УДК 004.7.056.53

НЕЙТРАЛИЗАЦИЯ DDOS-АТАК С ПОМОЩЬЮ ИМПУЛЬСНОЙ НЕЙРОННОЙ СЕТИ

В. В. Цюндык *Младший научный сотрудник, e-mail: vladim_zv@mail.ru,*

М. О. Жаров *старший научный сотрудник, ФКУ НПО «СТиС» МВД России» г. Москва, Россия*

NEUTRALIZATION OF DDOS-ATTACKS USING A PULSED NEURAL NETWORK

V. V. Tsyundyk *Junior Researcher, e-mail: vladim_zv@mail.ru,*

M. O. Zharov *Senior Researcher, FKU NPO «STiS», Ministry of Internal Affairs of Russia, Moscow, Russia*

Abstract. The article is devoted to the issues of ensuring the availability and security of data during DDoS-attacks. The use of an impulse (spike) neural network (hereinafter – IMN) is considered. The principle of operation of DDoS attacks has been analyzed, and a comparison has been made between the IMNS with other information security systems.

Keywords: information; networks; pulsed neural network; DDoS-attacks; malicious traffic; information security.

Одним из ключевых требований информационной безопасности, является преемственное обеспечение доступности самой информации. Причинами недоступности данных могут быть удаленные сетевые атаки или несанкционированный трафик.

Для современных бизнес-процессов данные факторы являются серьезной угрозой, которые влекут за собой в конечном итоге существенные финансовые, репутационные и клиентские потери.

Такие киберугрозы можно разделить на однонаправленные (Denial of Service, DoS – «Отказ в обслуживании») и распределенные (Distributed Denial of Service, DDoS – «Распределенный отказ от обслуживания») атаки [1]. Различие между ними в том, что однонаправленное нападение идет из одной точки, а распределенная атака более масштабна и идет одновременно с большого числа компьютеров (ботнета).

Причины таких киберугроз различные: недобросовестная конкуренция, вымогательство, шантаж, политические протесты, развлечения или личная неприязнь.

Чаще других киберугрозам подвергаются сайты и сервера правительственных и государственных учреждений, платежных систем, банков, крупных компаний, средств массой информации (СМИ), игровых сервисов. В последнее время участились кибератаки на онлайн-кассы гипермаркетов и больших торговых центров.

Основная цель кибератаки – сделать сайт или серверы «жертвы» недоступными для пользователей, заблокировав их работу.

На данный момент однонаправленные атаки потеряли свою актуальность, так

как их эффективно отфильтровывают на уровне центров обработки данных (ЦОД).

Главным отличием распределенной атаки (DDoS-атаки) является то, что здесь помимо усиления трафика, атакующий сервер выполняет предварительное сканирование и исследование инфраструктуры, подсетей, портов и серверов атакуемого ресурса («жертвы») на предмет выявления потенциально слабых мест [2]. Определив такие места, злоумышленники распространяют троянские программы (например, через e-mail рассылки, социальные сети или сайты) с целью создания компьютерной сети с вредоносным программным обеспечением – ботнета. Далее злоумышленники отправляют специальные команды захваченным компьютерам, а те генерируют огромный объем трафика, способный перегрузить любую систему.

Одним из способов решения данной проблемы является использование импульсной (спайковой) нейронной сети (далее – ИмНС) для блокировки несанкционированного трафика. Использование ИмНС позволяет получить следующие результаты:

- равномерное распределение сетевой нагрузки;
- выявление, анализ и нейтрализация несанкционированного трафика в автоматическом режиме;
- расчет ресурсов и их загруженности;
- создание базы данных с различными видами DDoS – атак, что позволяет ИмНС составлять правила межсетевого экранирования в режиме реального времени.

Импульсная (спайковая) нейронная сеть представляет собой искусственную нейронную сеть (ИНС) третьего поколения, основное отличие которой от скоростных частотных и бинарных ИНС заключается в обмене нейронами, короткими импульсами одинаковой амплитуды. Разработка способа защиты от DDoS-атак на основе ИмНС обусловлена тем, что ИмНС является динамичной, многозадачной, высокоскоростной и быстро обучаемой. Данные особенности позволяют не только анализировать, обнаруживать и нейтрализовать DDoS-атаки, но и равномерно распределять сетевую нагрузку по физическим и логическим ядрам процессора каждого физического сервера в кластере, что в конечном итоге дает преимущество в производительности всей системы [5].

