

# ПРОСТО. ЧЕТКО. КОМПЕТЕНТНО.

Как Райффайзенбанк защищает своих  
клиентов с Group-IB Fraud Hunting Platform

|GROUP|IB|

Год основания:

**1996**

Отрасль:

**ФИНАНСЫ**

Деятельность:

**ПРЕДОСТАВЛЕНИЕ  
РОЗНИЧНЫХ БАНКОВСКИХ  
УСЛУГ**

**БАНКОВСКОЕ  
ОБСЛУЖИВАНИЕ МАЛОГО  
И СРЕДНЕГО БИЗНЕСА  
(SME)**

**ЧАСТНОЕ БАНКОВСКОЕ  
ОБСЛУЖИВАНИЕ**

**КОРПОРАТИВНО-  
ИНВЕСТИЦИОННЫЙ  
БИЗНЕС**

Райффайзенбанк – один из ведущих универсальных банков в России, создающий качественные и удобные финансовые решения для своих клиентов во всех сегментах бизнеса: от физических лиц до крупных компаний. Райффайзенбанк входит в список 11 системно значимых банков и обладает лучшей композицией кредитных рейтингов на российском рынке.

**>2 млн**

физических лиц

**>120 тыс.**

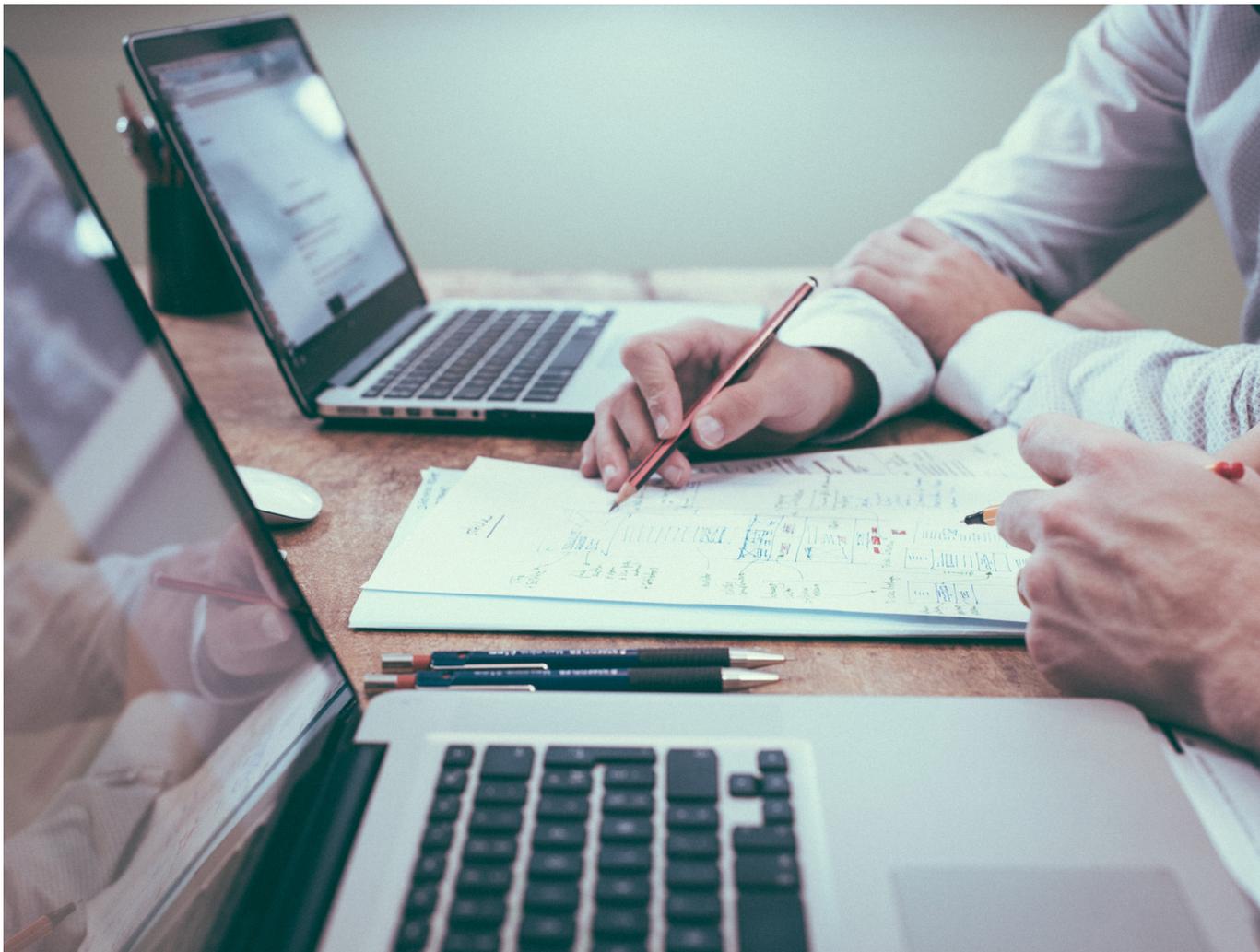
компаний-клиентов

**139**

количество отделений  
и филиалов



**Райффайзен  
БАНК**



## Предпосылки внедрения

Райффайзенбанк уделяет большое внимание вопросу безопасности банковских операций и продуктов. Для этого в банке выстроена высокотехнологичная система защиты от кибератак. Но с развитием информационных технологий эволюционируют и киберугрозы.

В 2019 году в российских банках участились случаи попыток мошенничества с использованием социальной инженерии и программ для удаленного доступа, направленного на пользователей онлайн-банкинга.

