

# Управление доступом к объектам распределенных информационных систем под управлением программных средств с открытым исходным кодом

А.А. Иткес<sup>1</sup>

<sup>1</sup>Научно-исследовательский институт механики Московского государственного университета имени М. В. Ломоносова

*Аннотация* — В сообщении рассматриваются вопросы разработки математических моделей и реализующих их программных средств с открытым исходным кодом для управления логическим разграничением доступа субъектов к объектам распределенных на сетевой среде информационных систем.

*Ключевые слова* — Управление сетевым доступом, распределенные информационные системы, логическое разграничение доступа.

## I. Введение

Логическое разграничение доступа является одним из важнейших аспектов обеспечения безопасности информационных систем, в том числе, распределенных. Важно отметить, что на практике доступ субъекта к удаленному на сетевой среде объекту в распределенных информационных системах обычно осуществляется посредством другого субъекта, который в контексте доклада называется доверяющим субъекту, осуществляющему доступ. По этой причине в сообщении для управления доступом субъектов к удаленным объектам распределенных информационных систем используется управление доверием между субъектами этих систем.

## II. Программный комплекс Nettrust

Основное внимание в сообщении уделено спроектированному и реализованному автором программному комплексу с открытым исходным кодом, называемому Nettrust. Этот комплекс предназначен для управления доверием между удаленными субъектами распределенных информационных систем под управлением операционной системы Linux, а

значит, и для управления доступом субъектов к объектам таких систем. Вместе с тем, для обоснования корректности функционирования данного программного средства появляется необходимость в разработке некоторой теоретической базы, на основе которой происходит объединение математических моделей логического разграничения с помощью отношений доверия. По этой причине рассмотрены несколько распространенных в настоящее время математических моделей и реализующих их программных механизмов логического разграничения доступа субъектов к объектам информационных систем. Сформулирован ряд утверждений, гарантирующих возможность объединения разных математических моделей логического разграничения доступа с помощью отношений доверия. Исследованы вопросы представления моделей логического разграничения доступа, реализуемых различными средствами повышения защищенности информационных систем под управлением операционной системы Linux, в терминах базовых математических моделей. В совокупности, перечисленные утверждения гарантируют, что все разрешенные виды доступа субъектов к объектам информационной системы, работающей под управлением разработанного и реализованного программного комплекса, могут быть описаны с помощью формальной математической модели.

### III. Заключение

Одним из основных достоинств комплекса Nettrust является поддержка взаимодействия с различными программными механизмами управления доступом к объектам локального узла, и, как следствие, поддержка различных математических моделей логического разграничения доступа. При этом, Nettrust может функционировать в информационной системе, разные узлы которой используют различные математические модели и реализуемые их программные механизмы управления доступом к объектам локального узла. Установка Nettrust не требует массовой существенной модификации приложений в составе подконтрольной распределенной информационной системы, так как управление доверием между субъектами осуществляет специальный модуль ядра операционной системы. Кроме того, комплекс имеет специальные функции, позволяющие существенно упростить управление доверием между субъектами очень больших, сложно организованных распределенных информационных систем. В сообщении перечислены основные требования, предъявляемые к данному программному комплексу, и базовые принципы его разработки, направленные на достижение этих требований. Представлены сведения об управлении Nettrust, которое осуществляется с помощью протокола Netlink, традиционно используемого для управления сетевыми конфигурациями Linux, либо с помощью специальных прикладных утилит.