Структура ИмНС изображена на рисунке 1. Информация считывается с сетевого интерфейса физических серверов, в автоматическом режиме кодируется и в последующем импульсная нейронная сеть может в автоматическом режиме самообучаться.

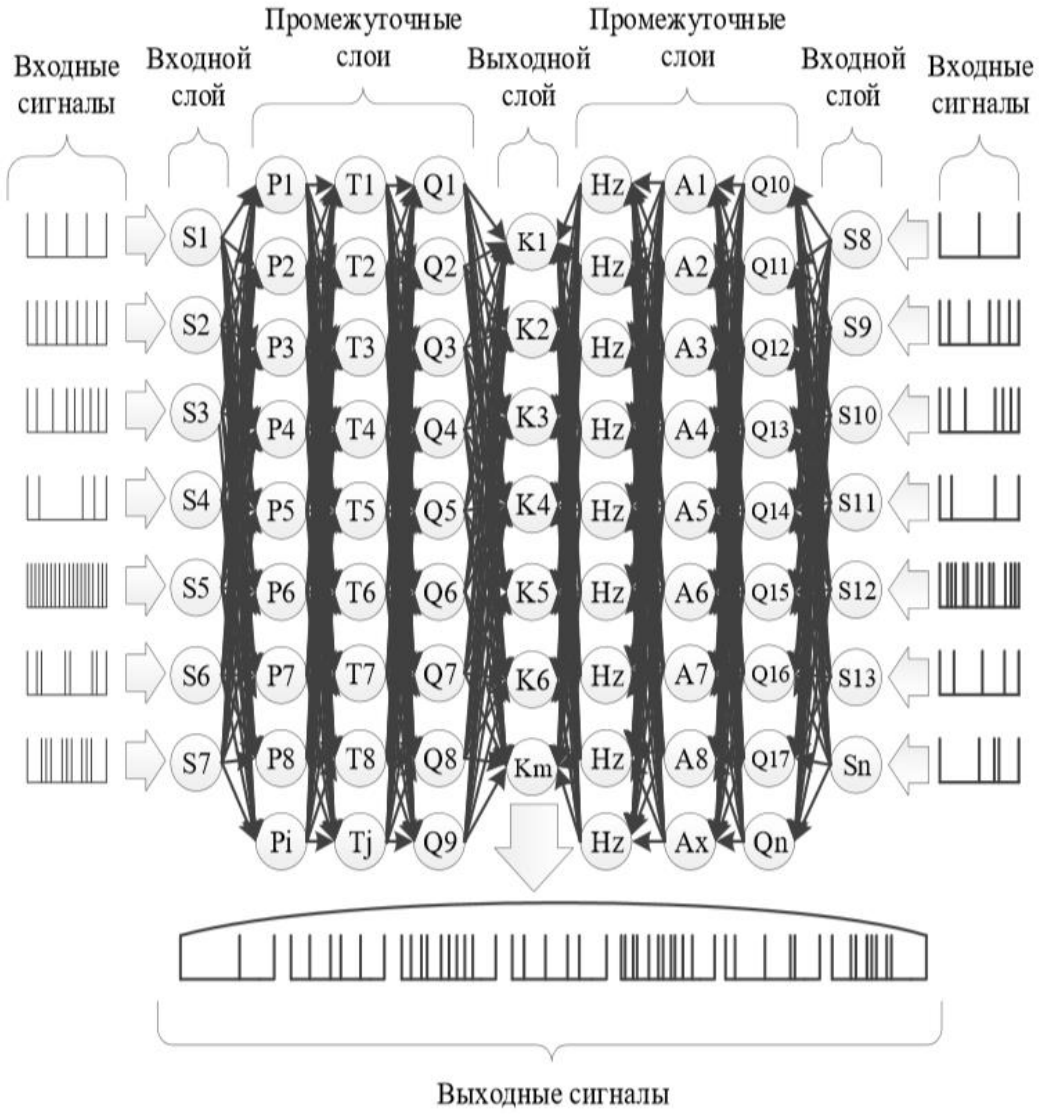

Рис. 1. **Структура ИмНС**

В результате на выходе получается преобразованное правило фильтрации, при этом сохраняется возможность распределения сетевой нагрузки.

