РАЗРАБОТКА МОДЕЛИ ПОВЕДЕНИЯ ЗЛОУМЫШЛЕННИКА, ОСУЩЕСТВЛЯЮЩЕГО ДЕЙСТВИЯ ПО ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПРИМЕНИТЕЛЬНО К АВТОМАТИЗИРОВАННЫМ БАНКОВСКИМ СИСТЕМАМ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. В работе описывается процесс разработки модели нарушителя, осуществляющего легализацию (отмывание) доходов, полученных преступным путем. Рассмотрены основные положения 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» с целью выявления обязательных к соблюдению правовых норм, а также паттернов мошеннического поведения пользователей. Выявленные особенности платежного поведения необходимы при разработке паттернов отклонения для автоматизации процессов выявления мошенничества в банковских системах дистанционного обслуживания и их интеграции с искусственным интеллектом.

Ключевые слова: поведенческие модели; легализация (отмывание) доходов; системы дистанционного банковского обслуживания; финансовый мониторинг; платежное поведение пользователей; мошенничество; информационная безопасность.

DESIGNING OF THE MODEL OF BEHAVIOR AN ATTACKER APPLICABLE TO AUTOMATED BANKING SYSTEMS OF REMOTE SERVICING, PERFORMING ACTIONS FOR THE LEGALIZATION PROCEEDS FROM CRIME

M. Fedosenko, *Security Information Technology ITMO University.*

Annotation. The paper describes of compiling the model of offender for the process of legalizes (launders) proceeds from crime. The paper are considered the main provisions of 115 federal law «On countering the legalization of illicit gains (money laundering) and terrorism financing» in order to identify necessary legal norms, as well as patterns of fraudulent user behavior. The revealed features of payment behavior are necessary for developing deviation patterns for automating fraud detection processes in remote banking systems and their integration with artificial intelligence.

Keywords: behavioral models; legalization (laundering) of income; remote banking system; financial monitoring; payment behavior of users; fraud; information security.

Введение

Задача обеспечения информационной безопасности платежных данных является ключевой для организаций финансового сектора, в том числе важной задачей для организаций, осуществляющих банковскую деятельность. Ключевой особенностью данных организаций, помимо защиты собственных вычислительных ресурсов и обеспечения соблюдения норм ФСТЭК, является защита своих клиентов – физических и юридических лиц от мошеннических действий со стороны. Основным способом отъема денег у физических лиц является применение

социальной инженерии и атаки на пользовательское программное обеспечение [1]. Однако, в процессе своей деятельности, банковские организации, также обязаны обеспечить соблюдение норм Федерального закона 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (кратко – закон о противодействии легализации доходов)[1], при этом не допускать использование своих услуг в качестве инструмента осуществления незаконных финансовых операций. Для достижения цели, мошенники используют различные финансовые институты, основным из которых являются банки [2]. Причем в данном случае, нарушителем является обслуживаемое лицо, действия которого необходимо тщательно контролировать и пресекать в случае необходимости. Это доставляет массу неудобств, поскольку одной из обязанностей финансовых организаций в рамках этого закона является выявление и предотвращение осуществления данных деяний (статья 7).

Анализ положений Федерального закона о противодействии легализации доходов (115-ФЗ)

На основе вышесказанного, при разработке моделей злоумышленников, применимых к банковским системам дистанционного обслуживания, необходимо прежде всего учитывать положения закона о противодействии легализации доходов. Рассмотрим основные понятия, используемые в данном федеральном законе, согласно статье 3:

- доходы, полученные преступным путем – денежные средства или ценное имущество, которое было получено в результате преступной деятельности;
- легализация (отмывание) доходов – придание законного статуса денежным средствам, полученным в результате преступной деятельности для их дальнейшего пользования и владея на официальных основаниях;
- процедура замораживания (блокирования) денежных средств и ценных бумаг – адресованный владельцу запрет на осуществление операций с данным имуществом в силу наличия признаков возможного их причастия к незаконным финансовым сделкам или финансирования экстремизма и терроризма.

Таким образом, финансовые организации являются прямым посредником в осуществлении указанных действий. Однако, задача по их выявлению и предотвращению имеет ряд сложностей. Они заключаются в том, что преступники хорошо мимикрируют незаконные сделки под законные с целью осуществления легальных операций с нелегальными денежными средствами. Иначе говоря, в данных транзакциях достаточно сложно выявить мошеннические признаки в силу их отсутствия как такового.

