ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ПРИЛОЖЕНИЕ 2
к приказу ректора
от 14.06.2018 № 538-ОД

ТРЕБОВАНИЯ

к парольной защите НИУ «БелГУ»

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 университета.

1.2. Все пользователи интрасети НИУ «БелГУ» (включая работников и обучающихся) несут ответственность за выполнение требований настоящего документа. В случае нарушения настоящих Требований учетные записи блокируются до устранения причин блокировки.

1.3. Цель настоящих Требований – 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, а также удовлетворять признакам сложных паролей указанных в п.4.3. настоящих Требований.

2.2. Срок действия паролей доменных учетных записей пользователей 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 учетным записям НИУ «БелГУ» 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 учетной записи пользователя интрасети и для учетной записи с административными привилегиями).

2.6.3. Сообщать другому лицу свой пароль, в том числе подчиненным, руководителю, 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 своем пароле, находясь рядом с посторонними лицами.
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 коллегам 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 учетной записи или пароля сообщите об этом в управление информатизации и измените все пароли.

3. Требования к разработчикам программного обеспечения

3.1. Разработчики программного обеспечения (далее - 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 поддерживать аутентификацию на основе LDAP.
3.1.3. Программы должны хранить пароли в зашифрованном (но не в открытом или легкораскрываемом) виде согласно действующему законодательству Российской Федерации.
3.1.4. 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 НИУ «БелГУ» используются пароли для различных целей: доступ к электронной почте, в личный кабинет, выход в Интернет, доступ к различным автоматизированным системам. Следует знать, как выбрать стойкий пароль и избежать использования слабого пароля.

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, имена друзей, сотрудников, вымышленных персонажей, кличку животного и т. д.
4.2.5. Содержат компьютерные термины и названия, команды, названия сайтов, организаций, оборудования, программного обеспечения.
4.2.6. Содержат название университета или географические наименования, например «БелГУ», «Белгород» или их 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: 12345, аааббб, qwerty, zyxwvuts, 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 (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).

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. Не следует использовать функцию «Запомнить пароль» в любых приложениях (электронная почта, ICQ, Messenger и др.).

4.5. Создавайте легкозапоминаемые пароли. Один из способов создания таких паролей – это использование песен, стихов и других легкозапоминающихся 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!