МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Ф.М. ДОСТОЕВСКОГО

ОМСКИЕ НАУЧНЫЕ ЧТЕНИЯ – 2020

Материалы Четвертой Всероссийской научной конференции

(Омск, 30 ноября – 5 декабря 2020 г.)

ISBN 978-5-7779-2529-9

Омск

ИЗДАТЕЛЬСТВО ОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

2020

DDoS-АТАКИ КАК КАТАСТРОФА ТИПА «БАБОЧКА»

А.К. Гуц

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

DDoS-ATACKS AS CATASTROPHES OF BUTTERFLY TYPE

A.K. Guts

Dostoevsky Omsk State University, Omsk, Russia

Аннотация. Дается описание DDoS-атак в форме дифференциального уравнения с параметрами, которые можно представить как катастрофы типа $\mathbf{A_5}$ (бабочка) в рамках математической теории катастроф. Показано, каким образом данные атаки представляются в геометрической форме.

Abstract. A description of DDoS attacks is given in the form of a differential equation with parameters that can be represented as catastrophes of the $\mathbf{A_5}$ type (butterfly) within the framework of the mathematical theory of catastrophes. It shows how the attack data is presented in geometric form.

Ключевые слова: DDoS-атака, катастрофы, компьютерная система, атаки хакеров, катастрофа «бабочка».

Keywords: DDoS-atack, catastrophes, computer system, hacker attacks, butterfly catastrophe.

DDoS-атака (от англ. Distributed Denial of Service) — это хакерская атака на сервер типа «отказ в обслуживании». При ее исполнении создается ситуация, при которых пользователи не смогут получить доступ к сайту или веб-сервису из-за его перегрузки. Для обслуживания запросов у сервера не хватает необходимой производительности. В результате атаки владельцы проектов, размещенных на сервере, несут серьёзные убытки.

DDoS-атак совершаются на четырех уровнях OSI [1]. Прежде всего возможны «низкоуровневые атаки:

- **Атаки на сетевом уровне** OSI представляют из себя «забивание» канала. Примером может быть CMP-флуд — атака, которая использует ICMP-сообщения, которые снижают пропускную способность атакуемой сети

и перегружают брандмауэр. Хост постоянно «пингуется» нарушителями, вынуждая его отвечать на ping-запросы. Когда их приходит значительное количество, пропускной способности сети не хватает и ответы на запросы приходят со значительной задержкой. Для предотвращения таких DDoS-атак можно отключить обработку ICMP-запросов посредством Firewall или ограничить их количество, пропускаемое на сервер.

- **Атаки транспортного уровня** выглядят как нарушение функционирования и перехват трафика. Например, SYN-флуд или Smurf-атака (атака ICMP-запросами с изменёнными адресами). Последствия такой DDoS-атаки — превышение количества доступных подключений и перебои в работе сетевого оборудования.

А также имеем высокоуровневые атаки:

- **На сеансовом уровне** атакам подвергается сетевое оборудование. Используя уязвимости программного обеспечения Telnet-сервера на свитче, злоумышленники могут заблокировать возможность управления свитчем для администратора. Чтоб избежать подобных видов атак, рекомендуется поддерживать прошивки оборудования в актуальном состоянии.

- Высокоуровневые **атаки прикладного уровня** ориентированы на стирание памяти или информации с диска, «воровство» ресурсов у сервера, извлечение и использование данных из БД. Это может привести к тотальной нехватке ресурсов для выполнения простейших операций на оборудовании. Наиболее эффективный способ предупреждения атак – своевременный мониторинг состояния системы и программного обеспечения» [1].

В [2,3] была предложена катастрофическая модель описания DDoS-атак, которая имеет вид:

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

или

$$\frac{dx}{dt} = -\frac{\partial}{\partial x}V(x, p, \tau),$$

где

$$V(x,p,\tau)=\frac{1}{4}x^{\mathrm{m}+2}-\frac{1}{2}(p-p_0)x^2-(\tau-\tau_0)x.$$

где $x(t)$ – число откликов на запросы в момент времени t, τ – трафик и p – производительность сервера, p_0 и τ_0 – «типичные» характерные для данного сервера величины. Величина *m=2* в [2] и *m=7* в [3]. С учетом сказанного о каналах OSI, подвергаемых DDoS-атаках, более реалистично брать *m=4*.

Таким образом, модель системы, подвергаемой DDoS-атакам, описывается уравнением

$$\frac{dx}{dt}=[(p-p_0)-x^4(t)]x(t)+(\tau-\tau_0),$$

которое соответствует частному случаю катастрофы бабочка

$$V(x,\mathrm{A},\mathrm{B},C,D)=\frac{1}{6}x^6+Ax^4+Bx^3+Cx^2+Dx.$$

Рассматриваются стационарные равновесия изучаемой системы и находятся их бифуркационные множества. При изменении τ и p в случае пересечения ими бифуркационного множества будут наблюдаться катастрофические скачки величины *x*. *Это соответствует резкому падению (росту) числа откликов сервера на запросы.*

Бифуркационное множество для катастрофы «бабочка» изучены в [4, 5]. На рис. 1 мы приводим изображение бифуркационного множества при *A=B=*0. Следовательно, используя данные из литературы по бифуркационным множествам катастрофы «бабочка», мы сможем изучить ситуации, критические для серверов в случае DDoS-атак. Это было бы крайне трудно сделать в настоящее время для катастроф типа $\boldsymbol{A_8}$, которые рассматривались в [3].

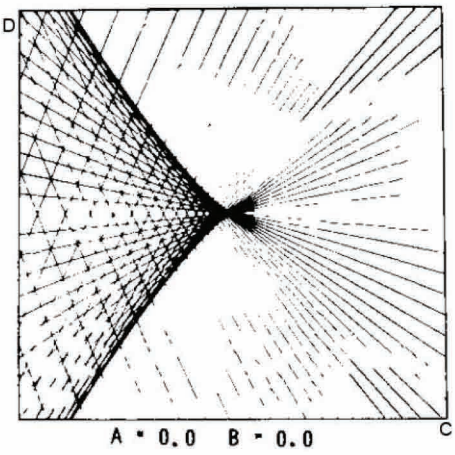

Рис.1. Бифуркационное множество в плоскости (C,D)=(p, τ).

Линии, принадлежащие бифуркационному множеству в плоскости (C,D) – это огибающие семейств прямых линий, изображенных на рисунке [5, с.20].

Список литературы:

1. DDoS-атаки: виды атак и уровни модели OSI [Электронный ресурс]. URL: https://www.reg.ru/support/hosting-i-servery/bezopasnost-hostinga/ddos-ataki-vidy-atak-i-urovney-modeli-OSI (дата обращения: 15.11.2020).

2. Гуц А.К., Лавров Д.Н. Описание DDoS-атаки с помощью катастрофы «сборка» // Математические структуры и моделирование. 2013. Вып. 27. С. 42–45.

3. Гуц А.К., Лавров Д.Н. Flood-атаки на компьютерные серверы как катастрофы типа A_8 // Математическое и компьютерное моделирование: сборник материалов V Международной научной конференции (Омск, 1 декабря 2017 г.). Омск: изд-во Омск. гос. ун-та, 2017. С.33–34.

4. Брёкер Т.,Ландер Л. Дифференциальные ростки и катастрофы. Волгоград: ПЛАТОН, 1997.

5. Woodcock A. E. R., Poston T. A Geometrical Study of the Elementary Catastrophes // Lecture Notes in Mathematics. No.373. 1974.