Построение модели нарушителя

При реализации системы противодействия легализации денежных средств, стоит прежде всего описаться на нормы 115-ФЗ, а именно на те характеристики, которые подлежат обязательной проверке в рамках данного закона. Согласно статье 6, имеем следующую совокупность:

- Сумма транзакции больше 600 тыс. руб. для любых физических и юридических лиц.

[1] Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» N 115-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения 15.11.2022).

- Сделки с имуществом на сумму больше 3 млн руб.
- Сделки на сумму больше 10 млн руб. для лиц, имеющих стратегическое значение для оборонно-промышленного комплекса и безопасности РФ.
- Операции, осуществляемые с иностранной структурой, обладающие самостоятельной правоспособностью.
- Почтовый перевод на сумму больше 100 тыс. руб.
- Операции по возврату аванса на сумму больше 100 тыс. руб.
- Операции на сумму свыше 10 тыс. руб. для лиц, о которых установлены сведения о причастности к осуществлению незаконных финансовых операций (например, перечень Росфинмониторинга).

Как было упомянуто ранее, перечень включает действия, подлежащие обязательной проверке. Однако факт проведения данных проверок не гарантирует выявления мошенников в силу того, что осуществление указанных операций происходит и в повседневной жизни легитимных клиентов банка в то время, как мошенники различными способами избегают осуществление указанных операций. Следовательно, использование только перечня информации, указанной в 115-ФЗ не является достаточным условием, но является необходимым – в силу обязательности проведения данных проверок на законодательном уровне.

Для построения качественной модели выявления незаконных финансовых операций необходимо исследовать особенности их осуществления и характеристики осуществляющих лиц [3]. Для этого нужно привести описание процесса, которое состоит из следующей последовательности:

1. Деньги и другие ценности получены в результате совершения преступления.
2. Их необходимо ввести в официальный и контролируемый оборот для возможности дальнейшего использования с официальным статусом.
3. Для этого их необходимо отразить в официальных документах, платежных поручениях, транзакциях.
4. Поскольку данные финансы не задействованы в легитимных сделках, то их нужно создать фиктивным путем.
5. Для фиктивных сделок необходимы фиктивные лица: юридические и физические.
6. Фиктивные сделки необходимо оформить по официальным документам и выдать за настоящие.
7. По данным документам необходимо выполнить платежные операции с незаконно полученными денежными средствами.
8. Платежные операции необходимо повторить несколько раз с целью окончательного перевода денежных средств от фиктивных лиц к их настоящему владельцу.

Из описанной последовательности действий по приданию законного статуса деньгам и финансовым ценностям следует, что основной упор при моделировании данного процесса с целью использования в качестве опорной информации для выявления мошеннических транзакций стоит сделать на его субъекты, а именно физические и юридические лица.

Выделение параметров модели для выявления нарушителя в банковских системах дистанционного обслуживания

В настоящее время практически во всех сферах жизни общества наблюдается активное внедрение информационных технологий. Их развитие обусловлено современным техническим прогрессом, основная задача которого –

упростить жизнь людям. Технологии являются не идеальными, точнее – не имеют идеальную защиту. То, что было создано человеком – человеком может быть и сломано. И сломанная информационная система приносит большие убытки. Преступники, совершающие атаки на информационные системы называются киберпреступниками. Их атаки – киберугрозами. А меры, направленные на предотвращение и недопущения киберпреступниками киберугроз – кибербезопасностью. У злоумышленников существует несколько основных целей для атак. Проведя исследование принципов и механизмов работы компаний, осуществляющих незаконный оборот денежных средств, в достижении цели которых необходимо обеспечить непримечательность финансовых операций, были выделены основные моменты субъектов, которые прямо или косвенно могут указывать на правонарушение. В силу свойства мимикрии, перечень не является исчерпывающим, а совпадение по тем или иным пунктам не дает стопроцентной гарантии, что мошенник найден [4]. Но рассматривая совокупность признаков и обучая модели искусственного интеллекта выявлять их взаимосвязь, задача по выявлению подозрительных лиц в рамках легализации денежных средств, а также уменьшении числа ложных подозреваемых среди легитимных пользователей платежных сервисов является решаемой. Среди основных характеристик, присущих большинству лиц, причастных к преступлениям, предусмотренным 174 статьей УК РФ[2], выделяют следующие:

