DOI 10.37882/2223-2966.2026.03.27

ФОРМИРОВАНИЕ СИНТЕТИЧЕСКИХ ДАННЫХ ДЛЯ ОБНАРУЖЕНИЯ DDOS-АТАК С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

GENERATION OF SYNTHETIC DATA FOR DETECTION OF DDOS ATTACKS USING MACHINE LEARNING

E. Novikov
V. Afanasyev
N. Kunin

Summary. The constant increase in the number of distributed denials of service (DDoS) attacks necessitates the improvement of detection approaches. This paper examines the possibility of using machine learning methods to improve the accuracy of DDoS attack detection. It is noted that the most important step in developing DDoS attack detection models is the creation of a training dataset. A technology for generating training data for models using virtual machines and specialized tools for generating and analyzing network traffic is proposed.

Keywords: cybersecurity, intrusion detection system, DDoS attacks, machine learning, synthetic data, network traffic.

Новиков Евгений Иванович
кандидат технических наук, доцент,
МИРЭА — Российский технологический университет
novikov_ei@mirea.ru
Афанасьев Вадим Владимирович
кандидат технических наук, доцент,
МИРЭА — Российский технологический университет
afanasev_v@mirea.ru
Кунин Никита Тимофеевич
старший преподаватель,
МИРЭА — Российский технологический университет
kunin@mirea.ru

Аннотация. Постоянное увеличение количества атак типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) обуславливает совершенствование походов к их обнаружению. В работе рассматривается возможность использования методов машинного обучения для повышения точности обнаружения DDoS-атак. Отмечается, что наиболее важным этапом разработки моделей обнаружения DDoS-атак является создание обучающего набора данных. Предложена технология формирования данных для обучения моделей с использованием виртуальных машин и специализированных инструментов для генерации и анализа сетевого трафика.

Ключевые слова: кибербезопасность, система обнаружения вторжений, DDoS-атаки, машинное обучение, синтетические данные, сетевой трафик.

С развитием информационных технологий и увеличением количества сетевых устройств проблема кибербезопасности становится все более актуальной. Одной из наиболее распространенных и опасных угроз являются распределенные атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS), которые могут привести к значительным финансовым и репутационным потерям.

Количество DDoS-атак ежегодно увеличивается. В 2024 году эксперты ГК «Солар» зафиксировали 508 тысяч DDoS-атак на российские организации, что почти в два раза больше аналогичного показателя 2023 года [1]. Неутешительные прогнозы предоставляет и компания StormWall. По ее данным количество DDoS-атак в 2024 году в мире выросло на 108 % по сравнению с 2023 годом [2]. По разным оценкам, только за 2024 год, DDoS-атаки нанесли $8–12 млрд совокупного ущерба различным компаниям, а средний ущерб для бизнеса — $150–300 тыс. за одну атаку.

Ключевым фактором роста DDoS-атак стало расширение ботнет-сетей (botnet). Так к IV кварталу 2024 года этот показатель вырос до 38000. При этом распределение носит крайне неравномерный характер: наряду с компактными ботнетами (несколько тысяч узлов) существуют масштабные сети, контролирующие миллионы зараженных устройств.

Существенный рост частоты DDoS-атак в последние годы, актуализирует задачу разработки более эффективных механизмов обеспечения кибербезопасности. Организации должны инвестировать в современные технологии, а также внедрять различные стратегии защиты, например, такие как система обнаружения вторжений.

Традиционные системы обнаружения вторжений (Intrusion Detection Systems, IDS) представляют собой специализированные программно-аппаратные решения, предназначенные для выявления несанкционированного доступа к компьютерным системам через интернет. Несмотря на их ключевую роль в кибербезо-

пасности, эффективность IDS ограничена: они не всегда способны обнаруживать новые и сложные угрозы, часто дают ложные срабатывания и требуют значительных вычислительных ресурсов для работы. Эти ограничения связаны с используемыми методами анализа, которые не всегда адекватно определяют современные виды атак [3].

Архитектура IDS состоит из трех основных элементов: сбор данных, анализ и реагирование [4].

Сбор данных является наиболее важным этапом работы системы обнаружения вторжений. От качества и полноты собранных данных зависит эффективность последующего анализа и реагирования. В контексте DDoS-атак данными, необходимыми для обнаружения, будут являться характеристика сетевого трафика. К таким характеристикам относятся атрибуты сетевых пакетов, такие как структура и содержимое заголовков различных уровней сетевой модели, временные характеристики передачи, размеры и частота поступления пакетов, интенсивность трафика, объем переданных данных, длительность сессии, время между запросами и др.

