amended on December 28, 2016)]. [Online] Available from: http:// http://www. consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137356#0.

8. Russian Federation. (2001) *Ugolovno-protsessual'nyy kodeks Rossiyskoy Federatsii. Federal'nyy zakon ot 18.12.2001 № 174-FZ (v red. ot 19.12.2016)* [The Criminal Procedure Code of the Russian Federation. Federal Law No. 174-FZ of December 18, 2001 (as amended on December 19, 2016)]. [Online] Available from: http://www. consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137356#0.

9. Russian Federation. (1996) *Ugolovnyy kodeks Rossiyskoy Federatsii. Federal'nyy zakon ot 13.06.1996 № 63 (v red. 19.12.2016)* [The Criminal Code of the Russian Federation. Federal Law No. 63 of June 13, 1996 (as amended on December 19, 2016)]. [Online] Available from: http://www.consultant.ru/cons/ cgi/online.cgi?req= doc;base=LAW;n=137356#0.

10. Russian Federation. (2016) *Ob utverzhdenii Polozheniya o Ministerstve vnutrennikh del Rossiyskoy Federatsii i Tipovogo polozheniya o territorial'nom organe Ministerstva vnutrennikh del Rossiyskoy Federatsii po sub"ektu Rossiyskoy Federatsii: ukaz Prezidenta Rossiyskoy Federatsii ot 21.12.2016 № 699* [On approval of the Regulations on the Ministry of Internal Affairs of the Russian Federation and the Model Provisions on the territorial body of the Ministry of Internal Affairs of the Russian Federation for the subject of the Russian Federation: Presidential Decree No. 699 of December 21, 2016]. [Online] Available from: http://www.consultant.ru/cons/ cgi/ online. cgi?req=doc;base=LAW;n=137356#0.

11. Westley, W. (1953) Violence and the Police. *American Journal of Sociology*. 59. pp. 34–41.

12. Weitzer, R. (2002) Incidents of police misconduct and public opinion. *Journal of Criminal Justice*. 30(5). pp. 397–408. DOI: 10.1016/S0047-2352(02)00150-2

13. Izhvanov, Yu.L. & Kurakin, D.V. (2016) O kontseptsii razvitiya informatsionno-tekhnologicheskoy infrastruktury sfery nauki i tekhnologii [On the concept of development of information technology infrastructure of science and technology]. *Informatizatsiya obrazovaniya i nauki*. 2(30). pp. 92–105.

14. Conley, A. (2013) Torture in US Jails and Prisons: An Analysis of Solitary Confinement Under International Law. *Vienna Journal on International Constitutional Law*. 7(4). pp. 415–453. DOI: 10.1515/icl-2013-0402

15. Walmsley, R. (n.d.) *World Prison Population List*. 10th ed. [Online] Available from: https://www. prisonstudies.org/sites/prisonstudies.org/ files/resources/ downloads/ wppl_10.pdf.

16. Troshina, S.M. & Ryazanova, T.P. (2016) Chelovecheskiy faktor kak ugroza informatsionnoy bezopasnosti [The human factor as a threat to information security]. *Vestnik Uralskogo finansovo-yuridicheskogo instituta*. 2(4). pp. 93–97.

17. Petrov, Yu.I. (2016) Zashchishchennost' kak odna iz naibolee aktual'nykh kharakteristik sovremennogo programmnogo obespecheniya [Security as one of the most actual characteristics of modern software]. *Informatizatsiya obrazovaniya i nauki*. 2(30). pp. 106–116.

18. Konterimov, Yu.E. (2016) [The state control over the activities of operators that process personal data. Application of the risk-oriented approach and ensuring the interaction of the regulator and the industry]. *International Conference on Protection of Personal Data*. Moscow: Renesans Moskva Monarkh Tsentr. [Online] Available from: http://zpd-forum.com/programm.html. (In Russian).

19. Soldatova, G.V. (2016) Rossiyskie shkol'niki: privatnost' i bezopasnost' v Seti [Russian schoolchildren: privacy and security on the Net]. *International Conference on Protection of Personal Data*. [Online] Available from: http:://zpd-forum.com/.

20. Emelyannikov, M. (n.d.) *Kak zashchishchat' personal'nye dannye v internete* [How to protect personal data on the Internet]. [Online] Available from: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/kak-zaschischat-personalnye-dannye-v-internete.