Г. О. Крылов, М. М. Тараскин, С. А. Чешуин

КОМПЬЮТЕРНЫЕ АТАКИ С «РАСПРЕДЕЛЕННЫМ ОТКАЗОМ В ОБСЛУЖИВАНИИ» НА ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ И МЕХАНИЗМЫ ЗАЩИТЫ ОТ НИХ НА ОСНОВЕ СТРУКТУРНО-СТАТИСТИЧЕСКОГО АНАЛИЗА ВХОДНОГО ПОТОКА ДАННЫХ

Надежное и безопасное функционирование современных компьютерных систем, базирующихся на использовании глобальной информационной сети Интернет, невозможно без реализации эффективных механизмов информационной защиты, в том числе предупреждения и препятствования выполнению компьютерных атак: их обнаружения, отслеживания источника атак и противодействия им [1, 2].

Компьютерные атаки на вычислительные сети осуществляют специальные службы иностранных государств, представители криминальных структур, хакеры и т. п. Одной из разновидностей компьютерных атак является атака с «распределенным отказом в обслуживании» (Distributed Denial of Service, DDoS), в ходе которой злоумышленник сначала компрометирует («взламывает») большое количество сетевых компьютеров (хостов) для запуска на них средств реализации атак «Отказ в обслуживании» (Denial of Service — DoS), а затем реализует одновременное нападение на хост (сеть) — цель атаки. Использование данного типа КА для нанесения ущерба обусловлено простотой их организации, малой стоимостью, отсутствием необходимости глубоких знаний компьютерных технологий и языков программирования для их реализации.

Первые атаки DDoS произошли летом 1999 г. Одна из первых крупномасштабных атак DDoS была осуществлена против Yahoo.com в феврале 2000 г. Эта атака привела к недоступности Yahoo из Интернета в течение примерно двух часов и большим убыткам Yahoo. Другая известная атака DDoS была реализована 20 октября 2002 г. Она была направлена против 13 корневых серверов, которые обеспечивают DNS-услуги для пользователей Интернета во всем мире. Из последних локальных событий можно отметить продолжительные DDoS-атаки на сайты www.mobile-revievvs.com и www.ultracomp.ru в период с августа по сентябрь 2007 г., а также на вычислительные сети (ВС) РФ в ходе грузино-югоосетинского конфликта на Северном Кавказе в августе 2008 г. [3].

Атака с «распределенным отказом в обслуживании» — это скоординированное действие, направленное на нарушение доступности услуг (сервисов) некоторой системы или сетевого ресурса, инициированное посредством использования множества скомпрометированных компьютеров (хостов), размещаемых в сети Интернет. Она базируется на реализации множества отдельных атак «Отказ в обслуживании». Хосты (компьютерные системы, в том числе сети), подвергающиеся атаке, часто называются «первичными жертвами» (первичными целями атаки), в то время как скомпрометированные хосты (системы), используемые для реализации атаки, называются «вторичными жертвами» (вторичными целями атаки).

Практически все реализации атак DDoS основаны на трехуровневой архитектуре, показанной на рис. 1.

Атакующий (или несколько атакующих) контролирует один или несколько серверов, на которых размещаются агенты-мастера, или менеджеры (masters), каждый из которых управляет множеством агентов-исполнителей атаки – демонов (daemons), распределенных по различным хостам сети Интернет.

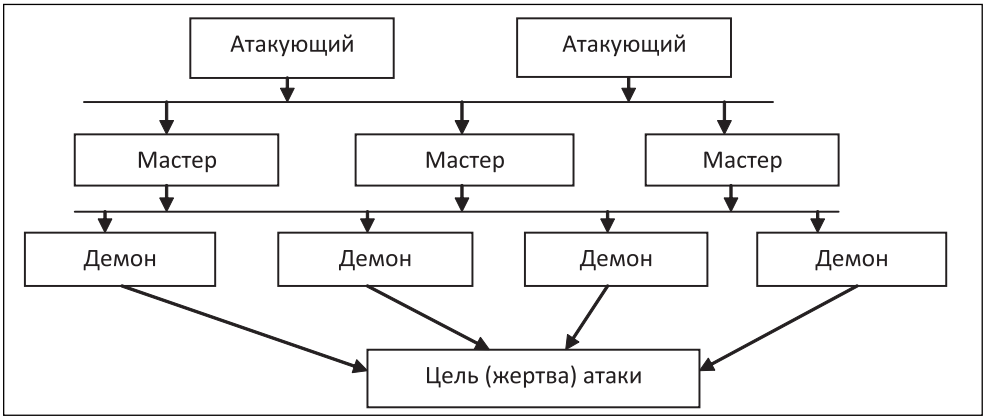

Рис. 1. Обобщенная архитектура реализации атак DDoS

Элементы вычислительной сети, на которые может осуществляться воздействие, представлены на рис. 2.

