электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.492.2

Методы распознавания мошеннических операций при эквайринге

***Железнов Д.Е.**, магистрант*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Быков А.Ю., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
bauman@bmstu.ru

Введение

Распространение мошеннического эквайринга носит глобальный характер. Рост мошеннических операций во многом связан с техническим развитием способов накопления и тратой денежных средств.

На самом деле мошеннические финансовые операции возникли вместе с тем как человечество решило ввести уникальный обменный товар – денежные единицы. С приходом денег мошеннические операции начали свой бурный рост, а с переводом цифровых технологий деньги стали тоже «цифровыми» и проводить с ними мошеннические операции стало ещё удобней ведь теперь для этого даже не обязательно выходить из дома.

Методы распознавания так же совершенствовались со временем.

Сейчас банки всего мира имеют системы обнаружения признаков финансового мошенничества и целые отделы сотрудников, занимающихся выявлением и предотвращением мошеннического экваринга. Удаленные системы обнаружения признаков финансового мошенничества являются неэффективными и дорогостоящими, и они улавливают случаи мошенничества гораздо реже, чем благодаря использованию комплексных решений (так называемых, антифрод-систем). Для предотвращения убытков, ненамеренного уклонения от ответственности перед регуляторами и защиты своей компании необходима комплексная платформа для предотвращения мошенничества (антифрод) на уровне всего предприятия.

Методы распознавания мошеннических операций

Основные методики выявления мошеннических операций:

1. Логико-вероятностная
2. Динамического анализа паттернов поведения мошенников
3. Выявлении и оценке индикаторов мошенничества
4. Нейронные сети

Логико-вероятностного метод

Использовать математический аппарат на основе логики, дискретной математики и комбинаторики для решения социальных и организационных задач (включая проблемы выявления и анализа мошенничества, взяток и коррупции) предложили американские ученые Джон фон Нейман и Норберт Винер [1]. Среди российских ученых разработок в этой области занимается Е. Д. Соложенцев, который создал модели применения логико-вероятностного (ЛВ) подхода при оценке риска неуспеха и выявления взяток [2]. Построение ЛВ-модели риска системы осуществляют в следующей последовательности: формулируют сценарий риска, строят структурную модель риска, записывают Л-модель риска, выполняют ортогонализацию Л-модели риска и получают В-модель (полином) риска [3]

Динамического анализа паттернов поведения банков

Такой анализ проводится на основе системы показателей, учитывающей ключевые аспекты деятельности банков. Как правило, берется система CAMELS. Банки классифицируются в зависимости от заданных исследователями критериев. Далее модель выявляет характерные паттерны поведения банков. Существенное отклонение в различные периоды деятельности банка от паттернов, свойственных для его классификационной группы, может говорить о смене стратегии, взятии на себя повышенных рисков или мошенничестве и фальсификации отчетности. Наиболее известны в этой области работы ученых Национального исследовательского университета «Высшая школа экономики» [4].

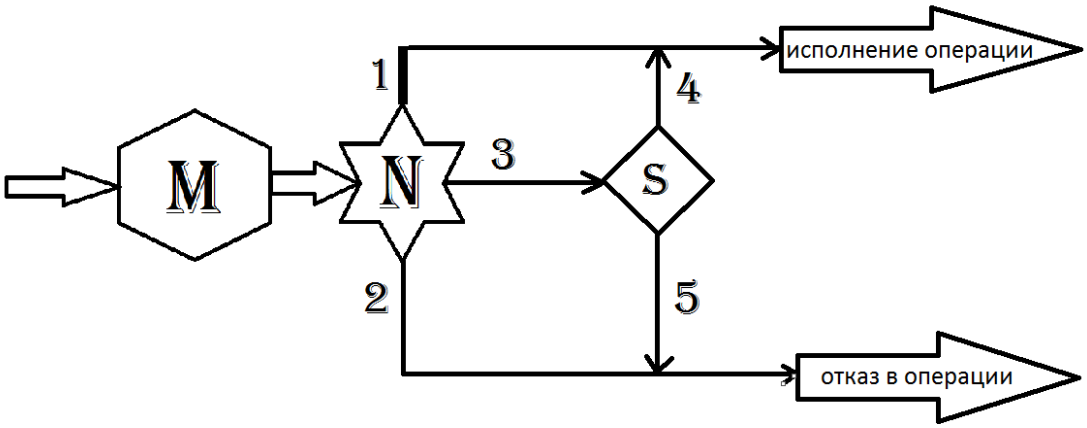
Выявление и оценка индикаторов мошенничества