Анализатор выполняет обработку поступающих данных с целью выявления потенциально опасной активности. Его основная функция состоит в выделении среди всего множества наблюдаемых сетевых событий тех, которые демонстрируют характеристики, позволяющие отнести их к проявлениям злонамеренных или нетипичных действий.

Модуль реагирования в IDS реализует механизмы обработки выявленных угроз безопасности. При обнаружении потенциальной угрозы менеджер реагирования собирает и анализирует данные о тревожных событиях, поступающие от сенсорных компонентов системы, после чего передает соответствующую информацию администратору безопасности для принятия решений и выполнения необходимых защитных мер.

В современных IDS применяются два различных подхода к детектированию аномальной активности:

— обнаружение на основе сигнатур (Signature-Based Detection);
— обнаружение на основе аномалий (Anomaly-Based Detection).

IDS на основе сигнатур анализируют сетевой трафик путем сопоставления с базой известных шаблонов атак, которая может храниться локально или в облачном хранилище. Хотя такой подход обеспечивает быстрое и точное обнаружение известных угроз, он имеет существенные ограничения: неспособность выявлять новые и полиморфные атаки, необходимость постоянного обновления сигнатур. Кроме того, IDS на основе сигнатур практически не способны обнаруживать атаки «нулевого дня» [5].

Системы обнаружения вторжений, основанные на анализе аномалий, используют несколько методов: машинное обучение (machine learning, ML), статистические методы и методы, основанные на знаниях. В таких системах создаётся «нормальная» модель поведения компьютерной системы. Значительное различие между фиксируемым сетевым трафиком и модельным позволяет предположить наличие вторжения. В большинстве IDS для анализа аномалий применяются методы машинного обучения, которые позволяют устранить недостатки сигнатурного подхода [6]. При этом перспективным подходом является создание комплексных IDS, сочетающих применение сигнатурного анализа и ML [7].

Разработка модели машинного обучения включает выполнение следующих этапов:

— сбор данных о сетевом трафике;
— очистка и подготовка данных для обучения;
— подбор модели, поиск оптимальных гиперпараметров и обучение;
— оценивание качества модели;
— внедрение модели и ее сопровождение.

Безусловно ключевой задачей является подготовка исходных данных для обучения модели. При этом они должны базироваться на максимально полном признаковом пространстве и отражать актуальные типы атак.

Для синтеза моделей машинного обучения, как правило, используются специализированные наборы размеченных данных. Среди них общедоступными и наиболее популярными являются следующие: DARPA1998, KDD Cup 1999, Kyoto 2006, NSL-KDD 2009, ISCX 2012, CTU-13, UNSW-NB15, CIDDS-001, UGR-16, CICIDS 2017, CICIDS 2018 и др. Однако многие исследователи отмечают существенные недостатки их применения и обосновывают необходимость разработки собственных наборов данных для обучения моделей [8].

Синтетические данные — это искусственно сгенерированные данные, которые имитируют реальные, но создаются алгоритмами, а не собираются из естественных источников. Данная методология обладает рядом существенных преимуществ, включая полный контроль над параметрами генерируемого трафика, возможность масштабирования объемов данных и соблюдение требований правового регулирования. Следует отметить, что синтетические данные не являются универсальным инструментом, из-за требований индивидуальной адаптации под специфику каждой конкретной корпоративной сети. Синтетические данные представляют оптимальный подход для проведения контролируемых экспериментов в области анализа сетевой безопасности, отвечая ключевым требованиям научной достоверности.

Создание синтетических данных, характеризующих сетевой трафик требует комплексного подхода, сочетающего специализированное программное обеспечение и контролируемую тестовую среду.

Процесс создания начинается с конфигурации виртуального стенда, представляющего собой изолированную сетевую инфраструктуру, развернутую на платформе виртуализации. В работе использовался экспериментальный стенд на основе двух виртуальных машин с ОС Kali Linux, имитирующих атакующую систему и систему-жертву. Сетевые интерфейсы виртуальных машин настроены в режиме «сетевой мост», что обеспечивает их прямое подключение к физической сети и функционирование в качестве автономных сетевых устройств в пределах локального сегмента. Особенностью этой конфигурации является минимальная сетевая активность виртуальных машин в штатном режиме работы, что позволяет однозначно идентифицировать все поступающие на узлы пакеты данных либо как элементы имитационной атаки, либо как ответные реакции на нее. Такой подход обеспечивает чистоту экспериментальных данных и исключает влияние постороннего сетевого трафика на результаты исследования.

