Инструкция по организации парольной защиты в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

1. Общие положения

1.1. Инструкция по организации парольной защиты разработана с целью обеспечения требований информационной безопасности в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства» в соответствии с Доктриной информационной безопасности Российской Федерации», утвержденной указом Президента Российской Федерации от 05.12.2016 № 646, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральным законом Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных».

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированных системах, подсистемах, прикладных задачах, и т.д. (далее – АС), Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства» (включая информационный системы персональных данных - ИСПДн), а также контроль за действиями пользователей системы при работе с паролями.

1.3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения комплексной безопасности защищаемой информации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства».

1.4. Нарушение настоящей Инструкции влечет за собой 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, контроль за действиями пользователей системы при работе с паролями, возлагается на администратора информационной безопасности.

2.2. Пароли должны выбираться, и вводится 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 (спец.символы),

например, !, $, #, %, и т.д.

- Не разрешается использовать в качестве пароля имя входа в систему, простые пароли типа «123...», «111…», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе, об учреждении.

- Не разрешается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

- Не разрешается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, qazwsx, 123456, и т.п.).

- Не разрешается выбирать пароли, которые уже использовались ранее. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

Для автоматизации выполнения требований по парольной защите допускается применение администратором локальной вычислительной сети соответствующих доменных политик.

2.3. Плановая смена паролей пользователем должна проводиться регулярно, не реже одного раза в год.

2.4. Смена паролей в операционной системе Windows производится при нажатии комбинации клавиш <Ctrl>, <Alt>, <Del>. И далее, в соответствующем поле вводятся старый пароль, а затем - новый (новый пароль вводится с подтверждением, т.е. дважды).

2.5. 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, а также в случае необходимости применения действий администратором, направленных на ликвидацию (предотвращение) нештатной ситуации.

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

2.7. В случае компрометации личного пароля, пользователь АС должен немедленно сообщить об этом администратору информационной безопасности и предпринять меры по смене пароля.

3. Хранение паролей

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

4. Контроль

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