Е.А. Любякина, Ю.Е. Карякин
Тюменский государственный университет, г.Тюмень

В.Г. Логачев, А.М. Игнатьева
Тюменский индустриальный университет, г. Тюмень

УДК 004.9, 519.6

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОПРЕДЕЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Аннотация. В статье представлено математическое описание процесса выявления несанкционированных переводов денежных средств в системах дистанционного банковского обслуживания. Предложены частные критерии и интегральный критерий для их использования в системе фрод-мониторинга.

Ключевые слова: математическая модель, транзакция, несанкционированный перевод, банковские системы, фрод-мониторинг

В настоящее время вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы являются приоритетным направлением регулятивной и надзорной деятельности центральных банков и финансовых регуляторов во всем мире. Указанное внимание финансовых регуляторов вызвано, прежде всего, стремительным внедрением поднадзорными организациями современных ИТ-технологий, что так же привлекает интерес и внимание криминалитета. При этом, с применением ИТ-технологии сегодня осуществляется значительная доля операций, имеющих финансовые последствия, в первую очередь платежных транзакций.

Проникновение информационных технологий в сферу банковского обслуживания привело к повышению удобства и скорости выполнения транзакций, снижению операционных затрат кредитных организаций, а с другой стороны потребовало внедрения процессов выявления и предотвращения несанкционированных транзакций.

В целях снижения рисков осуществления несанкционированных переводов денежных средств при использовании электронной системы платежей Банком России с 16 марта 2015 года введены дополнительные требования к обеспечению защиты информации, в частности, требования к обеспечению защиты при использовании систем Интернет- и мобильного банкинга, банкоматов и платежных терминалов, платежных карт, внедрение технологий, направленных на подтверждение операции, и использование систем фрод-мониторинга [1].

Совершенствование систем фрод-мониторинга, применяемых в банковской сфере требует разработки нового программного обеспечения, учитывающего вновь возникающие угрозы со стороны кибер-преступников. Это в свою очередь влечет за собой разработку новых математических моделей. При построении математической модели необходимо использовать следующие основные метрики:

- ***точность*** (соотношение количества ошибочно отклоненных платежей к общему количеству легитимных платежей) и полнота (соотношение количества мошеннических платежей, пропущенных моделью, к общему количеству мошеннических платежей) обнаружения;
- ***ускорение реакции*** на изменения и угрозы;
- ***автоматизация*** (соотношение количества платежей, поступивших на верификацию (в том числе, ошибочно) в результате внедрения модели к числу платежей, поступивших на верификацию в ходе привычной процедуры);
- ***снижение трудоемкости*** (сравнение количества человеко-часов, затрачиваемых на анализ одного платежа, до и после внедрения модели).

Метрики можно свести к финансовым показателям, как следствие, обосновать внедрение.

Данные, необходимые для построения и реализации модели поступают из следующих источников:

1) интернет-ресурс для определения местонахождения по IP-адресу (GeoIP);

2) ресурс для вычисления расстояния по геодезической линии между населенными пунктами.

3) списки получателей платежей («черные» и «белые»):

- на основе списка FATF (ПОД/ФТ)
- на основе информации от платежных систем (VISA, MasterCard, НСПК)
- на основе собственных расследований кредитной организации
- на основе истории платежей отправителя платежа
- предопределенные (сервисные организации и локальные поставщики услуг: ТСЖ, муниципальные и государственные организации и т.п.)

4) валютный справочник с сайта cbr.ru для определения типичности признаков валютной операции.

5) справочник БИК и SWIFT кодов с сайта cbr.ru для определения корректности реквизитов платежей.

6) база данных с историей платежей (АБС) для определения типичности сумм платежей, периодичности их совершения

7) база данных СДБО для определения типичности параметров сессии пользователя (ID устройств, IP-адреса, время входа).

Программный модуль, разрабатываемый на основе математической модели должен принять решение:

- пропустить платеж без дополнительной верификации;
- отправить платеж на дополнительную верификацию специалисту кредитной организации;
- отказать платеж без формирования инцидента;
- отказать платеж, заблокировать операции по счету клиента и сформировать инцидент.

Необходимые для принятия решения коэффициенты определяются, отвечая на следующие вопросы.

