

СОГЛАСОВАНО

Председатель ПК:



И.Ан. Кашеева.

УТВЕРЖДАЮ

Директор МБОУ Богутраевской СОШ:



И.А. Кашеева

Приказ № 43 от 17.03.2017 г.



ИНСТРУКЦИЯ по организации парольной защиты

1. Общие положения

1.1 Настоящая инструкция устанавливает порядок и правила генерации, использования паролей в информационных системах организации.

1.2 Требования настоящей инструкции распространяются на всех сотрудников организации.

1.3 Бесконтрольность в определении и использовании паролей может повлечь риск несанкционированного доступа к информации организации, повлечь мошеннические и другие действия информационных системах, которые могут нанести материальный вред и ущерб репутации организации.

2. Требования к паролям

2.1 Пароли не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок и т.д.

2.2 Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.

2.3 Пароли должны содержать символы как минимум из трех следующих групп:

- Строчные латинские буквы: abcd...xyz;
- Прописные латинские буквы: ABCD...XYZ;
- Цифры: 123...90;
- Специальные символы: !%() _+ и т.д.

2.4 Требования к длине пароля:

- Для обычных пользователей - не менее 8 символов;
- Для администраторов (*локального\доменного*) - не менее 15 символов;
- Для сервисных идентификаторов, разделяемых ключей (*shared keys*) - не менее 14 символов;
- Для SNMP Community Strings — не менее 10 символов.

2.5 Периодичность смены пароля:

- Административные – каждые 60 дней;
- Пользовательские – каждые 90 дней;
- Сервисные – не реже двух раз в год;
- Shared keys SNMP Community Strings — не реже одного раза в год.

2.6 Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (*локальная вычислительная сеть, интернет, электронная почта*).

2.7 . В ходе работы не должны использоваться встроенные идентификаторы. Для них должны быть назначены пароли, отличные от установленных производителем. К ним предъявляются требования, аналогичные требованиям к сервисным паролям.

2.8 Пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

2.9 Хеши паролей должны проверяться в ходе внутреннего аудита администратором информационной безопасности не реже двух раз в год с помощью типовых атак на подбор.

Возможна также проверка соответствия пароля требованиям данной инструкции в присутствии пользователя: пользователь называет свой пароль, а проверяющий

осуществляет ввод пароля и его проверку. После такой проверки требуется обязательная и немедленная смена пароля.

2.10 Пароли сервисных идентификаторов должны входить в процедуру управления паролями УА, включающую хранение их в защищенном месте, разделение секрета, периодическую смену (*1 раз в год*).

3. Требования к настройкам безопасности информационных систем

3.1 Учетная запись должна блокироваться после 5 неверных попыток доступа не менее, чем на 15 минут.

3.2 Запрещается использовать функции «*Запомнить пароль*» в любом программном обеспечении.

4. Требования к паролям сервисных учетных записей

4.1 Пароли для сервисных учетных записей должны формироваться ответственным за сервисную учетную запись и администратором информационной безопасности.

4.2 Длина каждой половины пароля должна быть не меньше 7 символов, сложность пароля указана в п.2.3. Перед запечатыванием конверта, обязательно проверить правильность смены пароля в информационной системе, делая соответствующую запись в журнале.

4.3 Пароль должен меняться не реже двух раз в год, или немедленно в случае увольнения или смены полномочий одного или двух ответственных за формирование пароля.

4.4 Каждая половина пароля сохраняется в отдельном конверте, исключающем возможность увидеть пароль через конверт, например, путем просвечивания конверта ярким светом. Конверты хранятся в сейфе начальника УА.

4.5 Каждая генерация\смена\вскрытие пароля или конверта должна обязательно формироваться соответствующей записью в журнале.

4.6 Администратор информационной безопасности, должен ежемесячно проверять наличие конвертов, целостность.

4.7 Вскрытие конвертов может произвести:

- ответственный за информационную систему;
- администратор информационной безопасности;
- Начальник УА

4.8 Конверты вскрываются одним лицом, с последующей регистрацией в журнале, при этом обязательно информирование администратора информационной безопасности с использованием почтовой рассылки.

4.9 В случае вскрытия\использования конвертов, по окончании выполнения работ необходимо произвести работы по созданию нового пароля с п.4.1

4.10 Администраторы оказывают помощь и содействия администратору информационной безопасности при проведении аудитов, управление сервисными, административными паролями, shared keys и SNMP Community Strings, включая генерацию паролей, их изменение и хранение в безопасном месте, а также настройку информационных систем для соблюдения данных требований.

4.11 Администратор по информационной безопасности несёт осуществляет аудит требований данной политики, разрабатывает процедур управления идентификаторами.

4.12 Пользователи информационных ресурсов обязаны соблюдать требования данной Инструкции при выборе пароля и работе с ним.

5. Ответственность

5.1 Виновные в нарушении условий настоящей Инструкции несут ответственность в соответствии с законодательством Российской Федерации, трудовым договором, должностной инструкцией.

6. Заключительные положения

6.1 Общий текущий контроль исполнения настоящей инструкции осуществляет АИБ.

6.2 АИБ поддерживает настоящую инструкцию в актуальном состоянии.

6.3 Изменения и дополнения в настоящую инструкцию утверждаются директором организации.

6.4 Инструкция вступает в силу с момента утверждения директором организации.