



СИСТЕМА ЗАЩИТЫ И МОНИТОРИНГА САЙТОВ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Сергей Лоскутов, генеральный директор ООО "Сайтпатрол"



Виды атак

Сетевые атаки могут осуществляться **на уровнях L3/L4/L7 модели OSI**, особенно опасны на уровне приложений **L7** в виде, так называемых атак **«умных» ботов**, которые используют функциональные особенности атакуемой платформы и умеют мимикрировать под поведение легитимных посетителей.

DDoS-атаки (от английского Distributed Denial of Service, или "Распределенный отказ в обслуживании") определенный вид кибератак, направленных на замедление работы или отказ в работе веб-сервисов, сайтов и серверов.

Парсинг (scraping) – это автоматический сбор данных и их копирование ботами.

Поиск уязвимостей (vulnerability scanning) – это выявление слабых мест ресурса для дальнейшего их использования в кибератаках.

Атака на системы авторизации – сюда можно отнести как взлом аккаунтов (account takeover), так и создание фейковых аккаунтов и заброс спама (fake account creation).

Захват товаров (denial of inventory) – складирование в корзине онлайн-магазина каких-либо товаров, чтобы легитимные пользователи не могли их купить.

Кликфрод (скликивание рекламы) и атаки на ухудшение поведенческих метрик сайта.

Модель OSI

Тип данных	Уровень (layer)	Функция	Примеры протоколов
Данные	7. Прикладной (application)	Доступ к сетевым службам	HTTP, SMTP, DNS, etc.
	6. Уровень представления (presentation)	Представление и шифрование данных	MIME, SSL
	5. Сеансовый (session)	Управление сеансом связи	NetBIOS, именов.пайпы
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежностью	TCP, UDP
Пакеты (датаграммы)	3. Сетевой (network)	Определение маршрута и логическая адресация	IP, ICMP
Кадры	2. Канальный (data link)	Физическая адресация	IEEE 802.3, ARP, DHCP
Биты	1. Физический (physial)	Работа со средой передачи и двоичными данными	IEEE 802.3

Актуальность проекта

- Распределенные атаки типа «отказ в обслуживании» (DDoS) и атаки ботов нанесли **ущерб экономике РФ** порядка **1,4 трлн. рублей** за 2023 год.
- Ущерб по отрасли электронной коммерции более **350 млрд. рублей** за 2023 год
- Прямые потери могут достигать для крупного онлайн ритейла **1,5 млн. рублей в час**
- Интеллектуальные атаки уровня L7 и атаки “умного” botnet, умеют отражать **менее 5%** хостинг-провайдеров, высокая техническая сложность противодействия
- Количество “умных” атак выросло в **4,5 раза** за период с 2022 по 2024 год

В 2023-2024 году средний объем трафика, который создали боты на сайтах составил более 40% от всех посещений

*Информация по данным Tadvise.ru и anti-malware.ru

Система SitePatrol (www.sitepatrol.ru)

Мы реализовали и развиваем **SaaS-решение для защиты сайтов от атак ботов и DDoS-атак на L7**, основываясь на экспертной системе и машинном обучении (ML) с эффективным применением **на серверах небольшой мощности и shared-хостингах**.

Решение выросло из внутреннего сервиса для клиентов от нашей основной ИТ-компании (Vedita), которая специализируется на разработке, продвижении и поддержке e-com проектов. К системе подключено более 200 сайтов, где производится сбор данных, анализ/разметка и защита.

Есть РИД, оформленный на ООО «Сайтпатрол». Номер государственной регистрации договора: **РД0465189**

Компания ООО «Сайтпатрол» является резидентом «Сколково» с июня 2023 года
<https://navigator.sk.ru/orn/1125413>

