МУП «Йошкар-Олинская ТЭЦ-1»

УТВЕРЖДАЮ
Директор
МУП «Йошкар-Олинская ТЭЦ-1»
_____ И.Л. Бондарчук

«10» июня 2012 г.

ПОЛИТИКА
безопасности персональных данных, обрабатываемых в информационных системах персональных данных МУП «Йошкар-Олинская ТЭЦ-1»

Йошкар-Ола
2012 г.

Содержание

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 (ИСПДн) – 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 (СКЗИ) – 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 (НСД) – 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 ПДн (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 МУП «Йошкар-Олинская ТЭЦ-1» (далее по тексту – Предприятие), является официальным документом и разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных Предприятия.

Политика безопасности ПДн, обрабатываемых в ИСПДн Предприятия (далее по тексту – Политика) разработана в соответствии с требованиями:

– Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Постановления Правительства Российской Федерации от 11 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности 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 из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к работникам Предприятия, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн Предприятия.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности персональных данных (ПДн) Предприятия от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн.

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 для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности ПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень персональных данных, подлежащих защите представлен в Положении об обработке персональных данных в МУП «Йошкар-Олинская ТЭЦ-1».

Состав ИСПДн подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных.

2. Область действия

Требования настоящей Политики распространяются на всех работников Предприятия, контрагентов Предприятия и других лиц.

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн) строится на основании:

- Отчета о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных;
- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных;
- Частных моделей угроз 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 ПДн в каждой ИСПДн Предприятия. На основании анализа актуальных угроз безопасности ПДн, описанных в Частных моделях угроз безопасности персональных данных и Отчета о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Рекомендациях по приведению информационных ресурсов, содержащих ПДн, в соответствие требованиям законодательства в области защиты персональных данных.

Для каждой ИСПДн должен быть составлен список используемых технических средств, а также программного обеспечения участвующего в обработке ПДн, подлежащих защите.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн 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 список должны быть включены функции защиты, обеспечиваемые штатными средствами ИСПДн и операционных систем (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

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

Список используемых технических средств отражается в Отчете о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава системы защиты персональных данных или элементов ИСПДн должны быть согласованы с Администратором информационной безопасности и утверждены директором Предприятия.

4. Требования к подсистемам СЗПДн

СЗПДн 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 СЗПДн имеют различный функционал в зависимости от класса ИСПДн, 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 ИСПДн;
– 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 ПДн (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 ПДн, программных и аппаратных средств ИСПДн Предприятия, 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 ИСПДн.

4.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты объектов вычислительной техники Предприятия.

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 на все элементы ИСПДн.

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 ИСПДн при его локальных запросах на доступ;
– регистрации входа (выхода) Администратора информационной безопасности или Администратора ИСПДн в систему (из системы) либо загрузки и инициализации системы и 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 ЛВС.

4.5. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПДн, 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 ИСПДн, 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 ИСПДн Предприятия, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн

В Концепции безопасности ПДн определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

Пользователи ИСПДн делятся на следующие категории:

– пользователи ИСПДн, непосредственно обрабатывающие персональные данные:

1. Администратор ИСПДн;
2. Оператор ИСПДн;

– пользователи ИСПДн, не осуществляющие обработку персональных данных, но сопровождающие и обслуживающие ИСПДн:

1. Системный администратор;
2. Администратор информационной безопасности.

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 ИСПДн

Администратор ИСПДн, сотрудник Предприятия, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора ИСПДн) к элементам хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

– обладает полной информацией о технических средствах и конфигурации ИСПДн;

– имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

– обладает возможностями внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

– обладает правами конфигурирования и административной настройки технических средств ИСПДн.

5.2. Оператор ИСПДн

Оператор ИСПДн, сотрудник Предприятия, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

5.3. Системный администратор

Системный администратор, работник Предприятия, ответственный за функционирование телекоммуникационной подсистемы ИСПДн, обслуживание и настройку периферийного оборудования ИСПДн. Системный администратор не имеет полномочий для управления подсистемами обработки данных и безопасности.

Системный администратор обладает следующим уровнем доступа и знаний:

- обладает информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- обладает возможностями внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- обладает возможностями внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5.4. Администратор информационной безопасности

Администратор информационной безопасности, сотрудник Предприятия, назначаемый приказом руководителя Предприятия, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор информационной безопасности обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор информационной безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения вторжений, в соответствии с которыми пользователь (Оператор ИСПДн) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты информации;
- осуществлять контроль за действиями пользователей ИСПДн 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.

6. Требования к работникам по обеспечению защиты ПДн

Все работники Предприятия, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового работника непосредственный руководитель структурного подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Работники Предприятия, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Предприятия должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства идентификации и аутентификации).

Работники Предприятия должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи ИСПДн должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Работникам запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с ПДн в ИСПДн работники Предприятия обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов объектов вычислительной техники.

При завершении работы с ИСПДн работники обязаны защитить объекты вычислительной техники с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники Предприятия должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция Администратора ИСПДн;
- Инструкция Оператора ИСПДн;
- Инструкция Системного администратора;
- Инструкция Администратора информационной безопасности.

8. Ответственность пользователей ИСПДн

В соответствии со ст. 24 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного 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).

Администратор ИСПДн и Администратор информационной безопасности 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 работниками Предприятия – Администратором информационной безопасности и пользователями ИСПДн правил, связанных с безопасностью ПДн, 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 Предприятия.

9. Список использованных источников

1. Конституция Российской Федерации;
2. Трудовой кодекс Российской Федерации;
3. Семейный кодекс Российской Федерации;
4. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
5. Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
6. Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
7. 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»;
8. 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»;
9. 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»;
10. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн:
10.1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г;
10.2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 14.02.08 г.

Инженер по защите информации СРЭБ _____ Д.В. Донской
23.05.12 г.

СОГЛАСОВАНО:

Гл. инженер _____ И.Н. Пакин

Начальник СРЭБ _____ В.А. Бастраков
23.05.12 г.

Начальник отдела кадров _____ И.Ф. Науменко
23.05.12.

Старший мастер участка АСУ и ВТ _____ В.Ф. Леухин