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

ОПИСАНИЕ СТРУКТУРЫ СИСТЕМЫ ОБНАРУЖЕНИЯ ИНСАЙДА НА БИРЖЕ НА ОСНОВЕ ТЕОРЕТИКО-ГРАФОВОГО ПОДХОДА

DESCRIPTION OF THE STRUCTURE OF THE INSIDER DETECTION SYSTEM ON THE EXCHANGE BASED ON THE GRAPH-THEORETIC APPROACH

***Аннотация**: На сегодняшний день более 50% сделок, совершаемых на бирже, подозрительные. В статье описана структура система обнаружения подозрительного инсайда на основе анализа схожести совершенных сделок. Кроме того, описан принцип работы системы и приведен пример вывода результатов для пользователей.*

***Annotation**: Today more than 50% of transactions made on the exchange are suspicious. The article describes the structure of the suspicious insider detection system based on the analysis of the similarity of completed*

transactions. In addition, it describes how the system works and provides an example of output results for users.

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

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

На сегодняшний день информация является исключительным ценным ресурсом, а ее защита – критически важным элементом коммерческой деятельности и функционирования государство [1]. Однако, несмотря на современные технологии, обеспечить полную информационную безопасность невозможно.

Биржа – площадка для проведения торгов между ее участниками, брокерами. При этом каждый брокер стремится к получению максимальной прибыли от совершенных сделок и, как следствие, может использовать разные ценовые манипуляции, как [2]:

- повышение цены – одно из самых распространенных направлений, в котором брокер способствует повышению курса актива, а затем продает их покупателю по возросшей цене;
- стабилизация цен подразумевает искусственную стагнацию актива в районе цен, лучше тех, что установились бы без вмешательства брокера;
- снижение цены – наиболее редко встречающаяся операция, которая предполагает получение максимальной прибыли путем совершения коротких продаж без покрытия.

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 [3].

По этой причине разрабатывается система, позволяющая обнаружить подозрительных инсайдеров после торговой сессии. Для этого система использует теоретико-графовый подход, а именно строит сеть из подозрительных инсайдеров.

Принцип сети следующий. 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 [4]:

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

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.

Однако данный способ подразумевает большую вероятность ошибок первого рода, когда обнаруживается ложноположительный результат. Следовательно, для повышения эффективности обнаружения подозрительных инсайдеров целесообразно ввести второй этап проверки, например, анализ подозрительной активности, который будет работать при достаточном объеме анализируемой выборки.

Таким образом, можно составить несколько основных блоков-модулей, использующие более простые функции для узконаправленных задач. В этом случае систему можно представить в виде, показанным на рисунке 1:

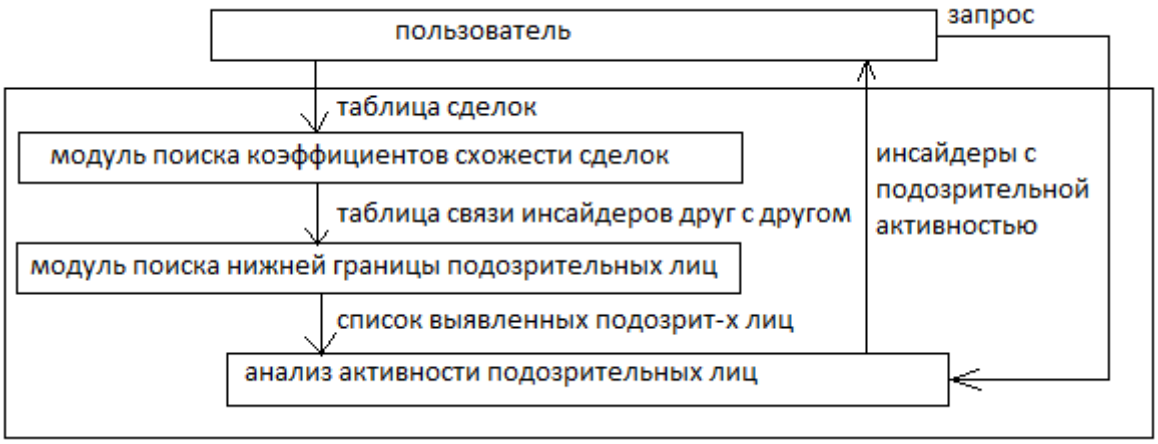


Рисунок 1 – Модульная структура системы обнаружения инсайда

Таким образом, система подразумевает наличие нескольких основных блоков, которые производят обработку информации по совершенным сделкам. Сами сделки занесены в некоторый внешний файл в виде таблицы, причем, этот файл может иметь как стандартное имя, так и имя, выбранное пользователем. В последнем случае необходимо указать системе имя этого файла.

После чтения файла производится первичная обработка, то есть составление списка, поиск всех инсайдеров, которые совершали сделки. Данный список необходим для поиска всех сделок каждой пары инсайдеров, работающей в одной компании.