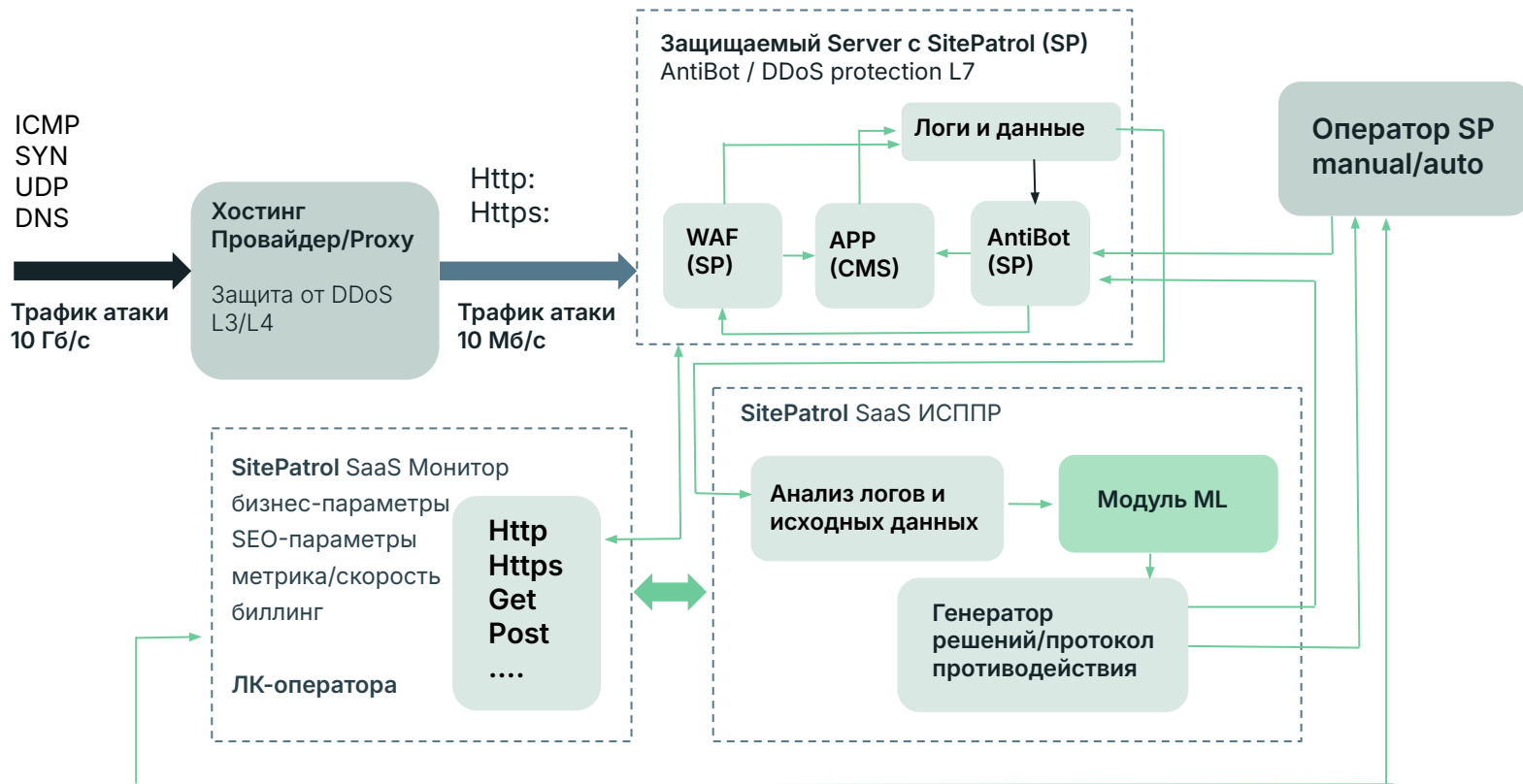
В ноябре 2024 получили **грант от Фонда содействия инновациям**.

Проводим активно НИОКР в области машинного обучения для повышения точности определения ботов.

Система SitePatrol (www.sitepatrol.ru)

- Собираются данные по поведению пользователей с помощью **собственного счетчика**: фиксируется движение мыши, клики, скролы, взаимодействие с DOM), а также параметры серверного окружения
- Работает **система защиты от атак ботов, таких как парсеры, сканеры уязвимостей, брутфорсеры, спамеры**, построенная на основе **экспертной системы и алгоритмов машинного обучения для поведенческого анализа**
- Есть система мониторинга сайтов и ресурсов. **Мониторим доступность сайта** раз в минуту, скорость работы сайта и сети, оплату домена, время окончания ssl-сертификата, наличие в черных списках и спам базах, уникальность текстов на страницах, тяжелые долгие страницы, индексацию поисковиками, критические ошибки на сайте (интеграции с Яндекс.Метрика и Яндекс.Вебмастер), а также при наличии доступа к панели сервера (интеграции с рядом хостинг-провайдеров): объем места на диске, нагрузку на процессор и бд.
- Работает мониторинг для **CMS Битрикс**: версия ПО, обновления, бекапы, защита, уязвимые скрипты и модули, защищаем и проверяем файлы robots и htaccess.
- Есть также подсистема независимого **автоматического резервного копирования в облако**.

Архитектура технического решения



SitePatrol интерфейс



8 (800) 555-14-36

sitepatrol.ru

8

SITEPATROL

История сигналов

Партнерка

Счет: 7065733.26 руб.

ТП: Corporate ещё 172 дн.

Сергей

Сайты

Подбор по параметрам

Поиск сайта по названию

+ ДОБАВИТЬ САЙТ

☐

айкомобилит-тамбов.ру

Домен истекает: 07.10.2024

SSL истекает: 11.11.2024

Срок лицензии: 02.09.2024

IP-адрес сайта: 45.130.41.22

Хостер: Beget

Баланс: 740 руб.

