НЕЙРОСЕТЕВЫЕ МЕТОДЫ РАСПОЗНАВАНИЯ ЭМОЦИЙ РЕЧИ ДЛЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В ТЕЛЕКОМУКАЦИОННЫХ СИСТЕМАХ

Филимонов А.В.[1], Осипов А.В.[2], Плешакова Е.С.[3], Гатауллин С.Т.[4]

Аннотация

Цель статьи: *разработка метода выявления мошенничества в телекоммуникационных системах на основе анализа содержания телефонного разговора, основанного на использовании нейросетевых методов распознавания эмоций речи*

Методы исследования: *анализ частотных характеристик текстовых представлений разговоров с мошенниками и динамики их изменения, анализ встречаемости ключевых слов*

Полученный результат: *предложен новый подход к выявлению мошенничества в телекоммуникационных системах, основанный на анализе эмоциональной и смысловой составляющих диалогов с мошенниками с помощью нейронных сетей и ассоциативных правил. Описана обобщенная схема метода выявления признаков мошенничества в телефонных разговорах. Предложен масштабируемый подход к выявлению подозрительных словосочетаний на основе алгоритма поиска ассоциативных правил Apriori. Создана многокомпонентная нейронная сеть с дифференцированной архитектурой. Было проведено исследование, как меняется эмоциональная составляющая диалогов с мошенниками в динамике, с целью выявления типовых схем эмоционального давления. Создан программный прототип, позволяющий оценивать наличие/отсутствие эмоционального давления в разговоре с мошенниками и оценивать, является ли разговор подозрительным или нет. Была оценена точность работы предложенного метода выявления телефонных мошенников.*

Научная новизна: *предложена новая технология обработки естественного языка, основанная на методах искусственного интеллекта.*

Вклад соавторов: *Филимонов А.В. — разработка программного прототипа, разработка многокомпонентной нейронной сети с дифференцированной архитектурой; Осипов А.В. – разработка подхода к выявлению подозрительных словосочетаний на основе алгоритма поиска ассоциативных правил Apriori; Плешакова Е.С. — оценка точности работы предложенного метода выявления телефонных мошенников, подготовка наборов данных для оценки точности работы предложенного метода выявления телефонных мошенников; Гатаулин С.Т. — общее руководство проектом, разработка схемы метода выявления признаков мошенничества в телефонных разговорах.*

Ключевые слова: *нейронные сети, ассоциативные правила, телефонное мошенничество, манипулирование, фишинг, вымогательство*

DOI:10.21681/2311-3456-2022-6-83-92

1. Введение

Бурное развитие информационных технологий оказали влияние на все сферы деятельности человека, привнося не только многочисленные потенциальные преимущества, но и новые риски, затрагивающие информационную безопасность (или кибербезопасность). В 2020 году, по данным Генпрокуратуры

1 Филимонов Андрей Викторович, кандидат физико-математических наук, доцент кафедры информационных технологий и цифровой экономики Ивановского химико-технологического университета, г. Иваново, Россия. E-mail: remueur@yandex.ru

2 Осипов Алексей Викторович, кандидат физико-математических наук, ведущий научный сотрудник Департамента информационной безопасности факультета информационных технологий и анализа больших данных Финансового университета при Правительстве РФ, Москва, Россия. E-mail: avosipov@fa.ru

3 Плешакова Екатерина Сергеевна, кандидат технических наук, доцент Департамента информационной безопасности факультета информационных технологий и анализа больших данных Финансового университета при Правительстве РФ, Москва, Россия. E-mail: espleshakova@fa.ru

4 Гатауллин Сергей Тимурович, кандидат экономических наук, декан факультета «Цифровая экономика и массовые коммуникации» Московского технического университета связи и информатики, ведущий научный сотрудник Департамента информационной безопасности факультета информационных технологий и анализа больших данных Финансового университета при Правительстве РФ, Москва, Россия. E-mail: s.t.gataullin@mtuci.ru

РФ, наиболее распространенным видом мошенничества стало мошенничество с использованием средств мобильной связи, на его долю приходится около 42% от общего числа киберпреступлений в России[5].

Одним из ключевых направлений обеспечения информационной безопасности по противодействию телефонному мошенничеству должны стать действия, направленные на предотвращение угроз и предупреждение атак. Для этого необходима разработка методов для противодействия мошенничеству в телекоммуникационных системах.

Традиционные подходы к выявлению мошенничества в сфере телекоммуникаций обычно основываются на составлении черного списка телефонных номеров мошенников. Однако злоумышленники могут просто избежать такого обнаружения, изменив свои номера, с помощью технологии VoIP (передача голоса по IP). Развитие данной технологии привела к увеличению количества методов, используемых злоумышленниками для совершения мошенничества [1]. Так, например, с появлением VoIP злоумышленники могут адаптировать инструменты, используемые киберпреступниками, такие как ботнеты, чтобы провести многоцелевые атаки [2]. К примеру, с помощью ботов злоумышленники могут автоматически набирать несколько номеров, что позволяет им ускорить этот процесс и охватить большее количество жертв.

В отличии от других методов борьбы с телефонным мошенничеством, основывающихся на блокировке номеров из черного списка, мы предлагаем анализировать непосредственно содержание звонка. В данной работе предлагается анализировать содержание телефонного разговора двумя способами: выявление давления на вызываемого абонента с помощью анализа эмоциональной составляющей и анализ ключевых фраз. Объединение обоих подходов дает устойчивый к обходу со стороны мошенников и точный метод выявления факта мошенничества. Модели взаимодополняют друг друга, что позволит повысить качество распознавания мошенников.

