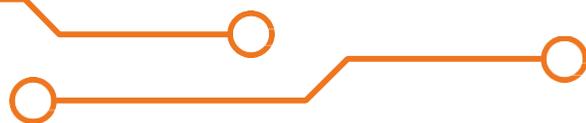




Вебмониторэкс

защита веб-приложений и API

**Российская платформа
для защиты веб-приложений и API**



Лидер российского рынка защиты веб-приложений и API



Продукты

Высокое качество, подтвержденное годами безупречной работы



Заказчики

Крупнейшие российские и зарубежные компании



Команда

Эксперты рынка, обладающие признанным авторитетом



Партнеры

Широкая партнерская сеть



Развитие

Активное как продуктивное, так и стратегическое



Инновации

Визионеры в сегменте защиты API

Вебмониторэкс в 2024 году

№1

Приоритет к особенностям
рынка ИБ в России

60+

Технических специалистов
среди сотрудников

200+

Довольных клиентов
в России

Топ-100

Крупнейших ИБ-компаний в
России

80+

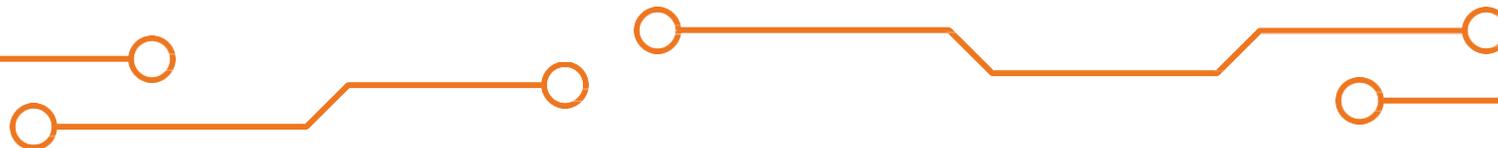
Технологических интеграций

100+

Партнеров-интеграторов

3

Дистрибьютора



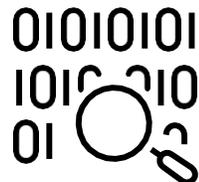
Платформа «Вебмониторэкс»

Защищает от атак на веб-приложения, микросервисы и API

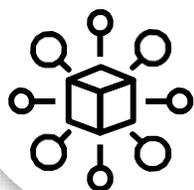
Продукт «ПроWAF»



Firewall
веб-приложений

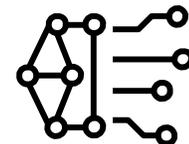


Сканер
периметра и уязвимостей

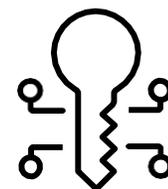


Модуль
перепроверки атак

Линейка продуктов «ПроAPI»



