Требования к парольной защите
в Красноярском аграрном техникуме

1. Общие положения

1.1. Пароль - один из важнейших аспектов информационной безопасности, так как плохо подобранный пароль повышает потенциальный риск несанкционированного доступа в информационно-телекоммуникационную систему техникума.

1.2. Все пользователи интрасети техникума (включая преподавателей, сотрудников и обучающихся) несут ответственность за выполнение настоящего документа. В случае нарушения учётные записи блокируются до устранения причин блокировки.

1.3. Цель настоящего документа установить стандарты создания сложных паролей, их защиту, хранение и частоту изменения.

2. Требования к паролям пользователей интрасети

2.1. Все пароли пользователей, в том числе системные пароли должны соответствовать данным требованиям настоящего документа, а также удовлетворять признакам сложных паролей (п.4.3).

2.2. Срок действия паролей учетных записей пользователей домена должен составлять не более 6 месяцев.

2.3. Пароли пользователей, имеющих административные привилегии в информационных системах, должны изменяться ежеквартально и быть уникальными по отношению к паролям других учетных записей данного пользователя.

2.4. Пароль не должен совпадать с тремя последними используемыми паролями пользователя.

2.5. Все пароли системных учетных записей, а также пароли приложений и активного оборудования необходимо хранить в недоступном месте (сейф, зашифрованная база данных и т.д.).

2.6. Пользователям **запрещается**:

2.6.1. использовать один и тот же пароль для доступа к учётным записям техникума и к другим ресурсам (например, доступ к Интернету из дома, PIN- код кредитной карты и т. д.);

2.6.2. использовать один и тот же пароль для различных аккаунтов (например, для учётной записи пользователя интрасети и для учётной записи с административными привилегиями);

2.6.3. сообщать кому-либо свой пароль, в том числе подчинённым, начальнику,

коллегам по работе, членам своей семьи, т.к. пароли являются конфиденциальной информацией;

2.6.4. сообщать свой пароль по телефону;

2.6.5. отправлять свой пароль по электронной почте;

2.6.6. говорить о своём пароле рядом с посторонними;

2.6.7. упоминать о содержимом пароля (например, «мой день рождения»);

2.6.8. указывать свой пароль в анкетах или опросниках;

2.6.9. сообщать свой пароль сослуживцам перед уходом в отпуск;

2.6.10. записывать пароль и хранить его на рабочем месте;

2.6.11. хранить пароль в файле на компьютере, включая переносной, без шифрования.

2.7. В случае компрометации вашей учётной записи или пароля сообщите об этом в инженеру-электронику и смените все пароли.

3. Требования к разработчикам программного обеспечения

3.1. Разработчики программного обеспечения (ПО) должны обеспечить в своих программах следующие меры безопасности:

3.1.1. Программы должны поддерживать аутентификацию отдельных пользователей, а не групп.

3.1.2. Программы должны хранить пароли в зашифрованном (но не в открытом или легкораскрываемом) виде согласно действующему законодательству РФ.

3.1.3. Программы должны обеспечивать своего рода передачу прав, чтобы один пользователь мог выполнять функции другого, не зная его пароль.

4. Рекомендации по созданию пароля пользователей интрасети

4.1. В техникуме используются пароли для различных целей: доступ к электронной почте, в личный кабинет, доступ к различным автоматизированным системам. Следует знать, как выбрать стойкий пароль.

4.2. Признаки простых, небезопасных паролей:

4.2.1. содержат менее восьми символов;

4.2.2. являются словом, которое содержится в словарях (русских или иностранных);

4.2.3. являются часто употребляемым словом;

4.2.4. содержат фамилию, кличку животного, имена друзей, сотрудников, вымышленных персонажей и т. д.;

4.2.5. содержат компьютерные термины и названия, команды, названия сайтов, организаций, оборудования, программного обеспечения;

4.2.6. содержат название техникума или географические наименования, например «КАТ» или его производные;

4.2.7. содержат даты рождения и иную личную информацию, например, адреса или номера телефонов;

4.2.8. содержат слово или число по шаблону типа: аааббб, qwerty, zyxwvuts, 12345 и т.д. или их обратная последовательность.

4.3. Признаки сложных, безопасных паролей:

4.3.1. содержат символы трех из четырех перечисленных ниже категорий:

- латинские строчные буквы (от a до z);
- латинские заглавные буквы (от A до Z);
- цифры (от 0 до 9);
- отличающиеся от букв и цифр знаки (! @#$%л&*()_+|~-=\'{}[]: ";'<>?,./);

4.3.2. состоят из восьми и более символов;

4.3.3. не являются словом на любом языке, диалекте, сленге, жаргоне и т.д.;

4.3.4. не основаны на персональной информации, например, фамилии, дате рождения и т.д.;

4.3.5. никогда не записываются и не хранятся on-line.

4.4. Создавайте легко запоминаемые пароли. Одним из способов создания таких паролей - это использование песен, стихов и других легко запоминающихся фраз. Например, из фразы: «*Белеет парус одинокий в тумане моря голубом!*» можно получить такие пароли: «*бПо19в85ТМг!*», «*[Бпо]В[тмГ]*» и другие варианты. Если вводить его русскими буквами в английской раскладке, то получится сложный и непроизносимый пароль, который просто запомнить.

Внимание: Не используйте ни один из перечисленных примеров в качестве пароля!

4.5. Не используйте функцию «Запомнить пароль» в любых приложениях (электронная почта, Messenger и др.).