2. Описание подхода выявления мошенничества в телекомукационных системах

Для выявления мошенничества в сфере телекоммуникаций большинство современных подходов основаны на маркировке номеров вызывающих абонентов, которые идентифицируются клиентами как мошеннические. В то же время есть также много исследователей, которые используют методы машинного обучения для обнаружения мошеннических звонков. Они выбирают функции на основе таких факторов, как номера телефонов и типы вызовов. Они используют алгоритмы машинного обучения для обучения моделей и используют эти модели для обнаружения мошеннических вызовов, что также позволяет достичь хорошей точности обнаружения.

Однако, поскольку программное обеспечение для изменения номера широко используется, мошенники используют программное обеспечение для постоянной смены своего телефонного номера или маскировки своего номера под официальный номер правительственных учреждений. Эти причины позволяют легко обойти обычные методы обнаружения на основе телефонных номеров.

Машинное обучение и современные методы искусственного интеллекта могут быть эффективно использованы в системах противодействия телефонному мошенничеству. Существенным ограничением использования традиционных подходов машинного обучения является сложность понимания относительно длинных предложений и контекстов. Предыдущие исследования показали, что использование архитектуры нейронной сети может быть полезным для решения некоторого ряда проблем [3-5]. Для контекстуализации обнаружения спама некоторые ученые предпочитают использовать архитектуру нейронной сети с улучшенными методами глубокого обучения [6]. Существует несколько уникальных подходов к извлечению признаков для создания архитектуры нейронной сети [7-8].

Авторами предлагается подход к обнаружению мошенничества в сфере телекоммуникаций путем анализа содержания звонка и его эмоциональной составляющей.

В данной работе делается несколько допущений, которые сужают область применения разработанного метода, но позволяют увеличить его точность. Первое допущение – это то, что общение между аферистом и потенциальной жертвой осуществляется на русском языке. Второе допущение (которое подтверждается статистикой разговоров и политической обстановкой) – манера ведения разговора со стороны злоумышленника укладывается в несколько типовых схем.
Обобщенно, предлагаемый метод можно представить в виде следующей схемы:

5 1.Банк России: официальный сайт. – Москва. – URL: https://www.cbr.ru/analytics/ib/review_4q_2022/ (дата обращения: 20.05.2022). 2.Мошенничество в сети: судебная практика и ключевые аспекты – https://rtmtech.ru/research/online-fraud-research/ RTM Group » Исследования »/ (дата обращения: 20.05.2022).

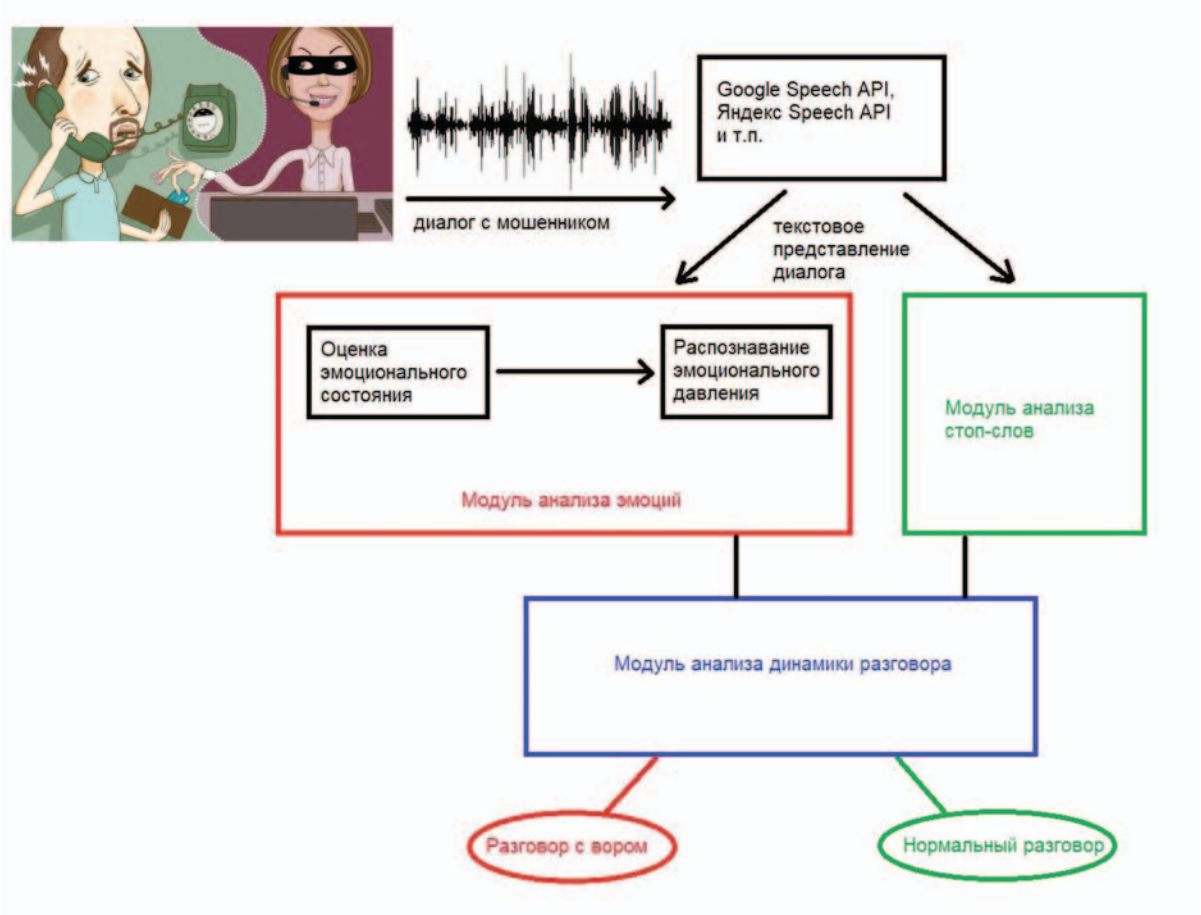

Рис. 1. Обобщенная схема метода выявления разговора с мошенником

Учитывая сложность работы с аудиозаписями, мы переводим речь в текст, используя API таких сервисов, как Google Speech API или Яндекс Speech API. Такой подход позволяет использовать встроенные в ОС библиотеки для распознавания речи, а, кроме того, мы получаем возможность увеличить размер обучающей выборки, скачивая образцы текстов мошеннического содержания с различных форумов или социальных сетей.

