114-ОД

Для служебного пользования

Ед. экз.

СОГЛАСОВАНО:

Генеральный директор

ООО "Единый оператор"

_____ Сапогов Н.В.

«23» декабря 2013 г.

м.п.

УТВЕРЖДАЮ:

Директор

МАОУ ДОД «ДШИ им. В.В. Знаменского»

_____ М.Е. Алехина

«23» декабря 2013 г.

м.п.

ПОЛИТИКА
информационной безопасности
МАОУ ДОД «ДШИ им. В.В. Знаменского»

г. Тюмень, 2013

Содержание

1. Введение

Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и «Постановления об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Правительством Российской Федерации от 01 ноября 2012 г. № 1119), на основании:

«Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного директором ФСТЭК от 05.01.2010 г. № 58;

«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 персоналу ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского», степень ответственности персонала, структура и необходимый уровень защищенности ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского».

2. Основные положения

Целью настоящей Политики является обеспечение безопасности объектов защиты 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 представлен в Перечне персональных данных, подлежащих защите.

Состав ИСПДн подлежащих защите, представлен в Перечне ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского».

Политика информационной безопасности была утверждена руководителем МАОУ ДОД «ДШИ им. В.В. Знаменского» и введена в действие Приказом № ____ от _____ 2013 г.

3. Область распространения.

Требования настоящей Политики распространяются на всех сотрудников МАОУ ДОД «ДШИ им. В.В. Знаменского» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4. Система защиты персональных данных.

Строится на основании:

- Актов обследования ИСПДн;
- Перечня персональных данных МАОУ ДОД «ДШИ им. В.В. Знаменского»;
- Актов классификации информационных систем персональных данных;

- Моделей угроз безопасности персональных данных;
- Положения об обработке и защите персональных данных в ИСПДн;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского». На основании анализа актуальных угроз безопасности ПДн, описанных в Модели угроз и Актов обследования ИСПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности 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.
- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

5. Состав 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 требуемого уровня защищенности ИСПДн, определенного в Акте классификации ИСПДн. В МАОУ ДОД «ДШИ им. В.В. Знаменского» было принято решение обеспечить 4-ый уровень защищенности для всех ИСПДн.

5.1.Подсистема управления доступом регистрации и учета

предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрация выдачи печатных (графических) материалов на бумажный носитель;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- 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. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

5.2.Подсистема обеспечения целостности и доступности

предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского», а также средств защиты, при случайной или намеренной модификации. В ней могут быть реализованные следующие функции:

- резервное копирование обрабатываемых данных;
- обеспечение целостности программных средств защиты персональных данных, обрабатываемой информации, а так же неизменность программной среды;
- периодическое тестирование функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных.

Реализуется с помощью организации резервного копирования обрабатываемых данных, проверкой контрольных сумм компонентов СЗИ при загрузке системы, ведением двух копий программных компонент средств защиты информации и их периодическим обновлением и контролем работоспособности, а также резервированием ключевых элементов ИСПДн.

5.3.Подсистема антивирусной защиты

предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского». В ней могут быть реализованы следующие функции:

- 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.

5.4.Подсистема межсетевого экранирования

предназначена для реализации следующих функций:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
- фильтрацию с учетом даты и времени;
- аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
- контроль целостности своей программной и информационной части;
- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

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

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

5.5.Подсистема анализа защищенности

должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского», которые могут быть использованы нарушителем для реализации атаки на систему. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами анализа защищенности.

5.6.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 обнаружения вторжений.

5.7.Подсистема криптографической защиты

предназначена для исключения НСД к защищаемой информации в ИСПДн при ее передачи по каналам связи сетей общего пользования и (или) международного обмена. Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

6. Пользователи ИСПДн.

В Политике информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности. Можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора безопасности ИСПДн;
- Оператора ИСПДн;
- Администратора сети;
- Программист-разработчик ИСПДн.

6.1. Администратор безопасности ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского»

- сотрудник, 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. 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.
- 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 безопасности уполномочен:

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

6.2.Оператор ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского»

- сотрудник, 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

6.3.Администратор сети МАОУ ДОД «ДШИ им. В.В. Знаменского»

- сотрудник, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности. 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.

6.4.Программисты-разработчики

(поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники МАОУ ДОД «ДШИ им. В.В. Знаменского», 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.

7. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники МАОУ ДОД «ДШИ им. В.В. Знаменского», 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 должностной инструкцией 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 МАОУ ДОД «ДШИ им. В.В. Знаменского»

- должны обеспечивать сохранность 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.
- должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
- 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.
- не могут устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
- не могут разглашать защищаемую информацию, которая стала им известна при работе с информационными системами (краткое наименование оператора), третьим лицам.
- обязаны при работе с ПДн в ИСПДн обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
- обязаны при завершении работы с ИСПДн защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
- 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.
- обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

8. Должностные обязанности пользователей ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского»

описаны в следующих документах:

- Инструкция администратора безопасности ИСПДн;
- Инструкция оператора ИСПДн;
- Инструкция сотрудника, ответственного за обработку ПДн;
- Инструкция по антивирусной защите;
- Инструкция по эксплуатации машинных носителей информации;
- Инструкция по организации парольной защиты;

9. Ответственность пользователей ИСПДн МАОУ ДОД «ДШИ им. В.В. Знаменского»

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего 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 безопасности ИСПДн несет ответственность за все действия, совершенные от имени своей учетной записи, если не доказан факт несанкционированного использования учетных записей.

При нарушениях операторами 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 должностных инструкциях пользователей ИСПДн.

Необходимо донести до пользователей ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

10. Список основных источников.

Основными нормативно-правовыми и методическими документами, на которых основывается настоящее Положение, являются:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;
- «Постановление об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Правительством Российской Федерации от 01 ноября 2012 г. № 1119);
- «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.;
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687;
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

- Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
- «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденное директором ФСТЭК от 05.01.2010 г. № 58

Уч. № ____ДСП

Отп. в ед. экз. на 11 листах

Экз. - в адрес МАОУ ДОД «ДШИ им. В.В. Знаменского»

Исп. А.А. Макаров, отп. А.А. Макаров

Тел. (3452)390-368

«23» декабря 2013 г.