ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОГО РЕПОЗИТОРИЯ DOCKER

С.Н. Петров[1], В.Н. Ганисевский[2], А.Д. Алам Яр[2]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

[2]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

Создание защищенного локального репозитория Docker может быть полезным для организаций, которые хотят иметь контроль над использованием образов Docker в своей среде. Защищенный репозиторий Docker призван обеспечить безопасность и целостность образов Docker, предотвратить использование поддельных образов.

После установки Docker и создания локального репозитория необходимо настроить механизмы аутентификации и авторизации пользователей для доступа к репозиторию. Первым делом создается файл конфигурации для авторизации Docker, для чего этого можно использовать достаточно популярную утилиту htpasswd, которая создает файл с именами пользователей и хэшами паролей. Результатом работы утилиты станет файл «docker-auth» с пользователем «user» и запросом пароля. Созданный файл конфигурации указывается в качестве источника аутентификации. Необходимо настроить клиентский доступ к репозиторию, используя учетные данные авторизации, для чего создается файл конфигурации Docker в домашней директории пользователя.

Доступ к репозиторию осуществляется по протоколу HTTPS.

Содержимое репозитория, Docker-образы, также должны быть защищено. Одним из механизмов защиты является цифровая подпись, которая позволяет обеспечить целостность образов Docker при их распространении и использовании. Это достигается путем создания уникального идентификатора образа (хэш-суммы) и его подписи цифровым сертификатом, который удостоверяет авторство создателя. Чтобы создать цифровую подпись образа Docker, сначала необходимо создать закрытый ключ (private key) и соответствующий ему открытый ключ (public key), используя криптографические алгоритмы. Затем создается подпись образа, используя закрытый ключ. Подпись включает хэш образа и другие метаданные. Когда образ Docker загружается на другой сервер или устройство, проверка цифровой подписи образа позволяет убедиться в его целостности и подлинности. Если образ был изменен, подпись становится недействительной, что предотвращает использование поддельных образов и защищает от возможных атак.

Для создания и использования цифровых подписей образов Docker существует множество инструментов и сервисов, таких как Notary, Docker Content Trust, Sigstore и других. Эти инструменты позволяют создавать и управлять цифровыми подписями, а также упрощают процесс проверки подписей при загрузке и использовании образов.