УДК 004.8
ББК 32.813.5

ОБЗОР ЛИТЕРАТУРЫ ДЛЯ ОБНАРУЖЕНИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Нумонова Нигора Рустамовна *- ассистент кафедры "Цифровая экономика" ХПИТТУ, e-mail:aron.21@mail.ru*

ШАРҲИ АДАБИЁТ БАРОИ ОШКОР КАРДАНИ ФАЛОБОДИИ МОЛИЯВӢ

Нумонова Нигора Рустамовна *- ассистенти кафедраи "Иқтисоди рақамӣ" дар ДПДТТ шаҳри Хуҷанд, e-mail:aron.21@mail.ru*

LITERATURE REVIEW FOR FINANCIAL FRAUD DETECTION

Numonova Nigora Rustamovna *- The Assistant of the Digital Economy Department at KPITTU, e-mail:aron.21@mail.ru*

Ключевые слова: *финансовое мошенничество, интеллектуальный анализ данных, нейронная сеть, обнаружение мошенничества.*

В связи с подъемом и быстрым ростом электронной коммерции, участились случаи, связанные с финансовыми махинациями, которые ежегодно приводят к краже миллиардов долларов по всему миру. Обнаружение мошенничества включает в себя тщательное изучение поведения групп пользователей с целью приблизительного определения, обнаружения или предотвращения нежелательного поведения. Само нежелательное поведение — это широкий термин, включающий правонарушения: мошенничество, нарушение прав и уклонение от учетной записи. На самом деле мошеннические транзакции перемежаются с подлинными транзакциями, и простых методов сопоставления с образцом часто бывает недостаточно, для точного обнаружения такого мошенничества. В этом обзоре основной акцент сделан на классификации мошеннического поведения, определении основных источников и характеристик данных, на основе которых было проведено обнаружение мошенничества. Представлен всесторонний обзор и обзор различных методов обнаружения финансового мошенничества, используемых в различных видах мошенничества, таких как обнаружение мошенничества с кредитными картами, мошенничество с онлайн-аукционами, обнаружение мошенничества в сфере телекоммуникаций и обнаружение компьютерных вторжений.

Калид вожаҳо: *қаллобии молиявӣ, истихроҷи маълумот, шабакаи нейрон, ошкор кардани қаллобӣ.*

Бо болоравӣ ва рушди босуръати тиҷорати электронӣ, ҳамчунин тақаллуби молии марбут ба он афзоиш ёфтааст, ки ҳамасола боиси дуздии миллиардҳо доллар дар саросари ҷаҳон мешавад. Муайян кардани қаллобӣ аз наздик омӯхтани рафтори гурӯҳҳои корбарон бо мақсади тақрибан муайян, ошкор ё пешгирӣ кардани рафтори номатлубро дар бар мегирад. Рафтори номатлуб истилоҳи васеъест, ки ҳуқуқвайронкуниҳо, аз қабили қаллобӣ, нақзи ҳуқуқ ва саркашӣ аз ҳисобро дар бар мегирад. Дарвоқеъ, муомилоти қаллобӣ бо муомилоти ҳақиқӣ печида аст ва усулҳои оддии мувофиқати намуна аксар вақт барои дақиқ муайян кардани чунин қаллобӣ кофӣ нестанд. Дар ин баррасӣ, мо ба таснифоти рафтори қаллобӣ, муайян кардани манбаъҳои асосӣ ва хусусиятҳои маълумот, ки дар асоси онҳо ошкор кардани қаллобӣ анҷом дода шудааст, тамаркуз хоҳем кард. Ин мақола баррасии ҳамаҷониба ва шарҳи усулҳои гуногуни ошкор кардани қаллобии молиявиро, ки дар намудҳои гуногуни қаллобӣ истифода мешаванд, аз қабили ошкор кардани қаллобӣ дар корти кредитӣ, қаллобӣ дар музоядаи онлайн, ошкор кардани қаллобӣ дар телекоммуникатсия ва ошкор кардани ҳамлаи компютерӣ пешниҳод мекунад.

