АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА «ГОРОД КАЛИНИНГРАД»
КОМИТЕТ ПО СОЦИАЛЬНОЙ ПОЛИТИКЕ
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА КАЛИНИНГРАДА
ДЕТСКАЯ МУЗЫКАЛЬНАЯ ШКОЛА «ЛИРА»

УТВЕРЖДАЮ
Директор

_____ Э.Б. Ляшенко

«19» марта 2018 г.

м.п.

Политика информационной безопасности

г. Калининград
2018 г.

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – **Политика**) ***муниципального автономного учреждения дополнительного образования Детская музыкальная школа «Лира»*** (далее – Учреждение) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В **Политике** определены требования к работникам, допущенным для работы в информационных системах персональных данных (далее – ИСПДн), степень ответственности данных работников, структура и необходимый уровень защищенности ИСПДн Учреждения, статус и 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 и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты утвержден приказами директора Учреждения:

- «Об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений»;
- «О создании комиссии по уничтожению документов, об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных, внесении изменений в должностные инструкции».

Состав ПДн, подлежащих защите, утвержден приказом директора Учреждения:

- «Об утверждении перечня персональных данных, подлежащих защите, списка лиц, имеющих доступ к персональным данным, установление им прав доступа к информационным и техническим ресурсам».

Настоящая **Политика** утверждена приказом директора Учреждения:

- «О создании комиссии по уничтожению документов, об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных, внесении изменений в должностные инструкции».

Требования настоящей **Политики** распространяются на всех работников Учреждения, а также всех иных лиц, взаимодействующих с Учреждением.

2. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

- результатов обследования информационных систем персональных данных Учреждения;
- перечня персональных данных, подлежащих защите;
- приказов по Учреждению;
- организационно-распорядительной документации, относящейся к системе защиты информации и персональных данных Учреждения;
- руководящих документов ФСТЭК и ФСБ России.

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

На основании анализа актуальных угроз безопасности ПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн Учреждения.

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

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.

Список используемых технических средств защиты отражается в «Журнале учета средств защиты».

Список используемых технических средств защиты информации должен поддерживаться в актуальном состоянии. При изменении состава ТСЗИ соответствующие изменения должны быть внесены в «Журнал учета средств защиты».

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 информационных системах персональных данных Учреждения.

4. ПОЛЬЗОВАТЕЛИ ИСПДН

Данные о пользователях, уровне их доступа и информированности отражены в приказе по Учреждению:

- «Об утверждении перечня персональных данных, подлежащих защите, списка лиц, имеющих доступ к персональным данным, установление им прав доступа к информационным и техническим ресурсам».

4.1. Пользователи

Пользователь - работник Учреждения, осуществляющий обработку ПДн.

Пользователи назначаются приказом директора Учреждения:

- «Об утверждении перечня персональных данных, подлежащих защите, списка лиц, имеющих доступ к персональным данным, установление им прав доступа к информационным и техническим ресурсам».

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) знакомит работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучает его правилам работы с ПДн в ИСПДн.

Работники Учреждения под роспись знакомятся с должностными инструкциями, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а также с Положением об обработке и защите персональных данных Учреждения.

Работники Учреждения, использующие технические средства аутентификации, в обязательном порядке обеспечивают сохранность идентификаторов (электронных ключей) и не допускают НСД к ним, возможности их утери, использования третьими лицами.

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

Работники Учреждения ознакомлены с правилами обеспечения надлежащей защиты оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Все работники, как пользователи, ознакомлены с требованиями по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также знают свои обязанности по обеспечению такой защиты.

При работе с ПДн работники Учреждения ознакомлены с требованиями обеспечения отсутствия возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ) или терминалов.

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

Работники Учреждения проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

Работники Учреждения 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 обработки ПДн возложен на Ответственного в соответствии с приказом директора Учреждения:

- «О назначении ответственного за обработку персональных данных, об утверждение комиссии по проведении работ по обеспечению безопасности персональных данных, разработке организационно-распорядительной документации».

Работники Учреждения, допущенные к работам с техническими средствами защиты, обязаны пройти обучение по правилам работы, хранения и учета технических средств защиты информации.

Работники Учреждения обязаны без промедления сообщать директору, Ответственному 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 также записывать на них защищаемую информацию.
- разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения третьим лицам.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ (ОПЕРАТОРОВ) ИСПДН

Должностные обязанности пользователей ИСПДн описаны в следующих организационно-распорядительных документах:

- инструкции ответственного за организацию обработки персональных данных;
- инструкции пользователя информационных систем персональных данных;
- инструкции по организации режима доступа в помещения;
- Положении об обработке и защите персональных данных;
- должностных инструкциях работников Учреждения.

7. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ УЧРЕЖДЕНИЯ, ОБРАБАТЫВАЮЩИХ ПДН В ИСПДН

Учреждение, как Оператор, **ОБЯЗАНО** назначить лицо, ответственное за организацию обработки персональных данных, в соответствии с приказом директора:

- «О назначении ответственного за обработку персональных данных, об утверждение комиссии по проведении работ по обеспечению безопасности персональных данных, разработке организационно-распорядительной документации».

Лицо, ответственное за организацию обработки персональных данных в Учреждении получает указания непосредственно от директора Учреждения и подотчетно ему.

Должностное лицо, ответственное за организацию обработки персональных данных в Учреждении, **ОБЯЗАНО**:

- 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.

Для решения вопросов по расследованию инцидентов информационной безопасности, возникших при обработке персональных данных и другой конфиденциальной информации, в Учреждении создана комиссия, утвержденная приказом директора:

- «О создании комиссии по уничтожению документов, об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных, внесении изменений в должностные инструкции».

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

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