УДК 004.056

Методы обнаружения сетевых атак типа “отказ в обслуживании”

Лапин Николай Андреевич
Университет ИТМО, Санкт-Петербург

Научный руководитель – Пантюхин Игорь Сергеевич
Университет ИТМО, Санкт-Петербург

Введение:

Сетевые атаки на отказ в обслуживании далеко не новая проблема, одна из первых известных атак была произведена еще в феврале 2000-го года и была направлена на ряд серверов электронной коммерции (Amazon, ebay.com, buy.com, etrade.com и другие). С того времени произошло еще множество атак данного типа, были нанесены серьезные ущербы. Проблема сетевых атак данного типа до сих пора актуальна, потому что универсального решения для защиты от них не было предложено.

Цель работы:

Разработка методов обнаружения сетевых атак типа “отказ в обслуживании” на сетевом уровне.

Промежуточные результаты:

В ходе выполнения работы были выявлены взаимосвязи сетевых атак со скачками использования ресурсов системы, входящим и исходящим трафиком.

Основной результат:

Атаки типа “отказ в обслуживании” не однотипны и являются целой группой атак. В ходе работы были выявлены подкатегории данного типа атак и для каждой из них представлены методы обнаружения.