ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА

Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области
(Управление Роспотребнадзора по Оренбургской области)

ПРИКАЗ

26.01.2015г. № 23-о.д.

г. Оренбург

Об утверждении «Политики
информационной безопасности
персональных данных в Управлении
Роспотребнадзора по Оренбургской области»

В целях исполнения Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Постановления Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г. №1119 и в целях обеспечения безопасности персональных данных в Управлении Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области (далее – Управление), п р и к а з ы в а ю:

1. Утвердить «Политику информационной безопасности персональных данных Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области» (далее – Политика) (Приложение № 1).

2. Заместителям руководителя, начальникам отделов и территориальных отделов Управления:

2.1. руководствоваться в работе положениями Политики для определения правил и обязанностей по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных в

информационных системах персональных данных Управления.

2.2. Руководствоваться иными документами и инструкциями, разработанными на основе Политики для обеспечения комплексной защиты персональных данных.

2.3. Обеспечить доведение содержания Политики до специалистов отделов, имеющих доступ к персональным данным, под роспись.

2.4. Требовать соблюдение сотрудниками отделов положений Политики по обеспечении защиты персональных данных.

3. Возложить персональную ответственность на заместителей руководителя, начальников отделов и территориальных отделов Управления за соблюдение требований Политики.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель Н.Е. Вяльцина

Приложение № 1
к п. № 23-о.д. от 26.01.2015г.

Политика
информационной безопасности персональных данных Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области

Оглавление

1. Общие положения

Настоящая Политика информационной безопасности (далее – Политика) персональных данных Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области (далее – Управление), разработана в соответствии с Федеральным законом Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 21 марта 2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Постановлением Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012г. №1119, Постановлением Правительства «Об утверждении положения об особенностях обработки персональных данных без использования средств автоматизации» от 15 сентября 2008г. № 687, Постановлением Правительства «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 6 июля 2008г. № 512, методических рекомендаций ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности информационных систем персональных данных Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Оренбургской области (далее – Концепция) и включает в себя все раскрытые в нем основные понятия (термины, определения) и список сокращений.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Управления.

Целью настоящей Политики является обеспечение безопасности объектов защиты Управления от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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 УБПДн.

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

Состав объектов защиты регламентируется в соответствии с Перечнем персональных данных, подлежащих защите.

Состав ИСПДн подлежащих защите, определяется в соответствии с Отчетом о результатах проведения внутренней проверки.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников Управления (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- отчета о результатах проведения внутренней проверки;
- перечня персональных данных, подлежащих защите;
- акта определения уровня защищенности информационной системы персональных данных;
- модели угроз безопасности персональных данных;
- положения о разграничении прав доступа к обрабатываемым персональным данным;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Управления. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;

- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (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;
- обеспечивать целостность данных;
- производить обнаружение вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Управления или лицом, ответственным за обеспечение защиты ПДн.

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 уровня защищенности ИСПДн, определенного в Акте определения уровня защищенности информационной системы персональных данных. В соответствии с уровнем защищенности ИСПДн, определяются методы и способы защиты информации от несанкционированного доступа.

В соответствии с постановлением правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн.

Для определения уровня защищенности необходимо выделить ряд параметров ИСПДн, описанных ниже.

Все ИСПДн по категориям обрабатываемых данных делятся на:

- обрабатывающие специальные категории персональных данных (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни);
- обрабатывающие биометрические категории персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта);
- обрабатывающие иные персональные данные.

Кроме того отдельно выделяют системы, обрабатывающие общедоступные персональные данные (данные субъектов персональных данных, полученные только из общедоступных источников).

Также отдельно выделены информационные системы, обрабатывающие персональные данные только сотрудников оператора.

В постановлении приведены три типа актуальных угроз.

- 1 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (операционная система).
- 2 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении (программы обработки ПДн).
- 3 тип. Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей.

В документе не дается указаний на способы выявления не декларированных возможностей программного обеспечения, поэтому Управление установило, что будет руководствоваться следующим правилом: если программное обеспечение лицензионное, выпущено серийно и имеет широкое распространение, то с большой долей вероятности можно сказать, что недекларированные возможности в нем отсутствуют. В противном случае есть высокая вероятность наличия недокументированных функций, способных нанести вред.

На основании указанных выше критериев определяется уровень защищенности ИСПДн.

4.1. Подсистемы управления доступом, регистрации и учета

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

- идентификации и проверка 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 регистрация загрузки и инициализации операционной системы и ее остановка.
- 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 и СУБД).

Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю.

4.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Управления, 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 серверов и АРМ пользователей ИСПДн Управления.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, 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 по следующим параметрам:
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана 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 не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

4.5. Подсистема анализа защищенности

Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО 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 Управления, при ее передачи по каналам связи сетей общего пользования и (или)

международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн

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

В ИСПДн Управления можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор ИСПДн;
- администратор безопасности;
- оператор АРМ;
- администратор сети;
- технический специалист по обслуживанию периферийного оборудования;
- программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

5.1. Администратор ИСПДн

Администратор ИСПДн, сотрудник Управления, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) 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 правами конфигурирования и административной настройки технических средств ИСПДн.

5.2. Администратор сети

Администратор сети, сотрудник Управления, ответственный за функционирование телекоммуникационной подсистемы ИСПДн.

Администратор сети не имеет полномочий для управления

подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

5.3. Администратор безопасности

Администратор безопасности, сотрудник Управления, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает правами администратора сети;
- обладает полной информацией об ИСПДн и телекоммуникационных системах Управления;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- имеет доступ к конфигурированию технических средств сети и программно-техническим средствам обработки информации.

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки телекоммуникационных систем, СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

5.4. Оператор АРМ

Оператор АРМ, сотрудник Управления, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

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.

5.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Управления, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5.6. Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Управления, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ 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.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Управления, 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 сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностным регламентом и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

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

Сотрудники Управления, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

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

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

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать мобильные устройства, средства подключения к интернету (модемы) и неучтенные должным способом носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Управления, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Управления обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники Управления обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Управления 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 принятую политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за информационную безопасность ПДн.

7. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн регламентируются в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;

Инструкции указанных групп пользователей ИСПДн утверждаются руководителем Управления и вводятся в действие приказом.

8. Ответственность сотрудников ИСПДн Управления

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 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 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 сотрудниками Управления – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.