|  |  |  |
| --- | --- | --- |
| Подсистема | Windows 10 | Astra linux |
| Управления доступом | **Учетные записи пользователей и группы** - Учетные записи определяют, кто может получить доступ к компьютеру, а группы позволяют администраторам применять права доступа к нескольким пользователям одновременно. **AppLocker -** позволяет администраторам ограничивать выполнение приложений и скриптов, что уменьшает риск внедрения вредоносного программного обеспечения. | **Access Control Lists (ACL)** - механизм тонкого управления правами доступа к объектам файловой системы. **Security-Enhanced Linux (SELinux) -** система принудительного контроля доступа, реализованная на уровне ядра. |
| Регистрации и учёта | **Local Security Authority (LSA) -** управляет аутентификацией пользователей при входе в систему. Он также участвует в процессе создания и хранения хэшей паролей. **Event Viewer** - регистрирует события, происходящие в системе, включая вход и выход пользователя, изменения в политиках безопасности, аудит безопасности и другие важные моменты. | **Linux Audit Daemon (Auditd)** — нативный инструмент, предназначенный для мониторинга событий операционной системы и записи их в журналы событий. **system log (syslog)** - стандарт отправки и регистрации сообщений о происходящих в системе событиях. |
| Криптографическая | **BitLocker** - обеспечивает шифрование диска и защиту данных на диске от несанкционированного доступа, может использоваться как на уровне всего диска, так и на уровне отдельных томов (Ключ может храниться как в TPM (Trusted Platform Module), так и на внешнем носителе). **Windows Hello** - предоставляет биометрические методы аутентификации, такие как сканер отпечатков пальцев, распознавание лица или PIN-код, чтобы обеспечить безопасный доступ к устройству. **Encrypting File System (EFS) -** механизм шифрования файлов на уровне файловой системы. | **Cryptsetup и Linux Unified Key Setup (LUKS) -** предоставляют механизмы для шифрования дисковых томов. Cryptsetup используется для настройки шифрования, а LUKS определяет формат метаданных для дисковых устройств. **OpenSSL** - библиотека, предоставляющая реализации различных криптографических алгоритмов, используется в многих приложениях для обеспечения безопасной передачи данных через сеть и других криптографических операций. |
| Обеспечения целостности | **System File Checker (SFC) -** инструмент, который позволяет администраторам проверять целостность и восстанавливать поврежденные системные файлы. Он может автоматически заменять поврежденные версии файлов на те, которые хранятся в кэше. **Trusted Platform Module (TPM) -** аппаратный модуль, который предоставляет безопасное окружение для хранения ключей шифрования и других секретных данных. Это обеспечивает целостность системы, предотвращая несанкционированный доступ к ключам. **Windows Defender -** В Windows Defender встроен механизм контроля целостности, который отслеживает изменения в системных файлах и других критических ресурсах. Если обнаруживается подозрительная активность, Windows Defender может предпринять меры для предотвращения угроз. | **AppArmor** — программный инструмент упреждающей защиты, основанный на политиках безопасности, которые определяют, к каким системным ресурсам и с какими привилегиями может получить доступ то или иное приложение. **Integrity Measurement Architecture (IMA) -** обеспечивает механизм измерения целостности файлов в системе. Файлы могут быть подписаны цифровой подписью, и IMA регистрирует хэши файлов, что позволяет обнаруживать изменения и подмену файлов. |