Вопросы обеспечения безопасности персональных данных в информационных системах МВД России

Шогенов Тимур Коммунарович,
начальник кафедры специально-технической подготовки Северо-Кавказского института повышения квалификации сотрудников МВД России (филиал) Краснодарского университета МВД России, к.ф.м.н., доцент, полковник полиции

Неотъемлемым условием информационного обеспечения деятельности подразделений, служб, организаций и учреждений Министерства внутренних дел Российской Федерации[1] при реализации их функций является активное использование современных информационных технологий, программных и аппаратных средств, а также информационных систем на их основе. Значительное количество задач, в том числе принятие юридически значимых решений, подразумевает использование информационных систем, в которых осуществляется сбор, систематизация, уточнение, накопление, хранение и передача персональных данных[2] различных категорий и объемов. Понимание важности и ценности информации о человеке, необходимость обеспечения соблюдения конституционных прав и законных интересов граждан Российской Федерации делают выполнение требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»[3] подразделениями МВД России одним из приоритетных направлений деятельности при реализации Министерством внутренних дел Российской Федерации государственной правоохранительной функции.

Актуальность обеспечения безопасности персональных данных в информационных системах МВД России, несмотря на значительный период времени, прошедший с момента принятия и вступления в действие Федерального закона «О персональных данных», не снижается, а, напротив, приобретает большую остроту. Это обусловлено, прежде всего, многообразием типов используемых информационных систем для обработки персональных данных[4] по их составу, структурному построению, категориям обрабатываемой информации, функциональному назначению. Ситуация осложняется тем, что большинство этих информационных систем введено в эксплуатацию до принятия Федерального закона «О персональных данных», и реализованные в них методы и способы защиты информации не отвечают требованиям безопасности объектов информатизации, сформулированным в нормативных документах Федеральной службы безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации и в государственных стандартах в области защиты информации. Кроме этого, в настоящее время в рамках реализации Концепции информатизации[5] Министерства внутренних дел Российской Федерации разрабатываются и внедряются новые информационные системы, внедрена и эксплуатируется единая информационно-телекоммуникационная сеть, позволяющая реализовать территориально распределенные информационные системы, в том числе предназначенные для обработки персональных данных различного уровня, архитектурного построения и функционального назначения.

Проведение работ по обеспечению безопасности персональных данных в информационных системах МВД России связано с необходимостью знания и понимания положений достаточно большого количества нормативных правовых актов, нормативных, руководящих и методических документов-регуляторов[6], государственных стандартов, разобраться в которых является непростой, требующей специальной подготовки в предметной области задачей.

Таким образом, концептуально[7] и методологически необходимо представлять себе, что обеспечение безопасности персональных данных в информационных системах МВД России — это не одномоментно решаемая задача, а непрерывный и наступательный процесс, требующий пристального внимания и активного участия со стороны руководителей подразделений МВД России, руководителей и должностных лиц, ответственных за эксплуатацию и эксплуатирующих ИСПДн, а также руководителей и специалистов подразделений по защите информации в подразделениях МВД России.

На сегодняшний день в Российской Федерации сформирована достаточно стройная многоуровневая система нор-

1 Далее — «подразделения МВД России»

2 Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

3 Далее — «Федеральный закон «О персональных данных»

4 Далее — «ИСПДн»

5 Приказ МВД России от 04.04.2009 года №280 «Об утверждении Концепции информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 года».

6 Регуляторами являются государственные органы, уполномоченные осуществлять контроль и надзор за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных». Регуляторами являются Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (Роскомнадзор), Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России).

7 Приказ МВД России от 14.03.2012 №169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года».

мативно-правовых, руководящих и методических документов, регламентирующих порядок осуществления организационных и технических мероприятий, направленных на обеспечение безопасности персональных данных. Условно эта система может быть представлена следующей схемой.

Федеральные законы в области защиты информации, персональных данных формулируют высокоуровневые требования, порядок реализации которых конкретизирован в Указах Президента Российской Федерации и Постановлениях Правительства Российской Федерации, а также в нормативно-методических документах регуляторов, в том числе и совместных. Эти документы формируют второй уровень и определяют последовательность выполнения организационных и технических мероприятий, основные этапы создания системы защиты персональных данных[8], формулируют требования, предъявляемые к ней, а также описывают механизм аудита эффективности реализованной СЗПДн. Третий уровень включает в себя ведомственные нормативные, в т.ч. концептуальные, документы в области обеспечения безопасности персональных данных в системе МВД России и методические рекомендации МВД России по порядку подготовки нормативной и распорядительной документации, разграничению полномочий и мерам ответственности субъектов при решении организационных и технических вопросов при создании системы защиты персональных данных в ИСПДн МВД России.

