УДК 002.58(076.9)

ИНТЕЛЛЕКТУАЛИЗАЦИЯ БИЗНЕС ПРОЦЕССА ПРИ ПРОВЕДЕНИИ БАНКОВСКИХ ОПЕРАЦИЙ

В.Я. ИЩЕЙНОВ[1]
С.М. ЧУДИНОВ[2]

[1] Российский государственный гуманитарный университет
[2] ОАО «СуперЭВМ», г.Москва
e-mail:
docent-47@mail.ru
chud35@yandex.ru

В статье рассмотрена методика интеллектуализации бизнес процесса при проведении оплаты платежными картами. Практическая реализации приведена на примере интернет-магазина «Agent.ru».

Ключевые слова: банковская платежная карта, фрод оплата платежная система, уровни опасности.

Банковская платежная карта, является персонифицированным платежным средством и позволяет ее законному держателю производить оплату товаров, услуг. В настоящее время в мире насчитывается свыше миллиарда банковских карточек. Использование компьютерных технологий в сфере платежей, покупок, кредитовании является характерной чертой повседневной жизни. Помимо множества удобства и достоинств, электронные платежные средства имеют и оборотные стороны. Мошенничество с банковскими картами развивается вместе с развитием банковских технологий. Постоянно растет количество преступлений, связанных с преступлениями в сфере информационных технологий. Новые технологии открывают мошенникам доступ к электронным счетам владельцев финансовых средств. Повсеместное использование карт для выплат заработной платы, расчетов в магазинах, получения кредитов привлекает разного рода мошенников, которые постоянно находят новые способы добычи информации о кредитных картах и несанкционированного снятия денежных средств. [1]

Фрод (мошенничество) – умышленные действия или бездействие физических и/или юридических лиц с целью получить выгоду за счет компании и/или причинить ей материальный и/или нематериальный ущерб.

Фрод с банковскими картами подразумевает использование данных вашей пластиковой карты для осуществления операций без вашего ведома. В зависимости от данных вашей карты, которые оказались в руках мошенников, возможны различные незаконные операции с карт счетом:

– если карта просто украдена, но не заблокирована, мошенник может осуществить покупку в магазине, сымитировав вашу подпись, образец которой есть на карте. Если есть карта и ПИН код, то с карты можно снять все денежные средства, если на карту открыт овердрафт, мошенник может снять и деньги по кредитному лимиту;

– перехват пластиковой карты, выпущенной и пересылаемой владельцу по почте. Кража обнаруживается с большим опозданием, в результате отсутствует возможность немедленного блокирования счета; к моменту кражи карточки, как правило, не подписаны, а значит, злоумышленник может поставить свою подпись и легально использовать карточку по своему усмотрению. Выявлены случаи, когда преступники специально устраивались работать на почту или в частные службы доставки, чтобы иметь возможность изымать конверты с пластиковыми банковскими карточками;

– двойная «прокатка» карты через терминалы в магазине. Прокатка карты осуществляется для оплаты, для снятия копии реквизитов карты. Двойная прокатка карты может привести к двойному снятию денег за оказанную услугу, либо покупку;

– мошенничество с использованием минимальных сумм покупки по карте.

Фальшивые карты мошенники используют в туристических поездках, делая вдали от своей страны покупки на небольшие суммы – до 100 долларов. При таких суммах покупки, терминалы магазинов не производят авторизацию счета карты

(терминал не связывается с банком для проверки счета). При покупке считывается только СЛИП карты. СЛИП передается в банк с небольшой задержкой по времени, так же с задержкой по времени обновляется СТОП – ЛИСТ банка. Используя задержки в обработке платежей, мошенник может сделать покупки на внушительные суммы;

– заказ товаров в интернет-магазинах возможен с указанием похищенных реквизитов настоящей карты.