Предполагается рассматривать эмоциональный фон диалогов жертвы и мошенника в динамике, т.е. оценка эмоционального содержания речи делается не усредненно по всему разговору в целом, а в динамике. За счет применения такого подхода можно отследить попытку эмоционального давления на жертву.

Вторая модель использует анализ ключевых слов, таких как «служба безопасности банка», «счет», «карта» и т.п. В основе модели лежит предположение, что мошенники используют устоявшиеся схемы и оперируют ограниченным набором ключевых фраз. При необходимости данный набор можно расширять.

Модели взаимодополняют друг друга, что позволит повысить качество распознавания мошенников.

Имея текстовое представление разговора с предполагаемым мошенником, мы делаем две взаимодополняющие проверки: проверка на эмоциональное давление со стороны одного из участников разговора (модуль анализа эмоций) и проверка на характерные шаблоны построения фраз (модуль анализа стоп-слов). Результаты работы обоих модулей сопоставляются в модуле анализа динамики разговора, на основании чего мы принимаем решение, является ли вызывающий абонент мошенником или нет.

3. Описание работы модуля анализа эмоций

Теоретический и системный анализ открытых источников диалогов из социальных сетей дали понимание, что мошенник в ходе общения с потенциальной жертвой не просто общается на отвлеченные темы, а осуществляет направленное манипулирование собеседником. Для этого мошенниками используются различные техники, но наиболее распространенная – это техника перегрузки, которая основана на превышении лимита восприятия поступающей информации. В

Таблица 1

Список полей для анализа

Поле	Комментарий	Поле	Комментарий
M_p	M_p-количество реплик для p-го участника	$f_{у,p}$	Частота встречаемости символа «у» для p-го участника
L_p	Средняя длина реплики для p-го участника	$f_{э,p}$	Частота встречаемости символа «э» для *p*-го участника
$f_{а,p}$	Частота встречаемости символа «а» для p-го участника	$f_{ю,p}$	Частота встречаемости символа «ю» для *p*-го участника
$f_{е,p}$	Частота встречаемости символа «е» для p-го участника	$f_{я,p}$	Частота встречаемости символа «я» для *p*-го участника
$f_{и,p}$	Частота встречаемости символа «и» для p-го участника	$f_{!,p}$	Частота встречаемости символа «!» для *p*-го участника
$f_{о,p}$	Частота встречаемости символа «о» для *p*-го участника	$f_{?,p}$	Частота встречаемости символа «?» для *p*-го участника

литературе такое явление описывается, как т.н. эриксоновский гипноз [9-10].

Для выявления эмоционального состояния участника разговора мы воспользовались фактом, что структура информационного текста принципиально отличается от структуры внушающего (манипулирующего) текста и характеризуется отсутствием намеренной ритмизации его лексических и фонетических единиц[6].

На практике это означает, что некоторые звукосочетания способны не только вызывать определенные эмоции, но и могут восприниматься в качестве определенных образов[7]. Например, в сочетаниях буква «и» с указанием предмета обладает свойством «уменьшения» объекта, перед которым (или в котором) она явно доминантно присутствует. Также, звук «о» производит впечатление мягкости и расслабленности. Преобладание звуков «а» и «э», как правило, ассоциируется с эмоциональным подъемом.

Логика выделения знаков соответствует физиологии человека. Например, когда человек волнуется, то ему требуется больше кислорода для дыхания, и поэтому он широко открывает рот. Соответственно, в его речи будут преобладать «кричащие» звуки: а, о, э и т.п. Даже когда человек использует письменную речь, а не устную, то все равно копирует звуковые диспропорции в соответствии со своим эмоциональным состоянием. Исходя из перечисленных выше предпосылок, нами были предложены для анализа поля, перечисленные в таблице 1. В данной таблице перечислены основные параметры реплик для участников разговора.

Таблица 1 не является исчерпывающей. На самом деле для анализа использовались все буквы русского алфавита, за исключением мягкого и твердого знаков, а также знаки препинания: точка, знаки восклицания и вопроса.

Значения этих полей рассчитываются по следующим формулам:

$$f_{x,p} = \frac{\sum_i^{M_p} N_{i,x,p}}{\sum_i^{M_p} N_{i,p}} \quad (1)$$

где p-порядковый номер участника разговора, i-порядковый номер реплики для p-го участника, Mp-количество реплик для p-го участника, x-символ, для которого делается расчет; Ni,x,p-количество символов x в i-й реплике p-го участника; Ni,p-общее количество символов в i-й реплике.

$$L_p = \frac{\sum_i^{M_p} N_{i,p}}{M_p} \quad (2)$$

Работа модуля анализа эмоций сводится к решению задачи классификации: беседа носит информационный характер или манипулятивный. Для решения этой задачи было предложено использовать гибридную нейронную сеть, которая состоит из нескольких слоев.

