ИССЛЕДОВАНИЕ УПРАВЛЕНИЯ ДИСПЕТЧЕРОМ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННОЙ СЕТИ

Скомороха Л.С
Научный руководитель – к.т.н., доц. Золотарев В.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр.Ленина,14, каф. Сети связи, тел.(057)702-14-29),

This given work is devoted consideration of questions and methods of realization of mandatory and discretionary mechanisms of access control to the resources by additional facilities of protection from unauthorized access.

В настоящее время для каждой корпоративной сети необходимо иметь четкую политику в области информационной безопасности.

Данная статья посвящена рассмотрению вопросов и способов реализации мандатного и дискреционного механизмов контроля доступа к ресурсам добавочными средствами защиты от несанкционированного доступа (СЗИ НСД). Необходимость подобного исследования обусловливается: во-первых, полномочный (мандатный) механизм контроля доступа к ресурсам по своей сути (обработка информации различных уровней конфиденциальности) предполагает использование на критичных объектах, к которым выставляются повышенные требования к защите информации от НСД. Во-вторых, данные механизмы не реализуются большинством ОС, поэтому, как правило, их реализация возлагается на добавочные средства защиты. В-третьих, именно с реализацией данных механизмов связано наибольшее количество вопросов, которые не всегда обоснованно решаются разработчиками добавочных СЗИ НСД. Основу мандатного управления доступом (англ.MAC) - составляет включение в схему управления доступом к ресурсам меток безопасности, отображающих полномочия субъектов и объектов. Задача, которая должна решаться дискреционным механизмом управления доступом (англ.DAC), используемым в дополнение к мандатному – это разграничения прав доступа к объектам, хранящим исполняемые файлы. Правила разграничения доступа здесь сводятся лишь к простейшей схеме – разрешить, либо нет исполнение процесса. Итак, в системе вычислительной техники должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Очевидно, что система, которая обеспечивает разделение данных и операций в компьютере, должна быть построена таким образом, чтобы её нельзя было «обойти».