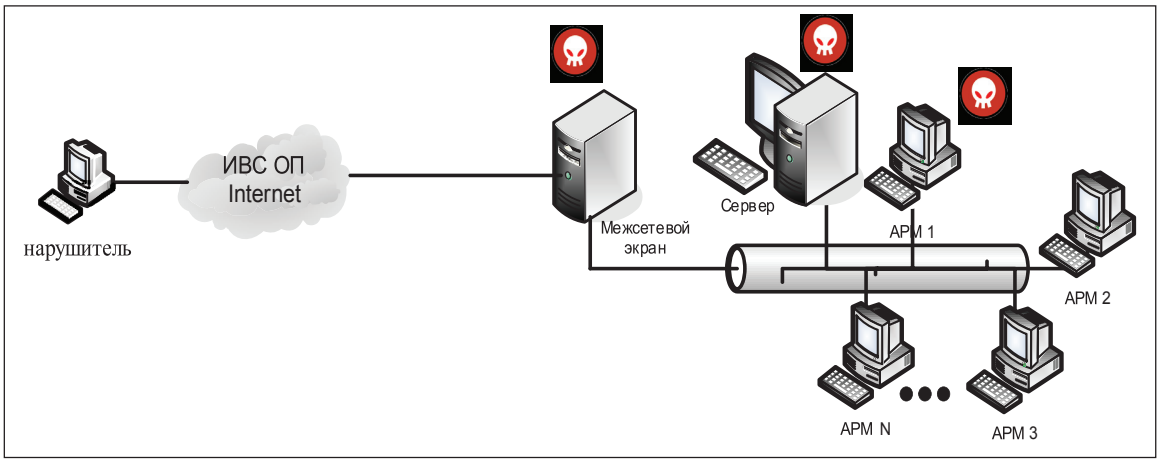

Рис. 2. Элементы вычислительной сети, на которые может осуществляться воздействие КА с «распределенным отказом в обслуживании»

Атаки осуществляются с помощью непосредственной посылки жертве большого количества пакетов (как, например, UDP и ICMP flood) или использования для этой цели промежуточных узлов (примеры — некорректные пакеты (Land) или большое количество трудоемких запросов (TCP SYN) и другие). Их классификация представлена на рис. 3.

Обнаружение факта атаки может осуществляться как на основе методов обнаружения аномалий (отклонений), так и на основе обнаружения злоупотреблений. В значительном числе случаев обнаружение выполняется по аномально высокому уровню нагрузки на сеть или узлы, а также большому трафику по определенному протоколу. Основа определения факта атаки — сравнение текущих параметров пакетов (трафика) с данными, свидетельствующими об атаке (по сигнатуре), которые размещаются в словарях признаков системы обнаружения атак (СОА) или по возникновению аномалий [2].

Необходимость внедрения такого рода систем обусловлена тем, что существующая технология межсетевого экранирования не всегда способна обеспечить защиту информационных ресурсов вычислительных сетей. Анализ известных способов и методов защиты информации с использованием межсетевых экранов (МСЭ) показал, что, хотя существующие МСЭ могут

служить достаточно надежным барьером для защиты от КА, тем не менее, они обладают целым рядом недостатков и существует перечень угроз, которым они не в состоянии противостоять:

• МСЭ уязвимы из-за неправильной конфигурации и настройки;

• до 80% источников нарушений находятся внутри сети, а не в ИВС ОП [4]. МСЭ не обеспечивают защиты сети в случае несанкционированного использования модемов для подключения к вычислительным сетям общего пользования (ИВС ОП) в обход МСЭ.