Фродом являются также и операции с поддельными картами. Подделываются кредитные карты так — берётся гибридная карточка (т.е. на карте предоставлены чип и магнитная полоса), копируются записи её магнитной полосы и переносятся на другую карточку только с магнитной полосой или на гибридную карточку с «кривым» чипом (например, сожжённым или неперсонализированным). Операции могут успешно выполняться: в режиме онлайн (в устройствах читающих магнитную полосу), в режиме оффлайн (подлимитные операции) или в режиме fallback (при невозможности читать чип устройство проводит операцию по магнитной полосе). Ответственность за такой фрод ложится на эмитента карточки или на эквайрера (если по правилам конкретной платежной системы возможен перенос ответственности).

Любая организация может быть жертвой мошенничества. Отсутствие контроля над уровнем фрода может привести компанию к большим финансовым потерям и остановке деятельности.

1. Идентификация фродовых платежей «Agent.ru».

Все платежи фиксируются с платежной системе БОПС (бэкофис платежной системы).

БОПС состоит из следующих разделов:

1. Платежи БК (банковской картой)/ Авторизация.
2. Платежи через СПП (систему приема платежей)/Все платежи.
3. Эл. наличность/Все платежи.
4. Счета/Все платежи.

Мошеннические операции отслеживаются в разделе – Платежи БК (банковской картой)/ Авторизация.

Данный раздел предназначен для отслеживания оплат, совершенных с помощью банковских карт. Здесь можно увидеть попытки оплаты клиентом заказа, возникающие ошибки, уровень возможного мошенничества, проведенные суммы возвратов и т.п.

Список платежей может быть отсортирован по любому параметру (по умолчанию – по времени регистрации), как по возрастанию, так и по убыванию значений.

Столбцы имеют следующие значения:

Регистрация: дата и время попытки оплаты заказа клиентом.

Заказ: номер заказа.

Платеж: сумма заказа.

PS: тип карты (VI – Visa, в том числе Electron; CA – MasterCard).

Номер: номер карты.

AT: результат проведения авторизации карты, например:

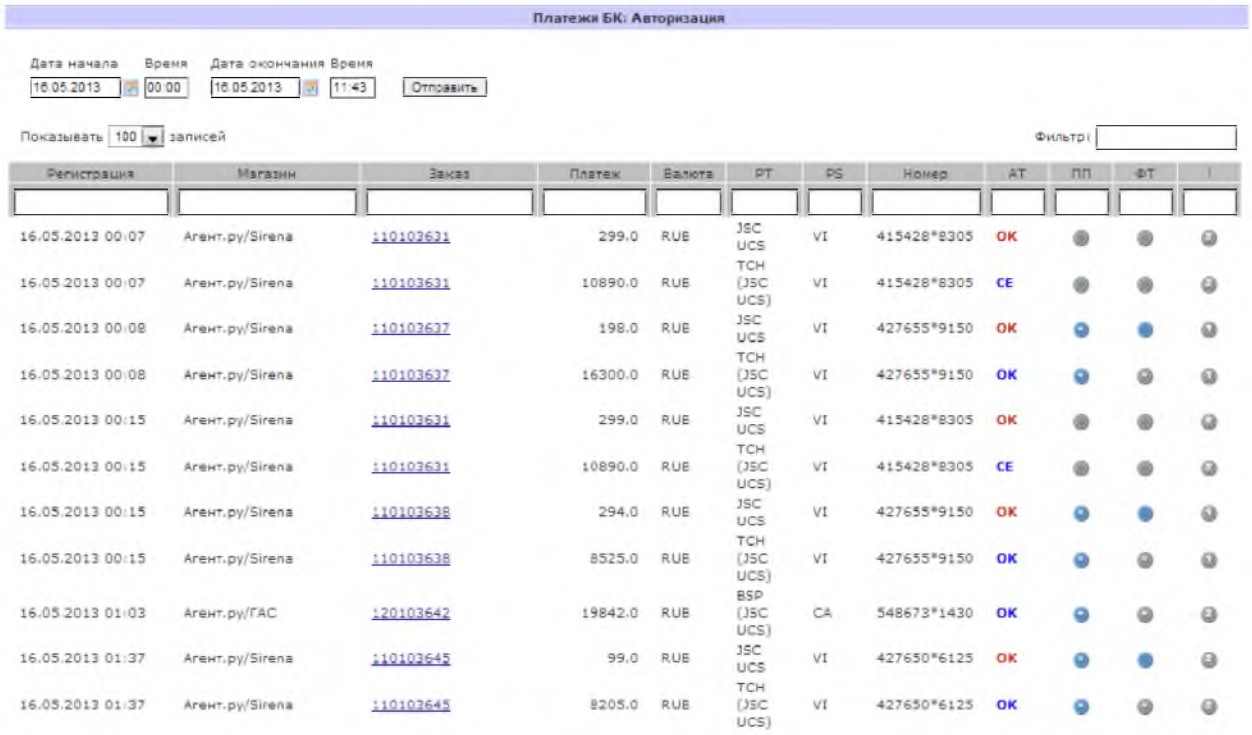
OK – успешная авторизация, деньги на карте заморожены в размере значения графы «платеж». Цвет не имеет значения.

