УДК 004.056.53

# Выбор средств защиты информации, обрабатываемой в информационных системах персональных данных

© А.А. Герасимов, А.В. Мозговой, К.А. Пугачев, В.А. Кузнецов

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

*Рассмотрены вопросы правильного выбора сертифицированных средств защиты информации, не отнесенной к сведениям, составляющим государственную тайну, обрабатываемой в информационных системах персональных данных, с учетом требований, предъявляемых актуальными нормативно-методическими документами ФСТЭК России к таким системам.*

***Ключевые слова:*** *защита информации, средства защиты информации, персональные данные.*

С выходом приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК) России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определились основные подходы и требования регулятора к защите персональных данных (ПДн), не отнесенных к сведениям, составляющим государственную тайну.

Кроме упомянутого приказа в пакет основных нормативных документов, определяющих вопросы обработки и защиты персональных данных, на текущий момент входят следующие основные документы:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства РФ от 1 ноября 2012 г. № 1119.

3. Перечень 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, утвержденный постановлением Правительства РФ от 21 марта 2012 г. № 211.

4. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.

Однако лишь в приказе № 21 впервые четко определены меры по обеспечению безопасности ПДн для каждого из уровней защищенности ПДн, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119. В общем случае к таким мерам относятся следующие:

• идентификация и аутентификация субъектов и объектов доступа путем присвоения им уникальных идентификаторов и дальнейшего сравнения предъявленного идентификатора с перечнем присвоенных, на основе чего принимается решение о возможности выполнения запрошенной операции;

• управление доступом субъектов доступа к объектам доступа в соответствии с правилами, указанными в разрешительной системе доступа, разработанной для информационной системы (ИС);

• ограничение программной среды в целях пресечения попыток запуска программного обеспечения, запрещенного к использованию в данной ИС;

• защита машинных носителей информации, включающая в себя как защиту носителей, предназначенных для обработки и хранения ПДн, от несанкционированного доступа (НСД) к ним, так и защиту ИС от несанкционированного подключения неучтенных внешних носителей информации;

• регистрация событий в целях обеспечения возможности дальнейшего реагирования на преднамеренные либо случайные попытки НСД, сбои в работе ИС и прочие события, связанные с нарушением штатного процесса обработки информации в ИС;

• антивирусная защита в целях обнаружения и блокирования работы в ИСПДн вредоносного программного обеспечения;

• обнаружение вторжений в целях предотвращения (либо иного реагирования) действий, направленных на осуществление НСД к обрабатываемой информации, нарушение основных характеристик ее

конфиденциальности либо нарушения работоспособности системы защиты информации ИС или ИС в целом;

• контроль защищенности ПДн посредством регулярных проверок состояния и эффективности системы защиты информации для обеспечения ее адекватности изменяющимся условиям функционирования ИС;

• обеспечение целостности как ИС, ее программного и аппаратного обеспечения, средств защиты информации (СЗИ), так и ПДн, обрабатываемых либо хранящихся в данной ИС;

• обеспечение доступности ПДн со стороны субъектов, имеющих право санкционированного доступа к ним;

• защита среды виртуализации ИС, ее компонентов, а также ПДн, обрабатываемых в ее виртуальной инфраструктуре;

• защита технических средств, входящих в состав ИС либо обеспечивающих ее штатное функционирование, от НСД;

• защита ИС, ее компонентов и ПДн, обрабатываемых ИС или хранящихся в ней, при ее взаимодействии с другими ИС;

• выявление инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ПДн, реагирование на них и осуществление мер, направленных на неповторение таких инцидентов при дальнейшем функционировании ИС;

• управление конфигурацией ИС и системы защиты персональных данных (СЗПДн), выявление необходимости внесения в нее изменений и анализ возможности их реализации [1, 3].

Указанные меры реализуются в составе СЗПДн, создаваемой для ИС, и могут осуществляться как с помощью организационных мероприятий, так и посредством применения в ИС СЗИ, прошедших в установленном порядке процедуру оценки соответствия.

