УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/hum/socio/1068.html

# ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ПОЯВЛЕНИЯ БОТНЕТОВ В КИБЕРБЕЗОПАСНОСТИ

**Н.С. Лосев** losevns@student.bmstu.ru
**Е.В. Глинская** glinskaya@bmstu.ru
SPIN-код: 5430-3023

*МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

Ботнеты представляют собой сеть инфицированных компьютеров, находящихся под управлением злоумышленников и являются одной из самых серьезных угроз для кибербезопасности. Используемые для рассылки спама, DDoS-атак, кражи данных и распространения вредоносного программного обеспечения, ботнеты могут наносить значительный ущерб как индивидуальным пользователям, так и организациям. Управление ботнетами осуществляется через ботмастеров — серверы или злоумышленников, координирующих их действия. В статье рассмотрены ключевые подходы к обнаружению ботнетов, включая сигнатурный, поведенческий и основанный на машинном обучении. Рассмотрены также методы поиска ботмастеров, такие как анализ сетевого трафика, использование honeypots и анализ следов вредоносных программ. Представлены результаты сравнительного анализа эффективности методов, предложены стратегии их дальнейшего совершенствования, включая комбинированные подходы и внедрение интеллектуальных систем предиктивного анализа.

**Ключевые слова:** ботнет, ботмастер, обнаружение, злоумышленник, машинное обучение, кибербезопасность, DDoS-атака, вредоносное программное обеспечение

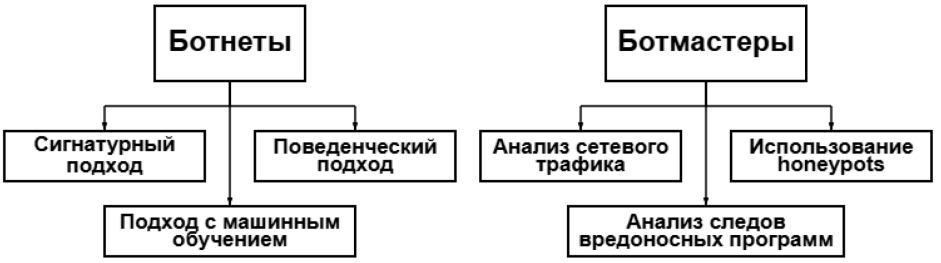
**Введение.** Ботнеты представляют собой сеть скомпрометированных компьютеров, ориентированных на выполнение вредоносных действий под контролем централизованного ботмастера. Эти компьютеры, часто называемые «ботами» или «зомби», используются для множества целей, включая рассылку спама, запуск распределенных атак типа отказа в обслуживании (DDoS) [1], кражу конфиденциальной информации и распространение вредоносного программного обеспечения (ПО). Обнаружение ботнетов представляет собой непростую задачу из-за сложности применения к ним стандартных методов обнаружения. Тем не менее разработка надежных методов идентификации ботнетов крайне важна для защиты данных и инфраструктуры от возможного ущерба [2].

Ключевую роль в функционировании ботнета играет ботмастер — удаленный сервер или лицо, управляющее зараженными устройствами. Поиск и нейтрализация ботмастеров являются важной стратегией борьбы с бот-

 ISSN 2541-8009

нетами, поскольку их блокировка может привести к дестабилизации всей сети зараженных компьютеров. Для обнаружения ботмастеров применяют такие методы, как анализ сетевого трафика, использование honeypots и исследование следов вредоносных программ (см. рисунок). Они позволяют выявить управляющие серверы ботнета и принять меры по их устранению.

Современные подходы к обнаружению ботнетов включают сигнатурный анализ, поведенческий анализ сетевого трафика и использование машинного обучения [3] (см. рисунок). Однако злоумышленники продолжают развивать свои методы, включая шифрование, полиморфизм и распределенные архитектуры, что усложняет процесс идентификации и устранения зараженных устройств [4].




Основные подходы и методы противодействия ботнетам и ботмастерам

**Поиск ботмастеров и противодействие им.** Ботмастеры служат центральным элементом управления ботнетами, координируя действия зараженных устройств. Их обнаружение и блокировка существенно затрудняют функционирование ботов. Существует несколько методов поиска ботмастеров.