IN – платеж находится в процессе (например, клиент аутентифицирует карту на сайте банка). Он должен смениться на другой статус в течение 10-15 минут.

TD – транзакции по данной карте запрещены, т.е. с ее помощью нельзя оплачивать покупки в интернете.

ПП – отметка о прохождении платежа.

! – признак возможного мошенничества («фрод»). Цифра означает уровень угрозы.



Платежи БК: Авторизация

Дата начала 16.05.2013 Время 00:00 Дата окончания 16.05.2013 Время 11:43 Отправить

Показывать 100 записей Фильтр:

Регистрация	Магазин	Заказ	Платеж	Валюта	PT	PS	Номер	AT	ПП	ФТ	!
16.05.2013 00:07	Агент.ру/Sirena	110103631	299.0	RUB	JSC UCS	VI	415428*8305	OK			
16.05.2013 00:07	Агент.ру/Sirena	110103631	10890.0	RUB	ТСН (JSC UCS)	VI	415428*8305	CE			
16.05.2013 00:08	Агент.ру/Sirena	110103637	198.0	RUB	JSC UCS	VI	427655*9150	OK			
16.05.2013 00:08	Агент.ру/Sirena	110103637	16300.0	RUB	ТСН (JSC UCS)	VI	427655*9150	OK			
16.05.2013 00:15	Агент.ру/Sirena	110103631	299.0	RUB	JSC UCS	VI	415428*8305	OK			
16.05.2013 00:15	Агент.ру/Sirena	110103631	10890.0	RUB	ТСН (JSC UCS)	VI	415428*8305	CE			
16.05.2013 00:15	Агент.ру/Sirena	110103638	294.0	RUB	JSC UCS	VI	427655*9150	OK			
16.05.2013 00:15	Агент.ру/Sirena	110103638	8525.0	RUB	ТСН (JSC UCS)	VI	427655*9150	OK			
16.05.2013 01:03	Агент.ру/ГАС	120103642	19842.0	RUB	BSP (JSC UCS)	CA	548673*1430	OK			
16.05.2013 01:37	Агент.ру/Sirena	110103645	99.0	RUB	JSC UCS	VI	427650*6125	OK			
16.05.2013 01:37	Агент.ру/Sirena	110103645	8205.0	RUB	ТСН (JSC UCS)	VI	427650*6125	OK			

Все заказы, оплаченные онлайн с помощью пластиковых карт, должны проходить проверку у операторов службы поддержки. Проводится данная проверка путем визуального контроля списка заказов в БОПС, в разделе – Заказы по БК /Авторизация.

Платежная система автоматически анализирует и проверяет оплаченные заказы по следующим признакам:

1. Неверный владелец карты.
2. Перевозка в одном направлении.
3. Параметры (телефон или e-mail) заказчика отличаются от параметров держателя карты.
4. Заказчик находится ни в одной из стран маршрута перевозки.
5. Заказчик находится не в стране выпуска карты.
6. Используется вторая карта заказчика.
7. Близкая дата вылета (менее 24 часов до вылета).
8. Более двух заказов одной картой в течение 24 часов с момента первого заказа.
9. Оплата разными картами с одного IP адреса.