ПроAPI Структура

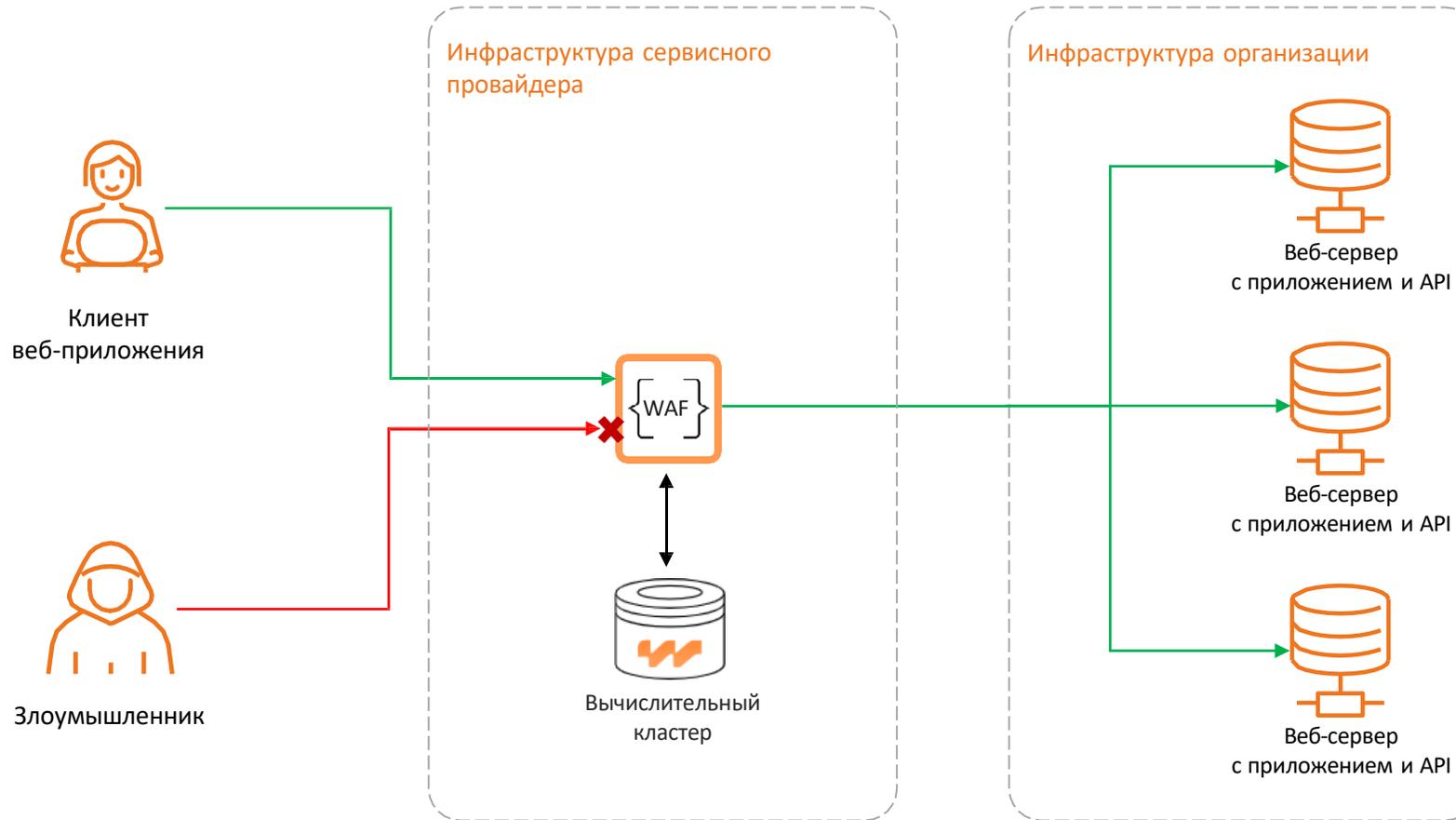


ПроAPI Тестирование



ПроAPI Защита

Схема работы WAF У сервисного провайдера



Всесторонняя защита веб-приложения:

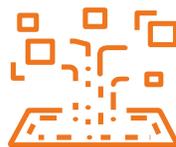
- Анализ входящих NT TP запросов
- Блокировка опасного трафика
- Инвентаризация активов
- Выявление уязвимостей
- Virtual patching
- Перепроверка на разных вариантах атаки



Фильтрующая нода (Web Application Firewall)

Основные задачи:

- Анализ трафика на периметре сети
- Блокировка действий злоумышленника



Вычислительный кластер «Вебмониторэкс»

Консоль управления фильтрующими нодами:

- Централизованное управление настройками безопасности
- Система аналитики и отчетности
- Средства интеграции

Средства построения комплексной защиты:

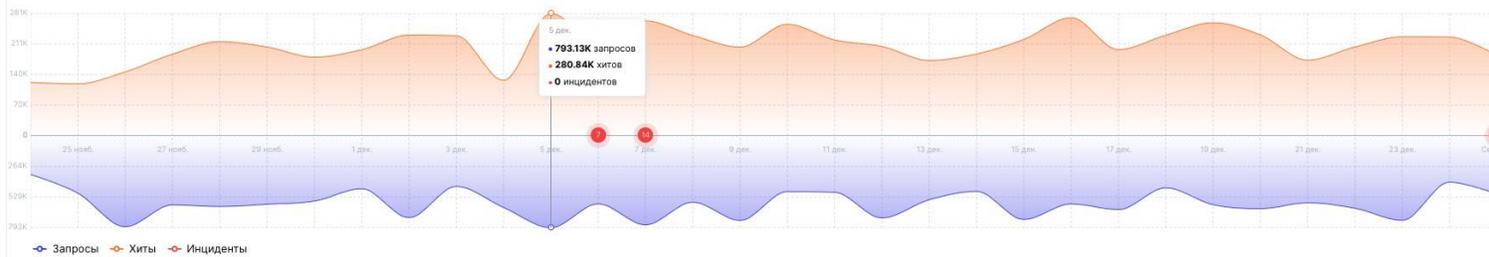
- Подсистема исследования и предупреждения атак
- Подсистема блокировки массовых атак
- Подсистема автоматического реагирования на события безопасности
- Сканер периметра и уязвимостей

- WebmonitorX
- Дашборды
- Аналитика угроз
- Структура API
- События
- Уязвимости
- Структура API
- Спецификация API
- Утечки API
- Сканер
- Триггеры
- Ноды
- Списки IP
- Правила
- Защита от BOLA
- Интеграции
- Настройки

Аналитика угроз

Приложение: 25 нояб. – 25 дек.

Обычный и вредоносный трафик



Сводка за период

- 27 Инцидентов (18.2% ↓)
- 6.5M Забл. хитов (4.14% ↓)
- 6.51M Хит (4.05% ↓)
- 18.5M Запроса

Источники атак



Местоположение	Хиты
Соединенные Штаты	232K
Великобритания	44.8K

Цели атак

Домены	Инциденты	Хиты	Тренд
main-api.ru.demo.webmonitorx.dev	27	6.5M	↓ 4.07%
api2.ru.demo.webmonitorx.dev	—	1.6K	↑ 20.7%
api1.ru.demo.webmonitorx.dev	—	1.21K	↑ 141%
api4.ru.demo.webmonitorx.dev	—	748	↓ 23.1%
api3.ru.demo.webmonitorx.dev	—	714	↑ 125%

Месячный лимит:
14.9M из ∞

Подсистема исследования и предупреждения атак



- Выявление атакующего элемента запроса
 - В реальном времени под высокой нагрузкой для протоколов HTTP и HTTPS, gRPC, WebSocket
 - Декодирование, нормализация и токенизация для вложенных типов данных
 - Парсинг данных внутри WebSocket соединений с учетом вложенных кодировок (json, gzip, xml)
- Определение и систематизация типов и классов атак
- Перепроверка возможности реализации атаки на веб-приложение с аналогичными, но видоизмененными запросами
- Virtual Patching - ограничение доступа к уязвимым частям приложения до их устранения

Подсистема исследования и предупреждения атак

440 атак 895.1К хитов

Сортировать по последнему запросу

Дата длительность	Хиты	Пайлоады	Топ IP / Источник	Домен / Путь ПРИЛОЖЕНИЕ	Код	Параметр	Активная проверка
25 дек, 11:57 7м 10с	56	1 SQLi	51.77.58.41 DC	main-api.ru.demo.webmonitorx.dev /admin/suppliers/view_details.php Application #888	403	QUERY id	✓

56 запросов

Отметить атаку как ложную

25 дек, 11:57 — 12:04

CVE-2023-2130 generic_sql



25 ДЕК, 11:57 25 ДЕК, 12:04

Дата	Вредоносный пайлоад	Источник	Код	Размер, B	Время, ms	Действия
25 дек, 12:04:18	1' AND (SELECT 968 ... ECT(SLEEP(6)))pn	51.77.58.41 DC	403	0	0	Правило Ошибка