Окончание оплаты: 29.12.2023

группа: Кирилл Карлюк

☐

айкарт-мобил.ру

Домен истекает: 27.06.2025

SSL истекает: 30.07.2025

Срок лицензии: 26.08.2023

IP-адрес сайта: 92.53.106.134

Хостер: Timeweb

Баланс: 8514 руб.

Окончание оплаты: 25.09.2024

группа: Игорь Панфёров

☐

harmatg.com

SSL истекает: 26.11.2024

Срок лицензии: данных нет

IP-адрес сайта: 45.130.41.251

Хостер: Beget

Баланс: 22305 руб.

Окончание оплаты: 27.06.2025

права подтверждены

Защита от ботов активна (базовый)

Код ответа: 200

Линк студии: есть

Фраза: есть

Уникальность: 51.27%

Яндекс Икс: 20

Пинг: 4320 ms

Метрика: 204 host

права подтверждены

Защита от ботов активна (базовый)

Код ответа: 200

Линк студии: есть

Фраза: есть

Уникальность: 72.45%

Яндекс Икс: 180

Пинг: 4556 ms

Метрика: 744 host

права подтверждены

Защита от ботов активна (базовый)

Код ответа: 200

Линк студии: нет

Фраза: есть

Уникальность: 72.45%

Яндекс Икс: 180

Пинг: 4970 ms

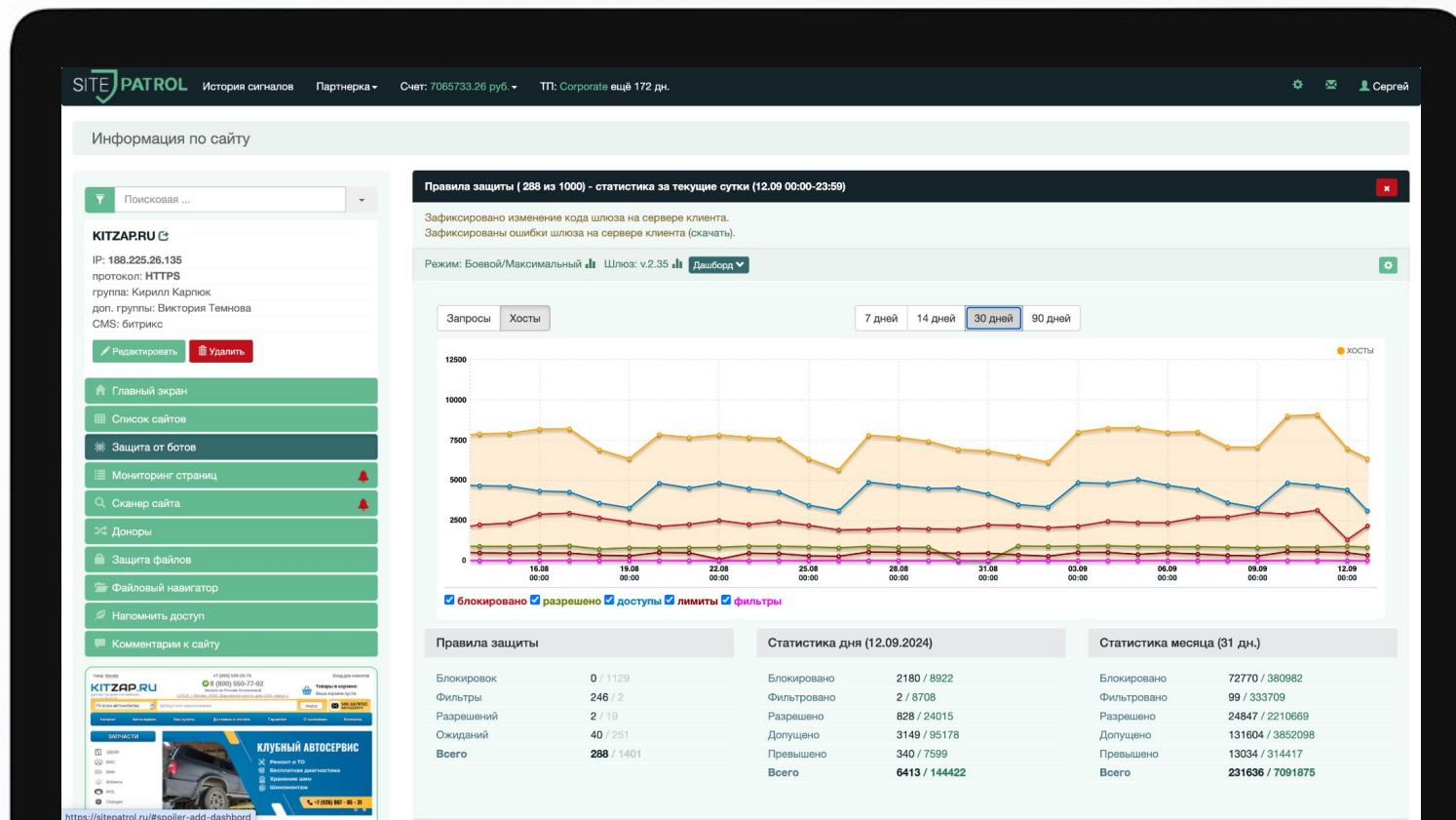
Метрика: данных нет

SitePatrol интерфейс



8 (800) 555-14-36 sitepatrol.ru

10



SitePatrol интерфейс



8 (800) 555-14-36

sitepatrol.ru

11

Все Фильтры Блокировки Разрешено Ожидают + ▼ ↺			
Объект (334)	Проверка	Действие и его срок	Статистика
🌐 🇷🇺 yandex [доверенный робот]	👤 много агентов нет данных	🟢 Разрешено Префильтр О неограничено	Блокировано - 0 Разрешено - 257095 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇺🇸 google [доверенный робот]	👤 много агентов нет данных	🟢 Разрешено Префильтр О неограничено	Блокировано - 1 Разрешено - 6507 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇷🇺 93.188.123.211 1С+Enterprise	👤 много агентов нет данных 🔗 парсинг	🔑 Капча Пользователь О неограничено	Блокировано - 0 Разрешено - 5582 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇺🇸 bing [поисковик]	👤 много агентов