ARBONIA

IT SECURITY

Политика информационной безопасности

Политика паролей

Версия:	1.0
Принято (дата):	08.07.2021
Статус:	RELEASED
Классификация:	RESTRICTED
Составлено (кем):	ICT Security Officer
Принято (кем):	Arbonia IT Board
Политика:	IS-ISP-GROUP-001-PASSWORD-POLICY_RU
Изменение:	н/д

Информация о политике

Цель	Политика паролей описывает и определяет принципы создания, обращения и использования паролей в группе компаний Arbonia.
Пользователи / получатели	▪ Все сотрудники группы компаний Arbonia ▪ Внешние поставщики / подрядчики / заказчики и партнеры, имеющие доступ к ICT-системам группы компаний Arbonia
Электронное хранение документов	https:\\security.arbonia.com

Лист регистрации изменений

Версия	Дата	Статус	Изменение	(кем)
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Содержание

Глоссарий 4
1 Цель, область применения и круг пользователей 5
2 Принципы управления 5
2.1 Важность паролей 5
2.2 Обязанности пользователя / владельца аккаунта 5
3 Политика паролей 6
3.1 Определение 6
3.2 Управление паролями 6
3.3 Требования к паролю 7
3.4 Стратегия управления паролями 8
3.5 Исключения / особые указания 8
4 Создание надежных паролей 9
5 Справочная документация 9
6 Вступление в силу 9
7 Соответствующие приложения 10

Список сокращений

Термин	Описание
ICT	Informations and Communications Technology (информационно-коммуникационные технологии)
OS	Operating System (Операционная система)
ISMS	Системы управления информационной безопасностью

Глоссарий

Термин	Описание
Брутфорс-атака (Brute Force Attack)	При брутфорс-атаке совершается попытка взлома пароля или имени пользователя посредством перебора всех возможных комбинаций.
Системы управления информационной безопасностью	Система управления информационной безопасностью представляет собой ряд методов и правил внутри организации, предназначенных для долговременного обеспечения, управления, мониторинга, поддержания и дальнейшего улучшения информационной безопасности предприятия.

1 Цель, область применения и круг пользователей

Данная политика описывает правила создания паролей и требования, необходимые для доступа к ICT-системам группы компаний Arbonia. В ней установлены правила безопасного управления паролями, их создания и использования.

Данная политика действительна в отношении всех областей применения системы управления информационной безопасностью (ISMS), т. е. для всех ICT-систем группы компаний Arbonia.

Пользователями и получателями данной политики являются все сотрудники группы компаний Arbonia, а также внешние поставщики / подрядчики / заказчики / партнеры и другие лица, запрашивающие доступ к ICT-системам группы компаний Arbonia.

2 Принципы управления

2.1 Важность паролей

Безопасность ICT-систем группы компаний Arbonia в частности зависит от того, насколько бережно пользователи обращаются с паролями и насколько соблюдают основные принципы использования паролей.

Главной целью взломщиков является кража пользовательских данных доступа с целью обеспечения доступа к ICT-системам группы компаний Arbonia, дальнейшего нахождения и злонамеренного использования их возможных уязвимостей. Взломщики пытаются присвоить себе привилегированные права доступа системного администратора, с помощью которых они — в худшем случае — способны незаметно проводить различные действия, такие как кража данных, промышленный шпионаж или установка вредоносного программного обеспечения. В связи с этим ненадежные пароли, равно как и ненадлежащее обращение с ними, представляют существенный риск. Этот риск повышается вдвойне в связи с необходимостью применения привилегированных прав доступа, неоднократно использующихся при осуществлении трудовой деятельности.

Поэтому крайне важно предотвращать кражу данных доступа и соблюдать следующие ниже обязательства.

