

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации в МБУ ДО Центре «Эдельвейс»

1. Общие положения

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 МБУ ДО Центре «Эдельвейс» (далее – Центр).

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

1. 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 Общества или сторонней организации, которым предоставлен доступ к ИС Общества, а также корпоративный доступ к ресурсам сети Интернет.

Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

III. Положения о паролях

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

- длина пароля должна быть не менее 6-8 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 подпись 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 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 сотрудников МБУ ДО Центра «Эдельвейс» на которых возложена эта ответственность руководителем.

1. Роли и ответственность

Пользователи:

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

Администратор парольной защиты:

-Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных 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.