Key words: *financial fraud, data mining, neural network, fraud detection.*

With the rise and rapid growth of e-commerce, there has also been an increase in financial scams associated with it, which annually lead to the theft of billions of dollars around the world. Fraud detection involves closely examining the behavior of groups of users in order to roughly identify, detect, or prevent unwanted behavior. Unwanted behavior is a broad term that includes offenses such as fraud, infringement, and account evasion. In fact, fraudulent transactions are interspersed with genuine transactions, and simple pattern matching methods are often not enough to accurately detect such fraud. In this review, we will focus on the classification of fraudulent behavior,

identifying the main sources and characteristics of data, based on which fraud detection was carried out. This paper provides a comprehensive review and overview of the various financial fraud detection methods used in various types of fraud such as credit card fraud detection, online auction fraud, telecommunications fraud detection, and computer intrusion detection.

Ассоциация сертифицированных специалистов по расследованию мошенничества (ACFE) определила мошенничество как «использование служебных обязанностей для личного обогащения путем преднамеренного неправомерного использования или использования ресурсов, или активов организации-работодателя» [1]. Мошенничество неблагоприятно сказывается на бизнесе. Различные методы, которые в настоящее время используются для обнаружения мошенничества, включают статистику, интеллектуальный анализ данных, нейронные сети и искусственный интеллект. К проблемам разработки новых методов обнаружения мошенничества относятся ограничение обмена идеями, недоступность наборов данных и скрытые результаты исследования. Мошенничество выявляется путем просеивания аномалий в данных и шаблонах, используя навыки бухгалтерского учета, аудита и расследования, а также математические, статистические модели и модели интеллектуального анализа данных [2].

Финансовое мошенничество. Незаконное присвоение активов, откаты и т.д. включены в финансовые мошенничества. Согласно опубликованной до настоящего времени статистики, можно сказать, что большая часть исследований посвящена выявлению внешних финансовых мошенничеств. К сожалению, очень мало работ написано по внутреннему финансовому мошенничеству. Определить внутреннее мошенничество можно такими методам, как искусственная нейронная сеть, генетический алгоритм, грубый и нечеткий набор, обнаружение правил, кластерный анализ и логистическая регрессия [3]. Эти структуры помогают аудиторам окончательно подтвердить, существует ли возможность мошенничества или нет.

Обнаружение финансового мошенничества (FFD) является жизненно важным для предотвращения часто разрушительных последствий финансового мошенничества. FFD включает в себя разделение мошеннических финансовых данных от достоверных, тем самым раскрывая мошенническое поведение или действия и позволяя лицам, принимающим решения, разрабатывать соответствующие стратегии для уменьшения воздействия мошенничества.

В общем, цель обнаружения мошенничества состоит в том, чтобы максимизировать правильные прогнозы и поддерживать неверные прогнозы на приемлемом уровне [4]. Высокая вероятность правильной диагностики может быть достигнута за счет сведения к минимуму вероятности необнаруженного мошенничества и ложных срабатываний. Ниже будут описаны некоторые технические термины по вероятности необнаруженного мошенничества и ложных срабатываний:

- Уровень ложных срабатываний — это процент законных транзакций, которые ошибочно идентифицируются как мошеннические.

- Показатель обнаружения мошенничества (или показатель истинного положительного результата или показатель точности обнаружения) — это процент мошеннических транзакций, которые правильно идентифицированы как мошеннические.

Целью этой статьи во–первых является всесторонний обзор различных методов обнаружения финансовых махинаций и определение существующих проблем в этой области для различных типов больших наборов данных и потоков. Он классифицирует, сравнивает и обобщает соответствующие методы и приемы обнаружения финансового мошенничества в опубликованных академических и отраслевых исследованиях. Во-вторых, выделить многообещающие новые направления из смежных противоборствующих финансовых областей, таких как обнаружение эпидемий и вспышек, инсайдерская торговля, обнаружение вторжений, отмывание денег, обнаружение спама и обнаружение терроризма. Знания и опыт из этих областей могут быть взаимозаменяемыми и помогут предотвратить повторение распространенных ошибок и повторное изобретение колеса.

