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 і 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. N781.

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.