1. Давно ли клиент использует систему дистанционного банковского обслуживания (СДБО)? Ответ на вопрос определяет коэффициент k_1, поскольку малый период использования (менее 0,5 года) приведет к снижению точности из-за недостаточного количества накопленных данных о поведении пользователя СДБО.

$$k_1 = \begin{cases} 1; & \textit{если более } 0{,}5 \textit{ года}; \\ 0{,}75; & \textit{если менее } 0{,}5 \textit{ года, но более } 0{,}25 \textit{ года}; \\ 0{,}5; & \textit{если менее } 0{,}25 \textit{ года, но более } 0{,}08 \textit{ года}; \\ 0{,}25; & \textit{если менее } 0{,}08 \textit{ года}. \end{cases} \quad (1)$$

2. Реквизиты платежа корректны? Определяется коэффициент k_2, а в случае необходимости создается i-ый инцидент. В инцидент записываются все реквизиты платежа и отправляются на доработку специалисту банка.

$$k_2 = \begin{cases} 1; & \textit{если платеж не отклоняется}; \\ 0; & \textit{если платеж отклоняется}. \end{cases} \quad (2)$$

$$f(i) = \begin{cases} 1; & \textit{если платеж отклоняется не более } 2 \textit{ раз за последние полчаса}; \\ 0; & \textit{если платеж отклоняется впервые}. \end{cases}$$

3. Получатель платежа? «Белый список» получателей формируется по двум критериям. Первый критерий – у банка существует определенны список организаций, если получателем платежа будет любая организация из этого списка реквизиты получателя не проверяются дополнительно сотрудником банка. Второй критерий – отправитель платежа самостоятельно может выбрать получателей, которые будут дополнительно вноситься в «белый список».

$$k_3 = \begin{cases} 1; & \textit{если в "белом списке"}; \\ 0{,}75; & \textit{если ранее платежи от данного отправителя не получал}; \\ 0{,}5; & \textit{если "на подозрении"}; \\ 0{,}25; & \textit{если в "черном списке"}. \end{cases} \quad (3)$$

Получатель относится к «подозрительным», если на его реквизиты за последний час зафиксирован хотя бы один сомнительный платеж.

4. Входил ли пользователь ранее с этого устройства (определяется по ID – это может быть IMEI или MAC-адрес)? Ответ на вопрос определяет коэффициент k_4:

$$k_4 = \begin{cases} 1; & \textit{если "да", неоднократно, в т.ч. и в прошлый раз}; \\ 0{,}75; & \textit{если "да", неоднократно, но предыдущий вход с другого, ранее применявшегося}; \\ 0{,}5; & \textit{если "да", однократно в предыдущий раз}; \\ 0{,}25; & \textit{если "нет"}. \end{cases} \quad (4)$$

5. Какое время прошло с момента последнего входа клиента в СДБО? Время входа клиента в СДБО определяется с помощью последнего времени и текущего. Это время необходимо для расчета изменения GeoIP.

6. Насколько изменилось GeoIP с предыдущего входа?

$$k_6 = \begin{cases} 1; & \textit{если "нет"}; \\ 0{,}75; & \textit{если "да", незначительно, не более 50 км}; \\ 0{,}5; & \textit{если "да", значительно, более 50 км.} \end{cases} \quad (5)$$

7. Провайдер IP-адреса, к какой группе риска относится? Коэффициент доверия определяется при помощи стороннего сервиса, который сообщает к какому группе риска относится провайдер IP-адреса. Веса на коэффициент устанавливаются самостоятельно пользователем.

$$k_7 = \begin{cases} 1; & \textit{если высокий коэффициент доверия}; \\ 0{,}75; & \textit{если средний коэффициент доверия}; \\ 0{,}5; & \textit{если состояние неизвестно или низкий коэффициент доверия.} \end{cases} \quad (6)$$

8. Мог ли пользователь переместиться на такое расстояние со времени предыдущего входа? Коэффициент присваивается в зависимости от отклонения.

