УДК 681.3.06

**С.Л. Михайлюта**, к.т.н.
**И.В. Степанушко**
**Б.А. Бабич**
**В.Ю. Ткаченко**
**В.С. Лавринович**

# ИССЛЕДОВАНИЕ СЕТЕВЫХ DOS-АТАК, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ ПРОТОКОЛА ICMP

Черкасский институт банковского дела, e-mail: sem_esit@mail.ru.
Черкасский государственный технологический университет, e-mail: ram_bb@mail.ru.

*В статье рассмотрены вопросы безопасности корпоративных сетей. Исследованы DOS – атаки. Описана корпоративная сеть, с помощью которой проведено моделирование DOS – атак. Рассмотрена процедура осуществления DOS – атак, методы детектирования, противодействия.*

## Постановка задачи

В период активного развития и внедрения в повседневную жизнь информационных технологий важную роль играет надежность систем, обеспечивающих хранение информации и доступ к ней. Применение электронных технологий наряду с преимуществами произвело новый вид угроз для современного общества — информационный. Разрушение, изменение, кража информации приводят к значительному экономическому ущербу. На сегодняшний день рядовыми стали случаи, когда стоимость «прецедентов» составляет сотни тысяч и миллионы долларов [1]. Потери такого уровня представляют угрозу национальной безопасности. Сверхинформатизация структур управления делает их чрезвычайно уязвимыми. Создание специальных профильных военных подразделений в США, Китае, России говорит о существенности угроз такого рода.

## Анализ публикаций

Атаки на компьютерные сети коммерческих структур — достаточно обыденная практика как аргумент экономической конкуренции. Изменился характер атак: они стали целевыми [2,3]. Т.о. вопросы, связанные с организацией и защитой от сетевых атак приобретают в настоящий момент особую значимость. Целевая кибератака соответствующим образом подготавливается с учетом технических, программных и человеческих ресурсов, цели атаки. Широкое распространение получили атаки «отказ в предоставлении сервиса», принцип которых заключается в том, что атакующий пытается загрузить (или саботировать) некоторые сервисы настолько, чтобы они перестали нормально функционировать (корректно отрабатывать запросы пользователей) [2,3]. Сегодня существуют утилиты, позволяющие проводить такие атаки даже непрофессионалам. На практике, проще нарушить работу сети или системы, чем получить к ней неавторизированный доступ.

Сетевые протоколы TCP/IP были разработаны без учета многих вопросов безопасности. Современная четвертая версия стека TCP/IP унаследовала эти "недостатки" предыдущих вариантов. Кроме того, многие системы имеют собственные ошибки в реализации стека, что снижает их способность противостоять атакам DoS.

## Цель исследования

Проведенное нами исследование выполнено в рамках проекта, целью которого является изучение принципов организации, методов распознавания и противодействия сетевым атакам DoS Ping Flooding и Smurfing в тестовой среде и в реальной сети компьютерной лаборатории.

## Описание лабораторной системы для моделирования сетевой атаки

Для моделирования атаки на практике использовалась локальная сеть из 9 компьютеров соединённых через неуправляемый switch. Все машины оснащены 2.8 ГГц процессорами Celeron и 1 Гб ОЗУ. На каждом компьютере установлена ОС Windows XP SP2 с актуальным набором обновлений безопасности.

Топология локальной сети приведена на рисунке 1.