Представляет собой метод выявления скрываемого факта по его косвенным проявлениям («индикаторам») [5]. Часто используется аналитиками в разных сферах деятельности, например, в аналитике и в разведке. Индикатор хищения — это факт,

который не скрывается или легко устанавливается и который обычно сопутствует хищению, но не является его прямым доказательством. Наличие одного и более индикаторов рисков хищений является для профессионала исходной информацией для углубленного изучения процесса на предмет возможных хищений. Присутствие одновременно нескольких индикаторов свидетельствует о повышенном риске хищений.

Функциональная схема работы распознавания мошеннических операций нейронный сети

На рисунке представлена схема работы распознавания мошеннической операции, где M - мониторинговая система, N – Нейронная сеть, S – группа специалистов.



Поступившие операции собираются системой мониторинга, собранные данные передаются нейронной сети, которая в свою очередь производит вычисления и проверяет операции на отклонения от нормы, по результату проверки она передаёт операции к исполнению (ветка 1) или прерывает их (ветка 2). В случае если нейронная сеть не может вынести решение на блокировку или отправку, она передаёт данную операцию группе специалистов (ветка 3), которые будут решать, что делать со спорной операцией и отправят её к исполнению (ветка 4) или прервут операцию (ветка 2).

Система мониторинга собирает всю доступную информацию по каждой операции [6]:

1. Онлайн
2. Центр дистанционного обслуживания
3. Системы интерактивного речевого ответа
4. Мобильная связь WAP
5. Мобильная связь SMS

6. Дистанционная оплата счетов
7. Внутренняя пересылка
8. Постоянные поручения клиентов банку
9. Банковские автоматизированные клиринговые системы
10. Телеграфные переводы / Обслуживание счетов
11. Доступ / вход в систему

Нейронная сеть проводит обнаружение мошенничества:

1. Определение поведенческих характеристик на всех уровнях - пользователь, счет, получатель платежа, устройство и т.д.
2. Сопоставление информации по каналам с информацией по операциям.
3. Корреляция действий по различным каналам удаленного доступа.
4. Возможность анализа значительных объемов операций.

Вывод

В результате были проанализирован существующие способы обнаружения мошеннических операций. Главное преимущество нейронных сетей является её способность к обучению что способствует её большей устойчивости к новым видам мошенничества, децентрализованность позволяющая разделить нагрузку входного потока финансовых операций по разным центрам, обеспечение оперативной обработки операций.

Менять существующие способы на нейросетевые является долгим процессом, но также это является наилучшем решением проблемы с мошенничеством поскольку другие методы узко направлены, а нейросеть будет гибким и идущим со временем решением.

Список литературы

[1]. Соложенцев Е.Д., Карасев В.В. Соложенцев В.Е. Логико-вероятностные модели риска в банках, бизнесе и качестве. СПб.: Наука, 1999. 120 с.

[2]. Соложенцев Е.Д. Управление риском и эффективностью в экономике. Логико-вероятностный подход. СПб.: Изд-во СПбГУ, 2009. 270 с.

[3]. Бабенков А.Н., Соложенцев Е.Д. К вопросу построения ЛВ-модели риска неуспеха комплексной структурно-сложной экономической системы. Управление в социально-экономических системах // Информационно-управляющие системы. 2011. № 4. С. 70–76

[4]. Алескеров Ф.Т., Солодков В.М., Челнокова Д.С. Динамический анализ паттернов поведения коммерческих банков России // Экономический журнал Высшей школы экономики. 2006. № 1. С. 48–62.

[5]. ACFE: Оценка рисков хищений как актуальное направление в безопасности бизнеса. Режим доступа: http://acfe-rus.org/ (дата обращения 17.03.2015)

[6]. Дистрибуция и внедрение инновационных продуктов и решений для корпоративного сектора – Предотвращение финансового мошенничества. Режим доступа: http://dis-group.ru/solutions/security_solutions/anti_fraud/ (дата обращения 15.03.2017).