2.2 Обязанности пользователя / владельца аккаунта

При выборе и использовании паролей пользователь обязан применять проверенные и надежные методы (подробнее в разделе 3):

- Необходимо всегда выбирать надежный пароль. Длина и формат пароля подбираются таким образом, чтобы брутфорс-атака требовала значительных затрат времени и не приводила к успеху
- Не разрешается передавать пароли третьим лицам. В том числе вышестоящим лицам, руководству или системным администраторам
- Не разрешается записывать или сохранять пароли ненадлежащим образом (например, в Excel), за исключением безопасных методов (например, менеджер паролей), допущенных к использованию ИТ-отделом
- Необходимо периодически менять пароль
- Необходимо изменить пароли при наличии признаков того, что пароли оказались в открытом доступе (переданы третьим лицам)
- О признаках неавторизованного использования необходимо немедленно сообщать ответственному ИТ-отделу
- Если в распоряжении пользователя имеется индивидуальный аккаунт с административными привилегиями, не разрешается использовать тот же пароль, что и в стандартном аккаунте
- Владелец аккаунта в любом случае несет ответственность за соблюдение политики паролей, в т. ч. если оно не является технически вынужденным. Ни в коем случае не допускается использование стандартных, пустых либо ненадежных паролей

3 Политика паролей

3.1 Определение

Чтобы достигнуть адекватного уровня информационной безопасности, используются различные политики паролей в соответствии с необходимыми привилегиями. Различают:

- общее пользование типа «Пользователь», без административных привилегий в ICT-системах
- специальное пользование типа «Администратор», с административными привилегиями в одной либо нескольких ICT-системах. Учетные записи типа «Администратор» подразделяются на:
    - служебные/системные/сервисные учетные записи (применяются для автоматизированных функций, установки или управления компонентами ICT-систем, такими как OS, базы данных, приложения или сетевые аккаунты и т. п.)
    - учетные записи администраторов (применяются для предоставления отдельным лицам привилегированных прав доступа к ICT-системам)

3.2 Управление паролями

1. Пароль закрепляется за однозначным идентификатором учетной записи (пользователь или администратор)
2. Как и идентификатор учетной записи, пароль также является уникальным. Пароль известен только ответственному лицу.
3. Не допускается хранение пароля в незашифрованном виде
4. Срок действия пароля не может превышать 360 и 540 дней соответственно (см. раздел 3.3)
5. Новый пароль будет отклонен, если он входит в список пяти последних использованных паролей
6. Количество неудачных попыток ввода пароля ограничено шестью попытками. После шестой попытки учетная запись блокируется до разблокировки администратором.
7. Счетчик неудачных попыток входа нельзя сбросить ранее, чем через 60 минут
8. Временные пароли могут иметь срок действия < 72 ч, при первом входе пользователю должно быть предложено изменить временный пароль. Данное правило действует, если это технически осуществимо. Если нет, то владелец учетной записи самостоятельно несет ответственность за изменение пароля
9. Автоматическая раздача паролей при создании учетной записи пользователя также осуществляется в соответствии с данными требованиями

Специальные положения для служебных/системных/сервисных учетных записей

- Исключение из правила №2: разрешается хранить пароли, привязанные к данным учетным записям, в безопасном (зашифрованном) менеджере паролей с защищенным доступом и передавать их через определенные ролевые группы пользователей и группы доступа третьим лицам в том случае, если это необходимо для осуществления их деятельности
- Исключение из правила №4: пароли, привязанные к данным учетным записям, при необходимости разрешается устанавливать бессрочно
- Исключение из правила №6: пароли, привязанные к данным учетным записям, не требуют автоматической блокировки

Сведения о работе с исключениями см. в разделе 3.5.

