ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КАЛИНИНГРАДСКИЙ ОБЛАСТНОЙ МУЗЫКАЛЬНЫЙ КОЛЛЕДЖ ИМ. С.В. РАХМАНИНОВА»

УТВЕРЖДАЮ

Директор ГБПОУ КОМК
им. С.В. Рахманинова

_____ С.Г. Грибовская

«17» ноября 2017 года

ПОЛИТИКА

информационной безопасности

г. Калининград
2017 г.

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – **Политика**) **государственного бюджетного образовательного учреждения среднего профессионального образования «Калининградский областной музыкальный колледж им. С.В. Рахманинова»** (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 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18 Февраля 2013 № 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, допущенных для работы в информационных систем 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 **только** 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 Учреждения утвержден приказами директора

- **«Об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений, администратора информационной безопасности, сроков подготовки документов»**;
- **«Об определении мест хранения материальных носителей персональных данных, внесении изменений в должностные инструкции».**

Состав ПДн подлежащих защите, утвержден приказом директора:

- **«Об утверждении списка лиц, имеющих доступ к персональным данным, перечня персональных данных, подлежащих защите».**

Политика утверждена приказом директора Учреждения:

- **«О назначении комиссии в по уничтожению документов, утверждении документов».**

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:

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

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, технических заданиях на разработку системы защиты информационных систем персональных данных делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия заносятся в:

- **План мероприятий по обеспечению безопасности персональных данных Учреждения.**

План мероприятий по обеспечению безопасности персональных данных утверждается приказом директора Учреждения:

- **«О проведении работ по обеспечению безопасности персональных данных».**

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 криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи.

Список используемых ТСЗИ отражается в:

- ***«Журнале учета средств защиты».***

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

Список используемых криптографических средств защиты (далее – КСЗИ) отражается в:

- ***«Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».***

Список используемых КСЗИ должен поддерживаться в актуальном состоянии. При изменении состава КСЗИ соответствующие изменения должны быть внесены в «Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

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 не декларированных возможностей;
- криптографической защиты.

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 Учреждения.

4. ПОЛЬЗОВАТЕЛИ ИСПДН

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

- администратор информационной безопасности;
- пользователь.

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

- **«Об утверждении списка лиц, имеющих доступ к персональным данным и перечня персональных данных, подлежащих защите»;**
- **«Об утверждении списков постоянных пользователей информационных систем персональных данных, допущенных в помещения и установлении им прав доступа к информационным и техническим ресурсам».**

4.1. Администратор информационной безопасности

Администратор информационной безопасности (далее – Администратор ИБ), штатный работник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку клиентской и серверной составляющих.

Администратор ИБ назначается приказом директора Учреждения:

- **«Об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений, администратора информационной безопасности, сроков подготовки документов».**

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор ИБ уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;

- ❖ устанавливать доверительные отношения своей защищенной сети с сетями других учреждений;
- ❖ осуществлять внутренние проверки режима защиты персональных данных в информационных системах персональных данных.

Сведения о проведении внутренних проверок фиксируются в **«Журнале внутренних проверок режима защиты персональных данных в информационных системах персональных данных»**.

4.2. Пользователи

Пользователь - работник Учреждения, осуществляющий обработку ПДн.

Пользователи назначаются приказом директора Учреждения:

- **«Об утверждении списка лиц, имеющих доступ к персональным данным и перечня персональных данных, подлежащих защите»,**
- **«Об утверждении списков постоянных пользователей информационных систем персональных данных, допущенных в помещения и установлении 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 Учреждения (далее – Ответственный за обработку ПДн) 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 так же 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, возможность 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 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 за обработку ПДн, в соответствии с приказом директора Учреждения:

- **«О проведении работ по обеспечению безопасности персональных данных».**

Контроль за выполнением технических мероприятий по обеспечению безопасности ПДн возложен на ответственного за эксплуатацию объекта информатизации (далее – Ответственный за ЭОИ), в соответствии с приказом директора Учреждения:

- **«О проведении работ по обеспечению безопасности персональных данных».**

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

Допуск работников Учреждения со средствами криптографической защиты информации утверждается приказом директора Учреждения:

- **«О защите персональных данных, обрабатываемых в информационных системах персональных данных, создании**

комиссии по расследованию инцидентов информационной безопасности, допуске лиц к работе со средствами криптографической защиты информации».

Работники Учреждения обязаны без промедления сообщать директору, Ответственному за обработку ПДн, Ответственному за ЭОИ 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 с информационными системами Учреждения третьим лицам.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ (ОПЕРАТОРОВ) ИСПДН

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

- инструкции ответственного за организацию обработки персональных данных;
- инструкции ответственного за эксплуатацию объекта информатизации;
- инструкции пользователя информационных систем персональных данных;
- инструкции по организации режима доступа в помещения;
- инструкции о порядке организации учета хранения и выдачи электронных (машинных) носителей информации;
- инструкции о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных;

- Положении по использованию средств криптографической защиты информации;
- руководстве ответственного пользователя средств криптографической защиты информации;
- руководстве пользователя средств криптографической защиты информации;
- инструкции по организации защиты средств криптографической защиты информации;
- инструкции о порядке учёта, хранения, выдачи и уничтожения средств криптографической защиты информации.
- должностных инструкциях (регламентах) 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 проведении работ по обеспечению безопасности персональных данных».**

Лицо, ответственное за организацию обработки персональных данных в Учреждения получает указания непосредственно от директора 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 Учреждения создана комиссия, и утверждена приказом директора:

- **«О защите персональных данных, обрабатываемых в информационных системах персональных данных, создании комиссии по расследованию инцидентов информационной безопасности, допуске лиц к работе со средствами криптографической защиты информации».**

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.**

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