После создания единого списка для каждого инсайдера рассматривается все остальные участники торгов, производится анализ, работают ли оба участника в оной фирме. Если подобное подтверждается, то производится подсчет коэффициента схожести сделок по формуле (1).

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

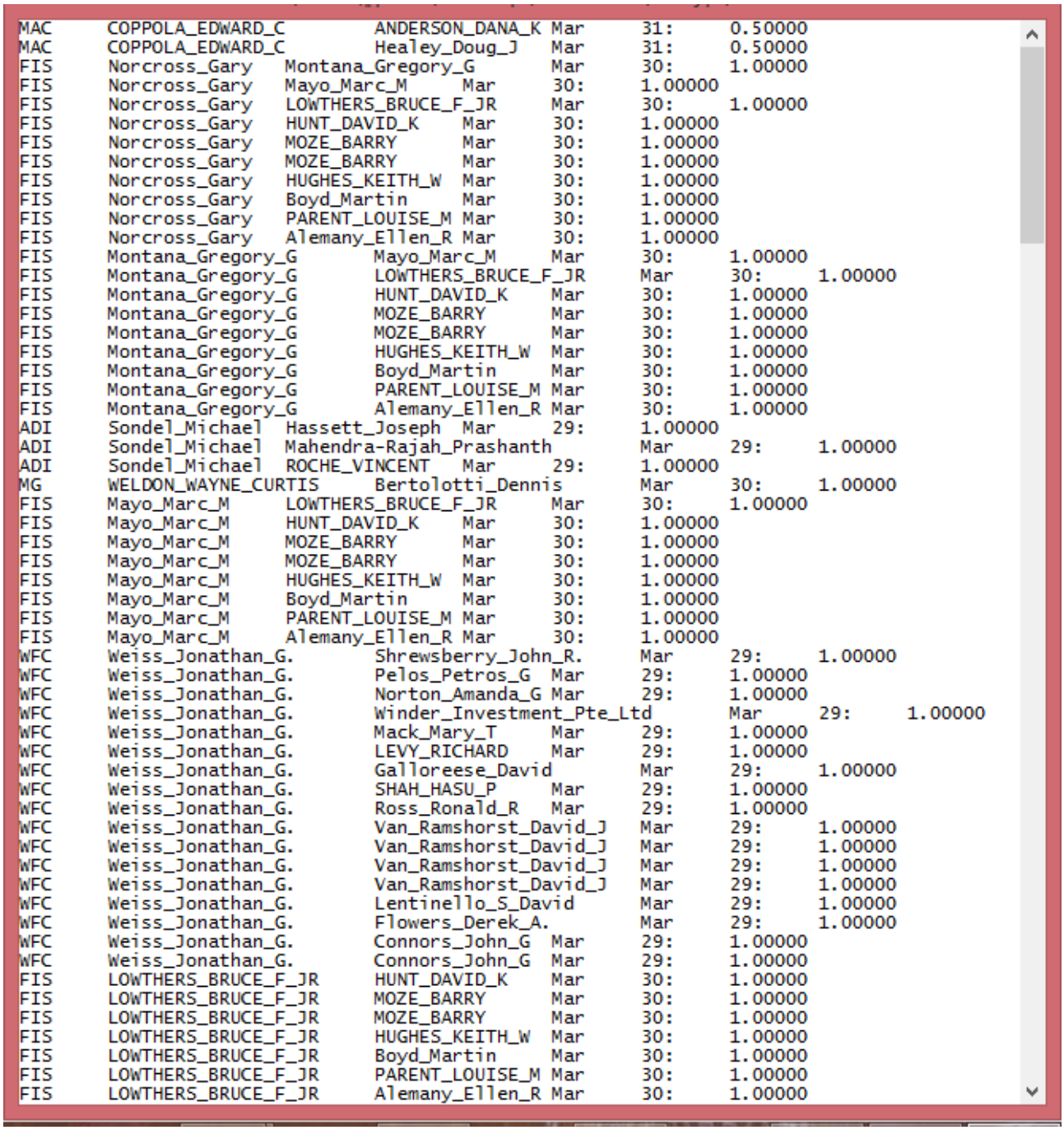
Когда были найдены все ненулевые коэффициенты среди участников торгов производится анализ нижнего предела, когда инсайдеры становятся

подозрительными. Данный критерий позволит произвести второй этап обработки с меньшим объемом информации.

После того, как системой были отсечены инсайдеры, которые не могут быть подозрительными, по желанию пользователя система предлагает выполнить второй этап работы, а именно – произвести анализ статистики работы подозрительных инсайдеров на бирже. Таким образом, можно дополнительно вывести, не было ли подозрительной активности в период до изменения ситуации на бирже.

Кроме того, система должна после каждого этапа работы выводить информацию в удобном для пользователя виде: в файл или на консоль. Сам анализ сделок долен проводиться на основе исходных данных, полученных из внешнего файла.