Структура нейрона показана на Рисунке 2 (где $n_n(t)$ – входные сигналы; W_n - синапсы). За основу взята модель ФитцХью-Нагумо [6, 7].

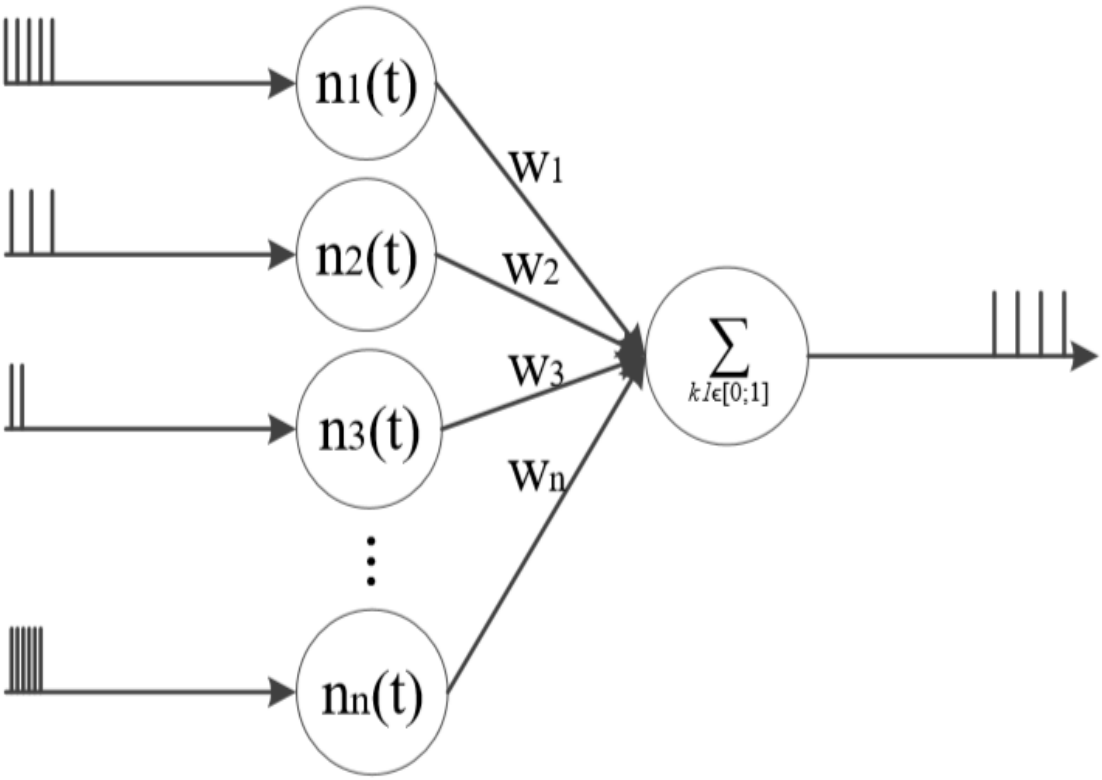

Рис. 2. **Структура нейрона ИмНС**

Модель нейрона описывается следующей системой уравнений:

$$\begin{cases} v = \frac{\alpha}{2} + I_{ext} \\ \tau \frac{dw}{dt} = v + \alpha + k1 \end{cases}$$

где α – потенциал нейрона; k1 – коэффициент реагирования на тип атаки в диапазоне от 0 до 1; I_{ext} – коэффициент внешнего воздействия; w – восстановление входного тока; ν – динамика мембранного потенциала; t – время угасания сигнала импульса.

Система реагирует на изменение вида несанкционированного трафика, анализирует его и блокирует. После обнаружения нового типа атаки вырабатываются правила фильтрации трафика, а самой атаке присваивается коэффициент реагирования и заносится в базу данных, пример представлен в таблице 1 [7].