*Анализ сетевого трафика*. Данный метод включает мониторинг и анализ сетевых взаимодействий с целью выявления аномальных коммуникаций между ботами и управляющим сервером. Определение таких аномалий может указать на присутствие ботмастера и помочь в его идентификации.

*Использование honeypots* — специально настроенных ловушек, имитирующих уязвимые системы. Они привлекают внимание злоумышленников и позволяют анализировать их поведение. Анализируя данные, полученные от honeypots, можно определить IP-адреса атакующих, выявить используемые уязвимости и методы управления ботами.

*Анализ следов вредоносных программ*. Этот метод включает исследование вредоносных файлов и сетевых взаимодействий для выявления связи с ботмастером. Определение уникальных характеристик вредоносного ПО, таких

как используемые домены и IP-адреса, помогает в выявлении командных серверов ботнета [5].

Применение комбинации этих методов позволяет эффективно выявлять и нейтрализовать ботмастеры, снижая уровень угрозы от подчиняемых им устройств и повышая уровень безопасности сетей.

**Ключевые подходы к обнаружению ботнетов.** Сигнатурный анализ — один из наиболее распространенных подходов к обнаружению ботнетов. Этот подход основывается на поиске уникальных шаблонов или «сигнатур», характерных для известных ботнетов. Он хорошо работает с уже известными угрозами, однако его эффективность снижается при обнаружении новых типов атак, поскольку злоумышленники используют сложные техники маскировки [6].

Поведенческий анализ предполагает мониторинг сетевого трафика на предмет подозрительной активности, например, высокой интенсивности исходящего трафика или связи с известными серверами управления ботнетов. В последние годы активно используются методы корреляционного анализа поведения устройств в сети, что позволяет выявлять ранее неизвестные ботнет-угрозы [7].

Одним из эффективных методов обнаружения ботнетов является логистическая регрессия, которая применяется для классификации сетевого трафика. Логистическая регрессия позволяет строить вероятностные модели, предсказывая вероятность принадлежности данных к вредоносному или безопасному классу. Она хорошо работает с линейно разделяемыми данными и обеспечивает высокую интерпретируемость модели, но может уступать по точности более сложным алгоритмам.

Случайный лес представляет собой ансамблевый метод, основанный на совокупности деревьев решений. Этот метод обладает высокой точностью и устойчивостью к шумам в данных. Развитие методов глубокого обучения, таких как нейросетевые модели, позволяет более точно анализировать сложные шаблоны сетевого взаимодействия, что упрощает обнаружение скрытых ботнет-активностей [8].

Сравнительный анализ показывает, что методы на основе машинного обучения имеют значительно более высокую точность, чем методы, основанные на традиционных подходах. Однако время обработки таких моделей значительно выше, что ограничивает их применение в реальных ситуациях [9].

**Заключение.** Обнаружение ботнетов — важный аспект обеспечения кибербезопасности. Они продолжают совершенствоваться, а это требует постоянного улучшения методов их идентификации. Использование машинного обучения в сочетании с традиционными подходами открывает новые возможности для более точного и своевременного обнаружения угроз. Однако

 ISSN 2541-8009

остаются нерешенными такие проблемы, как высокая вычислительная сложность и необходимость большого объема данных для обучения [10]. Кроме того, одним из ключевых направлений совершенствования методов защиты от ботнетов является поиск и нейтрализация ботмастеров. Выявление управляющих серверов позволяет подорвать структуру ботнета и снизить его активность.

В будущем важно сосредоточиться на разработке гибридных методов, сочетающих эффективность машинного обучения и простоту традиционных методов. Внедрение таких стратегий позволит повысить уровень защиты сетей от ботнет-угроз и минимизировать риски атак.

**Литература**

[1] Оралбаев Е.А. Обнаружения DDoS-атак ботнетов в сетях доступа IoT. *Актуальные вопросы современной науки и образования*. Пенза, Наука и Просвещение, 2021, с. 190–200. EDN: PADMSS.

[2] Еськин Д.Л. Botnet как угроза информационной безопасности. *Вестник научных конференций*, 2020, № 11–5 (63), с. 69–71. EDN: RRBWSG.

