УТВЕРЖДЕНА

приказом Министерства   
государственного имущества   
Республики Марий Эл

от 11 апреля 2013 года № 137-од

**ПОЛИТИКА**

**безопасности персональных данных, обрабатываемых  
в информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл**

## Определения

В настоящем документе используются следующие термины  
и их определения.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных– состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных  
при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации  
и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора   
с перечнем присвоенных идентификаторов.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных  
и обеспечивающих их обработку информационных технологий  
и технических средств.

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации   
и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное  
для соблюдения оператором или иным получившим доступ  
к персональным данным лицом требование не распространять  
их без согласия субъекта персональных данных или наличия иного законного основания.

**Средство криптографической защиты информации** – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Межсетевой экран – локальное (однокомпонентное)  
или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль  
за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных  
при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа   
с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств  
с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Технические средства информационной системы персональных данных– средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства  
и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые  
в информационных системах.

Персональные данные – любая информация, относящаяся   
к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Система защиты персональных данных** – совокупность органов   
и (или) исполнителей, используемой ими техники защиты информации,   
а также объектов, организованная и функционирующая по правилам  
и нормам, установленным соответствующими документами в области защиты персональных данных.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных   
в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Введение

Настоящая Политика безопасности персональных данных, обрабатываемых в информационных системах персональных данных   
в Министерстве государственного имущества Республики Марий Эл, является официальным документом и разработана в соответствии  
с целями, задачами и принципами обеспечения безопасности персональных данных изложенными в Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл.

Политика безопасности персональных данных, обрабатываемых   
в информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл (далее – Политика) разработана в соответствии с требованиями:

* Федерального закона от 27 июля 2006 года № 152-ФЗ   
  «О персональных данных»;
* Постановления Правительства Российской Федерации   
  от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказа ФСТЭК России от 5 февраля 2010 года № 58  
  «Об утверждении положения о методах и способах защиты информации»;
* Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования   
  для обеспечения безопасности персональных данных при их обработке   
  в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 года  
  № 149/6/6-662.

В Политике определены требования к сотрудникам Министерства государственного имущества Республики Марий Эл, степень ответственности сотрудников в Министерстве государственного имущества Республики Марий Эл, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников  
в Министерстве государственного имущества Республики Марий Эл, ответственных за обеспечение безопасности персональных данных   
в информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл.

# Общие положения

Целью настоящей Политики является обеспечение безопасности персональных данных в Министерстве государственного имущества Республики Марий Эл от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональным данным.

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. В информационных системах персональных данных должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности персональных данных.

В информационных системах персональных данных необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень персональных данных, подлежащих защите, определен   
в Положении об обработке персональных данных в Министерстве государственного имущества Республики Марий Эл.

# Область действия

Требования настоящей Политики распространяются  
на персональные данные министра государственного имущества Республики Марий Эл, государственных гражданских служащих Республики Марий Эл и работников (далее – сотрудники)  
в Министерстве государственного имущества Республики Марий Эл; граждан, обращающихся в Министерство государственного имущества Республики Марий Эл для получения государственных услуг и других лиц.

# Система защиты персональных данных

Система защиты персональных данных строится на основании:

* Перечня персональных данных, подлежащих защите;
* Акта классификации информационной системы персональных данных;
* Акта определения уровня защищенности персональных данных   
  при их обработке в информационных системах персональных данных;
* Частной модели угроз и нарушителя безопасности персональных данных;
* Положения о разграничении прав доступа к обрабатываемым персональным данным;
* Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности персональных данных в каждой информационной системе персональных данных в Министерстве государственного имущества Республики Марий Эл. Для каждой информационной системы персональных данных должен быть определен перечень используемых технических средств, а также программного обеспечения участвующего в обработке персональных данных, подлежащих защите.

В зависимости от уровня защищенности информационной системы персональных данных и актуальных угроз, система защиты персональных данных может включать следующие технические  
и программные средства:

* антивирусные средства для объектов вычислительной техники;
* средства межсетевого экранирования;
* средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в перечень должны быть включены функции защиты, обеспечиваемые штатными средствами информационной системы персональных данных и операционных систем, прикладным программным обеспечении и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

* управление доступом и разграничение доступа пользователей;
* регистрацию и учет действий с информацией;
* обеспечение целостности данных;
* обнаружение вторжений.

Перечень используемых технических средств отражается  
в «Справке об итогах анализа существующей организационной структуры и организационно-распорядительной документации  
по обеспечению безопасности персональных данных», полученной  
по результатам внешнего аудита. Перечень используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава системы защиты персональных данных или элементов информационной системы персональных данных должны быть согласованы   
с Администратором информационной безопасности и утверждены министром государственного имущества Республики Марий Эл.