Пример вывода представлен на рисунке:



MAC	COPPOLA_EDWARD_C	ANDERSON_DANA_K	Mar	31:	0.50000			
MAC	COPPOLA_EDWARD_C	Healey_Doug_J	Mar	31:	0.50000			
FIS	Norcross_Gary	Montana_Gregory_G	Mar	30:	1.00000			
FIS	Norcross_Gary	Mayo_Marc_M	Mar	30:	1.00000			
FIS	Norcross_Gary	LOWTHERS_BRUCE_F_JR	Mar	30:	1.00000			
FIS	Norcross_Gary	HUNT_DAVID_K	Mar	30:	1.00000			
FIS	Norcross_Gary	MOZE_BARRY	Mar	30:	1.00000			
FIS	Norcross_Gary	MOZE_BARRY	Mar	30:	1.00000			
FIS	Norcross_Gary	HUGHES_KEITH_W	Mar	30:	1.00000			
FIS	Norcross_Gary	Boyd_Martin	Mar	30:	1.00000			
FIS	Norcross_Gary	PARENT_LOUISE_M	Mar	30:	1.00000			
FIS	Norcross_Gary	Alemany_Ellen_R	Mar	30:	1.00000			
FIS	Montana_Gregory_G	Mayo_Marc_M	Mar	30:	1.00000			
FIS	Montana_Gregory_G	LOWTHERS_BRUCE_F_JR	Mar	30:	1.00000			
FIS	Montana_Gregory_G	HUNT_DAVID_K	Mar	30:	1.00000			
FIS	Montana_Gregory_G	MOZE_BARRY	Mar	30:	1.00000			
FIS	Montana_Gregory_G	MOZE_BARRY	Mar	30:	1.00000			
FIS	Montana_Gregory_G	HUGHES_KEITH_W	Mar	30:	1.00000			
FIS	Montana_Gregory_G	Boyd_Martin	Mar	30:	1.00000			
FIS	Montana_Gregory_G	PARENT_LOUISE_M	Mar	30:	1.00000			
FIS	Montana_Gregory_G	Alemany_Ellen_R	Mar	30:	1.00000			
ADI	Sondel_Michael	Hassett_Joseph	Mar	29:	1.00000			
ADI	Sondel_Michael	Mahendra-Rajah_Prashanth	Mar	29:	1.00000			
ADI	Sondel_Michael	ROCHE_VINCENT	Mar	29:	1.00000			
MG	WELDON_WAYNE_CURTIS	Bertolotti_Dennis	Mar	30:	1.00000			
FIS	Mayo_Marc_M	LOWTHERS_BRUCE_F_JR	Mar	30:	1.00000			
FIS	Mayo_Marc_M	HUNT_DAVID_K	Mar	30:	1.00000			
FIS	Mayo_Marc_M	MOZE_BARRY	Mar	30:	1.00000			
FIS	Mayo_Marc_M	MOZE_BARRY	Mar	30:	1.00000			
FIS	Mayo_Marc_M	HUGHES_KEITH_W	Mar	30:	1.00000			
FIS	Mayo_Marc_M	Boyd_Martin	Mar	30:	1.00000			
FIS	Mayo_Marc_M	PARENT_LOUISE_M	Mar	30:	1.00000			
FIS	Mayo_Marc_M	Alemany_Ellen_R	Mar	30:	1.00000			
WFC	Weiss_Jonathan_G.	Shrewsberry_John_R.	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Pelos_Petros_G	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Norton_Amanda_G	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Winder_Investment_Pte_Ltd	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Mack_Mary_T	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	LEVY_RICHARD	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Galloreese_David	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	SHAH_HASU_P	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Ross_Ronald_R	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Van_Ramshorst_David_J	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Van_Ramshorst_David_J	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Van_Ramshorst_David_J	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Van_Ramshorst_David_J	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Lentinello_S_David	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Flowers_Derek_A.	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Connors_John_G	Mar	29:	1.00000			
WFC	Weiss_Jonathan_G.	Connors_John_G	Mar	29:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	HUNT_DAVID_K	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	MOZE_BARRY	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	MOZE_BARRY	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	HUGHES_KEITH_W	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	Boyd_Martin	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	PARENT_LOUISE_M	Mar	30:	1.00000			
FIS	LOWTHERS_BRUCE_F_JR	Alemany_Ellen_R	Mar	30:	1.00000			

Рисунок 2 – Для каждой компании пары инсайдеров, выполняющие одинаковые операции в одну и ту же дату

Использованные источники

1. Защита от утечек информации. Поиск разумного компромисса //Антон Быков // Статья журнала «Информационная безопасность», №2, май 2018, издательство Grotesk, URL:http://information-

security.ru/articles2/Oborandteh/zaschita-ot-utechek-informatsii-poisk-razumnogo-kompromissa (Дата обращения 01.03.2020).

2. 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.

3. Новостной портал itWeek [Электронный документ]. URL:https://www.itweek.ru/sequrity/news-company/detail.php?ID=203601 (Дата обращения 01.11.2019).

4. Обнаружение инсайдерской торговли: Алгоритмы выявления и паттерны незаконных сделок [Электронный документ] URL: https://habr.com/company/iticapital/blog/273337/ (дата обращения 20.10.2018).