3.3 Требования к паролю

Пароль для учетной записи типа **«Пользователь» без** административных привилегий в ICT-системах должен соответствовать следующим требованиям:

- пароль содержит не менее 12 символов для срока действия 360 дней и не менее 16 символов для срока действия 540 дней
- пароль обладает сложностью четыре из четырех — это значит, что символы из следующих категорий должны быть использованы по меньшей мере один раз:
    - заглавные буквы
    - строчные буквы
    - цифры 0–9
    - знаки препинания или специальные символы (не все ICT-системы распознают все символы)
- пароль не должен содержать название учетной записи
- пароль не должен начинаться или оканчиваться цифрами
- пароль не должен содержать последовательности из трех одинаковых символов

Для паролей учетной записи типа **«Администратор» с** административными привилегиями в ICT-системах действуют следующие дополнительные специальные положения

Специальные положения для служебных/системных/сервисных учетных записей:

- содержит не менее 32 символов
- пароль должен быть случайно сгенерирован и документирован с помощью подходящего менеджера паролей (см. исключение к правилу №2, раздел 3.2)

Специальные положения для административных учетных записей:

- содержит не менее 15 символов

Специальные положения для сторонних систем (B2C / B2B и другие), использующихся группой компаний Arbonia:

требования к паролям в целом действуют и в отношении сторонних систем, однако при необходимости существует возможность адаптировать их под соответствующий бизнес-сценарий использования. Специальные положения в любом случае должны рассматриваться в соответствии с разделом 3.5.

Особые требования для учетных записей Windows — внутренне и автоматически утвержденные Arbonia:

- Новый пароль не должен содержаться в базе данных скомпрометированных паролей. Это предотвращает техническая проверка при назначении пароля
- Новый пароль не должен встречаться в пользовательском словаре. Данный словарь поддерживается централизованно и содержит, например, названия компаний. Неразрешенные слова сразу отображаются в случае совпадения
- Пароль должен быть изменен, если он появился в базе данных скомпрометированных паролей

3.4 Стратегия управления паролями

История паролей	5
Максимальный срок действия пароля	360 (12–15 символов) или 540 дней (≥ 16 символов)
Минимальный срок действия пароля	0
Сложность	4/4 (заглавные/строчные буквы / цифры 0–9 / знаки препинания или специальные символы)
Минимальная длина пароля o Пользователь o Служебные/системные/сервисные учетные записи o Административные учетные записи	 12 символов 32 символа (случайно сгенерировано) 15 символов
Обратное шифрование (Windows Domain)	отключено
Количество неудачных попыток входа до блокировки аккаунта	6
Срок блокировки аккаунта	До разблокировки администратором
Срок до сброса счетчика неудачных попыток	≥ 60 минут
Особые указания (Windows Domain)	Пароль не должен начинаться или заканчиваться цифрами Пароль не должен содержать последовательности из трех одинаковых символов

3.5 Исключения / особые указания

Все компьютерные способы аутентификации должны соответствовать требованиям данной политики настолько, насколько это возможно, и обеспечивать контроль за их соблюдением. При отсутствии технической возможности реализации данных требований их выполнение должно обеспечиваться соответствующим владельцем учетной записи вручную, и в рамках возможностей системы должен использоваться надежный пароль.

Сотрудник локальной службы информационной безопасности может предоставлять разрешения в порядке исключения из данной политики безопасности при соблюдении принципов информационной безопасности и отсутствии риска для ICT-систем группы компаний Arbonia. Сотрудник принимает решение о предоставлении разрешения в порядке исключения, при необходимости согласовывая его с сотрудником службы безопасности ICT, либо определяет дальнейшие меры по минимизации риска. Все исключительные разрешения должны письменно фиксироваться в реестре.

4 Создание надежных паролей

Существуют различные техники создания и запоминания надежного пароля.

Пример 1: создание надежного пароля на основе предложения

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.

Пример 2: создание надежного пароля посредством замены символов

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

При создании пароля никогда не используйте информацию, находящуюся в свободном доступе в социальных сетях. Дальнейшие рекомендации по обеспечению безопасности паролей вы получите на наших курсах по информационной безопасности IT Security Awareness.

5 Справочная документация

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Политика использования ИТ-систем в группе компаний Arbonia

6 Вступление в силу

Фамилия	Подразделение	Должность	Дата	Подпись
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastruc-ture	2021-07-08	n/a

7 Соответствующие приложения

№	Описание	Имя файла
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	