нет данных 🔗 парсинг	🔴 Блокировано Префильтр О неограничено	Блокировано - 4770 Разрешено - 0 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇷🇺 80.250.162.200	👤 один агент умный сложный 🔗 парсинг	⌚ Ожидание Система О до 12.09 23:59	Блокировано - 0 Разрешено - 0 Допущено - 2604 Превышено - 464 Фильтровано - 1
🌐 🇷🇺 46.48.14.250	👤 один агент умный сложный 🔗 ddos	⌚ Ожидание Система О до 12.09 23:59	Блокировано - 0 Разрешено - 0 Допущено - 2096 Превышено - 161 Фильтровано - 766
🌐 🇷🇺 sitepatrol [доверенный робот]	👤 много агентов нет данных	🟢 Разрешено Префильтр О неограничено	Блокировано - 0 Разрешено - 2962 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇸🇬 Bytespider [поисковик]	👤 один агент нет данных 🔗 идет анализ	🔴 Блокировано Префильтр О неограничено	Блокировано - 1560 Разрешено - 0 Допущено - 0 Превышено - 0 Фильтровано - 0
🌐 🇷🇺 Ведитат [офис ведита]	👤 много агентов нет данных	🟢 Разрешено Префильтр О неограничено	Блокировано - 0 Разрешено - 1182 Допущено - 0 Превышено - 0

Эшелонированная защита

1. Черные списки по известным сигнатурам, гео-зоны, подсети. Примитивные и сложные боты. Автоматическая блокировка.
2. Проверка на работу с cookies, js-челлендж: поддержка базовых возможностей и наличие полного стека js-событий мышь, скрол, тачпанель и тд. Примитивные и сложные боты. Автоматическая блокировка или фильтрация.
3. Анализ поведения посетителей: прохождение классификатора на базе ML и экспертной системы. Сложные “умные” боты. Автоматическая блокировка или фильтрация.
4. Возможна работа Оператора в экспертном ручном режиме, возможность принимать решения по каждому посетителю в реальном времени.

Блокировка: по ip, по сессиям, по сигнатурам на уровне черных списков и на уровне Оператора.

Фильтрация: капча на период времени, капча постоянно, редирект, снижение скорости отдачи страницы.

