Приложение № 1
к приказу № 78/2-ОД от 16.08.2021г

Инструкция
по организации парольной защиты в информационной системе МБДОУ «Ерёминский детский сад»»

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационной системе МБДОУ «Ерёминский детский сад» (далее – Инструкция) определяет порядок использования, генерации, смены и прекращения действия паролей пользователей в информационной системе МБДОУ «Ерёминский детский сад»(далее –ИС), а также контроль действий пользователя при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на администратора безопасностиИС.

2. Требования к организации парольной защиты

2.1. Формирование и учет паролей по доступу к базовым системам ввода вывода компьютеров, настройкам сетевого оборудования, настройкам операционных систем по запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации, настройкам средств защиты информации осуществляется администратором безопасности ИС.

2.2. Устанавливаемые пароли пользователей ИС должны соответствовать следующим требованиям:

– длина пароля должна быть не менее 8 символов;
– максимальный срок действия пароля не более 90 дней;
– алфавит пароля не менее 70 символов;
– пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);
– использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
– использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;
– новое значение пароля не должно совпадать с одним из четырех предыдущих значений;
– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.3. Устанавливаемые пароли администраторов ИС должны соответствовать следующим требованиям:

– длина пароля должна быть не менее 8 символов;
– максимальный срок действия пароля не более 30 дней;

– алфавит пароля не менее 70 символов;

– пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);

– использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

– использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;

– новое значение пароля не должно совпадать с одним из четырех предыдущих значений;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

– запрещается регистрировать пользователей в системе под своим паролем;

– пароли на доступ к различным ресурсам должны различаться, не допускается использование универсальных паролей для административных учетных записей.

2.4. После 15 минут бездействия (неактивности) пользователя в ИС происходит автоматическое блокирование сеанса доступа в ИС. Разблокирование учетной записи осуществляется пользователем путем ввода своего пароля.

2.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности ИС и изменить пароль.

2.6. Восстановление забытого пароля пользователя осуществляется администратором безопасности ИС на основании письменной либо электронной заявки пользователя.

2.7. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

2.8. Для предотвращения несанкционированного доступа в ИС должен быть реализован механизм блокировки учетной записи при трехкратном неправильном вводе пароля, разблокировку учетной записи производит администратор безопасности.

2.9. Пользователи и администраторы ИС обязаны:

– сохранять в тайне свой личный пароль;

– четко знать и строго выполнять требования настоящей Инструкции;

– своевременно сообщать лицу, ответственному за защиту информации в ИС, обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.10. При организации парольной защиты запрещается:

– умышленное и неумышленное несанкционированное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;

– запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;

– вход в систему с использованием чужих идентификаторов или паролей;

– сообщать посторонним лицам, в том числе сотрудникам МБДОУ «Ерёминский детский сад»свои пароли, а также пересылать открытым текстом в электронных сообщениях.

3

3. Порядок применения парольной защиты

3.1. Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к защищаемым ресурсам.

3.2. Набор личного пароля следует проводить, предварительно убедившись в отсутствии лиц, которые могут его увидеть.

3.3. При временном отсутствии на рабочем месте следует произвести блокировку компьютера.

3.4. Полная плановая смена паролей производится регулярно, не реже одного раза в 90 дней. Смена личных паролей пользователей осуществляетсяадминистратором безопасности ИС. Смена паролей по доступу к базовым системам ввода вывода компьютеров, настройкам сетевого оборудования, настройкам операционных систем по запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации, настройкам средств защиты информации осуществляется администратором безопасности ИС.

3.5. Внеплановая смена (удаление) личного пароля любого пользователя производится в следующих случаях:

– по окончании срока действия пароля;

– в случае прекращения полномочий пользователя (увольнение);

– при обнаружении факта успешной попытки несанкционированного доступа к элементам ИС;

– при обнаружении факта компрометации пароля.

3.6. Внеплановая полная смена паролей всех пользователей, а также паролей по доступу к базовым системам ввода вывода компьютеров, настройкам сетевого оборудования, настройкам операционных систем по запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации, настройкам средств защиты информации, должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности ИС.

3.7. Скомпрометированные пароли выводятся из действия немедленно.

3.8. По каждому случаю, связанному с компрометацией действующих паролей, ответственным за защиту информации в ИС организуется и проводится служебная проверка.

3.9. Результаты служебнойпроверки в виде служебной записки предоставляются руководству МБДОУ «Ерёминский детский сад». По результатам проверки лица, допустившие разглашение паролей, привлекаются к дисциплинарной ответственности.

3.10. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3.11. Контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности ИС.

Разработчик инструкции заведующий
МБДОУ «Ерёминский детский сад» Лукошенко Л.В. _____

Лист ознакомленияс инструкцией по организации парольной защиты в информационной системе МБДОУ «Ерёминский детский сад»

№ п/п	Ф.И.О. работника	Дата ознакомления	Личная подпись