УТВЕРЖДЕНО
приказом МБУДО «Детская
музыкальная школа №4» г. Кирова
от 01.10.2024 № 85-ОД

Инструкция по организации парольной защиты

1. Введение

1.1. В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативно-правовых актов настоящая инструкция определяет порядок действий администратора безопасности и пользователей информационной системы (далее - ИС) при прохождении процедур идентификации (узнавания) и аутентификации (подтверждении подлинности узнанного) в ИС.

1.2. Настоящая инструкция устанавливает требования к управлению процессом опознавания пользователей и устройств, полномочных осуществлять обработку конфиденциальной информации, в том числе персональных данных (далее - ПДн), в ИС на стадии ее эксплуатации.

2. Порядок идентификации и аутентификации пользователей ИС, являющихся сотрудниками МБУДО «Детская музыкальная школа №4» города Кирова (далее - учреждение).

2.1. Всем пользователям ИС, являющимся сотрудниками учреждений допущенным в установленном порядке к работе с ИС, присваиваются учетные записи в виде персональных идентификаторов. Идентификаторы определяют доступ к техническим средствам и информационным ресурсам ИС и системы защиты информации.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и передаётся пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в ИС и пароль, обеспечивающий аутентификацию (проверку подлинности) в ИС. Права пользователя по доступу к информационным ресурсам ИС, определяется списком (матрицей) доступа в соответствии с «Положением о разрешительной системе доступа».

2.3. Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более 90 дней. Персональные идентификаторы должны быть удалены из ИС при увольнении сотрудника, МБУДО «Детская музыкальная школа №4» г.

Кирова немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИС.

2.4. При приеме (увольнении) на работу сотрудника учреждения или изменении полномочий (временное или бессрочное) действующего сотрудника учреждения, включение (исключение) его данных в список доступа к информационным ресурсам ИС и генерацию (уничтожение) идентификатора и пароля, производит администратор безопасности на основании приказа директора о предоставлении (запрете) сотруднику доступа к информационным ресурсам ИС и утвержденного в учреждении перечня должностей, допущенных к обработке конфиденциальной информации, в том числе ПДн.

2.5. Первичный пароль генерируется администратором безопасности в момент создания идентификатора и выдается пользователю под роспись в журнале учета выдачи паролей (Приложение № 1 к настоящей инструкции).

2.6. При первом доступе пользователь обязан изменить выданный ему пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции (п. 2.7).

2.7. Требования к сложности пароля:

2.7.1. длина пароля должна быть не менее шести символов;

2.7.2. в числе символов пароля должны присутствовать строчные и прописные буквы;

2.7.3. пароль не должен включать в себя легко вычисляемые значения символов (имена, фамилии, имена детей или домашних животных, наименования информационных систем, типичных для организации профессиональных терминов, номера телефонов, номера или марки автомобилей, адреса и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

2.7.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в трех символах;

2.7.5. Пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.8. Администратор безопасности осуществляет настройку в информационной системе параметров количества вводов неправильного пароля. Количество вводов неправильного пароля устанавливается равным 3. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

2.9. Администратор безопасности организует настройку в информационной системе параметров блокирования сеанса доступа при времени бездействия пользователя более 30 минут или по запросу пользователя.

3. Порядок управления аппаратными средствами аутентификации

3.1. Выдачу, инициализацию, блокирование и утилизацию аппаратных средств аутентификации организует администратор безопасности.

3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор безопасности в журнале учета аппаратных средств аутентификации (Приложение № 2 к настоящей инструкции).

4. Порядок идентификации/аутентификации внешних пользователей ИС

4.1. Присвоение идентификатора и выдача атрибутов аутентификации внешним пользователям ИС, осуществляется администратором безопасности. Учет внешних пользователей, допущенных к обработке конфиденциальной информации, в том числе ПДн, осуществляет администратор безопасности в матрице доступа.

4.2. Выдачу и смену паролей, учет паролей, учет аппаратных средств аутентификации внешних пользователей, допущенных к обработке конфиденциальной информации, в том числе ПДн, организует администратор безопасности по правилам п.2, п.3 настоящей инструкции.

5. Обязанности пользователя ИС

5.1. Пользователь ИС является частью системы защиты информации и обязан соблюдать следующие правила информационной безопасности:

5.1.1. Помнить свой идентификатор и пароль.

5.1.2. Обеспечивать сохранность полученных аппаратных идентификаторов. Не предоставлять доступ к личному аппаратному идентификатору никому, кроме администратора безопасности.

5.1.3. Держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Администрации, в т.ч. руководителей) личный пароль.

5.1.4. Осуществлять ввод пароля только в условиях, исключающих его просмотр.

5.1.5. Не хранить записки-памятки с личным паролем на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.

5.1.6. Своевременно сообщать администратору безопасности о фактах компрометации пароля (когда пароль стал или может быть известен еще кому-либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИС до специального разрешения администратора безопасности.

6. Обязанности администратора безопасности

6.1. Администратор безопасности осуществляет организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИС, контроль действий пользователей ИС при их работе с персональными идентификаторами и паролями доступа.

6.2. Администратор безопасности обязан:

– создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИС;

– обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней;

– свой собственный пароль администратор безопасности должен изменять не реже одного раза в месяц;

– принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов;

– сообщать ответственному по организации обработки конфиденциальной информации, в том числе ПДн, о подобных инцидентах;

– выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.

6.3. Действия администратора безопасности при компрометации паролей и утрате аппаратных идентификаторов.

6.3.1. Заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора, к ИС.

6.3.2. Выявить действия, произведенные в ИС с использованием скомпрометированных персональных идентификаторов и паролей доступа.

6.3.3. Доложить ответственному за организацию обработки конфиденциальной информации, в том числе ПДн, об инциденте и предоставить результаты анализа инцидента.

6.3.4. Совместно с ответственным за организацию обработки конфиденциальной информации, в том числе ПДн, определить необходимость расследования инцидента.

6.3.5. Создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИС.

7. Заключительные положения

7.1. Пользователи ИС должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей инструкции.

7.2. Пользователи ИС должны быть ознакомлены с настоящей инструкцией до начала работы с ИС.

7.3. Обязанность ознакомления пользователей с настоящей инструкцией лежит на ответственном за организацию обработки конфиденциальной информации, в том числе ПДн.

Приложение № 1
к Инструкции по организации парольной защиты

МБУДО «Детская музыкальная школа №4» города Кирова
(наименование организации)

Журнал (форма)
учета выдачи паролей

Дата начала «01» октября 2024 г.

Дата окончания «___» _____ 20 __

№ п/п	Ф.И.О.	Тип пользователя	Персональный идентификатор	Дата выдачи	Подпись	Примечания

Приложение № 2
к Инструкции по организации парольной защиты

МБУДО «Детская музыкальная школа №4» города Кирова
(наименование организации)

ЖУРНАЛ (форма)

учета аппаратных средств аутентификации

Дата начала «___» _____ 20 __

Дата окончания «___» _____ 20 __

ИНВ. №	Дата периодического осмотра	Результат периодического осмотра	Подпись лица, производившего осмотр	Место нахождения	Дата выдачи в индивидуальное пользование	Ф.И.О. Подпись индивидуального пользователя	Примечание