При организации работ по обеспечению безопасности персональных данных в информационных системах актуален вопрос по лицензированию такой деятельности. Это обусловлено тем, что в соответствии с Указом Президента Российской Федерации от 06.03.1997 №188 персональные данные относятся к сведениям конфиденциального характера. Следовательно, подразделение МВД России, осуществляющее деятельность в области технической защиты конфиденциальной информации, либо деятельность, связанную с использованием сертифицированных средств криптографической защиты конфиденциальной информации, должно получить соответствующие лицензии. Так, лицензирование деятельности в области технической защиты конфиденциальной информации осуществляется в соответствии с Положением, утвержденным Постановлением Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации». ФСТЭК России в своем Информационном сообщении[9] указывает, что если техническая защита конфиденциальной информации необходима для достижения целей деятельности юридического лица (в нашем случае, подразделения МВД России), предусмотренных в учредительных документах, а также, если это юридическое лицо (уполномоченное лицо) обеспечивает техническую защиту конфиденциальной информации при ее обработке в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» по поручению обладателя информации конфиденциального характера и (или) заказчика информационной системы, то получение лицензии ФСТЭК России является обязательным. ФСБ России на основании Постановления Правительства РФ от 16 апреля 2012 г. №313 требует от всех организаций, эксплуатирующих средства криптографической защиты информации[10], получать лицензии на техническое обслуживание СКЗИ.

Обеспечение безопасности персональных данных в информационных системах МВД России — процесс многоэтапный, предусматривающий проведение комплекса организационных и технических мероприятий, направленных на выполнение требований Федерального закона «О персональных данных». В ходе выполнения этих мероприятий или по их результатам разрабатываются локальные нормативные акты, технические и технологические документы на каждую ИСПДн, принятую либо принимаемую в эксплуатацию в подразделении МВД России. Также Федеральным законом «О персональных данных» и подзаконными актами установлен ряд норм и требований, которые могут иметь отношение не ко всем подразделениям МВД России, но которые должны исполняться теми из них, для кого это является одним из направлений деятельности, например обработка биометрических персональных данных, вопросы трансграничной передачи персональных данных. При наличии таких оснований требуется выработка специальных мер и издание организационных и распорядительных документов, регулирующих данные процессы.

В зависимости от направления и специфики деятельности подразделений МВД России, в них могут функционировать информационные системы персональных данных различного уровня и назначения, например кадрового, финансового, дактилоскопического, миграционного и т.д. учета. Федеральным законом от 07.02.2011 года №3-ФЗ «О полиции» (статья 17) установлено, что полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах. Однако следует иметь в виду, что положения Федерального закона «О персональных данных» в соответствии с п.4 части 2 статьи 1 не распространяются на информационные системы органов внутренних дел, в которых обрабатываются сведения, составляющие государственную тайну и подлежащие засекречиванию. Обеспечение безопасности информации в таких информационных системах регламентируется законодательством Российской Федерации о государственной тайне, нормативными, руководящими и методическими документами ФСБ России и ФСТЭК России по защите информации, составляющей государственную тайну. В системе МВД России проведение работ по технической защите информации регламентируется Временным наставлением, утвержденным приказом МВД России от 5 июля 2001 года.

В соответствии с Инструкцией[11] по защите персональных данных, содержащихся в автоматизированных информационных системах органов внутренних дел Российской Федерации, руководители подразделений МВД России, являющихся операторами персональных данных, организуют выполнение мероприятий по обеспечению безопасности персональных данных. Указанные мероприятия должны быть включены в соответствующие разделы плана работы подразделения МВД России.

Очевидно, что на первоначальном этапе работ по обеспечению безопасности персональных данных должны быть определены структурные подразделения подразделений МВД России, в которых эксплуатируются или планируется эксплуатация информационных систем персональных данных; помещения, в которых размещаются или будут размещаться указанные ИСПДн с указанием лиц, доступ которым в данные помещения разрешен; перечень ИСПДн и состав персональных данных, обрабатываемых в них, цели и условия обработки, сроки хранения персональных данных различных категорий; струк-

8 Далее — «СЗПДн»

9 Информационное сообщение ФСТЭК России от 30.05.2012 №240/22/2222 «По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации».