Общее количество признаков мошенничества указывается в колонке «**!**» списка заказов цифрой в сером кружочке. Внутри заказа все найденные признаки мошенничества обозначены в блоке «Проверка на мошенничество»

Все заказы со статусом ОК, исходя из количества и совокупности признаков в списке заказов, выделяются цветовой индикацией:

1-й уровень – опасности (важный)

В него входят параметры:

1,8,9 и любая совокупность параметров по признакам от 5 -ти и более.

2-й уровень – средний

В него входят параметры:

2,4,7.

3-й уровень – слабый

В него входят все остальные параметры.

3,5,6.

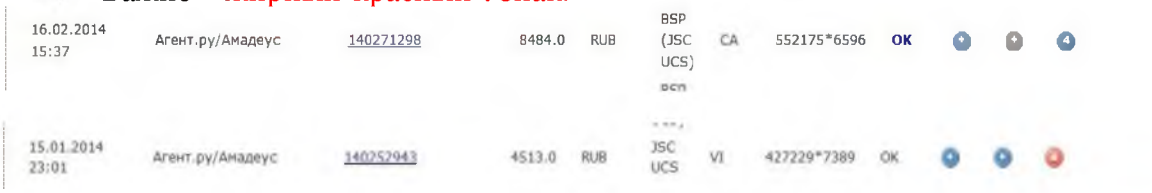
Ряд заказов в списке не имеют цветовой индикации, это значит, что карта, которой был оплачен этот заказ, ранее уже была проверена руководством и по особому распоряжению разрешена к оплате без дальнейшей верификации.

Помимо этого, коды редких типов карт – Diners club и JCB – дополнительно, даже в отсутствие явных признаков мошенничества, подсвечиваются красным в графе «карта» списка заказов.

Основная задача операторов: в процессе рабочего дня постоянно просматривать заказы и по итогам принимать решение о дальнейшей судьбе заказа.

Итог: после проверки заказов кружки меняются:

- Не важно = синий
- Важно = жирный-красный-! знак.



2. Методика выявления форд оплат.

Методика определяет порядок действий персонала, необходимый для своевременного обнаружения и устранения попыток возможных мошеннических оплат банковскими картами, на примере авиаперевозок, забронированных на сайте агентства. [2].

Для определения и предупреждения возможных мошеннических оплат проводится мониторинг показателей, к которым относится:

- предупреждения о возможном мошенничестве;
- попытки оплаты картами эмитированными зарубежными банками;
- количество попыток оплаты с одной и той же картой;
- количество попыток оплаты с одним и тем же заказчиком.

• Мониторинг осуществляется персоналом интернет-магазина в разделе «**Платежи БК/Все платежи**» специализированного веб-ресурса «Backoffice».

Флаги-предупреждения о возможных мошенничествах отображаются в колонке «**!**» на странице со списком платежей.

Цифры на флаге-предупреждении отображают количество обнаруженных подозрений на мошенничество:

1. 0 – СИСТЕМА НЕ ОБНАРУЖИЛА НИ ОДНОГО НЕСООТВЕТСТВИЯ;
- 1-3 – ОБРАТИТЬ ВНИМАНИЕ.
- 4 – МОШЕННИЧЕСТВО ВЕРОЯТНО!
- 5 (и более) – МОШЕННИЧЕСТВО С БОЛЬШОЙ СТЕПЕНЬЮ ВЕРОЯТНОСТИ!!

Выполнение функций определения и предупреждения возможных форд оплат обеспечивают сотрудники агентства, в соответствии с возложенными на них функциональными обязанностями, что представлено в таблице.

Таблица

Должность сотрудника агентства и его функции

Должность	Функция
Оператор интернет-магазина[1]	Осуществление мониторинга признаков предупреждения возможных мошеннических оплат
Администратор интернет-магазина	Проведение действий по проведению анализа «подозрительного» платежа на возможное мошенничество
Лицо, ответственное за принятие решения	Принятие решения о признании платежа мошенническим и возврат денег

[1] В некоторых интернет-магазинах функции оператора и администратора могут быть совмещены.

