F6

Attack Surface Management

История успеха

Как Сервис «Грузовичкоф»

усилил защиту от внешних киберугроз

Отрасль

Логистика и перевозки

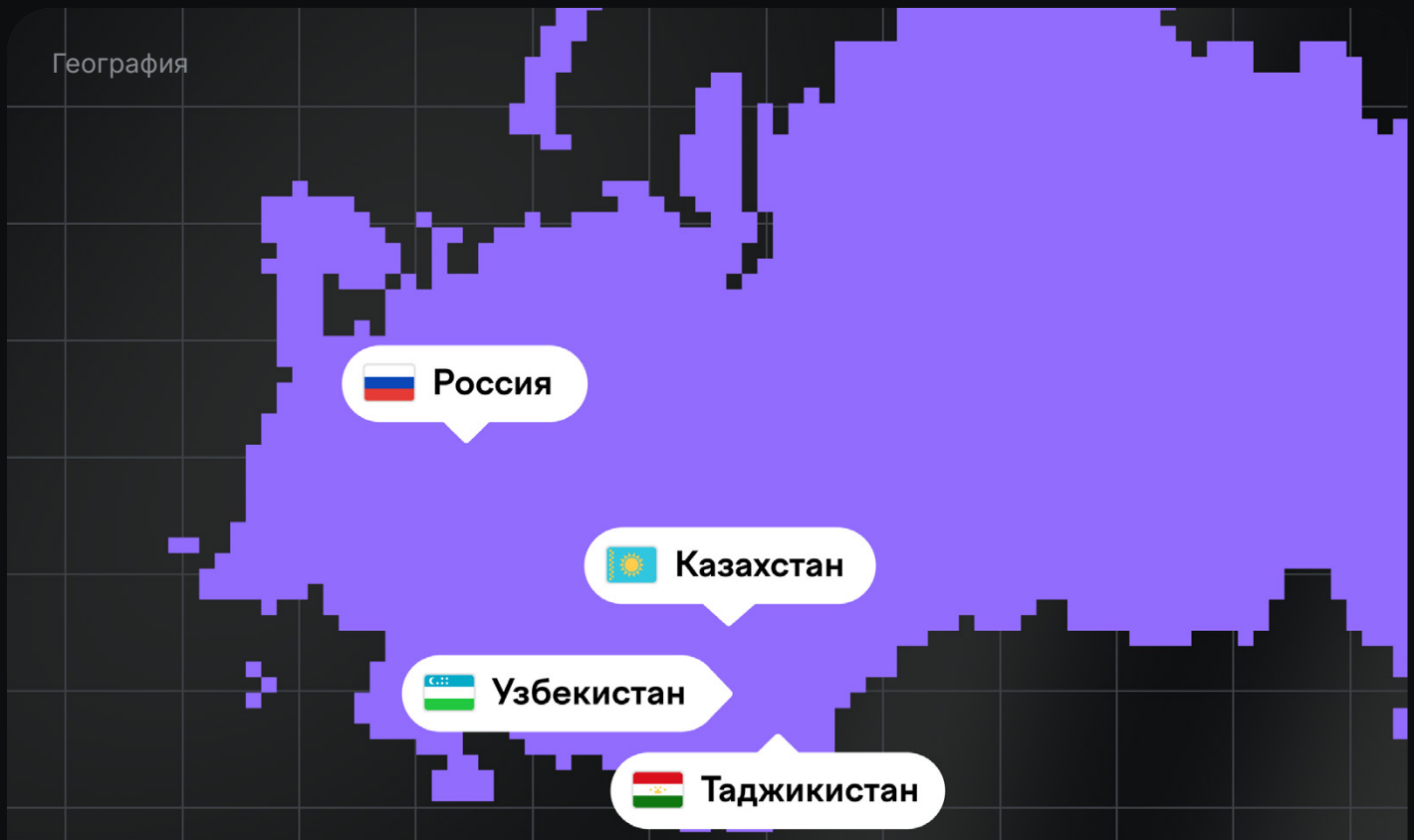
Основана

2005

О компании

Сервис «Грузовичкоф» — один из ведущих грузоперевозчиков на территории России и стран СНГ, а также признанный лидер в сфере транспортных и логистических услуг в Москве и Санкт-Петербурге. Основу бизнеса составляет цифровая инфраструктура: мобильные приложения, онлайн-сервисы для заказов и расчетов и другие информационные системы. Высокая зависимость от стабильности сервисов делает безопасность внешней и внутренней инфраструктуры ключевым условием бесперебойной работы и репутации.

