УДК 004.77

О.В. Крупица, ст. преп.;
А.С. Бихдрикер, доц., канд. техн. наук
К.К. Панайотов, доц., канд. техн. наук
(Луганский национальный университет им. В.Даля, г. Луганск)

ЗАЩИТА ОБЛАЧНОЙ АРХИТЕКТУРЫ НА ОСНОВЕ ТЕХНОЛОГИИ ОТКРЫТЫХ КЛЮЧЕЙ

Облачные технологии являются удобной виртуальной средой, которая используется для хранения и обработки информации. Использование облачных технологий помогает довольно быстро реагировать на появление новых бизнес-задач, снижает затраты и увеличивает эффективность предприятий и их подразделений.

При использовании облачных технологий особенно актуальным является защита информации. Одним из способов повышения эффективности защиты информации является применение единой инфраструктуры открытых ключей. При этом остро стоит вопрос конфиденциальности информации. Криптографические методы защиты являются одним их надежных методов обеспечения такой конфиденциальности.

Практика показывает, что пароли несложно расшифровать, используя технические методы или методы социальной инженерии. Администраторы облачных сервисов требуют от пользователей применение более длинных и сложных паролей, например, использование специальных символов, комбинаций букв обоих регистров, обязательного использования цифр. Это повышает надёжность пароля, но вызывает другую проблему. Пользователи в этом случае часто забывают пароль.

Цифровые сертификаты — это альтернативный способ идентификации пользователя в системе. При практической реализации технологии инфраструктуры открытых ключей (PKI-Public Key Infrustructure) требуется наличие персональных носителей ключевой информации в виде смарт-карт или USB-токенов, на которых хранятся соответствующие закрытые ключи и цифровые сертификаты. Для учета и контроля смарт-карт и токенов в рамках инфраструктуры открытых ключей используются системы класса Card Management, предназначенные для управления жизненным циклом ключевых носителей [2].

Цифровые сертификаты являются частью инфраструктуры открытых ключей, поэтому они обязательно содержат в себе данные об открытом ключе.

Закрытый ключ, который ассоциирован с этим открытым ключом, хранится отдельно от сертификата в защищенном хранилище. Соответственно к ассоциированному закрытому ключу имеет доступ только его владелец. Выделим основные принципы, на которых построены открытые и закрытые ключи [1]:

1. Владея открытым ключом, нельзя получить доступ к закрытому ключу и наоборот.
2. Если данные зашифрованы открытым ключом, то расшифровать их можно только ассоциированным с ним закрытым ключом.
3. Если данные зашифрованы закрытым ключом, то их может прочитать любой пользователь – это так называемая цифровая подпись. Цифровую подпись может создавать только владелец ключа.

Задачу внедрения защищённых файловых хранилищ с шифрованием можно реализовать на базе Windows Server 2016 с помощью службой File classification Infrastructure (FCI). Для реализации обязательного шифрования всех файлов, хранящихся на файловом сервере можно использовать службы FCI и Active Directory Right Management Services (AD RMS) или серверную роль File Server Resource Manager (FSRM). С помощью механизма FCI находят все файлы, которые необходимо защитить, и присваивают им определенные метки, затем для файлов с данными метками создаётся специальное задание RMS Encryption.

Таким образом, используя технологию открытых ключей, можно организовать защищённый обмен информацией между подразделениями предприятия.

ЛИТЕРАТУРА

1. Крупица, О.В., Бихдрикер, А.С. Использование инфраструктуры открытых ключей для защиты облачной архитектуры // Материалы II Республиканской научно-практической Интернет-конференции «Информационные технологии в экономике». Луганск: ЛНУ им. В.Даля, 2018. С. 87-90.
2. Инфраструктура открытых ключей (PKI) [Электронный ресурс]. URL:https://indeed-id.ru/infrastruktura_otkrytyh_kljuchej_pki.html (дата обращения 16.03.2018)