ML-модуль

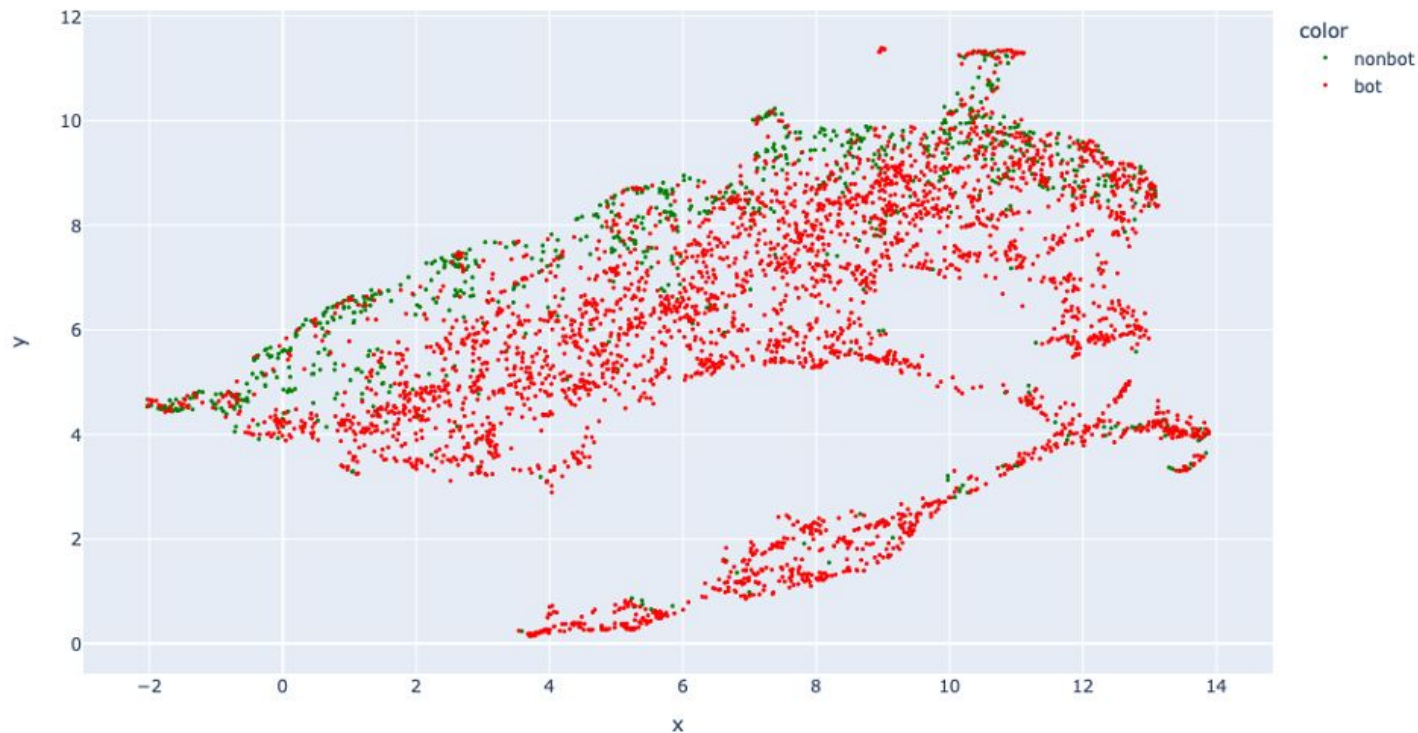
В рамках наших работ исследован подход к решению **задачи классификации пользовательских сессий**, основанный на неконтролируемом обучении (алгоритмы кластеризации, включая K-средних, MeanShift, DBSCAN, UMAP) для доразметки данных с последующей классификацией сессий контролируемыми методами машинного обучения (случайный лес, градиентные бустинги и нейронные сети).

Текущий вариант ML-модуля построен на базе **кластеризатора HDBSCAN** и ансамбля*, состоящего из модели нейронной сети и модели градиентного бустинга. В архитектуре **нейронной сети** используются полносвязные слои. В качестве реализации алгоритма градиентного бустинга используется библиотека **XGBoost**.

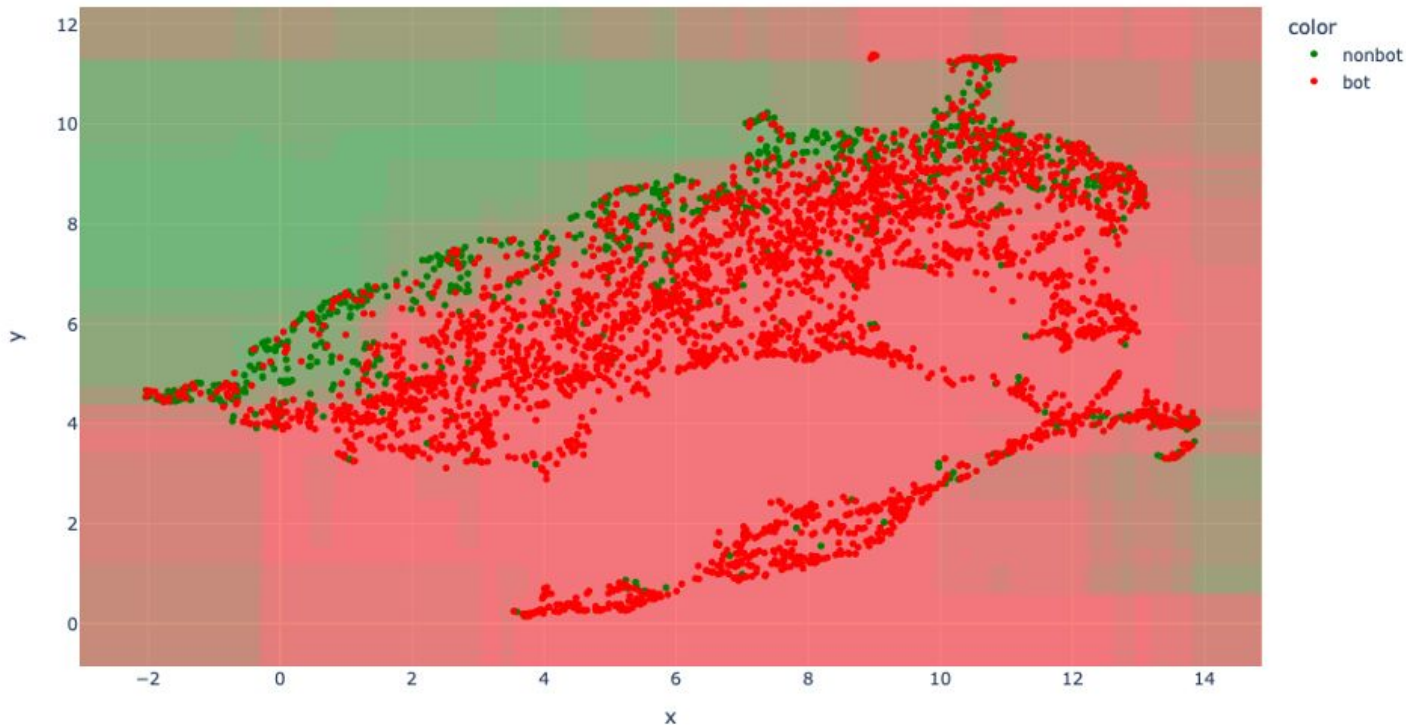
Наше решение позволяет классифицировать сессии пользователей и сложных «умных» ботов на основе логов доступа к сайтам, **с точностью до 80 %**.

