

СОГЛАСОВАНО

Педагогическим советом

протокол от «28» 12 20 23 г № 2 Директор МБУДО «ДТ «Русинка»

УТВЕРЖДЕНО



Ю.А. Тиркина

Приказ от «28» 12 20 23 г № 152/3
(Приложение № 23)

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации в МБДОУ «ДТ «Русинка»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в муниципальном бюджетном учреждении дополнительного образования «Дворец творчества «Русинка» г. Волжского Волгоградской области» (далее – Учреждение).

1.2. Данное положение разработано в соответствии с Конституцией РФ; Федеральным законом от 29.12.2012г. №273-ФЗ «Об образовании в Российской Федерации» в редакции от 25 июля 2022 года; Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006г. (в редакции федеральных законов от 27.07.2010 № 227-ФЗ,; Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27.07.2006г. (в ред. Федеральных законов от 14.07.2022 N 266-ФЗ,); Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997г. (в редакции указов Президента Российской Федерации от 23.09.2005 № 1111; от 13.07.2015 № 357)

1.3. Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении. Цель Положения определяет требования Учреждения к парольной защите информационных систем. Область действия Положения распространяется на всех пользователей и информационные системы (далее - ИС), использующих парольную защиту.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ИС

В данном случае любая информационная система, для работы с которой необходима аутентификация пользователя. Пароль - секретный набор символов, используемый для аутентификации пользователя. Пользователи - администраторы ИС и работники Учреждения, которым предоставлен доступ к ИС Учреждения, а также корпоративный доступ к ресурсам сети Интернет. Учетная запись - идентификатор пользователя, используемый для доступа к ИС

3. ПОЛОЖЕНИЯ

Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователем ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

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.

При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых 3 сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу ИС немедленно после окончания последнего сеанса работы данного Пользователя с системой. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на заместителя заведующего.

4. РОЛИ И ОТВЕТСТВЕННОСТЬ

Пользователи:

Исполняют требования Положения и несут ответственность за ее нарушение. Информировуют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

Администратор парольной защиты:

Принимает обращения пользователей по вопросам парольной защиты (например, блокировка учетных записей, нарушение Положения и др.). Организует консультации пользователей по вопросам использования парольной защиты. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования. Отвечает за безопасное хранение паролей встроенных административных учетных записей.