УДК 004.457

Лаврентьева М.А.

Lavrentyeva M.A.

студент магистратуры

graduate student

2 курс, факультет ИБ

2 course Faculty IB

МФ МГТУ им. Н. Э. Баумана

MF MSTU them. N.E. Bauman

Россия, г. Москва

Russia, Moscow

Научный руководитель: Коннова Н.С.

scientific advisor Konnova N.S.

доцент, кандидат технических наук

Associate Professor, Candidate of Engineering Sciences

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ ОБНАРУЖЕНИЯ ИНСАЙДА НА БИРЖЕ

OVERVIEW OF EXISTING SOLUTIONS FOR DETECTING INSIDER TRADING ON THE EXCHANGE

***Аннотация**: В этой статье рассмотрены существующие современные средства и методы по обнаружению подозрительных инсайдеров на основе совершенных ими сделок. Также проведен анализ этих методов, выявлены как достоинства, так и существенные недостатки.*

***Annotation**: This article discusses the existing modern tools and methods for detecting suspicious insiders based on their transactions. The analysis of these methods has also been carried out, and both advantages and significant disadvantages have been identified.*

***Ключевые слова**: информационная безопасность, биржа, инсайд, обнаружение подозрительных инсайдеров.*

***Key words**: information security, exchange, insider trading, detection of suspicious insiders.*

Обзор существующих методов обнаружения инсайда на бирже

На сегодняшний день информация является исключительным ценным ресурсом, а ее защита – критически важным элементом коммерческой деятельности и функционирования государство. Однако, несмотря на современные технологии, обеспечить полную информационную безопасность невозможно.

Проблемами и угрозами информационной безопасности являются внешние атаки и злоумышленники внутри компании: деструктивные действия хакерских групп, так и недобросовестные сотрудники, продающие конфиденциальную информацию, что приносит вред компании. Например, в следствие крупной утечки в американском в сентябре 2018 пострадало 147 млн человек [1]. В России при этом таких масштабных инцидентов на момент 2018 года не было зафиксировано [2]. При этом максимальный подтвержденный размер финансового ущерба от утечки информации в российской компании на момент 2019 года составляет $30 млн [3].

Это обозначает, что основная проблема заключается не только в защите информации извне, но и внутри организаций. В таблице 1 приведены типы инсайдеров, из-за которых может быть произведена утечка информации [4].

Таблица 1 – Типы инсайдеров, по вине которых может быть произведена утечка информации

Тип	Умысел	Корысть	Постановка задачи	Действия по возможности

Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обиженный	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Нет	Сам/Извне	Отказ/ Имитация/ Взлом
Внедренный	Да	Да	Извне	Взлом

До 2010 года [5] за неумышленное использование конфиденциальной информации производилось взыскание, а за умышленное причинение вреда путем торговли внутренними данными степень наказания работника заключалась в увольнении. Однако в 2010 году вступил закон (Федеральный закон от 27.07.2010 г. № 224-ФЗ [7]), предусматривающий уголовную ответственность за незаконное использование внутренней информации [8].

Несмотря на применяемые меры, из-за отсутствия рабочего механизма выявления инсайдерских сделок [9], проблема утечек, в частности по вине работников, остается актуальной и в последнее время. Ведь только на ликвидацию последствий одного инцидента в 2016 году затрагивалось около 1,6 млн рублей, а в крупных предприятиях – 20 млн рублей [6].

В большинстве случаев утечка внутренней информации по вине внутренних пользователей происходит на биржах.

Биржа [10] – форма объединения предприятий или собрание коммерческих посредников с целью проведения регулярных торгов, купли-продажи финансовых активов и товаров, а также контрактов на их поставку.

Современные технологии позволяют проводить на биржах миллионы сделок ежесекундно [10]. Основной причиной такого

является то, что сделки можно совершать, не выезжая в штаб-квартиру корпорации.

Разработано множество методов по борьбе с утечкой внутренней информации.