Оператор интернет-магазина (далее – Оператор) каждые 30 минут[1] обязан осуществлять мониторинг показателей предупреждения о возможных мошенничествах.

Если система отобразила обнаруженные подозрения (флаг «1», «2», «3» и т.д.), Оператор обязан передать информацию о таком платеже (таких платежах) администратору интернет-магазина (далее – Администратору).

Администратор обязан:

1. Ознакомиться с информацией на странице детализации «подозрительного» платежа.

2. Приостановить выполнение финансовой транзакции. Действия в Backoffice: на странице детализации платежа в блоке «Перевод» убрать галочку «К отчету» и нажать кнопку «Отправить».

3. Провести анализ и оценку степени важности обнаруженных подозрений, для чего:

- выполнить рекомендуемые действия по проведению анализа
обнаруженных признаков возможного мошенничества;
- при необходимости получить консультации у сотрудников КОКК по данному платежу для принятия окончательного решения о его законности.

4. В случае принятия решения о том, что данный платеж является законным и не является возможным мошенничеством:

– восстановить выполнение финансовой транзакции (включение платежа в сводный отчет для передачи в КОКК). Действия в Backoffice: на странице детализации платежа в блоке «Перевод» поставить галочку «К отчету» и нажать кнопку «Отправить»;

– отметить платеж пометкой «Не важно», означающей, что платеж проверен и с него снято подозрение на мошенничество. Действия в Backoffice: отметка ставится в блоке «Проверка на мошенничество»;

5. В случае принятия решения о том, что данный платеж является возможным мошенничеством, выполнить следующие действия:

– передать полную информацию о «подозрительном» платеже сотруднику, ответственному за принятие решения о возврате (далее – Ответственный сотрудник), для принятия им решения по дальнейшим действиям с данным платежом;

– отметить платеж пометкой «Важно», означающей, что платеж проверен и с большой степенью вероятности является возможной мошеннической операцией. Действия в Backoffice: отметка ставится в блоке «Проверка на мошенничество.

6. Если в результате принятого решения Ответственным сотрудником, что платеж признается не мошенническим, Администратор обязан выполнить следующий действия:

– восстановить выполнение финансовой транзакции (включение платежа в сводный отчет для передачи в КОКК). Действия в Backoffice: на странице детализации платежа в блоке «Перевод» поставить галочку «К отчету» и нажать кнопку «Отправить»;

– отметить платеж пометкой «Не важно», означающей, что платеж проверен и с него снято подозрение на мошенничество. Действия в Backoffice: отметка ставится в блоке «Проверка на мошенничество».

7. Если в результате принятого решения платеж признан мошенническим, Ответственный сотрудник дает следующие указания соответствующим службам агентства:

– осуществить возврат авиабилета и полный возврат денежных средств по соответствующему заказу;

[1] 30 минут – рекомендуемый интервал мониторинга. Интервал может быть уменьшен или изменен по решению владельца интернет-магазина.

– проинформировать соответствующие службы авиакомпании, на рейс которой была предпринята попытка мошеннической оплаты перевозки, об обнаружении такой попытки и действиях, предпринятых агентством.

Список литературы

1. Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе».
2. Модель безопасности конфиденциальной информации в информационной системе (статья). Чудинов С.М. Научные ведомости БелГУ № 13(132) Выпуск 23\1 раздел Компьютерное моделирование Белгород, 2012г. С. 205-210.

INTELLEKTUALIZACIYA BUSINESS OF PROCESS DURING THE LEADTHROUGH OF BANK TRANSACTIONS

V.J. ISCHEYNOV[1]
S.M. CHUDINOV[2]

[1] RGGU
[2] NII «Super EVM» Moscow

e-mail:
docent-47@mail.ru
chud35@yandex.ru

In the article the method of intellektualizaci is considered business of process during the leadthrough of payment pay maps.

Keywords: banking, payment card frand, the payment, the payment system, levels of risk.