Для определения конкретного перечня мероприятий, составляющих СЗПДн ИС, необходимо учитывать следующие ее характеристики: тип ИС; технологический процесс обработки ПДн; перечень актуальных угроз безопасности ПДн, установленный уровень защищенности ИС; минимальный набор требований к защищенности ПДн ИС определенного уровня защищенности.

Основными техническими средствами, применяемыми для защиты информации в таких ИС, являются средства вычислительной техники (СВТ) в защищенном исполнении, СЗИ от НСД, средства обнаружения вторжений (СОВ), средства антивирусной защиты (АВЗ) и межсетевого экранирования (МСЭ) [1–3]. Если необходимо применить указанные средства, то кроме требований к их функционированию предъявляются также требования к их сертификатам, подтверждающим соответствие установленным классам СЗИ, что необходи-

мо учитывать при выборе СЗИ для создания СЗПДн. Так, при использовании СВТ в защищенном исполнении для ИС 1, 2 и 3-го уровней защищенности они должны быть не ниже 5-го класса, для ИС 4-го уровня защищенности — не ниже 6-го класса [3]. Возможность применения СЗИ от НСД в ИС различных уровней защищенности в явном виде указывается в сертификатах соответствия СЗИ. Для наглядности основные требования к применяемым СЗИ в зависимости от уровня защищенности ИС, а также от наличия ее выхода в информационно-телекоммуникационные сети международного информационного обмена (ИТСМО) сведены в таблицу.

| Уровень защищенности ИС | Наличие ИТСМО | Требуемый минимальный класс СЗИ | | | |
|---|---|---|---|---|---|
| | | СВТ | СОВ | АВЗ | МСЭ |
| 1 | + | 5 | 4 | 4 | 3 |
| | – | 5 | 4 | 4 | 4 |
| 2 | + | 5 | 4 | 4 | 3 |
| | – | 5 | 4 | 4 | 4 |
| 3 | + | 5 | 4 | 4 | 3 |
| | – | 5 | 5 | 5 | 4 |
| 4 | + | 6 | 5 | 5 | 5 |
| | – | 6 | 5 | 5 | 5 |

Все применяемые СЗИ в ИС 1-го и 2-го уровней защищенности, а также 3-го уровня при актуальности для ИС угроз, связанных с наличием недекларированных возможностей в прикладном программном обеспечении, должны пройти процедуру контроля отсутствия недекларированных возможностей не ниже чем по 4-му уровню [2, 3].

В завершение необходимо сказать, что даже наиболее совершенные СЗИ не смогут выполнять свои функции без правильной их настройки и корректного выбора поддерживающих организационных мероприятий, а также без надлежащего контроля за их выполнением, о чем не стоит забывать при построении СЗПДн.

## ЛИТЕРАТУРА

[1] Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». *Российская газета*, 2006, 29 июля.

[2] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». *Российская газета*, 2012, 7 ноября.

[3] Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». *Российская газета*, 2013, 22 мая.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Герасимов А.А., Мозговой А.В., Пугачев К.А., Кузнецов В.А. Выбор средств защиты информации, обрабатываемой в информационных системах персональных данных. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1016.html

**Герасимов Антон Андреевич** родился в 1985 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Канд. техн. наук, доцент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 15 статей, 1 монографии и 3 методических указаний по тематике «Защита информации». e-mail: ger-anton@mail.ru

**Мозговой Андрей Валериевич** родился в 1986 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 10 статей и 1 методических указаний по тематике «Защита информации». e-mail: runc.nsd@gmail.com

**Пугачев Кирилл Александрович** родился в 1987 г., окончил МГТУ им. Н.Э. Баумана в 2010 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор 1 статьи и 1 методических указаний по тематике «Защита информации». e-mail: pugachev_ka13@mail.ru

**Кузнецов Виктор Александрович** родился в 1989 г., окончил МГТУ им. Н.Э. Баумана в 2012 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана». e-mail: viktor_kuznetsov@mail.ru