

Group-IB

FRAUD HUNTING PLATFORM

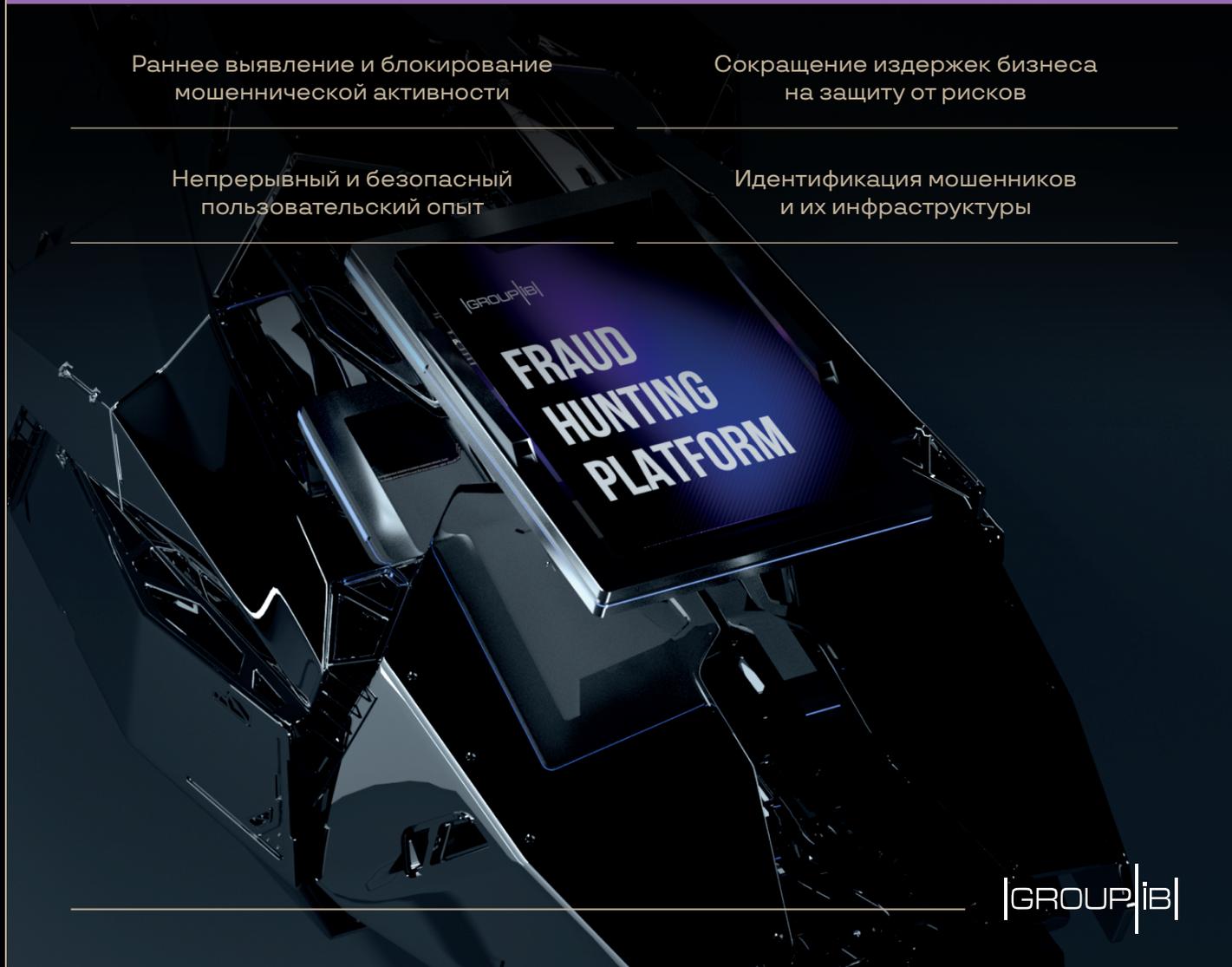
Система проактивной защиты цифровой личности и предотвращения мошенничества на всех устройствах пользователя в режиме реального времени