Далее генерируется легитимный и нелегитимный сетевые трафики с использованием специализированного инструментария, позволяющего моделировать различные типы атак с высокой степенью достоверности.

В качестве генератора тестового вредоносного трафика применялась утилита hping3, представляющая собой мощное сетевое средство, интегрированное в стандартный набор утилит операционной системы Kali Linux, не требующее дополнительной установки. Выбор этого инструмента обусловлен его расширенными возможностями по моделированию различных типов DDoS-атак, включая гибкую настройку параметров генерируемых пакетов и широкий диапазон регулируемых характеристик сетевого трафика [9]. Для обеспечения репрезентативности экспериментального исследования использовалась методика последовательной генерации DDoS-трафика с варьируемыми параметрами, включая изменение скорости отправки пакетов и ротацию IP-адресов источников, что позволяет достоверно имитировать сценарии различных распределенных атак. Процедура генерации вредоносного трафика предусматривает циклическое выполнение серии запусков с различными профилями нагрузки, автоматически прекращаемое по завершении заданного интервала сбора данных. Такой подход обеспечивает получение статистически значимой выборки сетевого трафика, необходимой для последующего анализа характеристик атакующих воздействий и верификации методов их обнаружения.

Для снятия легитимного трафика использовался скрипт на языке программирования Python, с использованием библиотеки Scapy. Несмотря на то, что для решения поставленной задачи может быть применён широкий спектр языков программирования, Python представляет собой один из наиболее развитых инструментов в современной компьютерной науке. Это обусловлено наличием детализированной документации, обширной экосистемы библиотек и модулей, а также высокой степенью адаптивности к различным областям исследований. Библиотека Scapy была выбрана благодаря своей способности обеспечивать гибкую настройку параметров сетевых пакетов, широкой поддержке различных сетевых протоколов, удобному Python-интерфейсу и полному доступу к заголовкам пакетов, что делает ее оптимальным инструментом для анализа и генерации сетевого трафика [10].

Разработанный скрипт позволяет захватывать данные канального, сетевого и транспортного уровня модели взаимодействия открытых систем (Open System Interconnection, OSI), приходящие на конечную машину, а также вычисляет разницу во времени между приходом пакетов и сразу записывает их в CSV-файл (Comma-Separated Values).

С целью демонстрации механизма создания синтетического набора данных выбран тип DDoS-атаки «ICMP flood» (Internet Control Message Protocol). Этот тип атаки характеризуется массовой генерацией и направлением на целевой узел сетевых пакетов ICMP, что приводит к исчерпанию его вычислительных ресурсов и канальной пропускной способности. Особую опасность подобные атаки представляют для сетевой инфраструктуры, поскольку такой трафик традиционно обладает более высоким приоритетом обработки по сравнению с другими типами сетевых пакетов.

При анализе ICMP flood-атак ключевое значение приобретает исследование сетевых заголовков на различных уровнях модели OSI. В контексте атаки особый интерес представляет заголовок сетевого (L3) уровня, содержащий критически важные для детектирования параметры. На сетевом уровне анализируются IP-заголовки, содержащие такие значимые поля как TTL (Time To Live) и IP-адреса отправителей, в то время как заголовки ICMP, относящиеся к этому же уровню, предоставляют информацию о типах и кодах пакетов. Анализ сетевых заголовков на различных уровнях модели OSI позволяет выявлять характерные признаки ICMP DDoS-атак, включая совпадение значений TTL у разных отправителей, свидетельствующее о ботнет-активности, аномальные размеры пакетов, указывающие на попытки переполнения буфера, наличие внутренних и локальных IP-адресов как признак подмены, фрагментированные пакеты, нестандартные типы пакетов и равномерные временные интервалы между пакетами, характерные

для автоматизированной генерации трафика. Комплексное рассмотрение этих параметров обеспечивает надежное обнаружение DDoS-атак.

После запуска созданного виртуального стенда инициируется комплексный процесс сбора легитимного трафика. Разработанный скрипт, запущенный на основном вычислительном узле, осуществляет захват легитимного сетевого трафика. Поскольку используется естественный сетевой трафик, формируемый в процессе штатной работы сети, то исключается необходимость применения дополнительных инструментов генерации искусственного трафика. После достижения достаточного объема данных, соответствующего требованиям репрезентативности эксперимента, выполнение скрипта останавливается и результаты записываются в CSV-файл. На рисунке 1 представлена таблица с признаками легитимного трафика, сформированная средствами библиотеки Pandas языка Python.