1) Data Mining – анализ информации с целью нахождения среди хранящихся данных раннее неизвестных, но при этом практически полезных знаний, которые необходимы для приятия решений в различных областях деятельности [11]. Прежде всего, это процесс нахождения скрытых закономерностей в хранящихся данных.

2) Анализ изменения стоимости ПТ на основе графа.

После завершения очередной сессии на бирже остаются конечные стоимости ПТ: активов, ценных бумаг и т.д., показывающее изменение цен после совершения сделок.

При этом может возникнуть ситуация, когда после падения цен идет резкое увеличение, а в этот промежуток происходит скупка определенного ПТ, или же наоборот, когда стоимость высокая и производится их продажа, затем последующее падение его стоимости.

Следовательно, на графике изменения цен ПТ на бирже за некоторый достаточно небольшой промежуток времени можно выявить резкие изменения цен и сличить, были ли проведены за промежуток «пика» операции купли-продажи.

Подобную модель [13] можно представить в виде графа, где узлами являются объекты торгов на бирже, а дугами – сама операция купли-продажи вместе со стоимостью. В течение некоторого промежутка времени, например, ряда сессий, система накапливает данные, особенно отслеживая моменты роста и падения цен.

Сама процедура анализа изменения цен выглядит следующим образом. Собранные на конец сессии данные разделяются по биржам,

причем, за один раз анализируется один торговый день. Котировки значений бид и аск компонуются по децилям. Для каждого такого набора вычисляется частота повышения цены. Подсчитывается число появлений каждой величины.

3) Анализ изменения стоимости ПТ на основе машинного обучения [14] предполагает машинное обучение системы прогнозирования цен на основе имеющихся данных и также сравнения их с реальными. Если после подъема стоимости конкретного ПТ после операции купли-продажи произойдет резкий рост (обвал) цены этого ПТ, то система отследит подобное изменение и уточнит, были ли перед этим проведены операции купли-продажи.

Процесс машинного обучения состоит из нескольких шагов: от выбора математических и программных инструментов, сбора входных данных, до выработки предсказаний и тестирования. Самый простой способ — это создание с помощью машинного обучения модели на основе исторических данных, ее тестирование и дальнейшее применение для генерирования прогнозов будущего движения цен.

Система построения сети подозрительных инсайдеров подразумевает следующий принцип работы. Из общего числа сделок выделяются все участники торгов из одной и той же компании. После этого система должна сравнить все сделки совершенные за определенный период у каждой пары инсайдеров одной компании. При этом находится коэффициент схожести сделок [15]:

$$S(T_H, U_H) = \frac{\left(\sum_{i=1}^{|T_H|}\sum_{j=1}^{|U_H|} I(t_i, u_j)\right)^2}{|T_H| \times |U_H|}, i \neq j. \quad (1)$$

Данный коэффициент может принимать значения в пределах от 0 до 1. При этом чем выше это значение, тем больше одинаковых сделок совершила рассматриваемая пара инсайдеров. Из этого

следует, что необходимо найти некоторый порог, выше которого следует считать участников торгов подозрительными, когда остальные случайно совершили одинаковые сделки.

Анализ рассмотренных методов

Большинство организаций, как ITInvest [16], создает свои программные комплексы, однако отсутствие принципов работы не дает полного представления о качестве защиты. Поэтому данные методы не рассматриваются в статье.

Система «Списки инсайдеров» также имеет ряд существенных недостатков:

- система производит сбор всех участников торгов, предоставляя дальнейший анализ сторонним организациям;
- система не собирает данных по произведенным транзакциям, лишь исключает нелегально торгующих лиц из списка;
- передача по открытому каналу увеличивает вероятность взлома системы.

Технологии Data Mining более универсальный способ нахождения скрытых связей и торговлей с использованием конфиденциальной информации.

В этом случае программный комплекс должен проанализировать базу данных всех произведенных транзакций, по косвенным признакам вычислить все сомнительные операции. Одними из главных недостатков этого метода являются быстродействие и память. База данных вполне может хранить информацию за год или несколько лет, находить одних и тех же инсайдеров, что тоже затрудняет процесс обработки информации.

