УТВЕРЖДЕНА
приказом заведующего
от 11.01.2017 № 05/01-18
Е.В.Чикишева

ПОЛИТИКА

информационной безопасности оператора ИСПДн

Введение

Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных оператором Муниципального дошкольного образовательного учреждения «Детский сад № 3 «Лукошко» Тутаевского муниципального района (далее - МДОУ № 3 «Лукошко»).

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и на основании:

- Приказа ФСТЭК России от 5.02.2010 N 58 зарегистрирован в Минюсте России 19.02.2010 № 16456 "Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных "

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 оператора.

1. Общие положения

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

1.2. 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.

1.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

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

1.5. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

2. Область действия

2.1. Требования настоящей Политики распространяются на всех сотрудников оператора (штатных, временных, работающих по контракту и т.п.).

3. Система защиты персональных данных

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

- Перечня персональных данных, подлежащих защите;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;
- Руководящих документов ФСТЭК и ФСБ России.

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

- антивирусные средства для АРМ пользователей и серверов;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

4. Требования к подсистемам СЗПДн

4.1. СЗПДн включает в себя следующие подсистемы:

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

4.2. Подсистемы СЗПДн не имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

4.3. 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.

4.4. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

4.5. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн оператора.

4.6. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

4.7. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

4.8. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн оператора, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

4.9. Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн

5.1. В ИСПДн оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора безопасности ИСПДн;
- Администратор ИСПДн;
- Системный администратор;
- Пользователь ИСПДн;

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

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

5.6. Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;

- 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).

5.7. Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Администратор ИСПДн) получает возможность работать с элементами ИСПДн;

- осуществлять аудит средств защиты;

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

5.9. Пользователь 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.

5.10. Системный администратор, сотрудник оператора, 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.

5.11. Системный администратор 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.

6. Требования к персоналу по обеспечению защиты ПДн

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

6.2. При вступлении в должность нового сотрудника необходимо 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.

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

6.4. Сотрудники оператора, использующие технические средства аутентификации, 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.

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

6.6. Сотрудники оператора 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.

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

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

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

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

6.11. Сотрудники оператора 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.

6.12. Сотрудники 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.

7. Должностные обязанности пользователей ИСПДн

7.1. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция администратора;
- Инструкция о действии в случае возникновения внештатных ситуаций;
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;
- Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации информационной системе персональных данных;
- Инструкция о порядке работы при подключении к сетям общего пользования и международного обмена (Интернет).

8. Ответственность сотрудников ИСПДн оператора

8.1. 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).

8.2. Администратор безопасности несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

8.3. При нарушениях сотрудниками оператора - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

8.4. Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников оператора.