Раннее выявление и блокирование
мошеннической активности

Сокращение издержек бизнеса
на защиту от рисков

Непрерывный и безопасный
пользовательский опыт

Идентификация мошенников
и их инфраструктуры



● Решение ключевых задач защиты от мошенничества



Выявление платежного мошенничества,

совершаемого с использованием вредоносного ПО, социальной инженерии, CNP



Блокирование ботов

как простых shell-ботов, так и продвинутых, имитирующих поведение пользователя



Противодействие отмыванию доходов,

включая обнаружение сетей нелегального обналичивания денег и схем ухода от налогов



Выявление бонусного мошенничества,

включая кражу баллов в интернет-магазинах и миль авиакомпаний



Защита API

от несанкционированного использования ботами



Идентификация мошенников

и их инфраструктуры для проведения расследования

● Защита бизнеса и улучшение пользовательского опыта

Повышение онлайн-конверсии

через устранение лишних шагов проверки пользователя (например, CAPTCHA) и выявление ботов, замедляющих работу приложений

Улучшение опыта пользователей

за счет упрощения процесса проверки безопасности

Сокращение издержек бизнеса

благодаря сокращению проверок и снижению нагрузки на фронт-мониторинг

Защита интеллектуальной собственности

благодаря выявлению ботов, получающих доступ к цифровому продукту компании для последующей перепродажи



Снижение количества ложных срабатываний на 80%



Отказ от 80% кодов подтверждений



Экономия миллионов рублей на СМС-рассылке

● Комплексный подход к защите от мошенничества



Дополнительные возможности

Услуги по аналитике и реагированию

- Мониторинг событий
- Управление инцидентами
- Аналитика по запросу
- Разбор критичных угроз
- Создание антифрод-правил

Расследование инцидентов

Использование данных Group-IB Fraud Hunting Platform для идентификации и поиска мошенников и их инфраструктуры



● Почему компании выбирают Group-IB Fraud Hunting Platform

24/7	Безопасность	120+ млн	Признание
Круглосуточная техническая поддержка и реагирование на инциденты	Защита скриптов, трафика и данных от перехвата третьими лицами. Конфиденциальная информация пользователей не собирается	клиентов крупнейших компаний России и мира защищены Group-IB Fraud Hunting Platform	Включено Gartner в список признанных решений по выявлению онлайн-мошенничества и в реестр отечественного ПО

● Готовая интеграция



Group-IB один из ведущих мировых разработчиков решений для детектирования и реагирования на кибератаки, предотвращения мошенничества и защиты интеллектуальной собственности в сети

Group-IB входит в число лучших мировых поставщиков решения класса Threat Intelligence по версии Gartner, IDC, Forrester, SC Media и Cyber Defenses Magazine.

Эксперты Group-IB проводили тренинги по кибербезопасности для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд и преподавателей университетов в Европе и Азии.



Официальный партнер

17 лет

практического опыта

60 000+

часов опыта реагирования

1 000+

расследований по всему миру

400+

специалистов и разработчиков

Сервисы Group-IB

Укрепите кибербезопасность с помощью специалистов с практическим опытом реагирования и расследования сложных атак, использующих одну из самых продвинутых систем слежения за киберугрозами в мире.



Узнайте больше о возможностях Fraud Hunting Platform

group-ib.ru



Свяжитесь с нами, чтобы провести тест-драйв Fraud Hunting Platform

fhp@group-ib.com



Познакомьтесь с Group-IB

group-ib.ru
facebook.com/GroupIB

Аудит и оценка рисков

- Тестирование на проникновение
- Анализ исходного кода
- Выявление следов компрометации сети
- Киберучения в формате Red Teaming
- Проверка готовности к реагированию на инциденты
- Оценка соответствия

Обучающие программы

- Реагирование на инциденты
- Анализ вредоносного кода
- Проактивный поиск угроз

Threat Hunting и реагирование

- 24/7 Центр реагирования CERT-GIB
- Проактивный хантинг угроз
- Выездное реагирование на сложные кибератаки
- Реагирование на инциденты «по подписке»

Криминалистика и расследования

- Компьютерная криминалистика
- Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