РАЗРАБОТКА ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ВЫЯВЛЕНИЯ ВНЕШНИХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

И.В. Рубан, д.т.н., проф.; Д.В. Прибыльнов
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В настоящее время одной из угроз государственной безопасности и безопасности вооружѐнных сил являются информационные операции в кибернетическом пространстве. Как показывает анализ событий протекающих в информационном пространстве, связанных с хакерскими и вирусными атаками на информационные ресурсы разных государств (Британия, Сирия, США, Грузия, Россия), существующая система информационного противодействия в кибер-пространстве не является совершенной. Проведенный анализ методов информационного воздействия в кибер-пространстве указывает на то, что наиболее распространѐнными атаками являются атаки типа «Отказ в обслуживании» или DOS-атаки. В настоящий момент, нерешѐнной задачей является противодействие медленным DOS-атакам. Это вызвано тем, что обнаружение данного типа атак затруднено из-за отсутствия явных проявлений изменений интенсивности информационных потоков на начальной стадии выполнения атаки. Механизм действия медленной DOS-атаки основан на особенностях рестарта протокола транспортного уровня TCP, и реализуется за счѐт формирования служебных пакетов с протокольными характеристиками в части выбора временного интервала поступления на вход информационного узла распределѐнной системы. Для решения задачи противодействия медленным DOS-атакам предлагается разработка метода распознавания данного типа атак за счѐт использования механизмов пассивного анализа протокольных характеристик. Части оценки временных и информационных параметров входящего трафика и активных механизмов блокирования информационных направлений инициирующих процедуру отказа в обслуживании протоколом TCP. Данный подход позволяет обнаружить пассивную DOS-атаку, классифицировать еѐ и блокировать вредоносные информационные направления.

ТЕХНОЛОГИЯ УПРАВЛЕНИЯ ДОСТАВКОЙ ПАКЕТОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

И.В. Рубан, д.т.н., проф.; М.И. Литвиненко, к.т.н.; А.О. Смирнов
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Современный этап развития общества характеризуется глобальным проникновением информационных технологий в нашу жизнь. Этот процесс сопровождается развитием способов обработки информации, важность и стоимость которой, зачастую, тяжело переоценить, а также ростом угроз информационной безопасности (ИБ). Следовательно, информационная безопасность становится обязательным условием и ставит перед нами новые задачи по еѐ обеспечению.

Одной из угроз информационной безопасности является несанкционированная деятельность нарушителя ИБ. На этапе организации атаки перед ним стоит задача получить максимум информации об атакуемой системе и среде еѐ функционирования. Для этого нарушителю, как правило, необходимо физически внедриться в атакуемую сеть и провести пассивный и активный сбор информации. Получить необходимую информацию возможно посредством проведения атак типа «Man-in-the-Middle», IP-спуфинг, сниффинг пакетов, подбор паролей. В основе данных атак лежат недостатки протоколов маршрутизации. Основными, на наш взгляд, являются необходимость создания виртуального канала связи между абонентами, и трансляция TCP-пакетов в