География



Россия и СНГ

Предпосылки проекта: логистика как лакомая цель для атак

Логистические компании входят в зону повышенного риска: их цифровая инфраструктура обеспечивает доступ к данным клиентов, маршрутам и сервисам. Любая атака может парализовать работу и привести к многомиллионным убыткам.

Основные угрозы в отрасли:

Утечки данных

персональные данные клиентов и информация о маршрутах быстро превращаются в товар на теневых площадках

Атаки на периметр

забытые поддомены, устаревшие лендинги и облачные сервисы становятся точками входа

Уязвимости API и трекинга грузов

использование слабых конфигураций дает злоумышленникам прямой доступ к системам мониторинга

Дмитрий Ляхов

директор по информационной безопасности «Грузовичкоф»

«Статистика красноречиво свидетельствует: подавляющее большинство инцидентов безопасности происходят из-за уязвимостей на внешнем периметре. Это не второстепенная задача, а критически важное направление защиты. Любой забытый поддомен, утечка данных на стороннем ресурсе или неиспользуемая облачная учетная запись становятся точкой входа для злоумышленников. Масштаб угрозы требует самого пристального внимания и проактивных мер»

Основные вызовы до начала проекта

- Отсутствие полной картины внешних цифровых активов.
- Ручной контроль поддоменов, API и облачных сервисов, что приводило к высокой нагрузке на ИБ-команду;
- Увеличение числа внешних угроз: от фишинга и сканирования периметра до атак на устаревшие активы;
- Недостаточная автоматизация процессов.

«Мы стремимся не просто закрывать критические точки, а иметь полную видимость всей поверхности атаки. Без этого невозможно эффективно противодействовать современным угрозам»

Дмитрий Ляхов

директор по информационной безопасности «Грузовичкоф»

Почему был выбран F6 ASM

После анализа нескольких решений команда ИБ остановилась на **F6 Attack Surface Management**.

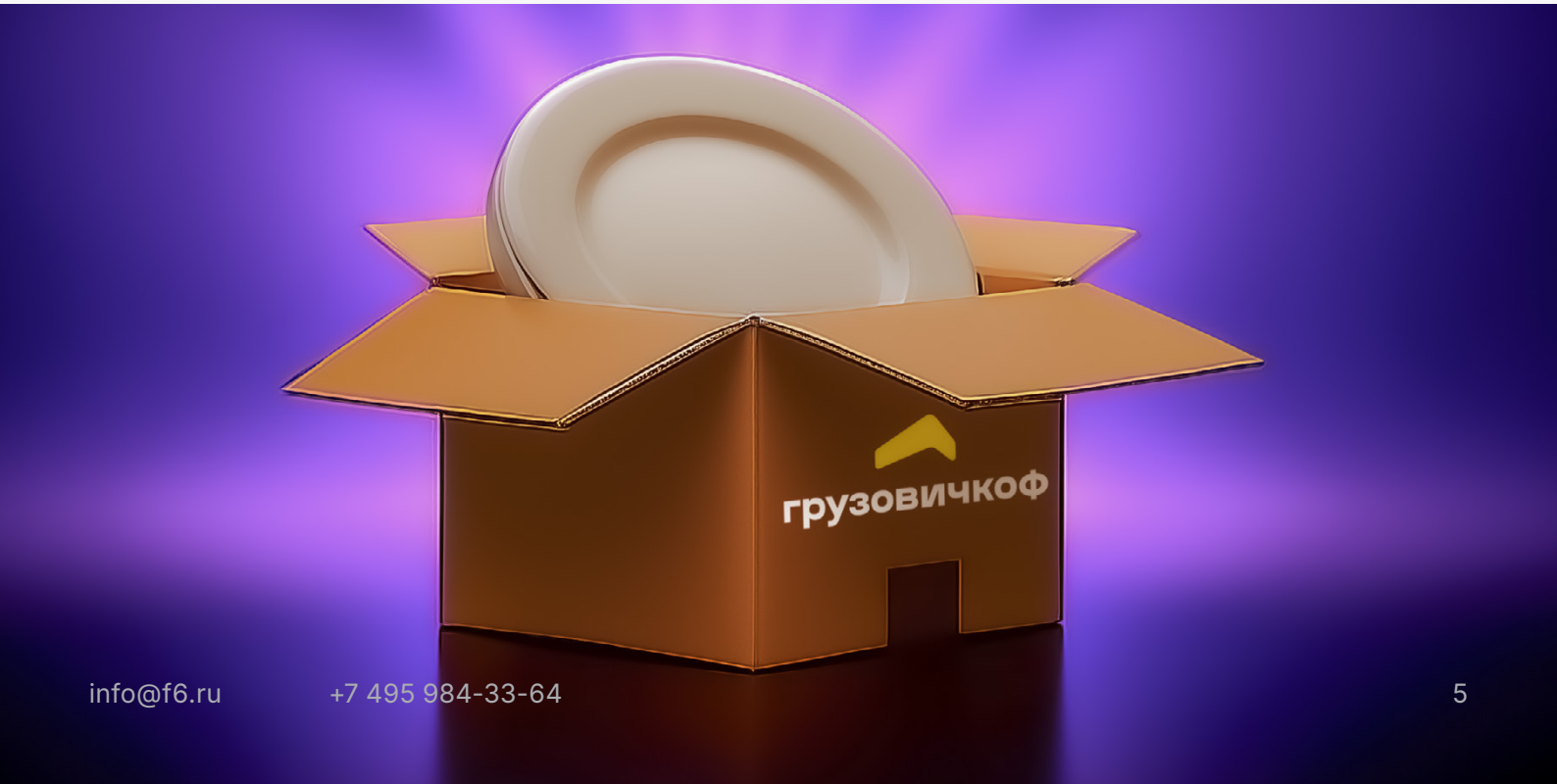
Ключевые факторы:

- Полная карта внешнего цифрового периметра;
- Автоматическое обнаружение забытых поддоменов, открытых портов и уязвимостей;
- Постоянный мониторинг утечек данных в публичных источниках;
- Настраиваемые оповещения и категоризация угроз;
- Удобный интерфейс с визуализацией динамики уязвимостей и уровня их опасности.

«Система F6 ASM позволяет не просто находить уязвимые активы, а видеть динамику снижения уровня риска. Это очень важно для мотивации команды и стратегического контроля»

Дмитрий Ляхов

директор по информационной безопасности «Грузовичкоф»



Ход проекта:

внедрение F6 ASM поэтапно

1. **Аудит и инвентаризация:**
   автоматическое выявление всех активов, связанных с основными доменами;
2. **Обнаружение теневых ресурсов:**
   десятки поддоменов, включая те, что имитировали основную платформу;
3. **Настройка сканирования:**
   ежедневный анализ DNS, SSL, открытых портов, мониторинг утечек и алерты о новых рисках;
4. **Обучение команды:**
   работа с интерфейсом и фильтрами, снижение ложных срабатываний;
5. **Оптимизация:**
   создание контрольных дашбордов для регулярного анализа.

Вызовы проекта

- **Масштаб инфраструктуры:**
  охват тысяч активов и сервисов
- **Сопротивление изменениям:**
  часть команды предпочитала ручной контроль;
- **Ложные срабатывания:**
  потребовалась настройка фильтров и тегов и обучение сотрудников.

«Ключевым результатом стало высвобождение времени ИБ-команды «Грузовичкоф» за счёт автоматизации рутины. Система последовательно находит новые активы и уязвимости, а дашборды помогают отслеживать динамику устранения — это упрощает приоритизацию и ускоряет закрытие рисков»

Дмитрий Ляхов

директор по информационной безопасности «Грузовичкоф»

Результаты:

Повышение безопасности и прозрачности

- Выявлены десятки потенциальных точек входа, ранее неучтенных;
- Снижена нагрузка на команду ИБ за счет автоматизации;
- Появилась прозрачная аналитика по динамике устранения рисков;
- Настроен постоянный мониторинг утечек в даркнете и публичных источниках.

На 80%

сократилось время на выявление уязвимых активов

Влияние на ИБ-стратегию

Внедрение F6 ASM позволило перейти на новый уровень зрелости киберзащиты:

- Полный контроль над внешним периметром;
- Проактивное управление рисками;
- Снижение вероятности утечек и репутационных потерь;
- Переход от реактивной защиты к предиктивной модели.

Отзыв команды

«**F6 ASM** — это не просто инструмент, а полноценный партнер. Он обеспечивает контроль внешней поверхности атаки и занимает важное место в арсенале средств защиты информации»

Дмитрий Ляхов

директор по информационной безопасности «Грузовичкоф»

Что можно особенно выделить

- Визуализация активов и их взаимосвязей через граф;
- История изменений и динамика устранения уязвимостей;
- Масштабируемость без сложного развертывания

Вывод

F6 Attack Surface Management стал для «Грузовичкоф» не просто системой поиска уязвимостей, а основой управления внешними рисками. Для логистики, где цифровая инфраструктура напрямую связана с операционной устойчивостью и доверием клиентов, такой инструмент становится стратегическим.

F6

Технологии для борьбы с киберугрозами

info@f6.ru +7 495 984-33-64 f6.ru