6 С.В. Болтаева, Т.В. Матвеева. Лексические ритмы в тексте внушения // Русское слово в языке, тексте и культурной среде. Екатеринбург, 1997, стр. 175-185

7 В.В. Киселёв. Автоматическое определение эмоций по речи // Образовательные технологии. №3, 2012, стр. 85-89

Первый слой – слой Кохонена. Его назначение – разбивка всех реплик на кластеры, каждый из которых соответствует какому-либо эмоциональному состоянию. Количество кластеров определялось автоматически в процессе обучения.

Второй слой – это сжимающий слой (скрытый слой автокодировщика). Его назначение – это сокращение количества кластеров и устранение шумов.

Третий слой (вернее два слоя) – это классификатор, построенный на базе обычного персептрона. Именно он определяет, является ли диалог манипуляцией или нет.

Схема сети представлена на рисунке ниже:

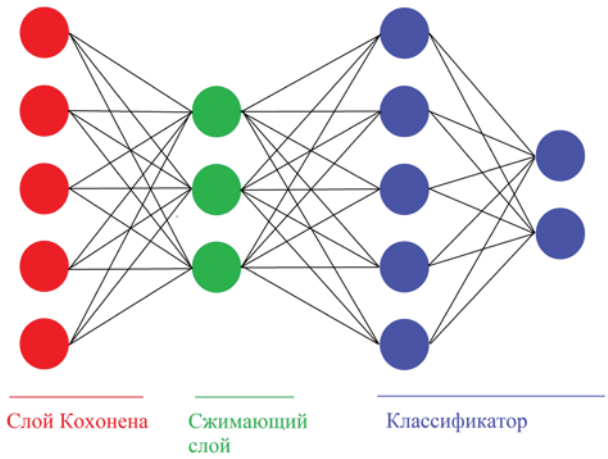

Рис. 2. Структура нейронной сети

При подготовке обучающего множества мы столкнулись с дефицитом данных для построения обучающего множества. Однако, учитывая, что наш классификатор, по сути, не определяет факт мошенничества, а классифицирует диалоги на манипулятивные и информационные, то мы для обучения классификатора использовали диалоги из социальных сетей. В любой дискуссии, особенно развернутой на какую-либо «острую» тему, обязательно присутствуют люди, провоцирующие других участников дискуссии. Они, как правило, достаточно легко идентифицируются остальными участниками дискуссии, и, следовательно, их реплики можно разметить, как манипулятивные. Благодаря этому приему мы сумели решить проблему объемов выборки для обучения.

На рисунке ниже представлены результаты разбивки участников дискуссий на кластеры с помощью сетей Кохонена.

Мы отрабатывали два варианта работы классификатора.

В первом варианте оценивались эмоциональные состояния участников разговора по всему диалогу в целом. Во втором варианте предполагалось, что эмоциональные состояния участников разговора должны меняться от реплики к реплике. И если разговор подчинен какому-то шаблону, то и переход от одного эмоционального состояния к другому должен быть типовым, подчиняющемуся какой-либо закономерности. Т.е. должны были иметь место типовые «маршруты» переходов из одного кластера в другой. Такие маршруты можно было бы выявить и классифицировать. На рисунках ниже приведены примеры переходов из одного эмоционального состояния в другое для одного из участников разговора. Текущие кластеры отмечены на рисунках красной «галочкой».

Точность выявления манипулятивного текста составила 76%.

4. Описание работы модуля анализа стоп-слов

Модуль анализа эмоций не определяет, является разговор мошенническим или нет. Его назначение – это определение, присутствует ли в разговоре попытка манипуляции или нет. Для классификации же диалога на мошеннический или нет необходим модуль анализа стоп-слов.

Имеются работы, в которых описаны попытки выявления телефонных мошенников, используя анализ смысловой составляющей телефонного разговора. Такой подход является наиболее сложным в реализации по сравнению с анализом внешних характеристик беседы (телефонный номер, время звонка, продолжительность звонков, частота и другие характеристики), но в то же время данный подход позволяет достичь наиболее впечатляющих результатов. Так в [11] была достигнута точность определения мошеннических звонков 98,53%.

Нами предлагается также анализировать содержание разговора, а именно вхождения ключевых слов. При этом опять встает проблема подготовки обучающего множества для построения классификатора.

Использование деревьев решений или нейронных сетей, как в [12] не является приемлемым вариантом, т.к. для обучения тех же нейронных сетей требуется изначально достаточно большая обучающая выборка, которой у нас нет. Кроме того, большинство алгоритмов машинного обучения требуют перестройки модели в случае добавления новых данных в обучающую выборку [13-14].

Нам же был необходим метод, который легко масштабируется без перестройки модели. Учитывая допущение о том, что манера ведения разговора со стороны злоумышленника укладывается в несколько