Выводы

Таким образом, рассмотрены различные существующие методы защиты от инсайда на бирже, при этом произведен анализ достоинств и недостатков данных методов. В некоторых случаях основной проблемой становится стоимость готового продукта, а также сложность в эксплуатации подобных систем.

По этой причине была поставлена задача создать простую в использовании, но эффективную систему, которая способна обнаружить подозрительных участников торгов с вероятностью ошибок первого и второго рода ниже 5%.

Для этого был выбран метод построения сети из подозрительных инсайдеров на основе поиска коэффициента схожести сделок. В силу работы системы с большим объемом данных поставлена задача найти предел, ниже которого участники торгов не будут рассматриваться, как подозрительные.

Использованные источники

1. Новостной сайт itWeek// Статистика утечек информации в мире [Электронный документ] – URL: https://www.itweek.ru/sequrity/news-company/detail.php?ID=203601 (дата обращения 20.09.2018).
2. Главной проблемой безопасности остается человек // Лев Матвеев // статья журнала «Информационная безопасность», №5, ноябрь 2018, стр. 42-47, издательство Grotesk, URL:www.itsec.ru
3. журнал «Информационная безопасность», №3, июль 2019, стр. 26, издательство Grotesk, URL:www.itsec.ru

4. Инсайдер // Портал трейдеров utmagazine, 30 апреля 2015 [Электронный документ] – URL: https://utmagazine.ru/posts/7670-insayder (дата обращения 20.09.2018).
5. Борьба с инсайдерством в России и за рубежом // Юридический центр защиты граждан и предприятий [Электронный документ] – URL: http://5898523.ru/borba-s-insajderstvom-v-rossii-i-za-rubezhom/ (дата обращения 20.09.2018).
6. Ирина Ли Объем утечек конфиденциальной информации в России за год вырос в 100 раз // Новостной сайт РБК, 2016 [Электронный документ] – URL: https://www.rbc.ru/technology_and_media/08/06/2017/5937ddda9a79471a1683d2a2 (дата обращения 20.09.2018).
7. Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации. СЗ РФ 02.08.2010, №31, ст. 4193.
8. Чиркова Е.В., Агамян Г.Р. Инсайдерская торговля на российском фондовом рынке перед объявлениями о сделках по слияниям и поглощениям // Universum: Экономический журнал ВШЭ: 2015. – Т. 19. № 3. – С. 395–422.
9. Федоров В.А. Математические методы выявления инсайда // Universum: ЭТАП: экономическая теория, анализ, практика: 2014. – С. 111-118.
10. Словари и энциклопедии на Академике // Биржа [Электронный документ] – URL: https://investments.academic.ru/734/Биржа (дата обращения 20.09.2018).
11. Технологии Data Mining // Файловый архив студентов [Электронный документ]. URL:

https://studfiles.net/preview/4431239/page:28/ (Дата посещения 20.11.2018).

12. Обнаружение инсайдерской торговли: Алгоритмы выявления и паттерны незаконных сделок, 17 декабря 2015 // harbr [Электронный документ]. URL: https://habr.com/post/95209/ (Дата посещения 20.11.2018).
13. Честный рейтинг форекс-брокеров // Инсайд Форекс [Электронный документ] – URL: http://brokers-fx.ru/articles/insajd-foreks (Дата обращения 01.02.2019).
14. Habr // Алгоритмы и торговля на бирже: Скрытие крупных сделок и предсказание цены акций [Электронный документ] – URL: https://habr.com/ru/company/iticapital/blog/271059/ (Дата обращения 01.02.2019).
15. Обнаружение инсайдерской торговли: Алгоритмы выявления и паттерны незаконных сделок [Электронный документ] URL: https://habr.com/company/iticapital/blog/273337/ (дата обращения 20.10.2018).
16. Как on-line broker защитился от работы инсайдеров // ITInvest [Электронный документ] URL: http://www.itinvest.ru/about/news/683092/https://habr.com/post/95209/ (Дата посещения 20.11.2018).