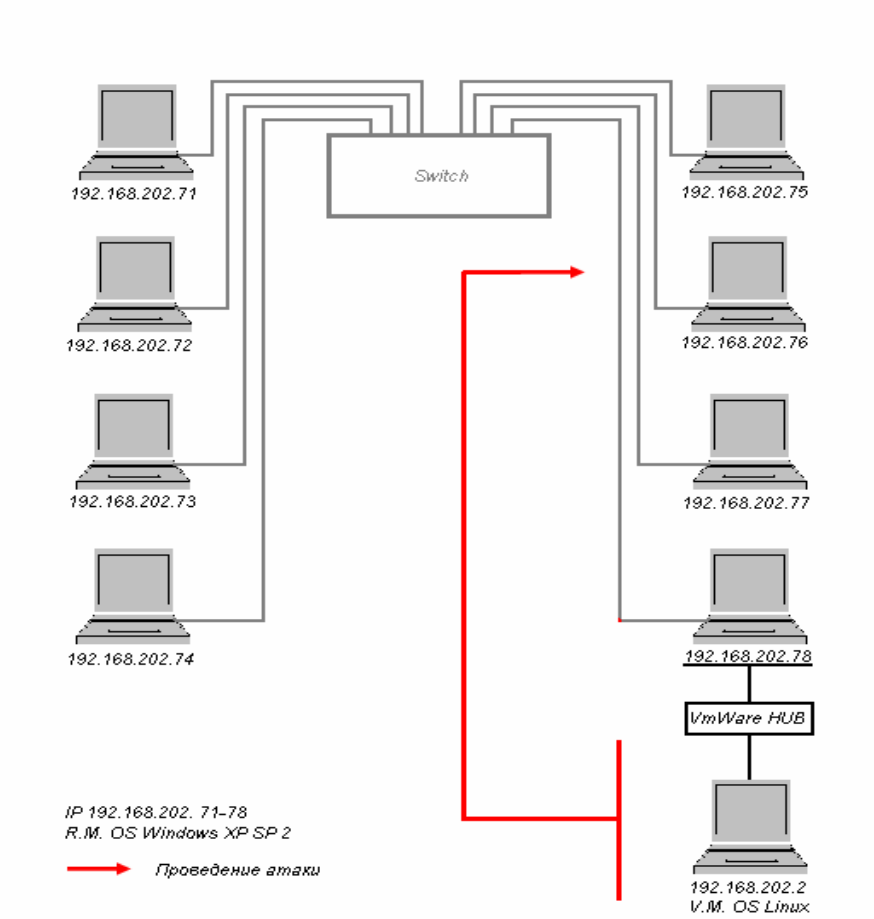


Рис. 1 – Топология локальной сети.

В ходе моделирования использовалось следующее программное обеспечение: ОС Windows XP SP2, ОС Linux, анализатор сетевых пакетов WireShark, генератор сетевых пакетов Hping2, система обнаружения вторжений SNORT.

**Выполнение атаки, результаты и следствия**

Проведение атаки смоделировано следующим образом:

1. На атакующей машине формируется непрерывный поток ICMP пакетов с помощью программы Hping2.

2. На атакуемой машине устанавливается анализатор пакетов и система обнаружения вторжений SNORT [4], анализируется структура приходящих пакетов, загрузка сетевого интерфейса, загрузка процессора.

Анализ трафика позволил установить наличие непрерывного потока фрагментированных пакетов, отправляемых на целевой хост машины-«жертвы», при этом адрес машины-отправителя постоянно изменяется, что дает атакующему некоторою анонимность и возможность нарушить работоспособность сети даже с узким каналом связи [5].

**Детектирование (обнаружение атаки)**

Существует мнение, что специальные средства для обнаружения DoS-атак не требуются, поскольку факт DoS-атаки невозможно не заметить. Во многих случаях это действительно так. Однако, часто отмечались успешные атаки, которые были замечены «жертвами» лишь через 2-3 суток. Иногда негативные последствия атаки (типа флуд) заключаются в излишних расходах по оплате трафика, что выяснялось лишь при получении счёта за трафик.

Методы, которыми возможно обнаружить атаки условно разделены на 3 группы: сигнатурные (основанные на качественном анализе трафика), статистические (основанные на

количественном анализе трафика), гибридные (сочетающие в себе достоинства двух предыдущих методов).

Хорошие результаты дает автоматизация слежения за работоспособностью сети — что является правилом хорошего тона при построении систем безопасности. Система обнаружения вторжений успешно распознает и регистрирует в журналах протоколов факт проведения атаки. К тому же, для эффективного противодействия необходимо знать тип, характер и другие показатели атаки, а оперативно получить эти сведения позволяют системы обнаружения вторжений.

**Противодействие (защита от DoS-атак)**

Говоря о конкретных мерах защиты систем, будем рассматривать наиболее эффективные методы. Меры противодействия DoS-атакам можно разделить на пассивные и активные, а также на превентивные и реакционные.

Ниже приведён краткий перечень основных методов:

- Предотвращение. Профилактика причин, побуждающих тех или иных лиц организовывать DoS-атаки. Очень часто атаки являются следствиями личной обиды, политических, религиозных разногласий, провоцирующего поведения жертвы и т. п.
- Фильтрация и блекхолинг. Эффективность этих методов снижается по мере приближения к цели атаки и повышается по мере приближения к её источнику.
- Устранение уязвимостей. Не работает против атак типа флуд, для которых «уязвимостью» является конечность тех или иных ресурсов.
- Наращивание ресурсов.
- Рассредоточение. Построение распределённых и продублированных систем, которые не прекратят обслуживать пользователей даже если некоторые их элементы станут недоступны из-за атаки.
- Уклонение. Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью.
- Активные ответные меры. Воздействие на источники, организатора или центр управления атакой. Меры могут быть как технического характера (не рекомендуется), так и организационно-правового характера.

**Заключение**

Проведенные исследования позволили сделать следующие выводы:

– Успех атаки зависит от конкретной конфигурации сети, наличия в ней средств детектирования атак и противодействия им.

– В простых сетях DoS атаки практически всегда успешны.

– DoS атаки на основе загрузки сети пакетами широко используемых протоколов (типа ICMP) в 90% случаев успешны.

– Необходимы новые средства защиты корпоративных сетей от DoS атак.

**Список литературных источников**


1. “Безопастность сетей” http://www.intuit.ru/department/security/netsec/3/4.html.
2. “Безопастность сетей” http://lagman-join.narod.ru/spy/index.htm.
3. “Denial of Service Attacks” http://www.cert.org/tech_tips/denial_of_service.html
4. “Обнаружение вторжений” http://snort.org
5. “Проблемы безопасности протоколов TCP/IP” http://athena.vvsu.ru/net/book/security.html.



***Ключевые слова:*** корпоративная сеть, безопасность, DOS – атака, моделирование, детактирование, противодействие.