- Наличие сведений о причастии субъекта к осуществлению незаконных финансовых операций: физическое или юридическое лицо находится в перечне Росфинмониторинга [5, 6] или стоп-листах различных финансовых организаций, или ранее было осуждено по статьям 174, 198, 199 УК РФ. Наличие лица в данных перечнях является вполне исчерпывающим основанием для приостановки финансовой операции, осуществляемой данным лицом, однако его недостаточность заключается в том, что не далеко не всегда ранее оступившиеся лицо вновь совершает неправомерную деятельность. Регулярное блокирование (заморозка) его операций приведет к неудовлетворенности лица качеством оказываемых банком услуг, хоть и является аргументированной в рамках 115-ФЗ.
- Срок жизни юридического лица менее 3-х месяцев: фирма была недавно зарегистрирована и/или осуществляет свою первую финансовую сделку. В рамках 115-ФЗ такая операция должна проходить обязательную проверку, однако если углубиться в более детальную информацию об операции (сумма транзакции, контрагент, причина) – то большинство сделок не осуществляется с целью легализации в силу своей неэффективности для преступников. Также, большинство имеющихся юридических лиц ведут законную деятельность вне зависимости от срока жизни. Учет данного фактора в совокупности с другими позволит сократить количество ложных срабатываний системы, что повысить лояльность клиентов к банку.
- Суммы транзакции, близкие к 600 тыс. руб.: поскольку данная сумма является граничной между допустимостью и обязательностью проверки транзакции в рамках 115-ФЗ, то мошенники не будут ее превышать. Однако транзакции, приближающиеся к данной сумме, все же стоит учитывать, поскольку они дают мошенникам максимальную эффективность в обороте денежных средств.

[2] Уголовный кодекс Российской Федерации N 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_law_10699/ (дата обращения 15.11.2022).

- Сделки с недвижимостью на суммы, превышающие 3 млн. руб.: положения 115-ФЗ позволяют проверять обстоятельства каждой такой сделки. Осуществление данной операции имеет целесообразность проверки для исключения прочих возможных случаев осуществления мошеннических операций. Однако купля/продажа недвижимости заверяется нотариусом, что в свою очередь уменьшает вероятность ее нелегитимности. Однако проведение дополнительной проверки со стороны банка не является избыточным
- Оплаты по аренде, долговым обязательствам: подавляющее большинство сделок, направленных на отмывание финансов, производятся в сфере нематериальных благ, что является противоположностью предыдущему пункту. Дело в том, что нематериальное проще придумать, описать в рамках договора, выставить стоимость, которую сложно оспорить и однозначно оценить. Поэтому, мошенники активно пользуются данным свойством и успешно мимикрируют под легитимные документы аренды и долговых обязательств. Однако сам по себе пункт не может являться исчерпывающим и оцениваться должен исключительно в совокупности с остальными.
- Выплаты за выигрыши (азартные игры, лотерея): аналогичным предыдущему пункту, в качестве выигрыша можно указать любую сумму и любого получателя, вне зависимости от его статуса. Сложнее обстоят дела с документальным оформлением, в силу необходимости уплаты налогов, регистрации выигрышей и азартной деятельности. Немаловажным является и тот факт, что данные сделки пользуются особым вниманием отделов по борьбе с экономическими преступлениями в силу законодательных ограничений на осуществление данного вида деятельности[3]. Аналогичным образом должны проверяться все транзакции, попадающие под данное назначение платежа.
- Общий классификатор видов экономической деятельности (ОКВЭД) [7]: осуществление незаконной предпринимательской деятельности возможно вне зависимости от регистрации ее вида. Однако выявление мошеннических лиц по ОКВЭД имеет место быть в силу того, что мошенники будут выбирать деятельность, которая в теории будет иметь финансовые операции большого объема, при этом, с минимальной документальной нагрузкой. Согласно исследованию, наиболее часто встречающимися категориями в процессе отмывания доходов являются следующие: 41, 43 – Строительство, 58 – Деятельность издательская, 62 – Разработка компьютерного ПО, 66 – Страхование и финансовые услуги, 73 – Реклама, 74 – Научная и техническая деятельность, 92 – Азартные игры и лотерея.
- Возраст физического лица: данный количественный показатель не может свидетельствовать о причастности индивида к преступной деятельности. Однако есть логическая закономерность: в большинстве случаев, фиктивными лицами при осуществлении незаконного оборота денежных средств являются наиболее финансово уязвимые лица: студенты, в силу невозможности иметь полноценную работу в связи с учебой, пенсионеры – в силу слабой финансовой грамотности и невозможностью работать. Данные категории выступают номинальными руководителями фирм-

[3] Федеральный закон «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» N 244-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_64924/ (дата обращения 15.11.2022).