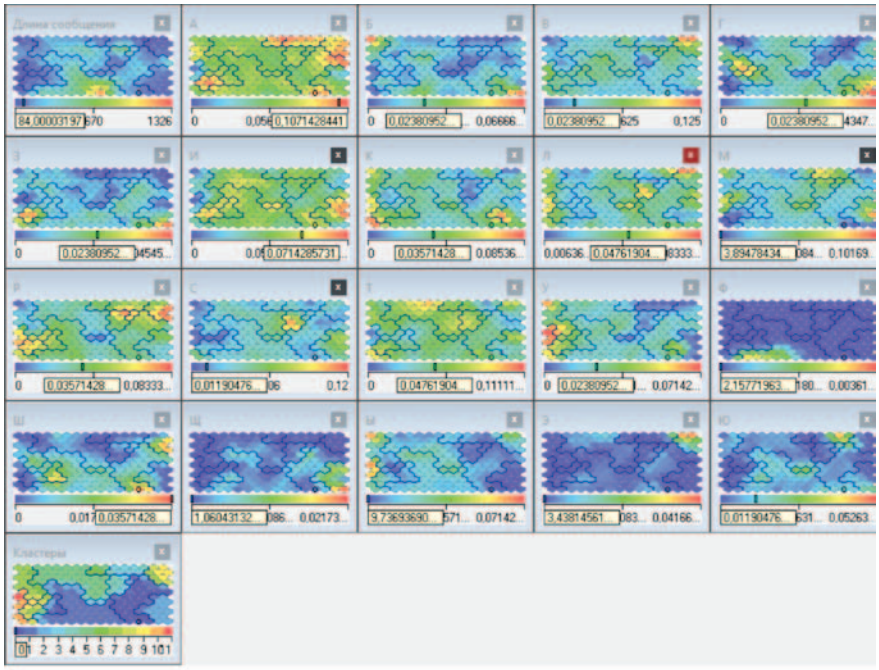

Рис. 3. Разбивка на кластеры участников дискуссии

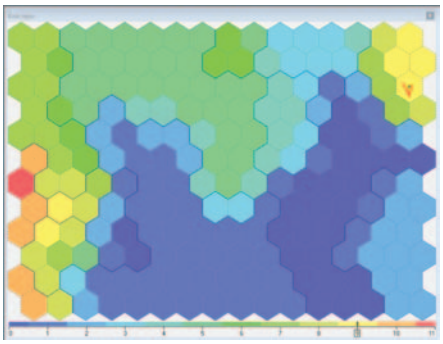

Рис. 4. Положение 1

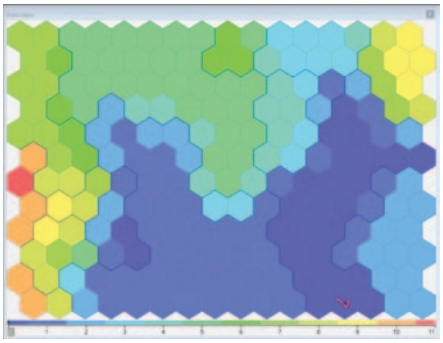

Рис. 5. Положение 2

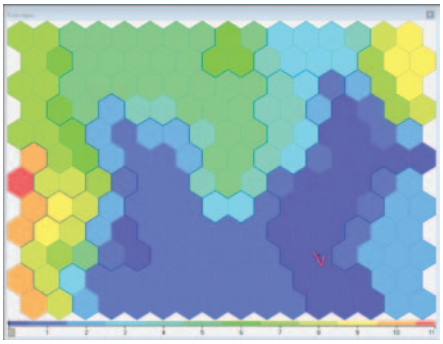

Рис. 6. Положение 3

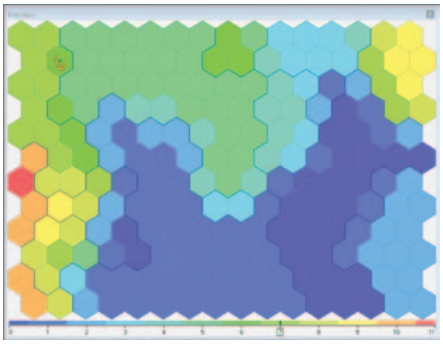

Рис. 7. Положение 4

типовых схем, мы предложили выявлять эти схемы с помощью т.н. ассоциативных правил.

Обучение ассоциативным правилам или поиск ассоциативных правил — это метод обучения на базе правил обнаружения связей между переменными в большой базе данных.

В нашем случае, мы выявляем связи между отдельными словами в рамках одного диалога. Например,

злоумышленники представляются сотрудниками службы безопасности банка и просят сообщить CVC-код карты. В этом случае, появляется ассоциация между словосочетаниями «служба безопасности» и CVC-код. Наличие данной ассоциации является индикатором мошеннического разговора.

Если мошенники изменят шаблон поведения и будут представляться сотрудниками прокуратуры и просить перевести деньги на зарезервированный счет, то мы можем просто добавить еще одну ассоциацию «прокуратура»-«счет», и, таким образом, наша модель уже сможет учитывать новый шаблон поведения мошенников без необходимости перестройки всей модели в целом.

Для выявления ассоциаций использовался алгоритм Apriori [15-16]. В рамках поиска ассоциативных правил транзакцией будет считаться отдельный телефонный разговор, а каждое слово в данной транзакции – это переменная. Для того, чтобы выявить ассоциации между словосочетаниями, а не между отдельными словами, мы использовали тройные ассоциации. Сочетания более высоких порядков встречаются крайне редко, поэтому мы их не рассматривали. Для примера работы алгоритма рассмотрим одну из последних схем мошенничества, которая появилась сравнительно недавно. Мы назвали ее «Здравствуйте. Меня зовут Александр». Делается звонок с произвольного мобильного телефона. Молодой человек произносит следующую фразу: «Здравствуйте. Меня зовут Александр. Алло, вас плохо слышно. Вы меня слышите?». Потом происходит сброс вызова. Здесь осуществляется прямая манипуляция собеседником, когда человека вынуждают произнести слово «Да». Цель простая – сбор образцов голоса с привязкой к номеру мобильного телефона.

Учитывая тот факт, что сейчас наблюдается бум голосовых помощников от разных сервисов, включая банковские сервисы, данный вид мошенничества очень опасен [17-18].

К номеру мобильного телефона очень часто привязана дебетовая или кредитная карточка, а банки активно продвигают голосовые сервисы, в том числе и операции со счетами [19]. Для подтверждения операций уже не требуется знание CVC-кода, а достаточно произнести голосом владельца карты слово «Да».Транзакцией будет считаться весь диалог. Переменные – слова из данного диалога.

Пусть звонки были от условных Александра, Василия и еще кого-нибудь.