*Ансемблирование моделей машинного обучения – это метод, при котором несколько моделей объединяются для улучшения общей производительности и надежности предсказаний.

Визуализация сессий



Нейронная сеть + градиентный бустинг



Конкуренты

	Site Patrol	Ростелеком (rt-solar)	Stormwall	Servicepipe	Variti	BlackWall	CloudFlare	Datadome
Целевой сегмент	микро, малый, средний, крупный бизнес	микро, малый, средний, крупный бизнес	малый, средний, крупный бизнес	малый, средний, крупный бизнес	малый, средний, крупный бизнес	Все сегменты	Все сегменты	Крупный, средний бизнес
Тарифная сетка	от 3 900 руб./мес.	от 1 800 руб./мес.	антибот доступен на тарифе от 150 000 руб./мес	от 50 000 руб./мес	от 22 000 руб./мес.	от 30 долл/мес	от 20 долл/мес	от 1500 долл/мес
Защита от "умных" ботов, наличие ML	есть защита и наличие ML	нет данных	нет данных	есть, ML	нет данных	нет данных	нет данных	есть, ML
Наличие доп. функций	lite WAF, мониторинг, бекапы	нет	нет	нет	нет	lite WAF	Нет	нет
Способ интеграции	скрипт, API, без проксирования	проксирование	проксирование	API, проксирование	проксирование	API, проксирование	проксирование	API, без проксирования

Преимущества нашего решения

- Точность определения примитивных ботов **до 99%**
- Специализация на отрасли еcom и определении сложных "умных" ботов
- Защита от DDoS на L7 и защита от сложных "умных" ботов **на минимальном тарифе**
- Доступно на **слабых серверах и shared-хостингах**
- **Не требуется отправка SSL** ключей шифрования трафика третьей стороне и **не ухудшает SEO**.
- Оказываем мониторинг доступности сайта 24/7, коммерческих и **бизнес-параметров сайтов**, поисковых факторов, скорости работы, а также выполняем автоматическое бекапирование ресурсов.

Целевая аудитория

Владельцы интернет-магазинов, сайтов коммерческих услуг/каталогов товаров. **Микро/малый/средний бизнес.**

Всего в РФ около **230 тыс. действующих интернет-магазинов и коммерческих сайтов:**

- Магазины одежды, электроники, запчастей и т.д.,
- Каталоги оборудования, мебели под заказ, с/х техники
- Сайты туроператоров, медицинских центров

На сайтах со средней посещаемостью 2000 хостов в сутки при конверсии 2,5% в заказ со средним чеком 20 000 руб. прямые финансовые потери могут составить **до 1 млн. руб. за один рабочий день простоя.**

- Нет возможности платить значительные суммы абонентской платы в месяц за защиту и мониторинг
- Нет возможности нанять в штат квалифицированного сотрудника
- Сложность реализации и поддержки самостоятельного решения
- Ухудшение SEO значительно влияет на бизнес

Расчет рынка в формате TAM/SAM/SOM (РФ), прогноз на 2026 год

TAM Рынок кибербезопасности (ПО)