ID запроса: 81f9143c8f7e6313758944358bb48073

IP ноды 127.0.0.1:8888

UUID ноды: 57b60162-f1f9-443a-876a-c0d8bc661542

Тэги: final_wallarm_mode: block libproton_version: 4.4.12 lom_id: 611

CVE: CVE-2023-2130 generic_sql

GET /admin/suppliers/view_details.php?id=1'+AND+(SELECT+9687+FROM+(SELECT(SLEEP(6)))pnac)+AND+'ARHJ'='ARHJ HTTP/1.0

Скопировать cURL

CONNECTION: close

ACCEPT: */*

ACCEPT-ENCODING: gzip

ACCEPT-LANGUAGE: en

AUTHORIZATION: Basic YWRtaW46Yk1kVEJ4b3RmaGh0QVhsUk9QZkUK

HOST: main-api.ru.demo.webmonitorx.dev

USER-AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36

X-REAL-IP: 51.77.58.41

X-FORWARDED-FOR: 51.77.58.41

X-FWD-APP: true

Подсистема блокировки массовых атак



Защита приложения от автоматизированных атак, нацеленных на сбор информации:

- Brute-force – перебор пар логин-пароль
- Credential Stuffing – перебор пароля к учетной записи
- Directory Busting – перебор директорий сайта с целью идентификации используемых сервисов
- Блокировка по IP-адресам



Подсистема блокировки массовых атак

Списки IP 🔍

Все 7 Белый список 2 Черный список 2 Серый список 3

Добавить объект ▼

Сейчас

Белый список 🔍

Объект	Приложения	Источник	Причина	Добавлен/Обновлен	Дата удаления	
<input type="checkbox"/> 4.4.4.4	Application #69	Public proxy	test2	25 дек. 2024, 15:25	25 дек. 2024, 16:25	⋮
<input type="checkbox"/> 92.34.23.67	Все	SE	test 3	25 дек. 2024, 15:25	25 дек. 2024, 15:40	⋮

Черный список 🔍

Объект	Приложения	Источник	Причина	Добавлен/Обновлен	Дата удаления	
<input type="checkbox"/> 🌐 Американское Самоа	Все		block	25 дек. 2024, 15:26	25 дек. 2024, 16:26	⋮
<input type="checkbox"/> 98.54.35.32	Application #9	US	test5	25 дек. 2024, 15:26	25 дек. 2024, 15:41	⋮

Серый список 🔍

Объект	Приложения	Источник	Причина	Добавлен/Обновлен	Дата удаления	
<input type="checkbox"/> 🌐 Tor	Application #100		Не легитимные источники	25 дек. 2024, 15:27	25 дек. 2024, 16:27	⋮
<input type="checkbox"/> 🌐 VPN	Application #100		Не легитимные источники	25 дек. 2024, 15:27	25 дек. 2024, 16:27	⋮
<input type="checkbox"/> 🌐 Public proxy 🌐 Web proxy	Application #100		Не легитимные источники	25 дек. 2024, 15:27	25 дек. 2024, 16:27	⋮

Подсистема автоматического реагирования



Умные уведомления (триггеры) основываются на разных событиях:

- Скорость атаки на приложение
- Количество IP в атаке
- Коды ответа приложения
- Тип атаки
- Прочие настраиваемые события

Уведомления доступны через почту, telegram и другие сервисы

Возможные кастомизированные действия:

- Блокировка IP
- Комплексная блокировка



Подсистема автоматического реагирования

Создать триггер

Тип триггера

 **Количество атак**
Как много атак обнаружено

Наименование

Test

Описание

Условия

 Атаки больше чем 10000 за день

Фильтры

Выбрать фильтр

Реакция

Добавить реакцию

Отмена

Доступные фильтры

-  **Тип**
Например: XSS, SQLi, Brute-force, и т.д.
-  **Приложение**
Ограничить диапазон по приложению
-  **IP**
Ограничить диапазон по IP
-  **Домен**
Ограничить диапазон по домену
-  **Статус ответа сервера**
Например: 200, 300, 400, 500
-  **Цель**
Ограничить диапазон по цели