Тогда мы имеем три транзакции вида:

1. {здравствуйте, меня, зовут, Александр, алло, вас, плохо, слышно, вы, меня, слышите}
2. {привет, я, Василий, вы, меня, слышите}
3. {здравствуйте, вы, меня, слышите}

На первом этапе работы алгоритма Apriori имеем парные ассоциации.

(здравствуйте, меня)$_2$
(здравствуйте, зовут)$_1$
(здравствуйте, Александр)$_1$
(здравствуйте, алло)$_1$
....
(вы, меня)$_3$
(меня, слышите)$_3$

Числа после скобок определяют количество повторений данной ассоциации в обучающей выборке (поддержка). Если число близко к единице, то это говорит о том, что данная ассоциация носит случайный характер и может быть отсеяна.

Строго говоря, поддержка определяется по формуле:

$$supp(X) = \frac{\{t \in T; X \in t\}}{|T|} \quad (3)$$

где X — множество переменных, а T — количество транзакций. Т.е. в общем виде это показатель «частотности» данного множества переменных во всех анализируемых транзакциях.

На втором этапе работы алгоритма Apriori выявляем тройные ассоциации. В этом случае парные сочетания с большой поддержкой, выступают в роли единого целого.

По итогам работы второго этапа выявлена единственная тройная ассоциация: (вы меня слышите) с поддержкой равной трем.

На более большом обучающем множестве поддержка данной ассоциации была бы гораздо больше, что говорит о том, что данное словосочетание не является случайным.

Т.е. если в разговоре встретилась данная ассоциация, то данный разговор можно считать подозрительным.

5. Описание работы модуля анализа динамики стоп-слов

Для понимания динамики появления стоп-слов используется график зависимости интенсивности их использования (рис.8). Модуль анализа динамики стоп-слов отслеживает динамику появления стоп-слов по ходу ведения разговора. Она неоднородна и сильно зависит от стадии разговора. Такую динамику можно представить графически (рис.8). На этом рисунке пред-

ставлен график зависимости отношения количества стоп-слов к общему количеству слов, представленному в динамике I(n). Обычно злоумышленник строит свой разговор по определенному сценарию. Сценарий разбивается на этапы, каждый этап имеет свою частоту появления стоп-слов. По графику можно судить о переходе между этими этапами. Что касается разговора, отображенного на рисунке 8, наиболее нагруженная стоп-словами часть представлена в его конце.

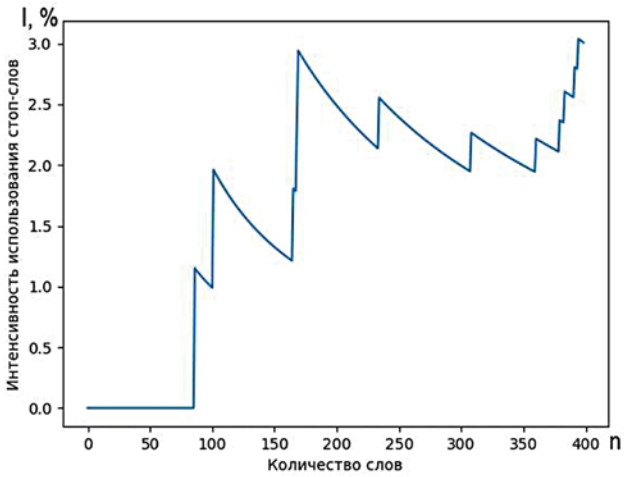

Рис.8. График интенсивности использования стоп-слов

6. Описание работы модуля анализа динамики разговора

Два предыдущих модуля могут работать независимо друг от друга. Однако их эффективность будет сомнительна без взаимодействия друг с другом.

Например, в примере «Здравствуйте. Меня зовут Александр» было выявлено подозрительное словосочетание «вы меня слышите». Однако наличие этого словосочетания в диалоге вовсе не означает, что диалог мошеннический. Вполне возможно, что у собеседника плохо прочищен динамик, и он сам плохо вас слышит.

Поэтому важно объединить оба подхода. С одной стороны, мы отслеживаем факт наличия манипуляции в диалоге, а с другой стороны смотрим, есть ли в диалоге подозрительные фразы.

Если присутствует и манипуляция, и подозрительная фраза, то диалог можно считать мошенническим.

Т.е. в самом простом виде модуль анализа динамики разговора – это простое правило вида:

ЕСЛИ ПРИСУТСТВУЕТ(манипуляция) И ПРИСУТСТВУЕТ(подозрительная фраза) ТОГДА ВЫВОД=мошенничество ИНАЧЕ ВЫВОД=все хорошо.

Однако, на самом деле более правильно было бы оценивать взвешенный вклад каждой из компонент в вывод.

Мы использовали обычный двухслойный персептрон, который в процессе обучения самостоятельно подбирал весовые коэффициенты для каждой из компонент.

7. Заключение

В данной работе был предложен метод выявления телефонных мошенников на основе анализа содержания телефонного разговора. Проверялась эмоциональная составляющая разговора на основе анализа частотных отклонений по каждой букве в диалоге. Цель проверки – выявить факт эмоционального давления на собеседника. Достоинством данного подхода является высокая устойчивость к попыткам обойти эту проверку со стороны мошенников.

Авторами был предложен подход к выявлению подозрительных словосочетаний на основе алгоритма поиска ассоциативных правил Apriori. Достоинством данного подхода является легкая масштабируемость алгоритма и его приспособляемость к новым формам мошенничества без необходимости перестройки существующей модели.

Итоговая классификация диалогов осуществляется с помощью нейронной сети, которая объединяет результаты эмоциональной оценки разговора с выявлением подозрительных словосочетаний в диалоге.

Точность данного метода составила порядка 92%.

