ПОЛИТИКА

назначения и смены паролей

Космический центр «Мир»

Настоящая политика регулирует порядок создания, использования и замены паролей для обеспечения безопасности информационных систем, научных данных и критически важной инфраструктуры Космического центра "Мир". Политика обязательна для всех сотрудников, включая инженеров, ученых, административный персонал и внешних подрядчиков, имеющих доступ к внутренним ресурсам.

1. Ответственные лица
   1. Главный администратор кибербезопасности – отвечает за внедрение политики, контроль соблюдения и реагирование на инциденты.
   2. Руководители подразделений – обеспечивают ознакомление сотрудников с требованиями и их выполнение.
   3. Пользователи – несут персональную ответственность за сохранность своих учетных данных.
2. Создание и первичная настройка паролей
   1. Первичные пароли назначаются администратором безопасности и должны быть изменены при первом входе в систему.
   2. Запрещено использовать стандартные или шаблонные пароли (например, Moscow2024, Cosmos123).
   3. Восстановление доступа осуществляется только через установку нового пароля, а не возврат к старому.
3. Требования к паролям
   1. Минимальная длина: 12 символов (для доступа к критическим системам – 16 символов).
   2. Обязательные элементы:
      1. Латинские буквы (верхний и нижний регистр)
      2. Цифры (минимум 2)
      3. Специальные символы (например, ! @ # $ % ^ & \*)
   3. Запрещено:
      1. Использовать имена, фамилии, названия проектов, даты запусков.
      2. Применять последовательности (например, 12345, qwerty).
      3. Повторять предыдущие пароли (новый пароль должен отличаться минимум на 6 символов).
4. Правила использования и хранения
   1. Запрещено:
      1. Записывать пароли на бумаге без шифрования.
      2. Хранить пароли в открытых файлах или облачных сервисах.
      3. Передавать пароли по незащищенным каналам связи (email, мессенджеры).
   2. Разрешено:
      1. Использовать менеджеры паролей, одобренные службой безопасности.
      2. Хранить зашифрованные пароли в сейфах или спецхранилищах.
5. Периодическая смена паролей
   1. Обычные пользователи: каждые 90 дней.
   2. Администраторы и инженеры критических систем: каждые 60 дней.
   3. Внеплановая смена:
      1. При подозрении на утечку.
      2. После увольнения или смены должности сотрудника.
      3. По требованию службы безопасности после кибератаки.
6. Действия при компрометации
   1. Немедленно сообщить в службу кибербезопасности.
   2. Заблокировать учетную запись до сброса пароля.
   3. Провести аудит действий, совершенных под скомпрометированным аккаунтом.
7. Доступ в чрезвычайных ситуациях
   1. В случае аварийных ситуаций (например, угроза безопасности миссии) доступ к данным может быть предоставлен по решению руководства центра.
   2. Все действия фиксируются в журнале безопасности с подписями ответственных лиц.

7.3 Контроль и обучение

7.3.1 Все сотрудники проходят ежегодный инструктаж по кибербезопасности.

* + 1. Проводятся внезапные проверки соблюдения политики.
    2. Нарушители привлекаются к дисциплинарной ответственности.