

УДК: 004.712

## СЕТЕВЫЕ АТАКИ В РОССИИ

*Тухфатуллова Э.И., студентка 3 курса экономического факультета  
Научный руководитель – Голубев С.В., к.э.н., доцент  
ФГБОУ ВО Ульяновский ГАУ*

**Ключевые слова:** сетевая атака, методы защиты, специализированные программы, информационные технологии, интернет.

*Работа посвящена изучению сетевых атак в России. Авторами выявлены основные виды сетевых атак, способы борьбы с ними и статистика сетевых атак в России.*

В настоящее время современный социум уже не может обойтись без информационных технологий. Информационные процессы внедрились во все сферы человеческой жизни. Их необходимой составляющей является глобальная сеть Интернет. Безусловно, одной из основных задач считается обеспечение безопасности обращения данных внутри сети. Одной из угроз для безопасности являются сетевые атаки.

Согласно взгляду Шаньгина В.Ф. под сетевой атакой подразумевается стремление воздействовать на удаленный ПК с внедрением программных способов. Задача сетевой атаки - хищение данных. Кроме этого, сетевые атаки также проводятся с целью получения доступа к чужому ПК и последующего изменения файлов, расположенных на нем (2, с.256).

В наше время акцентируют следующие атаки в России: DoS-атака, mailbombing, сетевая разведка, phishing-атаки, переполнение буфера, использование специализированных программ (вирусы, sniffеры) и инъекция (SQL-инъекция, PHP-инъекция).

Ниже приведены сведения, в которых были зафиксированы наиболее популярные разновидности сетевых атак в России за 2016 год.

Denial of Service (DoS) является наиболее известной формой хакерских атак. Она занимает 53 % в нашей статистике. Помимо этого, против атак такого типа труднее всего создать 100 %-ю защиту. Из числа хакеров атаки DoS считаются детской забавой, а их использование порождает презрительные усмешки, так как для организации DoS требуется минимум знаний и умений. Тем не менее, непосредственно простота реализации и огромные масштабы причиняемого ущерба привлекают к

■ DoS-атака   ■ Mailbombing   ■ Сетевая разведка   ■ Phising-атака

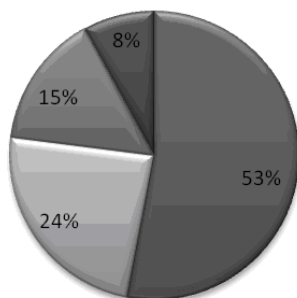


Рисунок 1 - Распространенные виды сетевых атак в России за 2016 г.

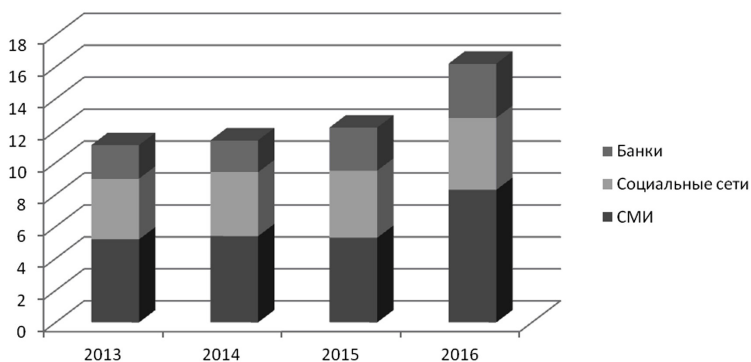


Рисунок 2 - Жертвы DoS-атаки за 2013-2016 г.

DoS пристальное внимание администраторов, отвечающих за сетевую безопасность (1). Далее представлены сведения о жертвах DoS-атаки за 2013-2016 годы.

Исходя из данных, можно сделать вывод о том, что самой сильной жертвой DoS-атаки являются средства массовой информации. На втором месте находятся социальные сети, и на третьем месте – банки. В 2013-2015 годах СМИ имел незначительный рост, а в 2016 году видно резкое повышение. Социальные сети и банки также с каждым годом растут, но не настолько значительно, как СМИ.

На втором месте – mailbombing (24%). Сущность атаки состоит в том, что на почтовый ящик пользователя посылается колоссальное число писем. Данная атака способна вызвать отказ работы почтового ящика или даже целого почтового сервера. Достаточно знать адрес сервера, который позволяет анонимно отправлять почтовые сообщения, и адрес пользователя, которому эти сообщения предназначены. Методы защиты:

- давать адрес электронной почты только проверенным источникам
- в качестве преграды для mailbombinga может выступать и Web-сайт провайдера, автоматически определяющий почтовые атаки.

На третьем месте находится сетевая разведка, занимающая 15 %. Это сбор данных о сети с помощью общедоступных приложений. Сетевая разведка проводится в форме запросов DNS (помогают понять, кто владеет тем или иным доменом), эхо-тестирования (позволяет увидеть, какие хосты работают в данной среде) и сканирования портов (позволяет составить полный список услуг, поддерживаемых этими хостами). В итоге добывается информация, применяющаяся для взлома. Методы защиты:

- отключение эхо ICMP и эхо-ответ на периферийных маршрутизаторах
- использование систем обнаружения вторжений.

И на четвертом месте нашей статистики - phishing-атаки (8%). Phishing это социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют спам или компьютеры-боты. Методы защиты:

- применять только проверенные ресурсы и пути доступа к ним
- применять антивирусные средства и регулярно обновлять их сигнатуры.

В заключении хотелось бы сказать, что данная сфера является наиболее развивающейся, так как идет непрерывная конкурентная борьба между злоумышленниками и организациями, которые гарантируют безопасность данных. Шаньгин В.Ф. считает, что, несмотря на возможное применение комплексных мер по защите компьютера, наиболее прочным методом защиты ПК является применение проверенных электронных ресурсов, чтение писем из проверенных источников, то

есть наибольшую защиту от атак может обеспечить сам пользователь, соблюдая меры осторожности (2, с.264).

*Библиографический список*

1. Шелухин, О.И. Обнаружение DOS и DDOS-атак методом дискретного вейвлет-анализа / О.И. Шелухин, Ю.А. Иванов, В.Ю.Ригов // Т-Сomm - Телекоммуникации и Транспорт. - 2011. - №1. - С. 4446.
2. Шелухин, О.И. Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского / О.И. Шелухин, А.С. Филинова // Т-Сomm - Телекоммуникации и Транспорт. -2013.-Том 7, № 10. - С. 116-118.
3. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин.- М.: ДМК Пресс, 2014. – 544с.

## **NETWORK ATTACKS IN RUSSIA**

*Tukhfatullova E. I.*

**Key words:** *network attack, methods of protection, specialized programs, information technology, Internet.*

*The work is devoted to the study of network attacks in Russia. The authors identified the major types of network attacks, ways of dealing with them, and statistics of network attacks in Russia.*