Таблица 1

Коэффициенты реагирования k1

Тип DDoS-атаки	Краткое описание DDoS-атаки	Коэффициент k1
UDP-флуд	Случайные порты хост-машины «жертвы» заваливаются пакетами по протоколу UDP, ответы на которые перегружает сетевые ресурсы	0,001
DNS-усиление	На атакуемый DNS-сервер «жертвы» отправляется короткий запрос, на который он отвечает уже большим по размеру пакетом	0,002
HTTP-флуд	На атакуемый сервер «жертвы» отправляется масса обычных или шифрованных HTTP-сообщений, забивающих узлы связи	0,003
Все виды ICMP-флуда	Перегружает хост-машина «жертвы» служебными запросами (например, ping), на которые она обязана давать эхо-ответы	0,004–0,120
MAC-флуд	Порты сетевого оборудования «жертвы» забиваются потоками «пустых» пакетов с разными MAC-адресами	0,121
SYN-флуд	«Жертву» заваливают многочисленными SYN-запросами без ответа. Канал «жертвы» забивается очередью TCP-подключений от исходящих соединений, ожидающих ответного ACK пакета	0,122
NTP-усиление	На атакуемый NTP-сервер «жертвы» отправляется запрос monlist, на который возвращается список из 600 последних клиентов ntpd, забиваются каналы связи	0,123
TCP-флуд (Reset)	Случайные порты хост-машины «жертвы» заваливаются пакетами по протоколу TCP, ответы на которые перегружают сетевые ресурсы	0,124
Source-флуд	Воздействие на аппаратные ресурсы «жертвы» (например, загрузка процессора или памяти выполнением кода через интерфейс CGI)	0,125
VoIP-флуд	На атакуемый VoIP-сервер «жертвы» направляется большое количество поддельных VoIP-пакетов с широкого диапазона IP-адресов, что вызывает перегрузку сетевых ресурсов	0,126
Неизвестные типы DDoS-атак	-	0,127–0,999

Обучение ИмНС происходит в пять этапов:

1. Прием данных с входного слоя (импульсов);
2. Равномерное распределение импульсов по нейронам;
3. Равномерное распределение скрытых слоев в ИмНС по ресурсам кластера;
4. Понижение информационной энтропии;
5. Подача данных на выходной слой.

Кроме ИмНС можно выделить несколько способов противодействия DDoS-атакам:

- программные решения на стороне клиента;
- решения операторов связи;
- распределенные сети фильтрации;
- программно-определяемые сети.

Программные решения на стороне клиента – это чаще всего, межсетевые экраны (стандартный брандмауэр или установленное программное обеспечение). Здесь преимущество использования обеспечивается за счет доступности (минимальные финансовые вложения) и относительной простоты в эксплуатации. В то же время стандартные решения не позволяют распределять сетевую нагрузку и не обладают достаточной эффективностью (не способны блокировать массивную DDoS-атаку).

Решения операторов связи представляют собой специализированные сети фильтрации с использованием оборудования, способного отслеживать большие объемы трафика. Основные преимущества решений операторов связи:

- эффективность обнаружения и нейтрализации низко активных атак внешним несанкционированным трафиком;
- возможность обработки большого количества сетевых пакетов (до 500 миллионов в секунду).

В качестве основных недостатков операторских решений по DDoS-атакам необходимо отметить следующее:

- дороговизна оборудования;
- неэффективность при массированных DDoS-атаках;
- невозможность распределения сетевой нагрузки;
- необходимость ручного редактирование правил фильтрации.

Распределенные сети фильтрации позволяют (как и следует из их названия) распределить сетевую нагрузку по узлам, избегая тем самым её концентрации в пределах одного ЦОДа. Следует отметить, что в данном случае достаточно эффективно блокируется несанкционированный трафик, однако имеются сложная конфигурация сети и высокая стоимость оборудования.

Программно-определяемая сеть (Software-Definer Networking, SDN) реализуется на программном уровне и представляет собой виртуальную сеть. При использовании данного метода защиты основная нагрузка ложится на управляющие коммутаторы, что зачастую сказывается на работоспособность сети в целом. К числу преимуществ данного метода можно отнести программное управление, самоанализ с принятием решений о перенаправлении трафика в автоматическом режиме.

