

Муниципальное бюджетное учреждение дополнительного образования
«Варгашинский детско – юношеский центр»

ПРИКАЗ

22.09.2020 года

№ 39-ОД

«Об утверждении инструкции по организации
парольной защиты в информационных системах
персональных данных »

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по организации парольной защиты в информационных системах персональных данных в МБУ ДО «Варгашинский детско-юношеский центр», согласно приложению к настоящему приказу.
2. Контроль за выполнением данного приказа оставляю за собой.

Директор



Л.А. Барышева

Приложение к приказу
МБУДО «Варгашинский детско – юношеский
центр» от 22 сентября 2020 года № 39 - ОД
«Об утверждении инструкции по организации
парольной защиты в информационных
системах персональных данных»

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах персональных данных

I. Общие положения

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) в информационной системе персональных (далее – ИСПДн) в МБУ ДО «Варгашинский детско – юношеский центр», (далее – Учреждение).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник ДОУ, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль над действиями Пользователей в ИСПДн осуществляет ответственный за обеспечение безопасности персональных данных в Учреждении (далее – Ответственный).

1.5. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) Пользователей осуществляет администратор ИСПДн в Учреждении (далее – Администратор).

II. Организация парольной защиты

2.1. Личные пароли должны создаваться Пользователями самостоятельно.

2.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

2.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

2.4. Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

2.5. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

2.6. Разблокирование учетной записи осуществляется Администратором и Ответственным для учетных записей Пользователя для АРМ и для ИСПДн соответственно.

2.7. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

III. Требования к формированию паролей

Пользователи при формировании паролей должны руководствоваться следующими требованиями:

- 3.1. Длина пароля должна быть не менее 8 символов.
- 3.2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:
 - буквы в верхнем регистре;
 - буквы в и нижнем регистре;
 - цифры;
 - специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, \$, &, *, % и т.п.).
- 3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).
- 3.4. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.
- 3.5. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.
- 3.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «111111», «wwwwww» и т.п.).
- 3.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).
- 3.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

IV. Правила ввода паролей

Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны руководствоваться следующими правилами:

- 4.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
- 4.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).
- 4.3. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн, Пользователю необходимо уведомить Администратора или Ответственный соответственно для проведения процедуры генерации нового пароля.

V. Обязанности

Пользователи ИСПДн обязаны:

- 5.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов ДООУ по парольной защите.
- 5.2. Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.
- 5.3. Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

VI. Ответственность

- 6.1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и к ИСПДн.