Обзор литературы. В результате различного восприятия, несколько групп исследователей приложили значительные усилия для изучения риска финансового мошенничества, для которого были поддержаны различные алгоритмы интеллектуального анализа данных. Например, в советах директоров фирм, не подвергшихся мошенничеству, значительно выше процент внешних членов, чем в фирмах, занимающихся мошенничеством, что было обнаружено с помощью регрессионного анализа Beasley [5]. Прогноз мошенничества со стороны руководства на основе набора данных, разработанных международной государственной секретарской фирмой, был сделан с помощью мощной модели качественного ответа Hanson J.V. и другие.[6]. Исследование было направлено на изучение использования экспертных систем для повышения производительности аудиторов [7]. Модель

классификации мошенничества в нейронной сети с использованием эндогенных финансовых данных была представлена Green и Choi [8]. Изученный шаблон поведения затем создал классификационную модель, которая применялась к тестовой выборке. Для прогнозирования управленческого мошенничества Fanning и Cogger [9] использовали искусственную нейронную сеть. Они нашли модель восемью переменных с высокой вероятностью обнаружения, используя общедоступные предикторы мошеннических финансовых операций. Стимулы и штрафы исследуются в связи с завышением доходов, прежде всего, в фирмах, в отношении которых Комиссия по ценным бумагам и биржам предпринимает действия по принудительному ведению бухгалтерского учета Beneish [10]. Abbott и др. [11] тщательно изучили и обсудили автономию комитета по аудиту и деятельность по смягчению вероятности мошенничества. Ряд исследователей пытались синтезировать литературу, такие как, Phua и др. [12]. Ими были отсортированы, сопоставлены, сокращены и резюмированы из примерно всех опубликованных технических и обзорных статей по автоматизированному обнаружению мошенничества за последние 10 лет. Тем не менее, исследование было сосредоточено на общих рисках, таких как обнаружение финансовых преступлений и терроризма, обнаружение спама и вторжений.

Финансовые учреждения теперь признали, что применение изолированных механизмов безопасности на отдельных каналах доставки просто больше не обеспечивает необходимых уровней защиты от несанкционированной активности на счетах [15] и [16]. Финансовые ИТ-платформы часто становятся легкой мишенью для мошенничества из-за их потенциальной возможности крупномасштабной кражи денег из-за многочисленных недостатков аутентификации и лазеек в моделях безопасности развернутых сервисных платформ. Таким образом, слабая аутентификация, обеспечиваемая механизмами подписи, PIN-кода, пароля и кода безопасности карты (CSC), продолжает способствовать незаконным финансовым транзакциям за счет разработки инновационных системных атак и методологий со стороны злонамеренных третьих лиц.

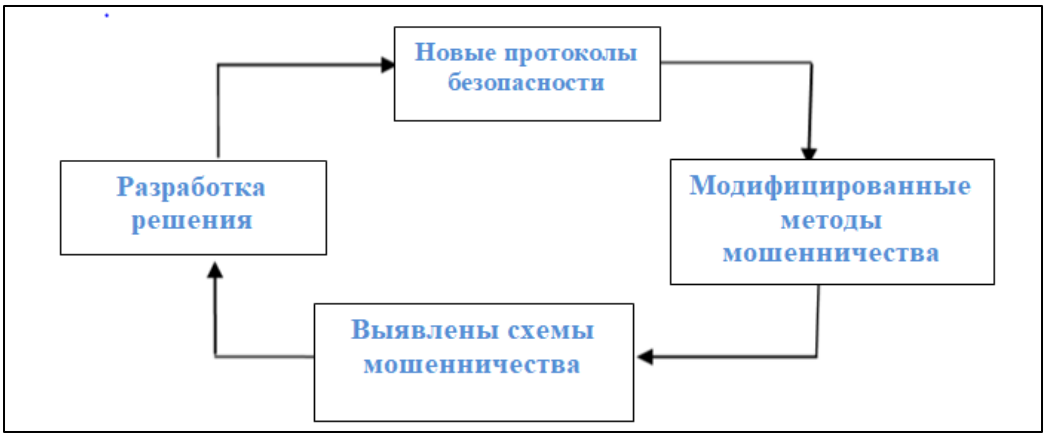

Рис. 1. Цикл угрозы мошенничества

Предотвращение мошенничества. Финансовые банки очень заинтересованы в быстром обнаружении мошенничества из-за его сильного влияния на итоговые операционные расходы, предоставление услуг и репутацию. Поэтому несколько учреждений объединяют типичные правила безопасности с разделением по каналам с избыточным уровнем безопасности, называемым «управление мошенничеством», чтобы компенсировать различные недостатки, от которых мошенники страдают в механизмах проверки подлинности с разделением по каналам. Технологии управления мошенничеством упрощают активную проверку данных об активности учетной записи, чтобы создать всеобъемлющую структуру контроля мошенничества с многоуровневой ассимилированной безопасностью во всех сетях передачи услуг.