Предполагается создание приложения для мобильных телефонов, которое позволит использовать предложенный метод для онлайн-обнаружения факта мошенничества до момента, когда будет нанесен ущерб вызываемому абоненту. Предложенные авторами методы предотвращения телефонного мошенничества могут быть реализованы на базе российской операционной системы в качестве отдельного модуля, рекомендуемого к установке социальным группам высокого риска.

Статья подготовлена в рамках государственного задания правительства Российской Федерации Финансовому университету на 2022 год по теме «Модели и методы защиты текстов в рамках противодействия телефонному мошенничеству» (ВТК-ГЗ-ПИ-30-2022).

Литература

1. Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021, July). Social engineering attacks: Recent advances and challenges. In International Conference on Human-Computer Interaction (pp. 417-431). Springer, Cham. DOI:10.1007/978-3-030-77392-2_27
2. Natarajan, A., Kannan, A., Belagali, V., Pai, V. N., Shettar, R., & Ghuli, P. (2021, November). Spam detection over call transcript using deep learning. In Proceedings of the Future Technologies Conference (pp. 138-150). Springer, Cham. DOI:10.1007/978-3-030-89880-9_10
3. Jacob Devlin, Ming-Wei Chang, Kenton Lee. Kristina Toutanova (2019, May) Bert: Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies (NAACL-HLT), pp 4171–4186
4. Kale, N., Kochrekar, S., Mote, R., & Dholay, S. (2021, July). Classification of Fraud Calls by Intent Analysis of Call Transcripts. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE. DOI:10.1109/ICCCNT51525.2021.9579632
5. 5. Meng, C. X., & ShangGuan, L. C. (2022, January). Abnormal Telephone Recognition Based on Ensemble Learning. In The International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (pp. 1037-1044). Springer, Cham. DOI:10.1007/978-3-030-89698-0_106
6. Yang, X., Yu, W., Wang, R., Zhang, G., & Nie, F. (2020 February). Fast spectral clustering learning with hierarchical bipartite graph for large-scale data. Pattern Recognition Letters, 130, 345-352. https://doi.org/10.1016/j.patrec.2018.06.024
7. Jiang, Z. H., Yu, W., Zhou, D., Chen, Y., Feng, J., & Yan, S. (2020). ConvBert: Improving Bert with Span-based Dynamic Convolution. Advances in Neural Information Processing Systems, 33, 12837-12848.
8. Abid, M. A., Ullah, S., Siddique, M. A., Mushtaq, M. F., Aljedaani, W., & Rustam, F. (2022, May). Spam SMS filtering based on text features and supervised machine learning techniques. Multimedia Tools and Applications, 1-19.
9. Тукаев Р.Д. Эволюция гипнотерапии: методические аспекты // Вестник психотерапии. 2020. № 76 (81). С. 7-29.
10. Кубекова А.С., Мамина В.П. Техники эриксоновского гипноза в деятельности психолога // Психология служебной деятельности: достижения и перспективы развития. Санкт-Петербург, 2020. С. 879-880. .К. Кулиева. — СПб.: Скифия-принт, 2020. — 1052 с. ISBN 978-5-98620-481-9
11. Kale, N., Kochrekar, S., Mote, R., & Dholay, S. (2021, July). Classification of Fraud Calls by Intent Analysis of Call Transcripts. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE. DOI:10.1109/ICCCNT51525.2021.9579632
12. Asha, R. B., & KR, S. K. (2021, January). Credit Card Fraud Detection Using artificial neural network. Global Transitions Proceedings, 2(1), 35-41. DOI:10.1016/j.gltp.2021.01.006
13. Shrestha, A., & Mahmood, A. (2019). Review of Deep Learning Algorithms and Architectures. IEEE access, 7, 53040-53065. DOI:10.1109/ACCESS.2019.2912200
14. Roh, Y., Heo, G., & Whang, S. E. (2019, October). A Survey on Data Collection for Machine Learning: A Big Data-Ai Integration Perspective. IEEE Transactions on Knowledge and Data Engineering, 33(4), 1328-1347. DOI:10.1109/TKDE.2019.2946162
15. Edastama, P., Bist, A. S., & Prambudi, A. (2021, October). Implementation of Data Mining on Glasses Sales Using the Apriori Algorithm. International Journal of Cyber and IT Service Management, 1(2), 159-172. DOI:10.34306/ijcitsm.v1i2.46
16. Singh, P. K., Othman, E., Ahmed, R., Mahmood, A., Dhahri, H., & Choudhury, P. (2021). Optimized recommendations by user profiling using apriori algorithm. Applied Soft Computing, 106, 107272. https://doi.org/10.1016/j.asoc.2021.107272
17. Subudhi, S. R. I. H. A. R. I. (2019). Banking on artificial intelligence: Opportunities & challenges for banks in India. International Journal of Research in Commerce, Economics & Management, 9(7).
18. Makhija, P., & Chacko, E. (2021). Efficiency and advancement of artificial intelligence in service sector with special reference to banking industry. In Fourth Industrial Revolution and Business Dynamics (pp. 21-35). Palgrave Macmillan, Singapore.
19. Theuri, J., & Olukuru, J. (2022). The impact of Artificial Intelligence and how it is shaping banking (No. 61). KBA Centre for Research on Financial Markets and Policy Working Paper Series.

