|  |  |  |
| --- | --- | --- |
| **Windows** | | |
| **Шаг** | **Действие** | **Описание** |
| 1 | Установить сложный пароль | Задать пароль длиной более 10 символов, с разным регистром, цифрами и символами. |
| 2 | Создать учетную запись администратора | Назначить другое имя для учетной записи администратора, отличное от стандартного "admin". |
| 3 | Отключить учетную запись гостя | Запретить использование учетной записи гостя для повышения безопасности. |
| 4 | Обновить ОС | Установить все доступные обновления безопасности, чтобы устранить известные уязвимости. |
| 5 | Включить брандмауэр | Включить встроенный брандмауэр для контроля сетевого трафика и защиты от несанкционированного доступа. |
| 6 | Включить Windows Defender | Активировать антивирусный и антишпионский инструмент Windows Defender для защиты от вредоносных программ. |
| 7 | Настроить обновления Windows | Настроить автоматическое обновление операционной системы для поддержания актуальной защиты. |
| 8 | Настроить систему мониторинга событий | Настроить журнал событий для мониторинга активности и выявления потенциальных угроз. |
| 9 | Отключить автозапуск программ в автозагрузке | Управлять списком программ, запускаемых при старте, чтобы предотвратить загрузку вредоносных приложений. |
| 10 | Задать правила файервола | Настроить брандмауэр для блокировки нежелательного сетевого трафика и ограничения доступа. |
| 13 | Включить BitLocker (если применимо) | Если устройство поддерживает, включить шифрование диска BitLocker для защиты данных на жестком диске. |
| 14 | Настроить аудит безопасности | Включить аудит безопасности для регистрации событий, связанных с попытками несанкционированного доступа. |
| 15 | Задать сложные логины для других учетных записей | Настроить сложные пароли для всех остальных учетных записей на компьютере. |

|  |  |  |
| --- | --- | --- |
| **Astra linux** | | |
| **Шаг** | **Действие** | **Описание** |
| 1 | Настройка пользователей и групп | Создать ограниченные учетные записи, запретить использование root для повседневных задач. |
| 2 | SSH-безопасность | Запретить аутентификацию по паролю, разрешить только ключи; ограничить доступ к SSH по IP; изменить порт SSH. |
| 3 | Файловая система | Задать правильные разрешения на критически важные файлы; включить шифрование дисков (LUKS). |
| 4 | Аудит безопасности | Включить и настроить аудит для мониторинга системных событий; создать централизованный журнал аудита. |
| 5 | Firewall | Настроить iptables или firewalld для фильтрации сетевого трафика; разрешить только необходимые порты и сервисы. |
| 6 | SELinux или AppArmor | Включить и настроить SELinux или AppArmor для контроля доступа к ресурсам; активировать "Enforcing" режим. |
| 7 | Обновления | Настроить автоматическое обновление пакетов и ядра; периодически проверять наличие обновлений и применять их. |
| 8 | Логи | Периодически анализировать системные логи; включить централизованный сбор логов, если возможно. |