Поскольку легитимный трафик представляет собой естественный поток данных, передаваемых в процессе нормального функционирования сети, его модификация или искусственное изменение не требуются.

	time_diff	eth_dst	eth_src	...	icmp_type	code
0	0.313016	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0
1	1007.572317	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0
2	0.799512	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0
3	1003.844426	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0
4	0.798161	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0
...	...	...	...	...	...	...
4214	134.507002	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	0.0	0.0
4216	1.855301	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0
4217	0.614267	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0
4218	0.699700	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0
4219	0.556114	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0

4219 rows × 19 columns

Рис. 1. Результат сбора характеристик легитимного трафика

	time_diff	eth_dst	eth_src	...	icmp_type	code	class
0	0.313016	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
1	1007.572317	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	0
2	0.799512	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
3	1003.844426	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	0
4	0.798161	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
...	...	...	...	...	...	...	...
4214	134.507002	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	0.0	0.0	0
4216	1.855301	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0	0
4217	0.614267	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0	0
4218	0.699700	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0	0
4219	0.556114	f0:57:a6:fd:88:b0	98:de:d0:ef:53:dc	...	11.0	0.0	0

4219 rows × 19 columns

Рис. 2. Маркированный набор характеристик легитимного трафика

Для обеспечения возможности контролируемого машинного обучения осуществляется маркировка собранных данных соответствующей меткой легитимного класса (например, 0) (рис. 2).

После завершения этапа генерации легитимного трафика реализуется генерация трафика с признаками выбранной разновидности DDoS-атаки. Для этого на целевой виртуальной машине объекта защиты запускается разработанный скрипт для захвата сетевых пакетов, обеспечивающий фиксацию всей входящей сетевой активности. Перед началом генерации атакующего трафика выполняется этап сетевой разведки с целью определения IP-адреса целевой системы. Для непосредственной генерации злокачественного трафика на виртуальной машине, имитирующей злоумышленника, используется утилита hping3 с вариативным набором параметров. Результат работы утилиты показан на рисунке 3.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --flood --rand-source  192.168.0.105
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.0.105 hping statistic ---
1944 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --faster --rand-source  192.168.0.105
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode set, 28 headers + 0 data
bytes
^C
--- 192.168.0.105 hping statistic ---
2025 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --fast --rand-source  192.168.0.105
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode set, 28 headers + 0 data
bytes
^C
--- 192.168.0.105 hping statistic ---
432 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рис. 3. Результат генерации DDoS-атаки

	time_diff	eth_dst	eth_src	...	ip_dst	icmp_type	code
0	-1.000000	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
1	0.422205	98:de:d0:ef:53:dc	08:00:27:06:f0:02	...	48.25.119.99	0	0
2	0.334507	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
3	0.311484	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
4	0.283606	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
...	...	...	...	...	...	...	...
6544	101.059578	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
6545	0.257860	98:de:d0:ef:53:dc	08:00:27:06:f0:02	...	248.139.55.58	0	0
6546	100.309331	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
6547	100.990807	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	192.168.0.105	8	0
6548	0.720896	98:de:d0:ef:53:dc	08:00:27:06:f0:02	...	45.89.221.209	0	0

6549 rows × 18 columns

Рис. 4. Результат сбора характеристик вредоносного трафика

	time_diff	eth_dst	eth_src	...	icmp_type	code	class
1	0.334507	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
2	0.311484	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
3	0.283606	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
4	0.296679	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
5	0.289928	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
...	...	...	...	...	...	...	...
3782	100.536918	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
3783	99.460220	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
3784	101.059578	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
3785	100.309331	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1
3786	100.990807	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8	0	1

3786 rows × 19 columns

Рис. 5. Маркированный набор характеристик нелегитимного трафика

	time_diff	eth_dst	eth_src	...	icmp_type	code	class
0	0.313016	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
1	1007.572317	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	0
2	0.799512	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
3	1003.844426	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	0
4	0.798161	08:00:27:c1:be:9a	08:00:27:06:f0:02	...	0.0	0.0	0
...	...	...	...	...	...	...	...
3781	100.536918	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	1
3782	99.460220	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	1
3783	101.059578	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	1
3784	100.309331	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	1
3785	100.990807	08:00:27:06:f0:02	08:00:27:c1:be:9a	...	8.0	0.0	1

8005 rows × 19 columns

Рис. 6. Размеченный набор данных

Собранные данные записываются в CSV-файл и могут быть прочитаны средствами библиотеки Pandas языка Python (рис. 4).

