университет, Институт спектроскопии РАН, Институт лазерной физики СО РАН, Институт прикладной физики РАН и целый ряд других научно-исследовательских центров. Росатом, ФПИ и Минобрнауки в апреле 2016 г. подписали соглашение о создании и поддержке совместных лабораторий, где будут разрабатывать технологии, необходимые для создания квантового компьютера. Проект рассчитан на 3,5 года с суммарным объемом финансирования 750 миллионов рублей. Предполагается, что создание квантового компьютера радикально поднимет уровень вычислений и позволит обеспечить революционные достижения во многих областях науки и техники.

Литература

1. IBM Quantum Experience. URL: http://www.research.ibm.com/quantum/ (дата обращения: 10.10.2016).
2. Quantum Computing Playground. URL: ttps://www.chromeexperiments.com/experiment/quantum-computing-playground (дата обращения: 10.10.2016).

УДК 004.38:004.94

А.К. Гуц, Т.В. Вахний

Омский государственный университет им. Ф.М. Достоевского, г. Омск, Россия

ОТРАЖЕНИЕ DDoS-АТАКИ И ДИФФЕРЕНЦИАЛЬНЫЕ ИГРЫ

Распределенная атака типа отказ в обслуживании является одной из самых распространенных и опасных сетевых атак. В случае совершенной DDoS-атаки может быть полностью нарушена работа любого ресурса – от небольшого информационного сайта до крупного интернет-магазина или почтового сервера. Существует множество видов DDoS-атак, большинство из них используют уязвимости в основном протоколе Internet (TCP/IP), а именно, способ обработки системами запроса SYN. При коллек-

тивной отправке с компьютеров злоумышленника бессмысленных вредоносных запросов атакуемый сервер не успевает их обрабатывать. В результате легитимные пользователи не могут получить доступ к предоставляемым системой ресурсам (серверам), либо такой доступ затруднён. Целью такой атаки является доведение компьютерной системы до отказа в обслуживании. Бороться с таким видом атак достаточно сложно ввиду того, что запросы поступают с различных сторон. Однако, несмотря на это, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния [1].

В данной работе DDoS-атаки рассматриваются как дифференциальная игра двух игроков – хакера и администратора, первый из которых управляет трафиком τ, а второй производительностью p компьютерной системы. Устанавливается наличие особого типа оптимального управления (τ^*, p^*), известного в теории игр под названием равновесие Нэша.

DDoS-атаку можно описать дифференциальным уравнением [2], в котором отражено требование, что больший трафик требует нарастания числа откликов на запросы:

$$\frac{dx}{dt} = [(p - p_0) - x^2]x + (\tau - \tau_0),$$

где $x(t)$ – число откликов в момент времени t компьютерной системы на внешние запросы, востребованные при обработке получаемых системой пакетов, p_0 – «типичная» характерная для данной системы величина производительности, τ_0 – «типичная» характерная для системы «нормальная» величина трафика.

Функционирующая компьютерная система способна справляться с ежедневным характерным трафиком τ_0 с определённым запасом надёжности системы. При таком большом количестве пакетов, которое невозможно обработать, наблюдается резкое возрастание входящего трафика. Увеличение трафика, в свою очередь, требует для его обработки увеличения свободных ресурсов системы. Существует равновесие (τ^*, p^*), которое мо-

жет установиться при DDoS-атаках, если ресурсы хакера наращивать трафик не беспредельны, а компьютерная система имеет достаточно высокий уровень производительности.

Для отыскания условий этого равновесия (τ^*, p^*) авторы в данной работе воспользовались теорией дифференциальных игр, изложенной в [3].

В результате проведенных вычислений найдено позиционное равновесие Нэша

$$p^* = p_0 - \frac{1}{2}x^2, \quad \tau^* = \tau_0 - \frac{1}{2}x,$$

и выигрышные/проигрышные функции

$$J_1 = \int_0^{+\infty} [\frac{5}{4}x^4 + \frac{1}{2}x^2 + (p - p_0)^2]dt,$$

$$J_2 = \int_0^{+\infty} [\frac{3}{2}x^4 + \frac{1}{4}x^2 + (\tau - \tau_0)^2]dt,$$

администратора и хакера соответственно.

Оптимальное число откликов в момент времени t компьютерной системы на внешние запросы, востребованные при обработке получаемых системой пакетов, задается формулой

$$x^2 = 1/(Ce^t - 3),$$

где C – константа интегрирования.

Литература

1. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем: учебное пособие. Омск: Изд-во ОмГУ, 2013. 160 с.
2. *Гуц А.К., Лавров Д.Н.* Описание DDoS-атаки с помощью катастрофы «сборка» // Математические структуры и моделирование. 2013. № 1(27). С. 42–45.
4. *Lewis F.L., Vrabie D.L., Syrmos V.L.* Optimal Control. John Wiley & Sons, Inc., 2012.