Финансовые организации стараются приумножить удобство финансовых услуг, внедряя современные методы обслуживания, включая пластиковые кредитные/дебетовые карты, банкоматы (АТМ), услуги интернет-банкинга и даже мобильные банковские приложения. Полученные запросы направляются смежными серверами сетевого уровня для управления финансовыми услугами на прикладном уровне в рамках основной бизнес-логики и логики данных.

Правила и методы безопасности на сетевом уровне применяются для аутентификации честных клиентов с использованием методов, основанных преимущественно на стандартах безопасности «что знает пользователь» и «что у пользователя есть». Таким образом, пользователи, по сути, предоставляют обязательную информацию о безопасности, такую как личные данные, личный

идентификационный номер, пароли и т. д., или сохраняют необходимое устройство безопасности, такое как смарт-карта, жесткий токен безопасности и т. д., чтобы подтвердить себя в качестве владельца учетной записи запрашиваемой финансовой службой.

В Reactive Fraud Management методы обнаружения знаний, такие как интеллектуальный анализ данных [6], применяются для алгоритмической обработки и сложных вычислений хранимых транзакционных данных. Случаи мошенничества распознаются либо по сравнению с заранее выявленными моделями мошенничества, либо как необычное поведение по сравнению с ранее зарегистрированным поведением. Несмотря на это, выполнение метода «сохранить сейчас, запросить позже» угрожающе увеличивает задержку обнаружения мошенничества из-за необходимости транзакционных данных в оцениваемом хранилище данных до применения используемых методов анализа данных. Новые протоколы безопасности получение превентивного ответа могут быть применены только после завершения транзакции и увеличения соответствующей фискальной стоимости.

Недостатком решений для реактивного управления мошенничеством является зависимость от помеченных исходных наборов данных для соответствия требуемым поведенческим моделям, по которым оценивают появление новых данных, а также потому, что новые появления данных по существу должны быть помечены, а модели постоянно переобучаются для обнаружения новейших угроз мошенничества из немаркированных входящих запросов на транзакции. Таким образом, происходит значительная задержка, поскольку достаточное количество помеченных случаев мошенничества распознается и помечается соответствующим образом для включения в набор обучающих данных, в течение которых случаи мошенничества останутся незамеченными и добавятся к значительным финансовым потерям.

