АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА
«ГОРОД КАЛИНИНГРАД»
КОМИТЕТ ПО ОБРАЗОВАНИЮ
муниципальное автономное дошкольное образовательное учреждение
города Калининграда центр развития ребенка - детский сад № 94

«Утверждаю»
Заведующий МАДОУ ЦРР д/с № 94
_____ Шевчук О.А.
«15» января 2013 г.

Политика информационной безопасности

г. Калининград
2013 г.

Введение

Настоящая Политика информационной безопасности (далее – Политика) ***муниципального автономного дошкольного образовательного учреждения города Калининграда центра развития ребенка - детского сада № 94*** (далее - Учреждения), разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- Федерального закона РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к работникам, допущенных для работы в информационных систем персональных данных (далее – ИСПДн), степень ответственности данных работников, структура и необходимый уровень защищенности ИСПДн Учреждения, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных (далее –ПДн) в ИСПДн Учреждения.

1. Общие положения

Целью настоящей Политики является: обеспечение безопасности объектов защиты Учреждения от всех видов угроз (внешних, внутренних, умышленных, непреднамеренных), минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - 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.

В Учреждении осуществляется своевременное обнаружение и реагирование на УБПДн, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты Учреждения утвержден приказами заведующего **«Об утверждении перечня информационных систем персональных данных, определении контролируемой зоны помещений», «О создании комиссии по уничтожению документов, об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных»**.

Состав персональных данных, обрабатываемых в ИСПДн Учреждении, подлежащих защите, утвержден приказом **«Об утверждении списка лиц, имеющих доступ к персональным данным, перечня персональных данных, подлежащих защите».**

Политика информационной безопасности была утверждена приказом по Учреждению **«О создании комиссии по уничтожению документов, об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».**

Требования настоящей Политики распространяются на всех работников Учреждения (штатных, работающих по различным видам договоров и т.п.), а также всех иных лиц.

2. Система защиты персональных данных

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

- аналитических отчетов по результатам обследования информационных систем персональных данных (далее – Аналитический отчет);
- частных моделей угроз безопасности персональных данных при их обработке в информационной системе персональных данных;
- перечня персональных данных, подлежащих защите;
- актов определения уровня защищенности персональных данных, при их обработке в информационной системе персональных данных;
- локальных актов Учреждения;
- организационно-распорядительной документации относящейся к системе защиты информации и персональных данных.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения.

На основании анализа актуальных угроз безопасности ПДн описанных в частных моделях угроз безопасности персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия отражаются в **Плане мероприятий по обеспечению безопасности персональных данных** Учреждения.

Для каждой ИСПДн в Аналитических отчетах составляется перечень используемых технических средств, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн, включающих в себя:

- перечень основных технических средств (далее – ОТСС);
- перечень вспомогательных технических средств, располагаемых совместно с ОТСС;
- перечень программного обеспечения, используемого в ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства защиты информации (далее – ТСЗИ):

- антивирусные средства для рабочих мест пользователей и серверов;
- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- средства технической защиты информации, используемые для защиты информации от несанкционированного доступа.

3. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрацией и учетом;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;

- анализа защищенности;
- обнаружения вторжений;
- отсутствие недекларированных возможностей.

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенного в акте определения уровня защищенности персональных данных, при их обработке в информационной системе персональных данных.

4. Пользователи ИСПДн

В ИСПДн Учреждения выделены следующие группы пользователей, участвующих в обработке и хранении ПДн:

- пользователи, имеющих доступ к персональным данным, в части выполнения своих должностных обязанностей;
- пользователи, непосредственно участвующие в обработке персональных данных, в части выполнения своих должностных обязанностей.

Данные о пользователях, уровне их доступа и информированности отражен в приказе по Учреждению «**Об утверждении списка лиц, имеющих доступ к персональным данным, перечня персональных данных, подлежащих защите».**

4.1. Пользователи (Оператор)

Пользователь - работник Учреждения, осуществляющий обработку ПДн.

Пользователи назначаются приказом по Учреждению **«Об утверждении списка лиц, имеющих доступ к персональным данным, перечня персональных данных, подлежащих защите».**

Пользователь имеет доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми знаниями для работы с ПДн;
- имеет личный идентификатор (имя пользователя) и аутентификатор (пароль).

5. Требования к персоналу по обеспечению защиты ПДн

Все работники Учреждения, являющиеся пользователями ИСПДн, должны четко знать, и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными со сборником руководящих инструкций по информационной безопасности Учреждения.

При вступлении в должность нового работника, ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в Учреждении (далее – Ответственный за обработку ПДн) обязан ознакомить работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучить его правилам работы с ПДн в ИСПДн.

Работники Учреждения должны быть ознакомлены с должностными инструкциями, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а так же с Положением об обработке и защите персональных данных Учреждения.

Работники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, возможность их утери, использования третьими лицами.

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

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

При работе с ПДн в ИСПДн работники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ).

При завершении работы с ПДн работники обязаны защитить АРМ с помощью блокировки (комбинация Ctrl-Alt-Del, далее Блокировка компьютера; комбинация Клавиша Windows+L).

Работники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Работники Учреждения должны быть ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности ПДн в соответствии с действующим федеральным законодательством Российской Федерации в области защиты информации и персональных данных.

Контроль за соблюдением режима безопасности ПДн возложен на Ответственного за обработку ПДн, в соответствии с приказом **«О проведении работ по обеспечению безопасности персональных данных».**

Работники Учреждения обязаны без промедления сообщать заведующему или Ответственному за обработку ПДн обо всех случаях работы ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Учреждения **ЗАПРЕЩАЕТСЯ**

- устанавливать постороннее программное обеспечение,
- подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
- разглашать защищаемую информацию, которая стала им известна при работе в информационных системах Учреждения третьим лицам.

6. Должностные обязанности пользователей (операторов) ИСПДн

Обязанности пользователей ИСПДн описаны в следующих организационно-распорядительных документах:

- инструкция пользователя информационных систем персональных данных;
- инструкция по организации режима доступа в помещения;
- должностных инструкциях работников Учреждения.

7. Ответственность работников Учреждения обрабатывающих ПДн в ИСПДн

Учреждение, как Оператор, обязано назначить работника, ответственного за организацию обработки персональных данных.

Работник, ответственный за организацию обработки персональных данных в Учреждении получает указания непосредственно от руководителя Учреждения и подотчетно ему.

Работник, ответственный за организацию обработки персональных данных в Учреждении, **ОБЯЗАН**:

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Учреждения положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (приказы, инструкции), требования к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных изложена в:

- Кодексе об административных правонарушениях Российской Федерации – статьи **5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2;**
- Уголовном Кодексе Российской Федерации – статьи **137, 140, 155, 183, 272, 273, 274, 292, 293;**
- Трудовом Кодексе Российской Федерации – статьи **81, 90, 195, 237, 391.**