АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА
«ГОРОД КАЛИНИНГРАД»
КОМИТЕТ ПО ОБРАЗОВАНИЮ
муниципальное автономное дошкольное образовательное учреждение
города Калининграда детский сад № 51

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
053917476B631C29DDF646FDFF7D64BC
Владелец: Ерошевич Маргарита Анатольевна
Действителен: с 20.06.2023 до 12.09.2024

Утверждаю
Заведующий МАДОУ д/с № 51
_____/Ерошевич М.А./

Политика информационной безопасности

г. Калининград
2017 г.

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;

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.