ЛИТЕРАТУРА

1. Расследование мошеннических действий, 2000 Меморандум хьюстонского системного административного университета, http://www.uhsa.uh.edu/sam /AM/01C04.html
2. Болонья, Джек и Роберт Дж. Линдквист, 1987 г. Аудит мошенничества и судебная бухгалтерия, Нью-Йорк: John Wiley & Sons, 240c.
3. Прабин К Паниграхи, 2011. «Структура для обнаружения внутреннего финансового мошенничества с использованием аналитики» в системах связи и сетевых технологиях (CSNT), международная конференция IEEE 2011, с. 323–327.
4. Stream Base, 2008 г. Entrust. www.entrust.com
5. Бизли М.С., 1996. «Эмпирический анализ связи между составом совета директоров и мошенничеством в финансовой отчетности», The Accounting Review, vol. 71, нет. 4, с. 443-465.
6. Дж. В. Хансен, Дж. Б. Макдональд и В. Ф. Мессье, 1997. «Обобщенная модель качественного ответа и анализ мошенничества в управлении», Management Science, vol. 42, с. 1022-1032.
7. Эйнинг М.М., Д.С. Р. Джонс и Дж. К. Леббеке, 1997. «Опирание на средства принятия решений: анализ аудиторской оценки мошенничества со стороны руководства», Аудит: Журнал практики и теории, том. 16, с. 1-19.
8. Б. П. Грин и Дж. Х. Чой, 1997. «Оценка риска управленческого мошенничества с помощью технологии нейронных сетей», Аудит, том. 16, с. 14-28.
9. К. Фаннинг и К. Коггер, 1998. «Обнаружение мошенничества в управлении с помощью нейронной сети с использованием опубликованных финансовых данных», Международный журнал интеллектуальных систем в бухгалтерском учете, финансах и менеджменте, том. 7, нет. 1, с. 21-24.
10. M.D. Beneish, 1999. «Поощрения и штрафы, связанные с завышением доходов, нарушающим GAAP», Accounting Review, vol. 4, с. 425-457.
11. Л. Дж. Эбботт, С. Паркер и Г. Ф. Питерс, 2001 г. «Характеристики комитета по аудиту и финансовые искажения: исследование эффективности некоторых рекомендаций комитета с голубой лентой», Труды аудиторской секции собрания AAA.
12. K. Fanning, K., Cogger, and R. Srivastava, 1995. «Обнаружение управленческого мошенничества: нейросетевой подход», Международный журнал интеллектуальных систем в бухгалтерском учете, финансах и менеджменте, том. 4(2), с. 113126.
13. Агиеманг М., Баркер К. и Алхадж, 2006 г. «Всеобъемлющий обзор числовых и символических методов извлечения выбросов», Интеллектуальный анализ данных, том 10, с. 521-538.
14. Коу Ю., Лу С. и Сирвонгваттана, 2004 г. «Обзор методов обнаружения мошенничества», Международная конференция по сетям, обнаружению и контролю, с. 749-754.
15. Мэсси, К. Мэсси, 2005 г. «Борьба с электронным мошенничеством — подход следующего поколения», Информационная статья Financial Insights.

LITERATURE

1. Investigating Fraudulent Acts, 2000 UNIVERSITY OF HOUSTON SYSTEM ADMINISTRATIVE MEMORANDUM, http://www.uhsa.uh.edu /sam/AM/01C04.htm
2. Bologna, Jack & Robert J. Lindquist, 1987. Fraud Auditing & Forensic Accounting, New York: John Wiley & Sons, pp. 240
3. Prabin K Panigrahi,2011. "A Framework for Discovering Internal Financial Fraud Using Analytics" in Communication Systems and Network Technologies (CSNT), IEEE 2011 International Conference, pp. 323 - 327
4. Stream Base, 2008 Entrust www.entrust.com
5. M. S. Beasley,1996. "An empirical analysis of the relation between the board of director composition and financial statement fraud," The Accounting Review, vol. 71, no. 4, pp. 443-465.
6. J. V. Hansen, J. B. McDonald, and W. F. Messier, 1997. "A generalized qualitative-response model and the analysis of management fraud", Management Science, vol. 42, pp. 1022-1032.
7. M. M. Eining, DS. R. Jones, and J. K. Loebbecke, 1997. "Reliance on decision aids: an examination of auditors‟ assessment of management fraud," Auditing: A Journal of Practice and Theory, vol. 16, pp. 1-19.
8. B. P. Green, and J. H. Choi, 1997. "Assessing the risk of management fraud through neural network technology," Auditing, vol. 16, pp. 14-28.
9. K. Fanning and K. Cogger, 1998. "Neural network detection of management fraud using published financial data," International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 7, no. 1, pp. 21-24.
10. M. D. Beneish, 1999. "Incentives and penalities related to earnings overstatements that violate GAAP," Accounting Review, vol. 4, pp. 425-457.
11. L. J. Abbott, S. Parker, and G. F. Peters, 2001. "Audit committee characteristics and financial misstatement: A study of the efficacy of certain blue ribbon committee recommendation," Proceedings of the Auditing Section of the AAA Meeting.
12. K. Fanning, K., Cogger, and R. Srivastava, 1995. "Detection of management fraud: a neural network approach", International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 4(2), pp. 113126.
13. Agyemang, M., Barker, K., & Alhajj, 2006. "A comprehensive survey of numeric and symbolic outlier mining techniques", Intelligent Data Analysis, vol.10, pp.521-538.
14. Kou, Y., Lu, C., & Sirwongwattana, 2004. "Survey of Fraud Detection Techniques", In International Conference on Networking, Sensing, and Control, pp.749-754.
15. Massey, K. Massey, 2005. "Combating eFraud – a next generation approach", Financial Insights White Paper.