10 Далее — «СКЗИ»

11 Приказ МВД России от 06.07.2012 №678 «Об утверждении Инструкции по защите персональных данных, содержащихся в автоматизированных информационных системах органов внутренних дел Российской Федерации»

турные подразделения и должностные лица подразделения МВД России, ответственные за обеспечение безопасности персональных данных при их обработке и за разработку, проведение мероприятий, направленных на выполнение требований по защите информации; список должностных лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных обязанностей; перечень разрешенного к использованию в ИСПДн программного обеспечения. В результате выполнения мероприятий на этом этапе разрабатываются и утверждаются руководителем подразделения МВД России соответствующие организационно-распорядительные документы для каждой информационной системы персональных данных. Также на первоначальном этапе устанавливается необходимый уровень правоотношений между подразделением МВД России, являющимся оператором персональных данных, и субъектом персональных данных. При необходимости должно быть получено, в том числе и в письменной форме, согласие субъекта на обработку его персональных данных. В целях обеспечения максимальной юридической чистоты в вопросах соблюдения прав субъектов персональных данных и во избежание инцидентов, связанных с нарушением этих прав, порядок реагирования на запросы со стороны субъектов персональных данных, внесения изменений в персональные данные, а также условия прекращения обработки персональных данных должны быть также определены документально в соответствующих приказах, инструкциях и рекомендациях, определяющих степень участия должностных лиц подразделения МВД России в обработке персональных данных и характер их взаимодействия между собой.

Следующий этап выполнения работ — классификация каждой ИСПДн, эксплуатируемой в подразделении МВД России. ИСПДн, подлежащие защите, должны быть однозначно идентифицированы как совокупности конкретных технических средств, размещенных внутри конкретных контролируемых зон и предназначенных для обработки конкретных категорий персональных данных с конкретными целями. Для проведения классификации приказом руководителя подразделения МВД России создается комиссия, в состав которой входят должностные лица, ответственные за обработку персональных данных и за обеспечение их безопасности.

Эффективность работ по обеспечению безопасности персональных данных в информационных системах подразделений МВД России в значительной степени зависит от качества и полноты исходных данных, собранных по каждой ИСПДн, глубины их анализа и правильности их классификации. Именно от класса ИСПДн будет зависеть адекватность моделей угроз безопасности и нарушителя, а, следовательно, и создаваемой системы защиты персональных данных.

Для того чтобы максимально полно собрать сведения об информационной системе, необходимо ответить на ряд вопросов, а именно:

- Предназначена ли информационная система для обработки персональных данных и имеются ли факты такой обработки?
- Каковы формы представления персональных данных?
- Каковы цели обработки персональных данных?
- Имеются ли законные основания для обработки персональных данных?
- Требуется ли получение оператором-подразделением МВД России согласия субъекта на обработку его персональных данных?
- Каковы способы, сроки и объёмы обработки персональных данных?
- Каковы источники получения персональных данных?
- Каков состав (категория) персональных данных?
- Какие аппаратные средства входят в состав информационной системы?
- Какое системное и прикладное программное обеспечение применяется в информационной системе?
- Является ли информационная система автономной, локальной или распределенной?
- Имеется ли подключение информационной системы к телекоммуникационным каналам общего пользования и (или) сетям международного информационного обмена?
- В каких помещениях размещается информационная система?
- Какова контролируемая зона на объекте информатизации?
- Какие вспомогательные технические средства и системы эксплуатируются на объекте информатизации?
- Какова схема электропитания и имеется ли система заземления на объекте информатизации?
- Какова исходная защищенность информационной системы персональных данных?

Получив ответы на все поставленные выше вопросы, руководствуясь Порядком[12] проведения классификации информационных систем персональных данных, можно приступать к определению класса информационной системы персональных данных. Целью классификации является установление методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных. По результатам работы комиссии готовится Акт классификации для каждой ИСПДн, который утверждается руководителем подразделения МВД России.

После проведения классификации информационных систем персональных данных на каждую из них разрабатывается модель угроз безопасности и модель нарушителя, а также формулируются требования к системе защиты персональных данных. Следует иметь в виду, что подавляющее большинство информационных систем персональных данных подразделений МВД России являются специальными, а следовательно, для каждой из них требуется разработка Модели угроз безопасности. В соответствии с п.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 года, комплекс мероприятий по обеспечению персональных данных включает определение актуальных угроз безопасности персональных данных при их обработке и построение на их основе Модели угроз для каждой информационной системы. Определение актуальных угроз безопасности персональных данных и разработка Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных осуществляется по Методике[13] на основе Базовой модели[14].

В случае использования в информационных системах для обеспечения безопасности персональных данных средств криптографической защиты при оценке актуальности угроз безопасности и разработке Модели угроз безопасности персональных данных необходим учет методологических положений, сформулированных в Методических рекомендациях ФСБ России[15].

12 Приказ ФСТЭК России, ФСБ России Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

13 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 года.

14 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15 февраля 2008 года.