Сбросить изменения

Создать

Доступные действия

Email и мессенджеры

-  **Отправить email**
Уведомление через email
-  **Отправить уведомление в Telegram**
Уведомление через Telegram
-  **Отправить уведомление в Slack**
[Настройте на странице Интеграции](#)
-  **Отправить уведомление в Microsoft Teams**
[Настройте на странице Интеграции](#)

Системы управления инцидентами и задачами

-  **Отправить событие в Opsgenie**
[Настройте на странице Интеграции](#)
-  **Отправить событие в PagerDuty**
[Настройте на странице Интеграции](#)

Сканер периметра и уязвимостей



Классика MITTRE ATT&CK: атака начинается с Reconnaissance – исследования объекта атаки

Сканер воспроизводит технику сканирования злоумышленников:

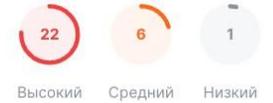
- Сбор данных об объектах сетевого периметра
- Поиск типовых уязвимостей и проблем безопасности
- Поиск уязвимостей на узлах, находящихся в периметре компании
- Актуализация информации о найденных ранее уязвимостях

Сканер способен обнаруживать все распространённые типы уязвимостей (в соответствии с рекомендациями OWASP Top-10), таких как SQLi, XSS, XXE и т.п.



Сканер периметра и уязвимостей

Сканер уязвимостей



Уязвимости

25 нояб. – 25 дек. ▾



Домен, IP или порт | Все ресурсы 152 | Новые 75 | Отключенные 11 | Ограничение RPS для IP или домена

Домены 92
 *.webmonitorx.ru 92

- webmonitorx.ru
- alertmanager.webmonitorx.ru
- www.alertmanager.webmonitorx.ru
- api.webmonitorx.ru
- www.api.webmonitorx.ru
- api-firewall.webmonitorx.ru
- www.api-firewall.webmonitorx.ru
- bbb.webmonitorx.ru
- www.bbb.webmonitorx.ru
- beta.webmonitorx.ru

IP-адреса 33

- 2a02:6b8::1da Search engine
- 45.89.190.18 VPN
- 51.68.82.68 DC
- 51.77.110.1 DC
- 51.250.33.244 DC
- 51.250.38.49 DC
- 51.250.68.124 DC
- 51.250.69.227 DC
- 57.128.163.38 DC
- 57.128.167.201 DC

Сервисы 27

- Unknown 12
- 8009 ajp13
- 21 ftp
- http 7
- 443 https
- 9001 https
- 9443 https
- 389 ldap
- 22 ssh
- 777 ssh

Сбросить изменения

Фильтровать по тегу

- Сканер уязвимостей
- CWE-200 Разглашение информации 19
- CWE-310 Криптографические уязвимости 3
- CWE-20 Некорректная проверка входных параметров 30

Настройка

CWE-200 Разглашение информации

Разглашение информации – это преднамеренное или непреднамеренное раскрытие информации субъекту, который явно не уполномочен иметь доступ к этой информации.

- Раскрытие данных из-за обработки файлов cookie
- Открытый доступ к коду и репозиторию под управлением SVN [SVN](#)
- Раскрытие данных через протокол TFTP [TFTP](#)
- Раскрытие данных через служебные сообщения Django [Django](#)

Технологические преимущества



Технологическая база международного уровня



Собственная независимая команда разработки



Продукты в реестре
российского ПО



Сертификат ФСТЭК России
по МЭ Г4



Техническая поддержка
24/7/365



Открытость и обратная связь
по всем продуктам

Технологический и инновационный лидер, **ориентированный на практический результат**