Коэффициент состоит из двух составляющих. Первое и самое главное – это рейтинг стран с высоким уровнем криминогенной обстановки. Второе – это расчет условного перемещения за данное время. При этих двух составляющих рассчитываются веса вероятностей.

$$k_8 = \begin{cases} 1; & \textit{если мог с высокой вероятностью, отклонение незначительно}; \\ 0{,}75; & \textit{если мог с низкой вероятностью, отклонение значительно}; \\ 0{,}5; & \textit{если не мог с высокой вероятностью.} \end{cases} \quad (7)$$

9. Время входа типично? Коэффициент, исходя из отклонения

$$k_9 = \begin{cases} 1; & \textit{если типично с высокой вероятностью, отклонение незначительно}; \\ 0{,}75; & \textit{если типично с низкой вероятностью, отклонение значительно}; \\ 0{,}5; & \textit{если не типично с высокой вероятностью.} \end{cases} \quad (8)$$

10. Сумма платежа типична? Все платежи подразделяются на типы. Критерии типичности определяется при помощи истории совершения транзакций клиента. Из этих данных анализируется типы платежей и суммы, на которые производился платеж. Помимо этого, если есть платежи, которые повторяются по типу в течение 30 минут то сумму платежей суммируют.

$$k_{10} = \begin{cases} 1; & \textit{если типична с высокой вероятностью, отклонение незначительно}; \\ 0{,}75; & \textit{если типична с низкой вероятностью, отклонение значительно}; \\ 0{,}5; & \textit{если не типична с высокой вероятностью.} \end{cases} \quad (9)$$

В общем виде формула интегрального критерия с учетом частных критериев (1)-(9) выглядит следующим образом:

$$K = \begin{cases} k_2 \cdot k_3 \cdot k_4 \cdot (k_6 \cdot k_8 + k_9 + k_{10}); & \textit{если } k_1 = 1 \textit{ или } k_1 < 1 \textit{ и } k_3 = 1; \\ k_2 \cdot k_3 \cdot k_4 \cdot (k_6 + k_8 + k_1 \cdot (k_9 + k_{10})); & \textit{если } k_1 < 1 \textit{ и } 0 < k_3 < 1. \end{cases} \quad (10)$$

Таким образом, платежи, имеющие К = 0, отклоняются, СДБО клиента или счет блокируется, регистрируется инцидент для принятия решения оператором. «Идеальный платеж» наберет К = 3 балла.

В зависимости от значений интегрального критерия (10) возникает определенная классификация платежей, требующих реакции персонала:

- сомнительный платеж – платеж, который система пропускает, но помещает получателя в список сомнительных на 1 сутки.
- подозрительный платеж – платеж, который система пропускает только после «ручной» верификации.

Коэффициенты в частных критериях, а также пределы изменения интегрального критерия для последующей классификации платежей могут быть скорректированы при тестировании на учебной выборке банковских платежей и внедрении программного модуля в процессинговой системе ПАО «Запсибкомбанка».

С каждым годом наблюдается рост количества несанкционированных операций с использованием платежных карт посредством сети «Интернет» и мобильных устройств (более половины от всех несанкционированных операций). В качестве основных факторов, влияющих на данную тенденцию, можно выделить растущую популярность сервисов оплаты товаров и услуг в сети «Интернет», а также относительную простоту осуществления таких операций без использования злоумышленниками специальных знаний и средств.

В качестве рекомендуемых к реализации кредитными организациями мер можно отметить информирование клиентов о рисках использования ЭСП, в особенности при использовании сети «Интернет», внедрение технологий, направленных на подтверждение операции, и использование систем фрод-мониторинга. Использование разработанной математической модели в подобных системах требует дальнейшего ее совершенствования с учетом большего количества факторов. При подборе коэффициентов в частных критериях и предельных значений интегрального критерия возможно применение различных математических метод, в частности нейронных сетей, посредством обучения на учебной выборке.

СПИСОК ЛИТЕРАТУРЫ

1. Банк России. Сведения о платежах, распоряжения по которым составлены и переданы в электронном виде клиентами кредитных организаций и самой кредитной организацией. - https://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet010.htm&pid=psrf&sid=ITM_18817
2. Компания Group-IB. Тенденции развития преступлений в области высоких технологий. - http://www.group-ib.ru/media/
3. Федеральный закон «О национальной платежной системе» от 27.06.2011 №161-ФЗ

4. Положение Банка России от 09.06.2012 №382-п «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
5. Стандарт безопасности данных индустрии платежных карт PCI DSS v. 3.2 от 01.04.2016
6. Запсибкомбанк. - https://ru.wikipedia.org/wiki/Запсибкомбанк
7. Транзакция (значения) - https://ru.wikipedia.org/wiki/Транзакция_(значения)
8. Дистанционное банковское обслуживание - https://ru.wikipedia.org/wiki/Дистанционное_банковское_обслуживание.