# Требования к подсистемам системы защиты персональных данных

Система защиты персональных данных включает в себя следующие подсистемы:

* управления доступом, регистрации и учета;
* обеспечения целостности и доступности;
* антивирусной защиты;
* межсетевого экранирования;
* анализа защищенности;
* обнаружения вторжений;
* криптографической защиты.

Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от класса информационной системы персональных данных, определенного в Акте классификации информационной системы персональных данных.

## 4.1. Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

* идентификации и проверки подлинности субъектов доступа  
  при входе в информационную систему персональных данных;
* идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
* идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
* регистрации входа (выхода) субъектов доступа в систему  
  (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова;
* регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
* регистрации попыток доступа программных средств  
  к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована  
с помощью штатных средств обработки персональных данных (операционных систем, приложений). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

## 4.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем персональных данных в Министерстве государственного имущества Республики Марий Эл, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов информационных систем персональных данных.

## 4.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты объектов вычислительной техники в Министерстве государственного имущества Республики Марий Эл.

Средства антивирусной защиты предназначены для реализации следующих функций:

* резидентный антивирусный мониторинг;
* антивирусное сканирование;
* скрипт-блокирование;
* централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта;
* автоматизированное обновление антивирусных баз;
* ограничение прав пользователя на остановку исполняемых задач   
  и изменения настроек антивирусного программного обеспечения;
* автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения во все элементы информационных систем персональных данных.

## 4.4. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

* фильтрации открытого и зашифрованного (закрытого) IP-трафика;
* фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
* идентификации и аутентификации Администратора информационной безопасности или Администратора информационной системы персональных данных при его локальных запросах на доступ;
* регистрации входа (выхода) Администратора информационной безопасности или Администратора информационной системы персональных данных в систему (из системы) либо загрузки  
  и инициализации системыи ее программного останова;
* контроля целостности своей программной и информационной части;
* фильтрации пакетов служебных протоколов, служащих   
  для диагностики и управления работой сетевых устройств;
* фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
* регистрации и учета запрашиваемых сервисов прикладного уровня;
* блокирования доступа неидентифицированного объекта   
  или субъекта, подлинность которого при аутентификации  
  не подтвердилась, методами, устойчивыми к перехвату;
* контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальной вычислительной сети.

## 4.5. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными   
и программно-аппаратными средствами.

## 4.6. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы информационной системы персональных данных, подключенные к сетям общего пользования  
и (или) международного обмена.

Функционал подсистемы может быть реализован программными   
и программно-аппаратными средствами.

## 4.7. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена  
для исключения НСД к защищаемой информации в информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

# Пользователи информационных систем персональных данных

В Концепции безопасности персональных данных определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей информационных систем персональных данных, определен их уровень доступа   
и возможности.

В информационных системах персональных данных в Министерстве государственного имущества Республики Марий Эл можно выделить следующие группы пользователей, участвующих в обработке персональных данных:

* Администратор информационной системы персональных данных;
* Оператор информационной системы персональных данных.

Данные о группах пользователей, уровне их доступа   
и информированности должны быть отражены в Положении  
о разграничении прав доступа к обрабатываемым персональным данным.

## 5.1. Администратор информационной системы персональных данных

Администратор информационной системы персональных данных, сотрудник в Министерстве государственного имущества Республики Марий Эл, ответственный за настройку, внедрение и сопровождение информационной системы персональных данных. Обеспечивает функционирование подсистемы управления доступом информационной системы персональных данных и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора информационной системы персональных данных)  
к элементам, хранящим персональные данные.

Администратор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

* обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;
* обладает полной информацией о технических средствах   
  и конфигурации информационной системы персональных данных;
* имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;
* обладает возможностями внесения изменений в программное обеспечение информационной системы персональных данных на стадии  
  ее разработки, внедрения и сопровождения;
* обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

## 5.2. Оператор информационной системы персональных данных

Оператор информационной системы персональных данных, сотрудник в Министерстве государственного имущества Республики Марий Эл, осуществляющий обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных  
в информационную систему персональных данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных.

Оператор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

* обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;
* располагает конфиденциальными данными, к которым имеет доступ.

