СЕКЦИЯ 2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

АРХИТЕКТУРА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ ГРИД-СИСТЕМЫ

В.В. Анищенко, А.В. Глевич

В данном докладе предлагается архитектура инфраструктуры открытых ключей (ИОК) грид-системы для аутентификации и защиты процесса обмена данными пользователей в грид-системе. Основная цель ИОК грид-системы — обеспечение, путем применения цифровых сертификатов, надежной связи открытых ключей с объектами, что позволяет другим объектам проверить эту связь и получить необходимые услуги для осуществления управления ключами в распределенной среде. ИОК интегрирует цифровые сертификаты, криптографию с открытыми ключами и органы сертификации в единую архитектуру безопасности грид-среды.

Сертификаты ключей используются для аутентификации пользователей, аутентификации шлюзов, аутентификации диспетчера сетевых заданий, подписи заданий, подписи программного обеспечения. В иерархии ИОК грид-системы предлагается использовать два уровня: корневой сертификационный центр (СЦ) и СЦ грид-системы. Корневой СЦ используется для подписи СЦ грид-системы и гарантирует его целостность. Сертификат СЦ грид-системы подписывается корневым СЦ и получает необходимые права для подписания пользовательских и серверных сертификатов с меньшим объемом прав. СЦ грид-системы использует собственный список отозванных сертификатов для отзыва вышедших из употребления сертификатов и сертификатов с нарушенной подписью, т.е. сертификатов, личные ключи которых похищены или потеряны. Сертификаты и списки отозванных сертификатов как корневого СЦ, так и СЦ грид-системы доступны для всех клиентов, так как они могут быть использованы при проверке цепочки сертификатов. Сертификат нижнего уровня действителен только тогда, когда действительны все вышестоящие сертификаты.

Особенно важным условием функционирования ИОК грид-системы является обеспечение комплексной безопасности — использование организационно-технических мер и программно-технических средств защиты.