



Kaspersky  
Fraud  
Prevention



Ready  
for GDPR

# Automated Fraud Analytics

Реализация стратегии безопасности связана не только с передовыми технологиями. Речь также идет о данных, которые поступают в ходе анализа пользовательской сессии, а также о способности использовать их наряду с технологиями.

Именно для этого существует Automated Fraud Analytics: бизнес должен знать о возможной мошеннической активности, когда она еще не началась, обладать данными, которые имеют решающее значение для принятия точных, своевременных решений и для выявления наиболее сложных случаев мошенничества.

## Угрозы

- Мошенничество развивается - растущие проблемы с клиентами
- Более высокий уровень фрода - штрафы со стороны регулятора
- Угроза пропустить стадию подготовки атаки
- Растущая сложность атак - привычные и устаревшие решения не справляются

## Функциональные возможности

- Построение и сопоставление связей на глобальном уровне
- Поведенческий анализ на основе глубинного обучения
- Гибкая настройка правил

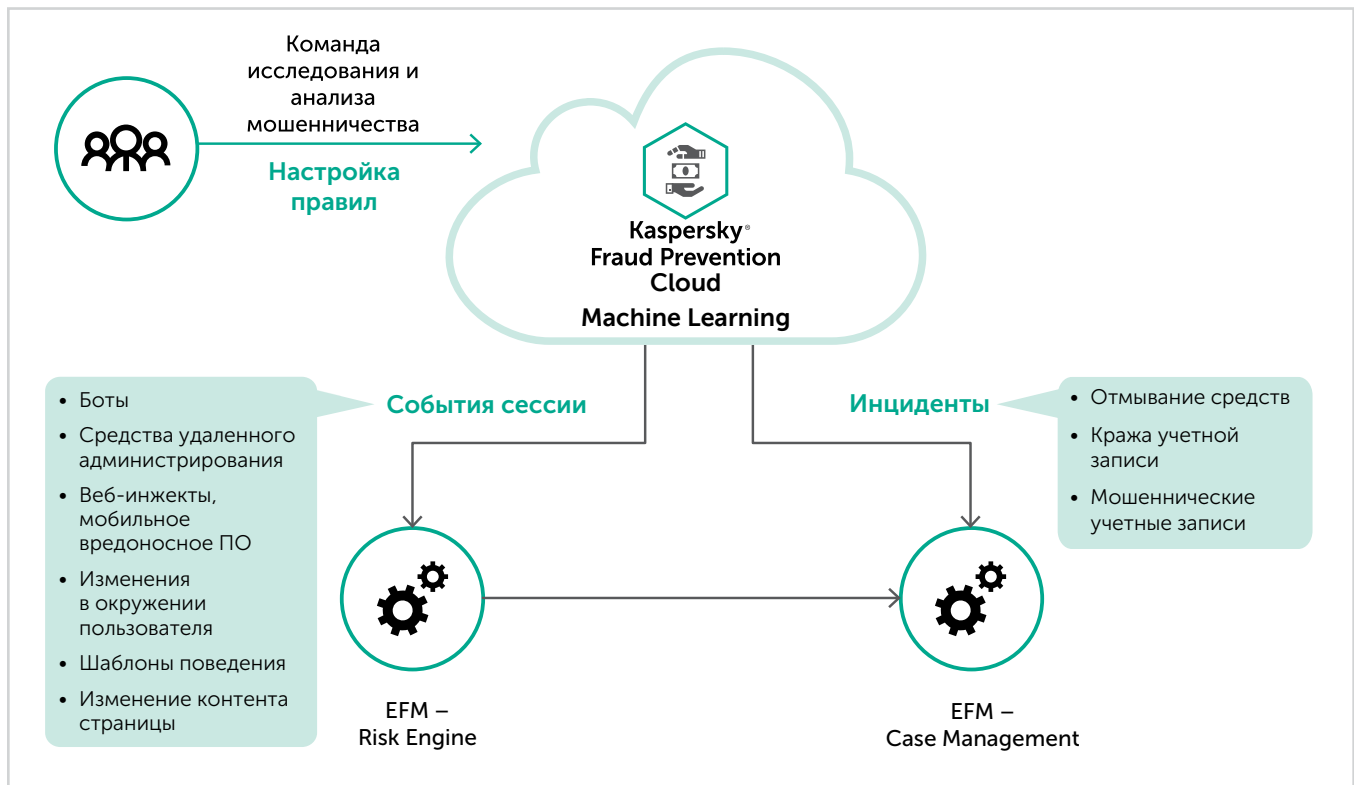
## Практическая применимость

**Кража учетной записи** – Что если бы вы были уверены, что ваши цифровые каналы в данный момент используются легитимными юзерами? Что если бы вы знали, как пользователь ведет себя в вашем приложении или на сайте? Это только часть того, что анализирует Kaspersky Fraud Prevention. Мы помогаем вам узнать больше о клиентах, предоставляя ценные данные и знания, чтобы увидеть аномалии и подозрительное поведение до того, как мошенничество было совершено, в то время как сами клиенты не теряют доступ к своей учетной записи.

