Государственное автономное образовательное учреждение дополнительного образования
«Центр для одаренных детей «Поиск»

УТВЕРЖДАЮ
Директор Центра

А. В. Жигайлов
«28» декабря 2020 г.

И Н С Т Р У К Ц И Я

по организации парольной защиты автоматизированной системы Центра «Поиск»

1. Общие положения

1.1. Инструкция по организации парольной защиты автоматизированной системы Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ «О персональных данных», Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе Государственного автономного образовательного учреждения дополнительного

образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»), а также контроль за действиями пользователей системы при работе с паролями.

1.3. Непосредственную ответственность за надлежащее выполнение инструкции всеми сотрудниками Центра «Поиск» несет директор Центра.

1.4. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Поиск» и не исключает обязательного выполнения их требований.

1.5. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Генерация и смена паролей

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы (далее – АС) Центра «Поиск», контроль за действиями пользователей системы при работе с паролями возлагается на администратора информационной безопасности.

2.2. Личные пароли пользователей АС должны генерироваться и распределяться централизованно, либо выбираться пользователями самостоятельно с учетом следующих требований:

– Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– Пароль должен состоять не менее чем из 6 символов.

– В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации об Операторе.

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

– Запрещается выбирать пароли, которые уже использовались ранее.

– При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

2.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

2.4. Для генерации паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления ответственных за информационную безопасность с паролями других сотрудников Центра «Поиск».

2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

2.6. Внеплановая смена личного пароля или удаление учетной записи пользователя АС в случае прекращения его полномочий должна производиться

администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

2.8. В случае компрометации личного пароля, пользователь АС должен немедленно сообщить об этом администратору информационной безопасности.

3. Хранение паролей

3.1. Не допускается хранение паролей на бумажных носителях в зоне свободного доступа.

3.2. Хранение пользователем значений своих паролей на бумажном носителе допускается в сейфе у заместителя директора по информационным и коммуникационным технологиям.

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