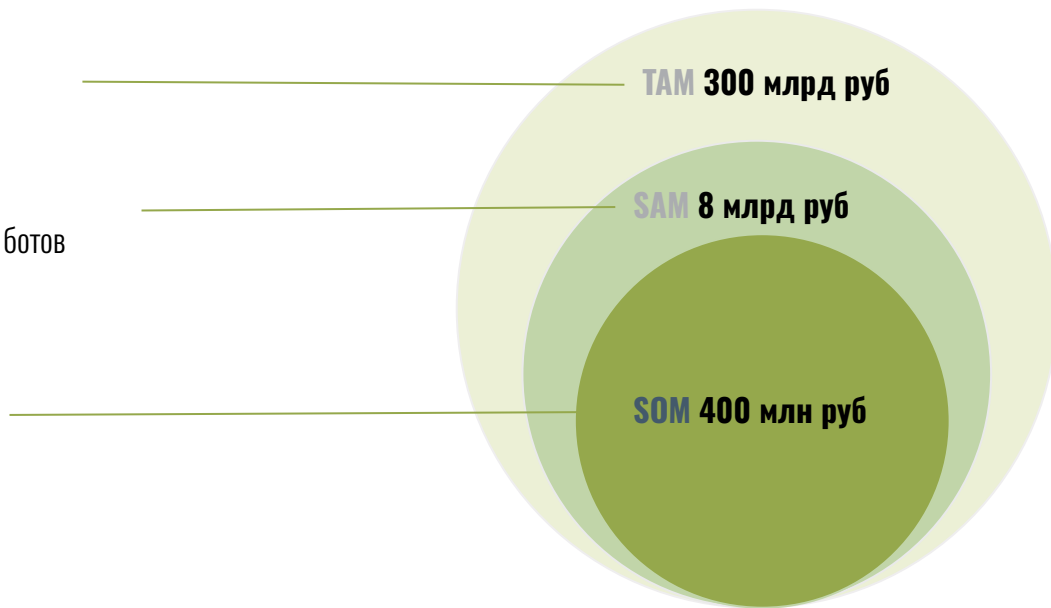
300 млрд. руб в год

SAM Рынок WAF и защиты от DDoS L7, ботов

8 млрд. руб в год

SOM Рынок решения (5%)

400 млн. руб. в год



Расчет рынка в формате TAM/SAM/SOM (Мировой), прогноз на 2026 год

TAM Мировой рынок кибербезопасности (ПО)

14 200 млрд. руб в год*

SAM Рынок WAF и защиты от DDoS L7, ботов

450 млрд. руб в год

SOM Рынок решения (0,5%)

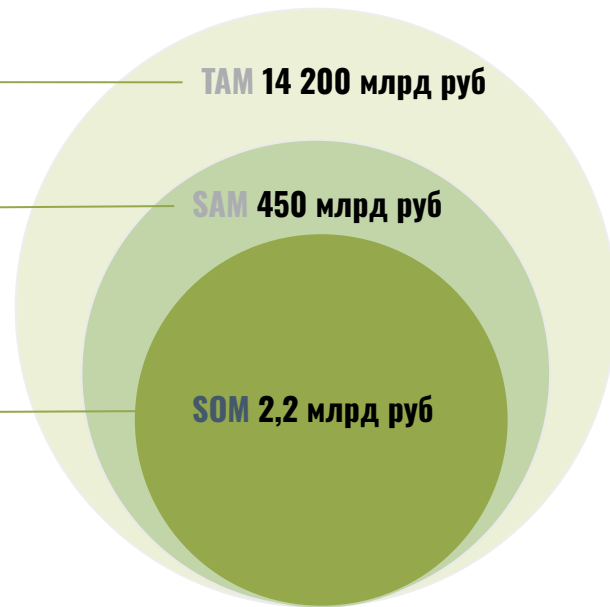
2,2 млрд. руб в год

TAM 14 200 млрд руб

SAM 450 млрд руб

SOM 2,2 млрд руб

**По курсу 80 руб. за 1 доллар.*



Расчет рынка (альтернативный вариант)

Примем за емкость целевой аудитории **230 000 субъектов МСП** с действующими сайтами интернет-магазинов в РФ.

Рассчитаем потенциальную выручку SaaS-модели сервиса "SitePatrol" в рублях в месяц в зависимости от доли рынка и минимального тарифа.

Стоимость тарифа минимального тарифа Start: 4 590 рублей / месяц.

- При доле рынка 0,1% : $230\,000 * 0,1\% * 4\,590 = 1\,055\,700$ рублей
- При доле рынка 1% : $230\,000 * 1\% * 4\,590 = 10\,557\,000$ рублей
- При доле рынка 1,5% : $230\,000 * 1,5\% * 4\,590 = 15\,835\,500$ рублей

До **190 026 000** рублей в год.

