Хорішко Артур Валентинович,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Галузеве машинобудування, 1 курс
Науковий керівник – Вакуленко Ю. В., кандидат сільськогосподарських наук,
доцент, доцент кафедри інформаційних систем та технологій

СУТНІСТЬ СУЧАСНИХ АНТИФРОД-СИСТЕМ

Розвиток інформаційних технологій та використання інтернету в побуті призвів не лише до швидкого обміну інформацією. Застосування інтернет-ресурсів при розрахунках та торгівлі спричинило появу нових видів шахрайства.

Інтернет-шахрайство негативно впливає не лише на покупців чи власників платіжних карт. Інтернет-магазини страждають від цього не менше, оскільки така ситуація шкодить репутації, прибуткам тощо.

Фрод (від англ. fraud) – це здійснення шахрайських дій у фінансовій сфері засобами інтернет [3]. У детальнішому розгляді, – це дії, які пов'язані з розкраданням чужого майна, активів або придбанням прав на чуже майно, активів, шляхом зловживання довірою потерпілого чи обманом. Обман в цьому випадку – це свідоме перекручування правдивої інформації (активний обман) і замовчування про справжній стан справ (пасивний обман) [1].

Усі дії проти жертви злочину, у випадку фроду, засновані на її обмані. Класичними прикладами для ІТ-галузі будуть [1]:

- фішинг – створення зловмисниками сайтів-аналогів;
- кардінг – різноманітні способи підробки платіжних банківських карт;
- вішинг – зловживання довірою покупця, клієнта;
- фармінг – здійснення переадресації на шкідливі сайти;
- мобільне шахрайство та інші види протиправних дій, пов'язані з соціальною інженерією.

Для фінансових організацій під фрод розуміють умисну дію або бездіяльність фізичних осіб і юридичних об'єктів з метою отримання неправомірної вигоди за рахунок іншої особи, компанії, і / або нанесення йому (їй) матеріальної чи нематеріальної шкоди.

Більшість таких шахрайств пов'язані з незаконним отриманням даних чи коштів із банківських платіжних карт, рідше – з викраденням самої карти.

Фрод необхідно запобігати вже на адміністративно-організаційному рівні. Попереджувальними заходами можна визначити наступні [2]:

- внутрішній аудит організації;
- навчання співробітників практичній протидії фрод;
- управління логічним і фізичним доступом до системи;
- виявлення і контроль над конфліктами інтересів в компанії;
- процедури узгодження та авторизації дій співробітників.

Часто таких заходів є недостатньо. У зв'язку з цим, усе більшої популярності та ефективності набувають антифрод-системи (Fraud Detection

System) – системи моніторингу та попередження шахрайських операція, які в режимі реального часу перевіряють кожен платіж [2]. Основна задача таких систем – перевірка транзакцій з метою виявлення підозрілих моментів. У разі виявлення неточностей чи підозр – відхилити його.

Антифрод-система складається з декількох компонентів: це автоматичний моніторинг транзакцій, що включає в себе велику кількість параметрів фільтрів, механізми аутентифікації власника картки і валідації карти, а також моніторинг транзакцій в «ручному» режимі для окремих випадків.

Загальна схема роботи практично будь-якого механізму фрод-моніторингу виглядає наступним чином: в момент здійснення оплати за допомогою банківської карти аналізується кілька показників (починаючи від IP-адреси і закінчуючи статистикою здійснення платежів картою). Кожен з фільтрів системи перевіряє користувача (його персональні і карткові дані). Мета системи – переконатися в тому, що користувач є реальним власником карти, що використовується для здійснення покупки на сайті. У разі виявлення підозрілої активності, тобто перевищення будь-якого значення параметра, фільтр автоматично блокує можливість здійснення платежу за цією карткою. Алгоритми роботи системи фрод-моніторингу дозволяють оцінити ряд факторів, серед яких основними є [2]:

- країна, з якої здійснюється платіж;
- країна банку, що випустив карту;
- обсяг платежу;
- кількість платежів з карти;
- платіжна історія банківської карти;
- профіль середньостатистичного платника магазину.

Транзакція проходить первинний аналіз на підставі цих та інших чинників. На підставі аналізу їй присвоюється «мітка», яка характеризує спосіб обробки транзакції:

- зелена – низька ймовірність виникнення шахрайської операції;
- жовта – шанс виникнення шахрайської операції вище середнього;
- червона – найбільша ймовірність шахрайських транзакцій.

Далі проводиться більш детальний аналіз і приймається рішення про здійснення чи відхилення транзакції.

Система такого рівня – досить вартісний програмний продукт, котрий можуть дозволити собі тільки великі банки, мережі магазинів та сервісів – гіганти ринку, а також спеціалізовані сервіси (платіжні агрегатори і процесингові центри, які спеціалізуються на прийомі платежів). Саме тому більшість онлайн-сервісів та інтернет-магазинів користуються послугами сторонніх підрядників для прийому платежів.

Плюси антифрод-систем очевидні – автоматичне відхилення сумнівних транзакцій, захист інтернет-магазину від подальших розглядів з банками,

платіжними системами і реальними власниками карт. І, як наслідок, мінімізація репутаційних і фінансових ризиків.

Але, як і у будь-якого сервісу, антифрод-системи мають свої недоліки. Відхилення платежів може призвести до втрати клієнтів. Необхідність проходження сертифікації відповідності вимогам стандарту PCI DSS, а також врахування обмеження на зберігання і обробку даних, регульовані законом. Найголовніший недолік – неможливість довести сам факт фрода.

Отже, антифрод-системи – це спеціальне програмне забезпечення, здатне протистояти кібератакам, хакерам і іншого роду шахрайства в банківських і платіжних системах. Найдосконалішими на сьогодні є інтелектуальні системи, що здатні до самонавчання під час роботи. Однак антифрод-системи поки що має ряд прикрих недоліків: ймовірність помилкового блокування платежів і переказів, неможливість протистояти людському фактору тощо.

Список використаних джерел

1. Антифрод-системы: описание, особенности и принцип работы. [Електронний ресурс]. – Режим доступу: https://ruud.ru/it/35142-antifrod-sistemy-opisanie-osobennosti-i-princip-raboty/.
2. Антифрод. Функциональные и нефункциональные требования (часть 2). [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/253731/.
3. Как работает антифрод знай врага в лицо! [Електронний ресурс]. – Режим доступу: https://skynetzone.org/threads/kak-rabotaet-antifrod-znaj-vraga-v-lico.8218/.