**Мошеннические учетные записи** – для защиты бизнеса от такого рода атак применяются поведенческий анализ и биометрия, а также анализ устройства и окружения для построения моделей легитимного и мошеннического поведения. Такой подход позволяет выявить отклонения в пользовательском поведении, и распознать как реального пользователя, пытающегося воспользоваться услугой, так и мошенника, намеревающегося нанести вред бизнесу.

**Отмывание денежных средств** – построение связей между пользователями и устройствами, а также использование уникальных идентификаторов позволяет выявлять группы учетных записей, доступ к которым осуществляется с одного и того же устройства. Поведенческий анализ повышает эффективность обнаружения, отличая легитимных пользователей от мошенников. Благодаря глобальной репутации устройств Automated Fraud Analytics раскрывает связи между мошенническими аккаунтами и предотвращает сложные преступные схемы, реализуемые в разных организациях.

**Аналитика мошенничества** – на протяжении всей сессии, с самого ее начала, события, происходящие с пользователем, устройством, а также биометрические и поведенческие показатели тщательно анализируются. Объединение технологий и экспертизы аналитиков позволяет более точно указать виды подозрительной активности, которая выявляется в процессе настраивать решение под запросы бизнеса, а также тщательно прорабатывать обнаруженные случаи мошенничества.

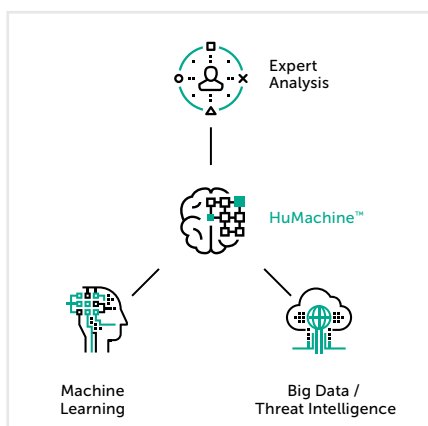


### Решение Advanced Authentication

- Повышает уровень удобства использования за счет снижения количества шагов аутентификации
- Снижает затраты на предоставление услуг второго фактора аутентификации
- Выявляет случаи кражи учетной записи, как на этапе логина, так и на протяжении всей сессии
- Помогает соответствовать законодательным требованиям, касающимся обеспечения безопасности платежей и противодействия мошенническим операциям

Advanced Authentication продолжает обеспечивать высокий уровень безопасности на протяжении всей сессии за счет **Непрерывной аутентификации** и анализа аномалий. Решение оценивает данные о поведении пользователя, репутации устройства и другую уже накопленную информацию, поступающую в Kaspersky Fraud Prevention Cloud. В случае обнаружения аномального поведения решение автоматически предоставляет данные об этом во внутренние системы мониторинга, а также задействует систему аутентификации для запроса второго фактора и определения легитимности транзакции и пользователя.

На основе обработки деперсонализированных данных и автоматического анализа информации Advanced Authentication выявляет случаи **Кражи учетной записи**. Решение умеет идентифицировать, а также выявлять новые, неиспользованные ранее устройства по уникальному отпечатку. Кроме того, анализ поведенческих и биометрических данных в режиме реального времени определяет отклонения от «типичного» пользовательского поведения. Своевременное обнаружение скомпрометированных учетных записей позволяет как на этапе логина, так и во время сессии ограничить уровень доступа к личному кабинету и сократить потенциальные финансовые потери для бизнеса и для клиентов.



Всё об интернет-безопасности:  
[www.securelist.com](http://www.securelist.com)

[www.kaspersky.ru](http://www.kaspersky.ru)  
[#truecybersecurity](https://twitter.com/truecybersecurity)  
[kfp@kaspersky.com](mailto:kfp@kaspersky.com)

© АО «Лаборатория Касперского», 2018. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.