К недостаткам данного метода относятся:

- высокая цена на оборудование;
- уязвимость контроллера SDN, а при его недоступности сеть не функционирует;
- отсутствие равномерного распределения нагрузки во время DDoS-атаки.

Существенными недостатками всех приведенных решений являются невозможность равномерного распределения сетевой нагрузки и автоматического обнаружения новых типов DDoS-атак. Решение данных задач позволит снизить за-

груженность сетевых ресурсов, а также повысить доступность информации, что положительно скажется на работоспособности каждого физического сервера в кластере. Таким образом, разработка новых способов защиты от атак внешним несанкционированным трафиком является на сегодня важной задачей [4].

Если сравнивать функциональные возможности ИмНС с другими методами защиты от DDoS-атак, то явно выделяются следующие преимущества ИмНС:

- большая адаптация под массивные атаки;
- обучаемость системы;
- высокая скорость реакции на нелегитимный трафик;
- отсутствие повышенных задержек;
- сохранение новых видов атак в базу данных (БД);
- малое потребление физических ресурсов;
- практически полностью автоматическая работа;
- равномерное распределение нагрузки.

Завершая рассмотрение актуальных вопросов обеспечения доступности и защищенности данных при DDoS-атаках, отмечаем, что ИмНС позволяет реализовать структуру самообучения искусственной нейронной сети на программном уровне. С внешнего сетевого интерфейса берутся данные о входящем трафике и преобразуются в импульсы на входном слое. После самообучения импульсы передаются на выходной слой и преобразуются в правила межсетевого экранирования с последующим сохранением в базе данных.

В продуктивной среде самообучение (новый вид атаки) занимает около 20 секунд, что является очень хорошим показателем.

Низкое потребление ресурсов в режиме отражения DDoS-атаки говорит о целесообразности использования ИмНС. Столь низкое потребление ресурсов кластера позволяет в минимальные сроки защитить каждый сервер кластера, повысить производительность и обеспечить доступность, что является одним из ключевых требований информационной безопасности.

Помимо защиты от кибератак, ИмНС позволяет избежать ошибок, связанных с некорректной настройкой сетевой инфраструктуры (человеческий фактор), а именно когда сетевое оборудование из-за неверной конфигурации сети само генерирует трафик и нагружает сеть, по сути создавая нелегитимный трафик.

Подводя итог сказанному, следует отметить, что использование ИмНС в качестве системы противодействия от DDoS-атак, позволяет сэкономить существенные финансовые ресурсы.

Библиографический список

1. Пальчевский Е. В., Халиков А. Р. Автоматизированная система защиты доступности информации от атак внешним несанкционированным трафиком в UNIX-подобных системах // Программные продукты и системы. 2018. Т. 31. № 3. С. 548–556. DOI: 10.15827/0236-235X.123.548-556.
2. Воробьева Ю. Н., Катасева Д. В., Катасев А. С., Кирпичников А. П. Нейросетевая модель выявления DDoS-атак // Вестн. технолог. ун-та. 2018. Т. 21. № 2. С. 94–98.
3. Краснов А. Е., Надеждин Е. Н., Никольский Д. Н., Репин Д. С., Галяев В. С. Детектирование DDoS-атак на основе анализа динамики и взаимосвязи характеристик сетевого трафика // Вестн. УдГУ: Математика. Механика. Компьютерные науки. 2018. Т. 28. № 3. С. 407–418.
4. Тарасов Я. В. К вопросу противодействия целенаправленным компьютерным атакам // Защита информации. Инсайд. 2018. № 4. С. 48–53.
5. Saied A., Overill R., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016, vol. 172, pp. 385–393.
6. FitzHugh R. Impulses and physiological states in theoretical models of nerve membrane. Biophys. J., 1961, vol. 1, pp. 446–466.
7. Nagumo J., Arimoto S., Yoshizawa S. An active pulse transmission line simulating nerve axon. Proc. IRE, 1962, vol. 50, iss. 10, pp. 2061–2070. DOI: 10.1109/JRPROC.1962.288235.