# Администратор информационной безопасности

Администратор информационной безопасности, сотрудник   
в Министерстве государственного имущества Республики Марий Эл, назначаемый приказом Министерства государственного имущества Республики Марий Эл, ответственный за функционирование системы защиты персональных данных, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор информационной безопасности обладает следующим уровнем доступа и знаний:

* обладает полной информацией об информационных системах персональных данных;
* имеет доступ к средствам защиты информации  
  и протоколирования и к части ключевых элементов информационных систем персональных данных;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор информационной безопасности уполномочен:

* реализовывать политики безопасности в части настройки средств криптографической защиты информации, межсетевых экранов и систем обнаружения вторжений, в соответствии с которыми пользователь (Оператор информационной системы персональных данных) получает возможность работать с элементами информационной системы персональных данных;
* осуществлять аудит средств защиты информации;
* осуществлять контроль за действиями пользователей информационных систем персональных данных при их работе с персональными данными;
* устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений.

Должностные обязанности Администратора информационной безопасности описаны в Инструкции Администратора информационной безопасности.

# Требования к сотрудникам в Министерстве государственного имущества Республики Марий Эл по обеспечению защиты персональных данных

Все сотрудники в Министерстве государственного имущества Республики Марий Эл, являющиеся пользователями информационных систем персональных данных, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности персональных данных.

При вступлении в должность нового сотрудника в Министерстве государственного имущества Республики Марий Эл непосредственный руководитель структурного подразделения обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем персональных данных.

Сотрудник в Министерстве государственного имущества Республики Марий Эл должен быть ознакомлен с настоящей Политикой, установленными процедурами работы с элементами информационных систем персональных данных и системой защиты персональных данных.

Сотрудники в Министерстве государственного имущества Республики Марий Эл, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники в Министерстве государственного имущества Республики Марий Эл должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства идентификации и аутентификации).

Сотрудники в Министерстве государственного имущества Республики Марий Эл должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи информационных систем персональных данных должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам в Министерстве государственного имущества Республики Марий Эл запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства  
и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам в Министерстве государственного имущества Республики Марий Эл запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с персональными данными в информационных системах персональных данных сотрудники в Министерстве государственного имущества Республики Марий Эл обязаны исключить возможность просмотра персональных данных третьими лицами  
с мониторов объектов вычислительной техники.

При завершении работы с информационной системой персональных данных сотрудники в Министерстве государственного имущества Республики Марий Эл обязаны защитить объекты вычислительной техники с помощью блокировки ключом  
или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники в Министерстве государственного имущества Республики Марий Эл должны быть проинформированы об угрозах нарушения режима безопасности персональных данных  
и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников в Министерстве государственного имущества Республики Марий Эл, нарушающих принятые политику и процедуры безопасности персональных данных.

Сотрудники в Министерстве государственного имущества Республики Марий Эл обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование  
на угрозы безопасности персональных данных.

# Должностные обязанности пользователей информационных систем персональных данных

Должностные обязанности пользователей информационных систем персональных данных описаны в следующих документах:

* Инструкция Администратора информационной системы персональных данных;
* Инструкция Оператора информационной системы персональных данных.

# Ответственность пользователей информационных систем персональных данных

В соответствии со ст. 24 Федерального закона от 27 июля  
2006 года № 152-ФЗ «О персональных данных» лица, виновные  
в нарушении требований Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Пользователи информационных систем персональных данных несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками в Министерстве государственного имущества Республики Марий Эл – Пользователями информационных систем персональных данных правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов  
по защите информации должны быть отражены в локальных нормативных и правовых актах в Министерстве государственного имущества Республики Марий Эл.

# Список использованных источников

* 1. Конституция Российской Федерации;
  2. Конституция Республики Марий Эл;
  3. Трудовой кодекс Российской Федерации;
  4. Семейный кодекс Российской Федерации;
  5. Федеральный закон от 27 июля 2006 года № 152-ФЗ   
     «О персональных данных»;
  6. Постановление Правительства Российской Федерации   
     от 15 сентября 2008 года № 687 «Об утверждении Положения   
     об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
  7. Постановление Правительства Российской Федерации   
     от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
  8. Постановление Правительства Российской Федерации   
     от 6 июля 2007 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
  9. Постановление Правительства Российской Федерации   
     от 21 марта 2012 года № 211 «Об утверждении перечня 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»;
  10. Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
  11. Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 года № 58 «Об утверждении Положения   
      о методах и способах защиты информации в информационных системах персональных данных»;
  12. Нормативно-методические документы Федеральной службы   
      по техническому и экспертному контролю Российской Федерации   
      по обеспечению безопасности персональных данных при их обработке   
      в информационных системах персональных данных;

12.1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15 февраля 2008 года;

12.2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено Заместителем директора ФСТЭК России 14 февраля 2008 года.