Как устроен Fraud-мониторинг

Руководство по созданию эффективных решений

АО «БИФИТ»

Как работает антифрод: выдержки из материалов

…нейронные сети…

…уникальные алгоритмы…

…кросс-канальный интеллект…

…анализ более 100 показателей…

…самообучающаяся система…

Хорошо – для маркетинга

Плохо – для осознанного выбора и понимания показателей решения

Эффективность антифрода: формализация задачи

Измеримые показатели:

1. Количество пропущенных мошеннических платежей
2. Количество ошибок первого рода
3. Затраты ресурсов на обработку инцидентов

Антифрод: оптимизация показателей работы

Обеспечить выявление всех попыток мошенничества – реальная задача

Пример:

- все платежи в пользу новых получателей считать подозрительными
- доля ложных срабатываний - ~15%

Ключевое направление повышения эффективности – снижение числа ложных срабатываний при сохранении показателей по выявлению мошенничества

Антифрод: оптимизация показателей работы

Путь снижения доли ложных срабатываний – увеличение количества анализируемых факторов и их учет при оценке уровня риска:

- платежная поведенческая модель
- поведенческая модель в прикладном ПО
- анализ среды работы клиента

Что же мешает?

- Сложность получения расширенной информации из внешних систем
- И так все работает

БИФИТ: компетенция в защите ДБО

Мы противостоим угрозе хищений с 2007 года

За это время:

- созданы и массово внедрены аппаратные решения для защиты ключей ЭП
- разработана промышленная система Fraud-мониторинга
- создан свой Security Lab (анализ вредоносного ПО, активное противодействие)
- создан Экспертно-Правовой Центр

Fraud-мониторинг компании «БИФИТ»

Преимущества плотной интеграции:

1. Снижение ложных срабатываний
2. Возможность проактивной борьбы с хищениями
3. Адаптивные механизмы аутентификации, подтверждения и подписи

Fraud-мониторинг и раскрытие данных

1. **Открытые данные**

   Принципы работы, архитектура решения

2. **Данные ограниченного доступа**

   Правила проверки транзакций, рекомендуемые значения оценок риска

   Предоставляются ответственным сотрудникам банков

3. **Секретные данные**

   Механизмы и алгоритмы выявления вредоносного ПО

   Не предоставляются третьим сторонам, включая банки

Спасибо

за внимание

shilov@bifit.com