однодневок или в качестве посредника при осуществлении транзакций. Показатель необходимо рассматривать лишь при наличии подозрений данного лица в участии в незаконной деятельности на основании рассмотренных ранее пунктов.

- Наличие информации об асоциальном поведении: данный показатель стоит учитывать при анализе лица, осуществляющего подозрительные транзакции. Это связано не только с тем, что он может вновь осуществлять противозаконную деятельность, но и уязвимость данных лиц быть номинально задействована в процессе незаконного оборота денежных средств в силу финансовых трудностей, круга общения, в силу неосведомленности. В эту же категорию стоит отнести лиц, имеющих или ранее имевших проблемы с законом. В данном случае стоит руководствоваться имеющейся у финансовой организации исчерпывающей информацией о данном лице.

Сравнение положений модели с видами банковского мошенничества, основанного на применении социальной инженерии

Как было упомянуто ранее, совпадение одного из признаков не может являться исчерпывающим для отнесения лица к разряду мошенников. Однако совпадение их совокупности является достаточным основанием для замораживания (блокировки) конкретной транзакции или в целом денежных средств лица для проведения дополнительной проверки силами отделов по борьбе с экономическим мошенничеством. Иначе обстоят дела для случаев выявления мошенничества при использовании методов социальной инженерии, где совпадение одного из признаков является весомым поводом для приостановки платежа. Далее, в табл. 1 приведена сравнительная характеристика признаков, которые будут использоваться в дальнейшем при формировании экспериментального набора данных и в качестве предикторов при построении моделей машинного обучения.

Таблица 1.

Социальная инженерия	**Легализация (отмывание) доходов**
Необходимо руководствоваться показателем отличия в поведенческих характеристиках пользователя. • Большое число транзакций *(C)* в единицу времени (*«C»* индивидуальна для каждого клиента на основе его стандартного платежного поведения). • Сумма транзакции *(S),* диапазон отличий ее суммы от стандартного поведения (*«S»* индивидуальна для каждого клиента). • Отличие региона транзакции (с учетом регионов с повышенным фродом), наличие «телепорта».	Учитывается совокупность факторов на основе анализа информации о данном физическом или юридическом лице. • Нахождение лица в реестре Росфинмониторинга или стоплисте. • Время регистрации юридического лица менее 3-х месяцев. • Суммы транзакции, близкие к 600 тыс. руб. • Сделки с недвижимость на сумму> 3 млн руб. • Осуществление платежей по арендным и долговым обязательствам. • Выплаты за выигрыши (азартные игры, лотерея).

• Взаимодействие с контрагентом, известным как нелегитимный. • Предшествующие данному поведению звонки клиенту, сообщение платежных реквизитов подозрительным источникам [1].	• ОКВЭД (41, 43 – Строительство, 58 – деятельность издательская, 62 – Разработка компьютерного ПО, 66 – Страхование и финансовые услуги, 73 – Реклама, 74 – Научная и техническая деятельность, 92 – Азартные игры и лотерея). • Возраст лица (до 22 лет, от 65 лет). • Наличие сведений о проблемах с законом.

На рис. 1 представлена схематическая модель злоумышленника, отражающая наиболее важные паттерны, необходимые для срабатывания правил по выявлению мошеннических действий для решения задачи автоматизации работы систем дистанционного банковского обслуживания.

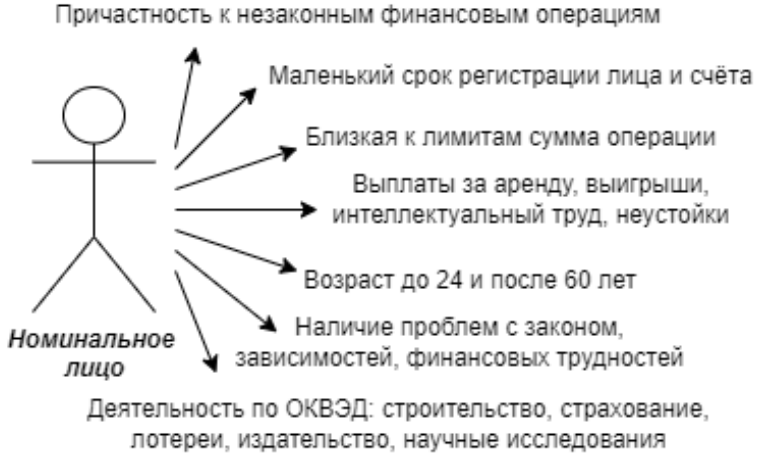

Рисунок 1

Использование данных характеристик их особенностей, подробно рассмотренных в табл. 1, также имеет важное значение для разработки банковских систем противодействия мошенничеству на основе искусственного интеллекта при использовании больших наборов данных пользовательских транзакций для обучения системы с последующей классификацией и кластеризации паттернов пользовательского поведения [8].