Было установлено, что полученные данные содержат некорректные значения признака «time_diff» (-1), которые должны быть удалены. Также в поле «icmp_type» есть сроки со значением «0», что является ответом операционной системы на DDoS-атаку. Соответствующие наблюдения необходимо удалить.

Далее в полученный набор данных для каждого наблюдения добавляется метка нелегитимного трафика (рис. 5).

На заключительном этапе необходимо объединить подготовленные наборы данных в один файл (рис. 6).

Разработанный подход к созданию синтетического набора данных позволяет осуществлять обучение моделей машинного обучения, с целью обнаружения DDoS-атак. При этом используется программное обеспечение, обеспечивающее формирование как легитимного, так и вредоносного трафика. Преимуществом представленного подходя является возможность его применения для генерации сетевых сессий, характеризующих широкий спектр DDoS-атак. Также формат создаваемых наборов данных обеспечивает его простую интеграцию в большинство известных библиотек и фреймворков машинного обучения.

ЛИТЕРАТУРА

1. Солар. Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в 2024 году [Сайт]. — 2024. — URL: https://rt-solar.ru/analytics/reports/5364/#2/ (дата обращения: 25.02.2025).
2. StormWall. DDoS-атаки 2024: Годовой отчет [Сайт]. — 2024. — URL: https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet (дата обращения: 25.02.2025).
3. Асхатова Л.И., Галимов Э.И., Габдуллин И.М. Архитектура системы обнаружения вторжений [Электронный ресурс] // Электронный научный журнал. — 2015. — URL: https://cyberleninka.ru/article/n/arhitektura-sistemy-obnaruzheniya-vtorzheniy/viewer/ (дата обращения: 07.03.2025).
4. Nuruddeen M., Nur A., Warusia M., Mohd F. Архитектура системы обнаружения вторжений: вопросы и задачи [Электронный ресурс] // Научный журнал «Технологические отчеты Университета Кансай». — 2020. — Т. 62, № 7. — ISSN 0453–2198. — URL: https://www.researchgate.net/publication/344468714_Intrusion_Detection_System_Architecture_Issues_and_Challenges (дата обращения: 30.03.2025).
5. Ashoor A.S., Gore S. Важность системы обнаружения вторжений [Электронный ресурс] // Международный журнал научных и инженерных исследований. — 2010. — URL: https://www.semanticscholar.org/paper/Importance-of-Intrusion-Detection-System-(-IDS-)-Ashoor/f9f623cd8d24a7643c7d3b628ba6e0d550234cfc/ (дата обращения: 15.03.2025).
6. Brison R., Wimmer H., Rebman Jr C. Обнаружение ботнетов в облачных средах с использованием машинного обучения [Электронный ресурс] // 20-й Международный симпозиум по сетевым вычислениям и приложениям (NCA). — 2022. — DOI: 10.48009/3_iis_2022_110. — URL: https://doi.org/10.48009/3_iis_2022_110/ (дата обращения: 12.03.2025).
7. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. 2022. №5. URL: https://cyberleninka.ru/article/n/sravnenie-sistemy-obnaruzheniya-vtorzheniy-na-osnove-mashinnogo-obucheniya-s-signaturnymi-sredstvami-zaschity-informatsii (дата обращения: 18.03.2025).
8. Ring M., Wunderlich S. et al. Computers & Security, vol. 86, 2019, pp. 147–167.
9. Тестирование сетевой безопасности, анонимизация трафика и взлом паролей: обзор инструментов hping3, proxychains и john the ripper. (2023). Международный научно-исследовательский журнал «Модернизация инженерных технологий и науки». https://doi.org/10.56726/irjmets38746/ (дата обращения: 27.03.2025).
10. Rejah Rehim, Effective Python Penetration Testing, Packt Publishing Ltd, 2016 p. 164.

© Новиков Евгений Иванович (novikov_ei@mirea.ru); Афанасьев Вадим Владимирович (afanasev_v@mirea.ru);
Кунин Никита Тимофеевич (kunin@mirea.ru)

Журнал «Современная наука: актуальные проблемы теории и практики»