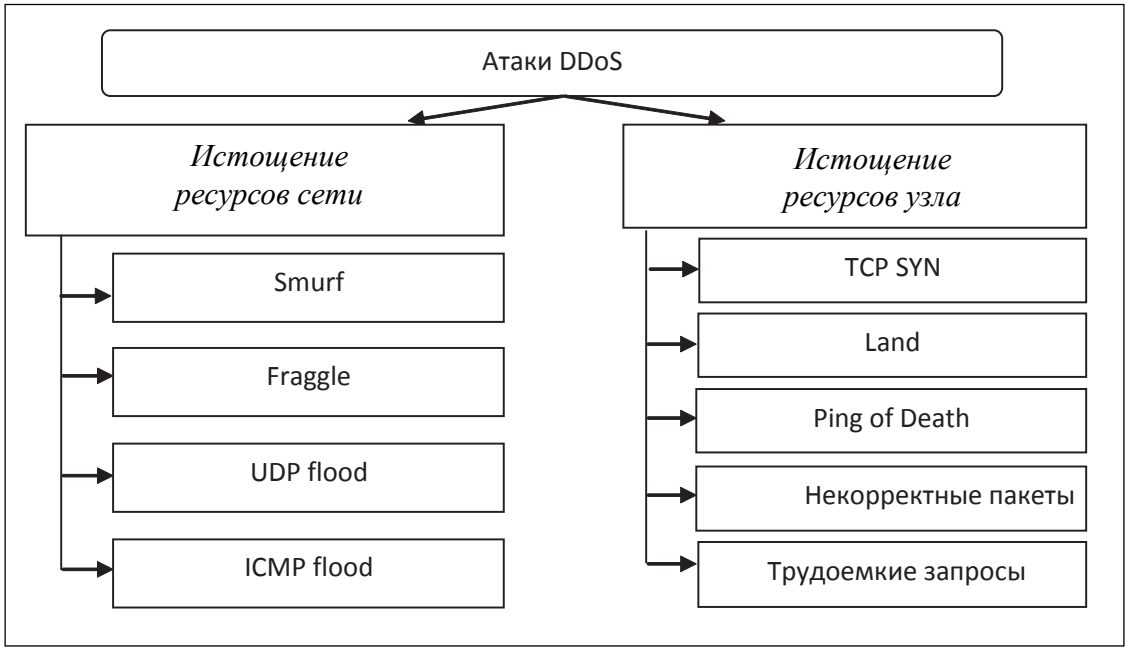

Рис. 3. Классификация атак DDoS

Применение МСЭ необходимо для обеспечения централизованного контроля над входящим/исходящим трафиком, но явно недостаточно для противодействия компьютерным атакам.

СОА являются более гибким и мощным средством, позволяющим производить обнаружение атак на вычислительные сети на начальном этапе и осуществлять слежение за аппаратно-программной средой [5].

Результаты анализа достоинств и недостатков существующих СОА позволяют предположить (это подтверждается и в ряде работ [6,7,8]), что в настоящее время ими не в полной мере обеспечивается обнаружение КА с требуемой эффективностью по критерию «своевременность — достоверность».

Проведенные исследования на моделях ВС показали, что более 40 % времени при функционировании вычислительной сети затрачивается на анализ входного трафика с целью обнаружения КА, а подпроцесс поиска признака в словаре признаков КА оказывается наиболее времяемким (более 37 %).

Исследования, проведенные в процессе рассмотрения различных способов поиска в словаре признаков, показали, что наиболее оперативным является способ, основанный на использовании хеш-функции. Однако при хешировании возможно возникновение коллизий. Для их устранения предлагается использовать «расширенное» хеширование, которое позволяет производить сравнение признаков пакета с ячейкой словаря признаков то количество раз, которое записано в дополнительной вспомогательной памяти СОА.

Для выявления признаков ранее неизвестных КА, с целью недопущения их пропусков, предлагается использовать два словаря признаков, в одном из которых находятся признаки КА,

а в другом — признаки легальных пакетов. В случае если пакет не соответствует признакам ни одного словаря признаков, то решение о его классификации предоставляется должностному лицу (ДЛ), ответственному за безопасность вычислительной сети.

Современные способы обнаружения КА обычно разделяют на структурные и статистические. Правильное обнаружение признаков КА по структуре обеспечивает достоверные исходные данные для статистического оценивания. Поэтому был разработан алгоритм комплексного обнаружения КА на ВС по структуре и статистике. Его общий вид представлен на рис. 4.

Общий выигрыш от использования разработанного алгоритма по критерию «своевременность – достоверность» по сравнению с существующим составляет более 10 %. В свою очередь, выигрыш по своевременности обнаружения КА – 40 % при некотором снижении достоверности обнаружения КА.

Проведенные расчеты эффективности обнаружения КА в вычислительных сетях для существующих и предлагаемого алгоритмов обнаружения КА позволяют сделать вывод о том, что внедрение разработанного алгоритма обнаружения КА в административную практику в виде аппаратно-программных средств и его комплексное применение позволят повысить эффективность функционирования как систем обнаружения атак, так и вычислительных сетей в целом.