Заключение

Действия нарушителей, направленные на легализацию (отмывание) доходов, полученных преступным путем, являются основным источником мошеннических действий в финансовой сфере. Однако, процесс по выявлению и недопущению подобного рода деятельности имеет тесное соприкосновение с информационной безопасностью, а автоматизация данного процесса с компьютерной криминалистикой [8]. В процессе разработки паттернов пользовательского поведения, сигнализирующих о незаконной финансовой деятельности, аналитика сталкивается со следующими сложностями:

1. Необходимость обеспечить четкое соблюдение положений законодательства «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2. Необходимость при четком соблюдении законодательства минимизировать ложные срабатывания системы для легитимных пользователей финансовых услуг, характер которых имеет схожесть с положениями 115-ФЗ.
3. Высокая степень мимикрии злоумышленников под легитимное поведение пользователей и большая степень проработки характера платежей под минимальное попадание под законодательные ограничения.

Для решения задачи качественного выявления мошеннических деяний, особенно при помощи искусственного интеллекта и средств автоматизации, разработка пользовательских моделей поведения и выявления из них паттернов отклонения является важным этапом. Ключевой особенностью деяний по легализации (отмыванию) доходов, полученных преступным путем, в отличии от очевидного мошенничества, осуществляемого против пользователей, является легитимный характер платежных операций. Поэтому, в вопросе формирования моделей поведения, необходим комплексный подход, учитывающий множество факторов (в том числе косвенных) и их взаимосвязь между собой [3]. В тоже время, совпадения косвенных признаков, не всегда являются нелегитимным характером операции и не могут являться неоспоримым доказательством в суде. Поэтому, в данной задаче, роль систем дистанционного банковского обслуживания на основе искусственного интеллекта имеет вспомогательный характер, и заключается в срабатывании на основе подозрительных признаков, автоматизированная корреляции которых помогает в процессе обязательного в рамках законодательства мониторинга финансовых операций. Ключевая роль в процессе анализа и принятия решения отводится аналитикам, специалистам по безопасности, а во время развития компьютерных технологий и специалистов в области информационной безопасности, машинного обучения, разработке программного обеспечения.

Литература

1. Менщиков А.А., Федосенко М.Ю. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество систем связи, 2021. – № 4 (22). – С. 36-47.
2. Гордюк Е.Ю. Тенденции в работе банков с клиентами, подпадающие под действие федерального закона № 115-ФЗ // Парадигмальные стратегии науки и практики в условиях формирования устойчивой бизнес-модели России: сборник научных статей по итогам Национальной научно-практической конференции, Санкт-Петербург, 03-04 октября 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2019. – С. 99-102.
3. Верников В.А., Коноваленко И.Е. Контроль банками своих клиентов по 115-ФЗ // Экономика и социум: современные модели развития, 2021. – Т. 11. – № 4. – С. 329-356. doi: 10.18334/ecsoc. 11.4.114052.
4. Багандова Л.К. Проблемы нормативно-правового регулирования отношений банков с клиентами в рамках применения федерального закона № 115-ФЗ // Вестник Саратовской государственной юридической академии, 2019. – № 5 (130). – С. 194-201.
5. Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму. [Электронный ресурс], 2021. – URL: https://www.fedsfm.ru/documents/terr-list (дата обращения 15.11.2022).
6. Перечень террористов и экстремистов. [Электронный ресурс]. URL: https://www.fedsfm.ru/documents/terrorists-catalog-portal-act (дата обращения 15.11.2022).

7. ОК 029-2014 (КДЕС Ред. 2). Общероссийский классификатор видов экономической деятельности. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_163320/ (дата обращения 15.11.2022).
8. Менщиков А.А., Федосенко М.Ю. Методы и подходы к предобработки данных платежей при условии сильной несбалансированности классов // Студенческий научно-образовательный журнал «StudNet», 2021. – Т. 4. – № 9.