15 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием

Проектирование и реализация системы защиты персональных данных в информационных системах являются достаточно затратными этапами с интеллектуальной и финансовой точек зрения. На основе анализа содержания Акта классификации ИСПДн и Модели угроз безопасности персональных данных разрабатываются техническое задание на создание либо модернизацию (для существующей ИСПДн) системы защиты персональных данных и технический проект системы защиты персональных данных, который затем реализуется путем закупки соответствующих программных, аппаратных и программно-аппаратных средств защиты информации, проведения монтажных и пусконаладочных работ, подготовки эксплуатационной и распорядительной документации, обучения должностных лиц, ответственных за обработку и обеспечение безопасности персональных данных, порядку их применения.

В техническом задании на создание (модификацию) СЗПДн и в техническом проекте СЗПДн должны быть сформулированы требования к системе защиты персональных данных в целом, а также составу, размещению, порядку установки, наладки, испытания и эксплуатации средств защиты информации.

Основным вопросом при проектировании системы защиты персональных данных является выбор методов и способов защиты информации, адекватных угрозам безопасности персональных данных в информационных системах определенного класса, способных полностью нейтрализовать возможности несанкционированного доступа к персональным данным и технические каналы утечки информации. Выбор соответствующих методов и способов защиты информации осуществляется в соответствии с Положением ФСТЭК России[16].

Подтверждение соответствия ИСПДн требованиям к безопасности персональных данных или аттестация ИСПДн представляет собой комплекс организационно-технических мероприятий, в результате проведения которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России (ФСТЭК России).

Следует отметить, что по состоянию на 31 июля 2012 года не принято каких-либо специальных нормативных документов, определяющих порядок аттестации объектов информатизации (информационных систем), предназначенных для обработки информации конфиденциального характера (в том числе персональных данных), не составляющей государственную тайну, учитывающих особенности данных систем и более низкий уровень требований по сравнению с защитой информации, содержащей сведения, составляющих в соответствии с законодательством Российской Федерации государственную тайну. В связи с этим аттестация таких информационных систем должна проводиться в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденным Государственной технической комиссией при Президенте Российской Федерации 25 ноября 1994 года. Также в системе МВД России при проведении аттестации ИСПДн необходимо пользоваться Временным наставлением по технической защите информации[17].

По результатам проведенных работ на каждую аттестуемую информационную систему выдается «Аттестат соответствия», подтверждающий эффективность созданной системы защиты информации и соответствие всех организационно-распорядительных, технических и технологических документов ИСПДн предъявляемым требованиям. Наличие Аттестата разрешает подразделению МВД России ввод в эксплуатацию информационной системы персональных данных.

После проведения оценки соответствия и ввода в эксплуатацию ИСПДн с внедренной в ее состав системой защиты персональных данных должно быть обеспечено выполнение всех требований по защите при ее эксплуатации. С этой целью в подразделении МВД России организуется и проводится периодический контроль эффективности применяемых мер защиты, в том числе с применением специальных сертифицированных средств контроля в соответствии с Руководящими документами ФСТЭК России (Гостехкомиссии при Президенте Российской Федерации).

Выполнив все установленные требования к СЗПДн в информационной системе, оператор-подразделение МВД России получает право начать обработку персональных данных. До начала обработки подразделение МВД России обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор). Порядок уведомления, содержание представляемых материалов регламентированы:

- Приказом Минкомсвязи России от 21.12.2011 №346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»;
- Приказом Роскомнадзора от 19.08.2011 №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

Разрешается осуществлять обработку персональных данных без уведомления уполномоченного органа (Роскомнадзора). Эти случаи определены в пункте 2 статьи 22 Федерального закона «О персональных данных». ИСПДн, в отношении которых уведомление в Роскомнадзор не направляется, подлежат учету в Реестре информационных систем МВД России[18].

Завершая рассмотрение такой многоаспектной сферы деятельности как обеспечение безопасности персональных данных в информационных системах подразделений МВД России, хотелось бы отметить, что в рамках одной статьи не представляется возможным и целесообразным осветить все тонкости этой кропотливой, а зачастую и рутинной работы, требующей знания и глубокого понимания положений нормативных правовых актов, руководящих и методических документов, технических и технологических вопросов. Однако, осознавая необходимость выполнения подразделениями МВД России требований законодательства Российской Федерации, ведомственных нормативных актов в области защиты прав и свобод человека и гражданина при обработке его персональных данных, выражаем надежду, что данная работа будет способствовать формированию общих подходов к решению этой важной государственной задачи.

средств автоматизации». Утверждены ФСБ России 21 февраля 2008 года №149/54–144.

16 Приказ ФСТЭК России от 05.02.2010 №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

17 Приказ МВД России от 05.07.2001 №029 «Об утверждении Временного наставления по технической защите информации в органах внутренних дел Российской Федерации и внутренних войсках МВД РФ».

18 Методические рекомендации по порядку регистрации информационных систем МВД России в Реестре информационных систем МВД России от 29.06.2012 года №9/3441.