Привычные средства защиты малоэффективны против таких схем хищений. Большинство антифрод-систем сконцентрированы на анализе транзакционной информации и данных, доступных на стороне банка (IP-адрес, возраст клиента и т.п.).

Если учитывать, что процесс мошенничества включает не только момент проведения транзакции, но и этапы подготовки и вывода денежных средств, становится очевидно, что транзакционные антифрод-системы «закрывают» лишь ограниченный спектр работы мошенников.

Чтобы максимально защитить своих клиентов от действий злоумышленников, Банку требовалось многофункциональное решение, которое позволило бы:

1. Предотвращать хищение средств со счетов клиентов Банка за счет выявления скомпрометированных аккаунтов.
2. Отличить действия мошенника от легитимного пользователя благодаря формированию глобального профиля.
3. Расширить возможности и повысить эффективность транзакционной антифрод-системы, используемой в банке.

## Как Райффайзенбанк защищает своих клиентов с Group-IB Fraud Hunting Platform



### Решение Group-IB

Система предотвращения онлайн-мошенничества Group-IB Fraud Hunting Platform и мобильный модуль Mobile SDK.

Эффективность продукта Group-IB достигается за счет применения высокотехнологичной поведенческой аналитики, выявления аномалий, ежедневных обновлений правил и сигнатур на основе данных системы мониторинга и прогнозирования киберугроз Group-IB Threat Intelligence, аналитики Лаборатории компьютерной криминалистики Group-IB. Этот комплексный подход позволяет банкам повысить уровень защиты пользователей, одновременно помогая соблюдать требования законодательства по защите средств физических и юридических лиц от мошенников.

Решение Group-IB анализирует каждую сессию и поведение пользователя как на веб-ресурсе, так и в мобильном приложении. Продукт создает уникальный цифровой отпечаток устройства активного пользователя, помогая выявлять подозрительную активность. Например, в случае обнаружения нелегитимных действий в отношении клиента банка Group-IB Fraud Hunting Platform отправляет в банк автоматическое уведомление в режиме реального времени.

В сумме это дает надежный инструмент для того, чтобы эффективно предотвращать кросс-канальное и кросс-банковское мошенничество.



Мы создали «умный» продукт, вобравший в себя уникальные технологии Group-IB: систему продвинутой идентификации устройства пользователя (device fingerprinting) и ряд запатентованных алгоритмов выявления работы мошенников и поведенческой аналитики.

**Павел Крылов,**  
руководитель направления по защите от онлайн-мошенничества Group-IB



## Почему выбрали решение Group-IB

В первую очередь Райффайзенбанку было важно, чтобы новое решение полностью покрывало главные каналы ДБО: онлайн-банкинг и мобильное приложение. Это требование оказалось реализуемо благодаря модулям Web Snippet для веб-версии и Mobile SDK для iOS и Android.

Второе важное требование — наличие веб-интерфейса и API для проведения ретроспективного анализа и выгрузки данных для дальнейшей аналитики.

Также на выбор в пользу решения Group-IB повлияли:

- скорость добавления новых функций по запросу заказчика — 1-2 недели с момента поступления запроса;
- готовая интеграция с действующей транзакционной антифрод-системой банка.

“

Group-IB Fraud Hunting Platform определяет различные факторы риска на устройствах клиента, что в свою очередь повышает точность антифрод системы.

Хотелось бы отметить пару особенностей решения:

1. Выявление банковских троянов и программ удаленного управления дает антифрод-системе дополнительный контекст при подсчете скоринга транзакции.
2. Экспертиза Group-IB в области Threat Intelligence позволяет создавать правила детектирования для наиболее актуальных угроз, направленных на пользователей онлайн-банка.

**Павел Нагин,**  
менеджер по информационной безопасности  
АО Райффайзенбанк

”

## Как Райффайзенбанк защищает своих клиентов с Group-IB Fraud Hunting Platform



### Реализация и результаты

Решение Group-IB Fraud Hunting Platform позволило специалистам информационной безопасности Райффайзенбанка:

1. Более оперативно выявлять скомпрометированные аккаунты клиентов Банка для того, чтобы в дальнейшем предотвращать хищение средств со счетов.
2. Расширить возможности и повысить эффективность транзакционной антифрод-системы, используемой в Банке, за счет получения множества нефинансовых показателей об окружении клиента, например, об его браузере или мобильном устройстве.
3. Защититься от участвовавших атак с использованием социальной инженерии.
4. Собирать дополнительную информацию из множества источников для формирования глобального профиля пользователя, позволяющего отличить действия мошенника от легитимного пользователя.

В течение 2019 года решение Group-IB Fraud Hunting Platform выявило десятки скомпрометированных пользователей онлайн банка и позволило предотвратить последующее хищение денежных средств клиентов. Кросс-банковская корреляция и машинное обучение повысили надежность скоринга транзакций в антифрод системе.

Внедрение Fraud Hunting Platform заняло всего 1 месяц, что также подтвердило правильность выбора решения компании Group-IB.



Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

По версии **Gartner** Group-IB является одним из ключевых поставщиков решений по выявлению онлайн-мошенничества.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.

**60 000+**

часов  
реагирования

**1000+**

успешных расследований  
по всему миру



Официальный  
партнер



Рекомендована Организацией  
по Безопасности и Сотрудничеству  
в Европе (ОБСЕ)

Узнать больше о Group-IB  
Fraud Hunting Platform

[group-ib.ru/fraud-hunting-platform](https://group-ib.ru/fraud-hunting-platform)  
[fhp@group-ib.com](mailto:fhp@group-ib.com)