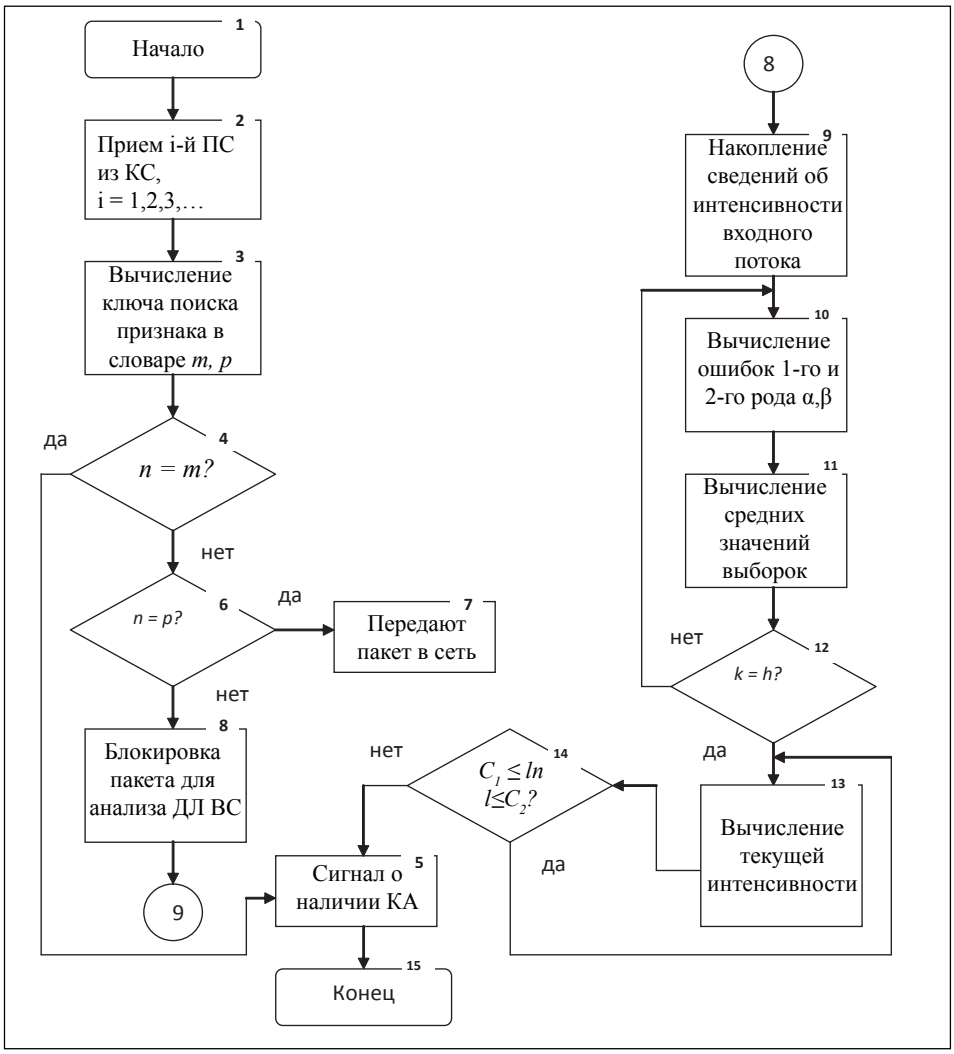

Рис. 4. Алгоритм обнаружения КА на вычислительные сети по структурным и статистическим признакам,

где ПС (n) — пакет сообщения; КС — канал связи; (m, ρ) — ключи поиска, вычисленные методом хеш-функции в словарях: признаков атак и признаков легальных пакетов соответственно; α — вероятность ошибки первого рода (ложной тревоги), β — вероятность ошибки второго рода (пропуска); k — интенсивность входного потока, характеризующая стационарное состояние (без «разладки»); h — вычисленные значения средних размеров выборок; ln l *(x_1 x_2 x_3, ... x_n) — логарифм отношения правдоподобия признаков входного потока, c_1 — нижний порог стационарного состояния, c_2 — верхний порог стационарного состояния.*

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «Об информации, информационных технологиях и защите информации» №149-ФЗ, 2006 г.
2. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001. — 376 с.
3. *Уланов А. В.* Многоагентное моделирование механизмов защиты от атак «распределенный отказ в обслуживании»: Дисс. ... канд. тех. наук. СПб., 2007.
4. *Лукацкий А. В.* Обнаружения атак. СПб.: БХВ-Петербург, 2001. — 624 с.
5. *Котенко И. В.* Теория и практика построения автоматизированных систем информационной и вычислительной поддержки процессов планирования связи на основе информационных технологий. Монография. СПб.: ВАС, 1998. — 404 с.
6. *Корт С. С.* Теоретические основы защиты информации. М.: Гелиус-АРВ, 2004. — 233 с.
7. *Горелик А. Л., Скрипник В. А.* Методы распознавания. Учеб. пособие для вузов. М.: Высш. Школа, 1977. — 222 с., илл.
8. Фомин Я.А. Распознавание образов. Теория и практика. М.: ФАЗИС, 2010-368 с.