

Новая политика паролей группы компаний Arbonia

Уважаемые сотрудники!

Надежный пароль является первой линией защиты систем и данных компании.

Основной задачей взломщиков является, в частности, кража данных доступа учетной записи пользователя с целью получения начального доступа к нашим сетям, серверам и ИТ-системам, и — в худшем случае — с целью незаметного проведения таких действий, как кража данных, промышленный шпионаж или установка вредоносного программного обеспечения. В связи с этим ненадежные или скомпрометированные пароли, равно как и ненадлежащее обращение с ними, представляют существенный риск. Для более успешного соответствия нашим требованиям к безопасности и обеспечения более надежной защиты от этих угроз группа компаний Arbonia выработала новую политику паролей.

Изменение политики паролей

Ниже наглядно представлена полная стратегия управления паролями. Изменения в основном затрагивают минимальную длину пароля, максимальный срок действия пароля, а также его сложность.



Минимальная длина пароля увеличивается с восьми до двенадцати знаков с целью затруднить взлом пароля, в то же время срок действия пароля увеличивается минимум до 360 дней. Если используется более длинный пароль (≥ 16 знаков), то срок действия пароля увеличивается до 540 дней. Необходимо в любом случае обеспечить высокий уровень сложности для новых паролей (= надежный пароль). Он достигается за счет комбинации заглавных и строчных букв, цифр 0–9, знаков препинания либо специальных символов.



Кроме того, автоматически блокируется использование ранее скомпрометированных и находящихся в свободном интернет-доступе паролей, а также слов из черного списка (например, названий компаний).



Если действующий пароль появляется в базе данных скомпрометированных паролей, автоматически поступает требование смены пароля.

Новая политика паролей автоматически активируется при следующем изменении вами пароля Windows или по запросу местного ИТ-отдела. Вы получите напоминание за 14 дней до истечения срока действия пароля. Данная политика действительна для всех ИСТ-систем группы компаний Arbonia, в т. ч. и для других операционных систем. Как владелец аккаунта, вы в любом случае несете ответственность за соблюдение политики паролей, даже если оно не является технически вынужденным.

Создание надежного пароля

Существуют различные техники создания и запоминания надежного пароля. Например, создайте надежный пароль на основе предложения или с помощью замены определенных последовательностей символов:

- Выберите предложение, которое легко сможете запомнить, и преобразуйте его в пароль. Например: «*Не так и трудно подобрать надежный пароль.*» Используйте начальные буквы или несколько букв для отдельных слов и дополните пароль цифрами и специальными символами. Например: «*Нткитрпод1нП.*»
- Выберите слово, которое легко сможете запомнить, например «Автомобиль», и определите специальную последовательность символов, например «1\$1». Теперь замените определенные части/буквы в слове выбранной последовательностью символов, чтобы получить надежный пароль. Например: «*Авт1\$1м1\$1биль*»

Спасибо за внимание! С уважением,
служба безопасности Arbonia



Стратегия управления паролями

История паролей (количество старых паролей, которые нельзя использовать снова)	5	Количество неудачных попыток входа до блокировки аккаунта	6
Минимальная длина пароля	12 символов	Срок блокировки аккаунта	До разблокировки администратором
Максимальный срок действия пароля	360 дней (12–15 символов) или 540 дней (≥ 16 символов)	Срок до сброса счетчика неудачных попыток	≥ 60 минут
Сложность	➤ Заглавные буквы ➤ Строчные буквы ➤ Цифры 0–9 ➤ Знаки препинания либо специальные символы	Особые указания (пароли Windows — внутренне и автоматически утвержденные Arbonia)	Пароль не должен начинаться или заканчиваться цифрами, а также содержать последовательности из трех одинаковых символов



Не используйте пароли, приведенные в этом документе в качестве примера. Данные пароли являются «скомпрометированными» и включены в черный список.



Также в дополнение к данному информационному письму обратите внимание на действующую политику паролей (IS-ISP-GROUP-001-PASSWORD-POLICY), доступную по ссылке <https://security.arbonia.com>



При изменении пароля Windows сразу отображаются необходимые требования.

- ✓ Должен содержать не менее 12 символов
- ✓ Должен содержать не менее 1 буквы верхнего регистра
- ✓ Должен содержать не менее 1 буквы нижнего регистра
- ✓ Должен содержать не менее 1 цифры
- ✓ Должен содержать не менее 1 специального символа
- ✓ Не должен содержать ваше имя пользователя
- ✓ Не должен содержать 3 или более одинаковых символов подряд
- ✓ Не должен заканчиваться цифрой
- ✓ Не должен начинаться с цифры

Соответствие этим правилам будет проверено после подтверждения пароля

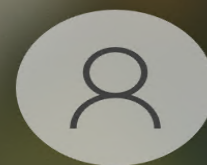
● Не должен находиться в списке взломанных паролей

Более длинный пароль будет иметь более длительный срок действия. Срок действия этого пароля истекает через **360** дней.

360 540

✓ Пароли совпадают

Powered by Specops Software



Change a password

CHAFG1\specops

Old password

.....

.....|

Sign in to: CHAFG1

How do I sign in to another domain?

Cancel