*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

e-mail: runc.nsd@gmail.com, ger-anton@mail.ru , viktor__kuznetsov@mail.ru , pugachev_ka13@mail.ru

*Рассматриваются 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.

# CHOOSING OF DATA PROTECTION FACILITIES IN THE INFORMATION SYSTEMS OF PERSONALLY IDENTIFIABLE INFORMATION

**A.A. GERASIMOV, A.V. MOZGOVOY, K.A. PUGACHEV, V.A. KUZNETSOV**

BMSTU, Moscow

e-mail: runc.nsd@gmail.com, ger-anton@mail.ru , viktor__kuznetsov@mail.ru , pugachev_ka13@mail.ru

*The paper studies the problems of correctly choosing certificated data protection facilities for information, not comprising state secret, processed in the information systems of personally identifiable information, according to the requirements of current regulatory and procedural documents of FSTEC of Russia.*

***Keywords:*** information security, data protection facilities, personally identifiable information.

С выходом приказа 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 по защите персональных данных (ПДн), не отнесенных к сведениям, составляющим государственную тайну.

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

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

2. «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утверждены 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», утвержден 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», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года.

7. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России от 15 февраля 2008 года.

Однако лишь Приказом №21 впервые четко определены меры по обеспечению безопасности ПДн для каждого из уровней защищенности (УЗ) ПДн, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

В их состав в общем случае входят:

- 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 ее основных характеристик 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 компонент, 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 компонент 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 реализация 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 при помощи как организационных мероприятий, так и посредством применения в ИС СЗИ, прошедших в установленном порядке процедуру оценки соответствия.

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

Основными техническими СЗИ, применяемыми для защиты информации в таких ИС, являются средства вычислительной техники (СВТ) в защищенном исполнении, СЗИ от НСД, средства обнаружения вторжений (СОВ), антивирусной защиты (АВЗ) и межсетевого экранирования (МСЭ) [1 - 3] . В случае необходимости применения указанных средств кроме требований к их функционированию также предъявляются и требования к их сертификатам, подтверждающим соответствие установленным классам СЗИ,

что также необходимо учитывать при выборе средств защиты информации для создания СЗПДн. Так, например, при использовании в ИС СВТ в защищенном исполнении, для ИС 1, 2 и 3 уровней защищенности они должны быть не ниже 5 класса, для ИС 4 уровня защищенности – не ниже 6 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 УЗ ИС, а также наличия ее выхода в информационно-телекоммуникационные сети международного информационного обмена (ИТСМО) сведены в следующую таблицу:

| УЗ ИС | Требуемый минимальный класс СЗИ | | | |
|---|---|---|---|---|
| | СВТ | СОВ | АВЗ | МСЭ |
| 1 (с ИТСМО) | 5 | 4 | 4 | 3 |
| 1 (без ИТСМО) | 5 | 4 | 4 | 4 |
| 2 (с ИТСМО) | 5 | 4 | 4 | 3 |
| 2(без ИТСМО) | 5 | 4 | 4 | 4 |
| 3 (с ИТСМО) | 5 | 4 | 4 | 3 |
| 3(без ИТСМО) | 5 | 5 | 5 | 4 |
| 4 | 6 | 5 | 5 | 5 |

Также, все применяемые СЗИ в ИС 1 и 2 уровней защищенности, а также 3 уровня при актуальности для ИС угроз, связанных с наличием

недекларированных возможностей в прикладном программном обеспечении, должны пройти проверку контроля отсутствия недекларированных возможностей не ниже чем по 4 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 их организационных мероприятий, а также надлежащего контроля за их выполнением, о чем не стоит забывать при построении СЗПДн.

# СПИСОК ЛИТЕРАТУРЫ

1. О персональных данных : федеральный закон : [принят Гос. Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.] // 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. N 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.

# REFERENCES

1. About the personally identifiable information : federal law : [adopted by the State Duma on July 8, 2006. : Federation Council approved July 14, 2006] // Russian newspaper. - 2006. - July 29;

2. Resolution of the Government of the Russian Federation dated November 1, 2012 number 1119 «On approval requirements for the protection of personally identifiable information during their processing in information systems of personally identifiable information» // Russian newspaper. - 2012. – November 7;

3. Order of the Federal Service for Technical and Export Control on February 18, 2013 N 21 «On approval of the composition and content of organizational and technical measures to ensure the security of personally identifiable information during their processing in information systems of personally identifiable information» // Russian newspaper. - 2013. - May 22.