Зарегистрировано в Минюсте РФ 19 февраля 2010 г. N 16456

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 5 февраля 2010 г. N 58

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О МЕТОДАХ И СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с пунктом 3 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 (Собрание законодательства Российской Федерации, 2007, N 48, ст. 6001), приказываю:

Утвердить прилагаемое Положение о методах и способах защиты информации в информационных системах персональных данных.

Директор Федеральной службы
по техническому
и экспортному контролю
С.ГРИГОРОВ

Приложение
к Приказу ФСТЭК России
от 5 февраля 2010 г. N 58

ПОЛОЖЕНИЕ О МЕТОДАХ И СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. Общие положения

1.1. Настоящее Положение разработано в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 (Собрание законодательства Российской Федерации, 2007, N 48, ст. 6001), и устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), или лицом, которому на основании договора оператор поручает обработку персональных данных (далее - уполномоченное лицо).

В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

1.2. К методам и способам защиты информации в информационных системах относятся:

методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);

методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

1.3. Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

1.4. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 г., регистрационный N 11462).

Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781.

1.5. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе создаваемой оператором (уполномоченным лицом) системы защиты персональных данных.

II. Методы и способы защиты информации от несанкционированного доступа

2.1. Методами и способами защиты информации от несанкционированного доступа являются:

реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

использование защищенных каналов связи;

размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

2.2. В системе защиты персональных данных информационной системы в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы определяются оператором (уполномоченным лицом) в соответствии с приложением к настоящему Положению.

2.3. В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

2.4. При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в пункте 2.1 настоящего Положения, основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

защита информации при ее передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

использование средств антивирусной защиты;

централизованное управление системой защиты персональных данных информационной системы.

2.5. Подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно-телекоммуникационным сетям международного информационного обмена осуществляется в соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (Собрание законодательства Российской Федерации, 2008, N 12, ст. 1110; N 43, ст. 4919).

2.6. Для обеспечения безопасности персональных данных при подключении информационных систем к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) с целью получения общедоступной информации помимо методов и способов, указанных в пунктах 2.1 и 2.4 настоящего Положения,

применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);

периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;

активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

Для реализации указанных методов и способов защиты информации могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

2.7. Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в пунктах 2.1 и 2.4 настоящего Положения, применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;

управление доступом к защищаемым персональным данным информационной сети;

использование атрибутов безопасности.

2.8. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в пунктах 2.1 и 2.4 настоящего Положения, применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

создание канала связи, обеспечивающего защиту передаваемой информации;

осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

2.9. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем разных операторов через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в пунктах 2.1 и 2.4 настоящего Положения, применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

создание канала связи, обеспечивающего защиту передаваемой информации;

аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;

обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

2.10. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств.

2.11. Подключение информационной системы к информационной системе другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов.

2.12. Программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия недекларированных возможностей.

Необходимость проведения контроля отсутствия недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов, определяется оператором (уполномоченным лицом).

2.13. В зависимости от особенностей обработки персональных данных и структуры информационных систем могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

III. Методы и способы защиты информации от утечки по техническим каналам

3.1. Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, определенные на основе методических документов, утвержденных в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781.

3.2. Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:

использование технических средств в защищенном исполнении;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

размещение объектов защиты в соответствии с предписанием на эксплуатацию;

размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

3.3. В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

3.4. При применении в информационных системах функции голосового ввода персональных данных в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для информационной системы 1 класса реализуются методы и способы защиты акустической (речевой) информации.

Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в информационной системе.

3.5. Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена

возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Приложение
к Положению
о методах и способах защиты
информации в информационных
системах персональных данных

МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЗАВИСИМОСТИ ОТ КЛАССА ИНФОРМАЦИОННОЙ СИСТЕМЫ

1. Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности персональных данных в информационных системах 4 класса и целесообразность их применения определяются оператором (уполномоченным лицом).

2. Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 3 класса.

2.1. Для информационных систем 3 класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.2. Для информационных систем 3 класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.3. Для информационных систем 3 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием

трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

2.4. Безопасное межсетевое взаимодействие для информационных систем 3 класса при их подключении к сетям международного информационного обмена, а также для распределенных информационных систем 3 класса при их разделении на подсистемы достигается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

контроль целостности своей программной и информационной части;

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Межсетевые экраны, которые обеспечивают выполнение указанных выше функций, применяются в распределенных информационных системах 2 и 1 классов при их разделении на отдельные части.

При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.

3. Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 2 класса.

3.1. Для информационных систем 2 класса при однопользовательском режиме обработки персональных применяются все методы и способы защиты информации от несанкционированного доступа, соответствующие информационным системам 3 класса при однопользовательском режиме обработки.

3.2. Для информационных систем 2 класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются все методы и способы защиты информации от несанкционированного доступа, соответствующие информационным системам 3 класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей.

3.3. Для информационных систем 2 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей реализуются все методы и способы защиты информации от несанкционированного доступа, соответствующие

информационным системам 3 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей.

3.4. Безопасное межсетевое взаимодействие для информационных систем 2 класса при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования, которые обеспечивают:

фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов;

регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

регистрацию запуска программ и процессов (заданий, задач);

контроль целостности своей программной и информационной части;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

4. Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 1 класса.

4.1. Для информационных систем 1 класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

дублирующий учет защищаемых носителей информации;

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов средств защиты информации, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.2. Для информационных систем 1 класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам);

идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

дублирующий учет защищаемых носителей информации;

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.3. Для информационных систем 1 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;

б) регистрация и учет:

регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с

указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;

физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4. Безопасное межсетевое взаимодействие для информационных систем 1 класса при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования, которые обеспечивают выполнение следующих функций:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов;

фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

фильтрацию с учетом даты и времени;

аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;

регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

регистрацию и учет запросов на установление виртуальных соединений;

локальную сигнализацию попыток нарушения правил фильтрации;

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

регистрацию запуска программ и процессов (заданий, задач);

регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;

возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;

контроль целостности своей программной и информационной части;

контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

5. Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности.

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

6. Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

7. Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.