NEURAL NETWORK METHODS FOR RECOGNIZING SPEECH EMOTIONS TO COUNTER FRAUD IN TELECOMMUNICATION SYSTEMS

Filimonov A.V.[8], Osipov A.V.[9], Pleshakova E.S.[10], Gataullin S.T.[11]

8 Andrey V. Filimonov, Ph.D. of Physico-mathematical Sciences, Associate Professor, Ivanovo Chemical-Technological University, Ivanovo, Russia. E-mail: remueur@yandex.ru

9 AlekseyV. Osipov, Ph.D. of Physico-mathematical Sciences, Leading Researcher of the Information Security Department of the Faculty of Information Technologies and Big Data Analysis of the Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: avosipov@fa.ru

10 Ekaterina S. Pleshakova, Ph.D. of Engineering Sciences, Associate Professor of the Information Security Department of the Faculty of Information Technologies and Big Data Analysis of the Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: espleshakova@fa.ru

11 Sergey T. Gataullin, Ph.D. of Economic Sciences., Dean of the Faculty of Digital Economy and Mass Communications of the Moscow Technical University of Communications and Informatics, Leading Researcher of the Information Security Department of the Faculty of Information Technologies and Big Data Analysis of the Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: s.t.gataullin@mtuci.ru

The purpose of the article *is to develop a method for detecting fraud in telecommunication systems based on the analysis of the content of a telephone conversation, based on the use of neural network methods for recognizing speech emotions.*

Research methods: *analysis of the frequency characteristics of text representations of conversations with scammers and the dynamics of their change, analysis of the occurrence of keywords*

Result: *a new approach to detecting fraud in telecommunications systems based on the analysis of the emotional and semantic components of dialogues with fraudsters using neural networks and association rules is proposed. A generalized scheme of the method for detecting signs of fraud in telephone conversations is described. A scalable approach to identifying suspicious phrases based on the Apriori association rule search algorithm is proposed. A multicomponent neural network with a differentiated architecture has been created. A study was conducted on how the emotional component of dialogues with scammers changes in dynamics, in order to identify typical patterns of emotional pressure. A software prototype has been created that allows you to assess the presence / absence of emotional pressure in a conversation with scammers and assess whether the conversation is suspicious or not. The accuracy of the proposed method for detecting telephone fraudsters was evaluated.*

Scientific novelty: *a new natural language processing technology based on artificial intelligence methods is proposed.*

Keywords: *Neural networks, association rules, phone fraud, manipulation, phishing, extortion*

References

1. Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021, July). Social engineering attacks: Recent advances and challenges. In International Conference on Human-Computer Interaction (pp. 417-431). Springer, Cham.
2. Natarajan, A., Kannan, A., Belagali, V., Pai, V. N., Shettar, R., & Ghuli, P. (2021, November). Spam detection over call transcript using deep learning. In Proceedings of the Future Technologies Conference (pp. 138-150). Springer, Cham.
3. Kenton JDMWC, Toutanova LK (2019) Bert: Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies (NAACL-HLT), pp 4171–4186
4. Kale, N., Kochrekar, S., Mote, R., & Dholay, S. (2021, July). Classification of Fraud Calls by Intent Analysis of Call Transcripts. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
5. Meng, C. X., & ShangGuan, L. C. (2021, July). Abnormal Telephone Recognition Based on Ensemble Learning. In The International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (pp. 1037-1044). Springer, Cham.
6. Yang, X., Yu, W., Wang, R., Zhang, G., & Nie, F. (2020). Fast spectral clustering learning with hierarchical bipartite graph for large-scale data. Pattern Recognition Letters, 130, 345-352.
7. Jiang, Z. H., Yu, W., Zhou, D., Chen, Y., Feng, J., & Yan, S. (2020). Convbert: Improving bert with span-based dynamic convolution. Advances in Neural Information Processing Systems, 33, 12837-12848.
8. Abid, M. A., Ullah, S., Siddique, M. A., Mushtaq, M. F., Aljedaani, W., & Rustam, F. (2022). Spam SMS filtering based on text features and supervised machine learning techniques. Multimedia Tools and Applications, 1-19.
9. Tukaev R.D. The evolution of hypnotherapy: methodological aspects / Bulletin of psychotherapy. 2020. No. 76 (81). pp. 7-29.
10. Kubekova A.S., Mamina V.P. Techniques of Ericksonian hypnosis in the activity of a psychologist / Psychology of official activity: achievements and development prospects. St. Petersburg, 2020, pp. 879-880.
11. Kale, N., Kochrekar, S., Mote, R., & Dholay, S. (2021, July). Classification of Fraud Calls by Intent Analysis of Call Transcripts. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
12. Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), 35-41.
13. Shrestha, A., & Mahmood, A. (2019). Review of deep learning algorithms and architectures. IEEE access, 7, 53040-53065.
14. Roh, Y., Heo, G., & Whang, S. E. (2019). A survey on data collection for machine learning: a big data-ai integration perspective. IEEE Transactions on Knowledge and Data Engineering, 33(4), 1328-1347.
15. Edastama, P., Bist, A. S., & Prambudi, A. (2021). Implementation of data mining on glasses sales using the apriori algorithm. International Journal of Cyber and IT Service Management, 1(2), 159-172.
16. Singh, P. K., Othman, E., Ahmed, R., Mahmood, A., Dhahri, H., & Choudhury, P. (2021). Optimized recommendations by user profiling using apriori algorithm. Applied Soft Computing, 106, 107272.
17. Subudhi, S. R. I. H. A. R. I. (2019). Banking on artificial intelligence: Opportunities & challenges for banks in India. International Journal of Research in Commerce, Economics & Management, 9(7).
18. Makhija, P., & Chacko, E. (2021). Efficiency and advancement of artificial intelligence in service sector with special reference to banking industry. In Fourth Industrial Revolution and Business Dynamics (pp. 21-35). Palgrave Macmillan, Singapore.
19. Theuri, J., & Olukuru, J. (2022). The impact of Artficial Intelligence and how it is shaping banking (No. 61). KBA Centre for Research on Financial Markets and Policy Working Paper Series.