Бизнес-модель

Формат использования продукта:

- SaaS-сервис с ML
- Установка Агента на сервер и сайт клиента.

Монетизация:

- подписка, стоимость от 3 900 руб./мес с полным набором всех функций для 1-го защищаемого сайта
- тарифные планы в зависимости от среднего количества посетителей сайта
- есть продажи 2024 год на сумму 3 млн. руб. с учетом функций защиты и мониторинга

Каналы продаж:

- собственная клиентская база
- контент-маркетинг, блоги VC, Sostav, Habr
- контекстная, таргетированная реклама
- ИТ-сообщества
- экспертные вебинары и семинары
- партнерская программа с производителями решений для сайтов и хостингов
- интеграция с хостинг-провайдерами
- размещение Модулей на маркетплейсы и сообщества популярных CMS (1C-Битрикс, Wordpress и т.д.)

Стратегия реализации проекта на 3 года

Период	2024	2025	2026
Исследования и разработка	Проведение НИОКР Наращивание объемов DataSet ML на PyTorch Обучение модели Разработка модуля ИСППР 1.0 Разработка Агента 1.0 Разработка MVP с уровнем точности свыше 30% на “холодном старте” Апробация., интеграция с боевыми контурами. Начало первых продаж	Запуск проекта в промышленную эксплуатацию. Расширение DataSet Версия ИСППР 2.0 Версия Агента 2.0 + WAF Повышение уровня точности до 80% Расширение клиентской базы до 500 компаний Реализация API-для интеграций с внешними системами и хостинг-площадками Развитие интерфейса	Масштабирование проекта, реализация новых технических решений. Версия ИСППР 3.0 (для партнеров) Версия Агента 3.0 Разработка Модуля 3.0 + WAF Расширение клиентской базы до 1 500 компаний Создание собственных центров очистки трафика. Интеграция с инфраструктурой крупных зарубежных хостинг-провайдеров
Орг. развитие и план по найму	Над проектом работают 5 сотрудников	Расширение команды в области DevOps, разработки, тех. поддержки и маркетинга до 18 сотрудников	Активный маркетинг в РФ. Выход на международный рынок, расширение международной команды
Привлечение инвестиций	Собственные средства/Грантовая поддержка	Собственные средства/ Грантовая поддержка/Внешние инвестиции	Собственные средства/Грантовая поддержка/Внешние инвестиции/Партнерство
Защита интеллектуальной собственности	Патентование способов обучения и архитектуру ИНС Авторское свидетельство SitePatrol в ФИПС уже есть	Патентование системы и продукта	-
Маркетинг, продажи, инвестиции	Начало маркетинговой активности и PR по проекту.	Стратегия маркетингового роста за счет привлечения партнеров: хостинг-провайдеров, производителей решений для CMS, digital-агентств Активная работа с блогерами и PR .	Локализация на английский, испанский языки и арабский Активный маркетинг и PR проекта на рынках ОАЭ, Южной Америки, Азии. Партнерство с хостинг провайдерами. Продажи системы на международный рынок
Планируемая выручка	3 млн. рублей	25 млн. рублей	100 млн. рублей



SITE PATROL

7 дней **БЕСПЛАТНО!**



sitepatrol.ru

8 (800) 555-14-36

Рассматриваем венчурные инвестиции в размере от 40 до 50 млн. рублей.

Расчет бюджетов по направлениям на 12 месяцев.

1. Маркетинг и PR.

Маркетолог

PR-менеджер

Копирайтер/блогер

Менеджер по партнерке

Расход на ФОТ в среднем **350 000 руб.мес.**

Рекламный бюджет на продвижение в РФ: контекст 250, посеы 100, статьи в СМИ 50, партнерки 50, выступления 50.

В среднем **500 000 руб.мес.**

2. Продажи.

Активные менеджеры по продажам + обработка входящих, 2 человека

Расход на ФОТ в среднем в месяц **300 000 руб.мес.**

3. Доработка и развитие системы

Продукт-менеджер, 200

Архитектор, 300

Техлид, 200

МЛ-специалист, 300

Разработчик бекенд 2, 300

Разработчик фронтенд 1, 150

Дизайнер UI/UX 1, 100

Девопс 1, 300

МЛ-специалист 1, 300

Тестирующий 1, 100

Расход на ФОТ в среднем **2 100 000 руб.мес.**

4. Тех. поддержка

Два специалиста

200 000 руб.мес.

5. Сервера

YandexCloud, Балансировщик, Приложения, СУБД, ML-модель

300 000 руб.мес.

ИТОГО, затратная часть 3 750 000 руб.мес., 45 000 000 рублей год.

К концу 2026 года 1 500 клиентов со средним чеком 10 000 руб.мес., общая сумма **15 000 000 руб.мес.**