# СОДЕРЖАНИЕ

[1. АНАЛИЗ ПРОБЛЕМАТИКИ ПРЕДМЕТНОЙ ОБЛАСТИ 2](#_Toc488424200)

[1.1. Эквайринг 2](#_Toc488424201)

[1.1.1. История возникновения 2](#_Toc488424202)

[1.1.2. Эквайринг в настоящее время 3](#_Toc488424203)

[1.1.3. Преимущества эквайринга 5](#_Toc488424204)

[1.1.4. Рынок эквайринга в России 6](#_Toc488424205)

[1.1.5. Виды эквайринга 7](#_Toc488424206)

[1.2. Интернет-эквайринг 8](#_Toc488424207)

[1.2.1. Преимущества и недостатки интернет-эквайринга 10](#_Toc488424208)

[1.2.2. Участники интернет-эквайринга 13](#_Toc488424209)

[1.2.3. Способы подключения 17](#_Toc488424210)

[1.3. Обеспечение безопасности платежей 18](#_Toc488424211)

[1.3.1. Антифрод 21](#_Toc488424212)

[1.4. Существующие системы антифрода 23](#_Toc488424213)

[2. ПОСТАНОВКА ЗАДАЧИ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ И ВЫБОР МЕТОДОВ ЕЁ РЕШЕНИЯ 26](#_Toc488424214)

[2.1. Постановка задачи 27](#_Toc488424215)

[2.2. Требования к разработке 28](#_Toc488424216)

[3. ПЛАН РАБОТЫ НАД ДИССЕРТАЦИЕЙ 30](#_Toc488424217)

[ЗАКЛЮЧЕНИЕ 31](#_Toc488424218)

[СПИСОК ЛИТЕРАТУРЫ 32](#_Toc488424219)

# АНАЛИЗ ПРОБЛЕМАТИКИ ПРЕДМЕТНОЙ ОБЛАСТИ

## Эквайринг

### История возникновения

Технический прогресс и развитие товарно-денежных отношений стали предпосылками к появлению банковских карт. Изначально они были созданы в целях упрощения обналичивания средств, хранящихся в банке, однако со временем функционал карт был значительно расширен, и на свет появился эквайринг. Этот термин скрывает за собой очень востребованную услугу, которая сделала банковскую карту инструментом естественного повседневного использования для миллионов людей.

Термин «эквайринг» в переводе с английского означает «приобретение», и используется в банковском сегменте для определения системы приема платежных карт для оплаты товаров и услуг. Проще говоря – это возможность расплатиться кредиткой, не используя наличные. С момента появления этой функции небольшой кусочек пластика, заменяющий «физические» деньги, стал настолько востребован, что многие люди уже не видят возможности обходиться без него. По значимости появление эквайринга вполне можно сопоставить с изобретением мобильного телефона.

Но, как и в случае с мобильными телефонами, изначально эквайринг был достаточно примитивным. Кассиры использовали специальное механическое устройство «импринтер», с помощью которого с карты снимался слип – бумажный «слепок» с ее реквизитами. Это было неудобно и небезопасно, поскольку такое устройство не имело никакой связи с банком, чтобы проверить наличие у покупателя нужной суммы на счете. Впрочем, если речь шла о дорогостоящем приобретении, кассир для уверенности мог позвонить в банк. Позже, с развитием технологий, на свет появился терминал – специальное электронное устройство, обеспечивающее связь с банком во время проведения операции. Сейчас покупки совершаются именно с его помощью [1].

### Эквайринг в настоящее время

Сейчас миллионы организаций, предприятий и магазинов используют эквайринг, отнюдь не только потому, что это удобно. Дело в том, что, предоставляя клиентам возможности оплаты покупки карточкой, организация:

* исключает риск приема фальшивых купюр;
* экономит на инкассации наличности.

Клиент в свою очередь:

* получает удобный способ расчета;
* не беспокоится, что кассир ошибется со сдачей.