[3] Tewogbade S.A., Ajasa M. Botnet attack detection in IoT using machine learning models. *International Journal of Science and Research Archive*, 2024, vol. 12, no. 1, pp. 2221–2229. https://doi.org/10.30574/ijsra.2024.12.1.0936

[4] Yu H. Research on botnet detection technology in network security. *Applied and Computational Engineering*, 2023, vol. 18, no. 1, pp. 81–87. https://doi.org/10.54254/2755-2721/18/20230967

[5] Молькова Л.Ю. Методы противодействия ботнет и поиска ботмастеров. *Научно-техническое и экономическое сотрудничество стран АТР в XXI веке*, 2024, т. 1, с. 292–294.

[6] Han S.Ju., Yoon S.Su., Euom I.Ch. The Machine Learning Ensemble for Analyzing Internet of Things Networks: Botnet Detection and Device Identification. *CMES — Computer Modeling in Engineering and Sciences*, 2024, vol. 141, no. 2, pp. 1495–1518. https://doi.org/10.32604/cmes.2024.053457

[7] Добот Ю.Н. Ботнет сети и их трафик. *Инновационные идеи молодых исследователей. XV Междунар. науч.-практ. конф.: сб. тр*. Уфа, Научно-издательский центр «Вестник науки», 2024, с. 49–56.

[8] Кабов А.А. Методы классического машинного обучения и нейросетевые модели как основа решения проблемы обнаружения ботов. *Актуальные вопросы фундаментальных и прикладных исследований. Междунар. науч.-практ. конф.: сб. ст*. Пенза, Наука и Просвещение (ИП Гуляев Г.Ю.), 2023, с. 17–20. EDN: FJYOQX.

[9] Bhattacharya S., Khanna A., Dubey R. Botnet Detection and Mitigation: A Comprehensive Literature Reviewю. *International Journal of Computer Trends and Technology*, 2024, vol. 71, no. 1, pp. 77–82. https://doi.org/10.14445/22312803/ijctt-v72i1p113

[10] Башмаков Н.М., Васильев В.И., Вульфин А.М. и др. Обнаружение сетевых атак ботнетов на основе технологий машинного обучения и переноса знаний. *Информационно-управляющие системы*, 2024, № 5 (132), с. 41–56. https://doi.org/10.31799/1684-8853-2024-5-41-56

***Поступила в редакцию 24.03.2025***

**Лосев Никита Сергеевич** — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Глинская Елена Вячеславовна** — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Научный руководитель** — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Ссылку на эту статью просим оформлять следующим образом:**
Лосев Н.С., Глинская Е.В. Обнаружение и предотвращение ботнетов в кибербезопасности. *Политехнический молодежный журнал*, 2025, № 05 (100). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1068.html

 ISSN 2541-8009

# DETECTION AND PREVENTION OF BOTNETS IN CYBERSECURITY

**N.S. Losev** losevns@student.bmstu.ru
**E.V. Glinskaya** glinskaya@bmstu.ru
SPIN-code: 5430-3023

*Bauman Moscow State Technical University, Moscow, Russian Federation*

Botnets are a network of infected computers controlled by intruders, being one of the most serious threats to cybersecurity. Used to send spam, DDoS attacks, data theft, and malware distribution, botnets can cause significant damage to both individual users and organizations. Botnets are managed through botmaster servers or intruders who coordinate their actions. The article discusses key botnet detection methods, including signature-based, behavioral, and machine learning-based approaches. Botmaster search methods such as network traffic analysis and the use of honeypots are also considered. The results of a comparative analysis of the effectiveness of the methods are presented, strategies for their further improvement are proposed, including combined approaches and the introduction of intelligent predictive analysis systems.

**Keywords:** botnet, botmaster, detection, attacker, machine learning, cybersecurity, DDoS attack, malware

***Received 24.03.2025***

**Losev N.S.** — Student of Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Glinskaya E.V.** — Senior Lecturer at Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Scientific advisor** — Basarab M.A., Dr. Phys. and Math. Sci., Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Please cite this article in English as:**
Losev N.S., Glinskaya E.V. Detection and prevention of botnets in cybersecurity. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 05 (100). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1068.html