Позитивная модель WAF

- Требуется создание профиля для каждого защищаемого приложения
- Требуется обновление настройки после каждого релиза
- Большое количество ложно положительных срабатываний
- Отсутствие реакции на zero - day

Негативная модель WAF

- Обнаруживает атаки сразу после установки
- Поддерживает непрерывный процесс безопасной разработки
- Позволяет сделать гибкую настройку для снижения ложно-положительных срабатываний
- Изучение каждого запроса на наличие атаки
- Защита от zero - day

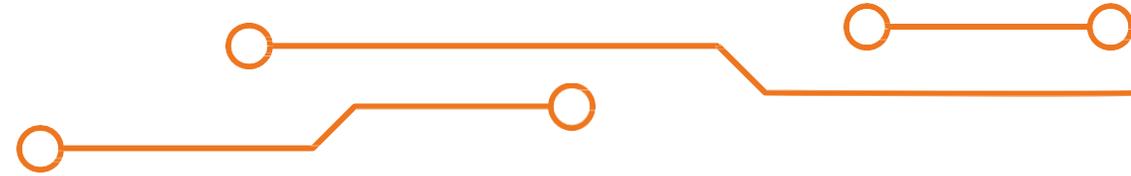
Первый на рынке WAF, анализирующий весь трафик

Собственный центр аналитики

Работаем с открытыми и специальными источниками уязвимостей

Минимальное время реагирования на 0-day уязвимости
Описание log4shell - 10 минут

Автоматическое обновление правил детекта



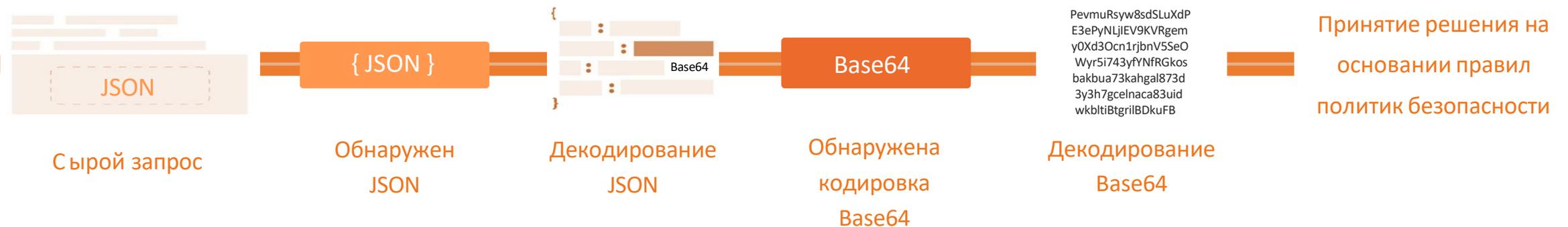
OWASP top 10:

- WEB
- API
- Mobile

Глубокий анализ запросов

Интеллектуальный парсинг

- Работает без конфигурации
- Не требует схемы
- Автоматически распознает форматы данных
- Применяет необходимые парсеры/декодеры
- Применяет цепочки парсеров
- Отлично работает в CI/CD



Концепция развития продукта



- Комплексная защита веб-приложений и API
- Работа с высоконагруженными приложениями
- Легкое масштабирование
- Низкая стоимость владения (ТСО):
 - ✓ не требуется специальных знаний или обучения для внедрения
 - ✓ нет необходимости в консалтинге и фулл-тайм администрировании
 - ✓ бесплатные вебинары по обновлениям продукта и его настройке
- Работа с быстроразвивающимися приложениями
- ГОСТ шифрование

Успешные кейсы сотрудничества Softline и Вебмониторэкс



Обещаем, что с нас памятные подарки для каждого, кто уделит нам время!



**Примите участие в
опросе о защите API**





Вебмониторэкс

защита веб-приложений и API



webmonitorx.ru



info@webmonitorx.ru



+7 495-740-35-44



[Нabr](#)



[Телеграм](#)



[ВКонтакте](#)

