Разработка новых принципов построения инфраструктуры безопасности распределенных информационно-вычислительных систем на основе открытых протоколов

СОГЛАШЕНИЕ № 14.604.21.0146

Срок исполнения: 2014-2016гг.

Заказчик: Министерство образования и науки Российской Федерации

Исполнитель: Федеральное государственное бюджетное образовательное учреждение высшего образования "Московский государственный университет имени М.В.Ломоносова" (МГУ имени М.В.Ломоносова)

Индустриальный партнер: ООО "Ниагара Компьютерз"

Страница проекта на сайте ФЦПИР:
http://fcpir.ru/participation_in_program/contracts/14.604.21.0146/

Цели выполнения ПНИ

Разработка комплекса новых научных и научно-технических решений в области создания программного обеспечения инфраструктуры безопасности распределенных информационно-вычислительных систем (РИВС) на основе открытых протоколов прикладного уровня, позволяющего существенно упростить использование РИВС для конечных пользователей, а также эксплуатацию (администрирование) инфраструктуры при условии обеспечения необходимого уровня безопасности РИВС.

Основные результаты проекта

Основные принципы, заложенные в предложенной архитектуре и алгоритмах работы модулей инфраструктуры безопасности соответствуют передовым технологиям, используемым для построения систем подобного рода, а конкретные функциональные возможности не имеют аналогов в мире. Новизна предложенного решения заключается в пересмотре подхода к построению инфраструктуры безопасности распределенных информационно-вычислительных систем (РИВС). В частности, предложено отказаться от использования прокси-сертификатов для доступа к ресурсам РИВС, а аутентификацию пользователей производить на время сессии посредством пары логин-пароль с возможностью использования многофакторной аутентификации в необходимых случаях. Четко разделен процесс первичной аутентификации пользователей и повторной аутентификации, а также предложено использовать сессионные

ключи с ограниченным сроком действия. Каждый сформированный пользователем запрос подписывается специально сгенерированным хешем, который позволяет предотвратить возможность модификации данного запроса злоумышленником и, как следствие, под видом авторизованного пользователя, выполнить подложный запрос. Разработанные и реализованные в качестве программного комплекса архитектура и алгоритмы позволяют существенно упростить использование РИВС для конечных пользователей, а также эксплуатацию инфраструктуры безопасности. При этом уровень безопасности при работе РИВС превосходит уровень систем, построенных с использованием инфраструктуры открытых ключей.