Кроме того, принимая кредитки, компании увеличивают объем своих продаж в среднем на 20–30% и приобретают новых платежеспособных клиентов: по статистике обладатели «пластиковых кошельков» более склонны к спонтанным покупкам и легче расстаются с деньгами. Также при установке специального оборудования банка для платежных карт, организация получает различные банковские услуги, участвует в дисконтных программах и т.д.

**Эквайринг** – комплекс услуг по приему банковских карт к оплате в торговой точке. Кредитная организация, которая их оказывает, называется банком-эквайером. Такой банк устанавливает в торговых точках оборудование для приема карт, а также производит все расчеты по операциям с их использованием.

**Банк-эквайер** (по определению ЦБ РФ) – это кредитная организация, осуществляющая расчеты с предприятиями торговли или услуг по операциям, совершаемым с использованием платежных карт, и/или выдающая наличные денежные средства держателям платежных карт, которые не являются клиентами банка-эквайрера. Данная кредитная организация имеет право одновременно проводить эмиссию банковских карт, эквайринг платежных карт, а также распространение платежных карт, что осуществляется на основе внутрибанковских правил, разработанных банком-эквайрером в соответствии с действующим законодательством.

Чтобы воспользоваться эквайрингом, необходимо заключить соответствующий договор с банком. В нем будут отражены условия установки и обслуживания необходимого для работы оборудования, размер комиссионного вознаграждения, срок возмещения денежных средств и т.д. Условия обслуживания формируются банком индивидуально для каждой торговой организации.

Комиссионное вознаграждение банка составляет определенный процент от суммы покупки в торговой точке по банковской карте. Размер его устанавливается банком для каждой торговой организации персонально, так как зависит от многих факторов. Например, от сферы деятельности организации, от ее среднемесячного торгового оборота, от того, как давно она работает на рынке и сколько имеет точек продаж, от объема занимаемой торговой точкой площади, от типа связи и т.д. Следует отметить, что определенный процент от полученной комиссии банк-эквайер отдает платежной системе (в среднем 1,1%) и банку-эмитенту, и это также отражается на ее размере. Иными словами, банк-эквайер с учетом этих выплат не может опустить величину комиссии ниже определенного уровня, ведь тогда он окажется в минусе. Из-за высокой конкуренции на данном рынке комиссии банков находятся примерно на одном уровне и на гране рентабельности, варьируясь в диапазоне от 1,5% до 4% от суммы транзакции. Если оборот предприятия значительный, то комиссия снижается до минимальной отметки, примерно до 1,5%.

Как правило, банки устанавливают и подключают необходимое оборудование, проводят обучения персонала и предоставляют расходные и рекламные материалы бесплатно. В ряде банков оборудование может отдаваться в аренду, за которую необходимо будет вносить ежемесячную плату.

Эквайрингом могут воспользоваться как те торговые предприятия, у которых уже есть расчетный счет в банке, так и те, у которых он не открыт. Это не является обязательным условием банка. Просто в том случае, если у организации нет счета в банке, ей придется предъявлять большее количество документов, необходимых для заключения договора.

Сроки возмещения в банках – от одного до трех дней. Зачастую, если у предприятия расчетный счет открыт в банке-эквайере, зачисление общей суммы операций за день за вычетом банковской комиссии происходит на следующий рабочий день. Если счет открыт в другом банке, то перевод средств осуществляется посредством межбанковских расчетов. В таком случае срок зачисления возмещения увеличивается и может достигать двух-трех дней. Бывает и так, что банки сначала ждут полного возмещения со стороны платежных систем и только после этого осуществляют перевод средств. При таком подходе сроки возмещения могут достигать трех-пяти дней [2].

Эквайринг позволяет торговой организации увеличить количество покупателей, а вместе с тем и оборот средств, снизить затраты на инкассацию и риски по операциям, связанным с наличными денежными средствами.

### Преимущества эквайринга

Для начала стоит отметить, что компания, принимающая для оплаты товаров и услуг банковские карты, выглядит в глазах клиентов престижнее и надежнее, а альтернативный способ расчета обеспечивает дополнительное удобство, что положительно отражается на имидже компании. Ведь покупатели могут без проблем оплачивать свои приобретения любыми картами в любой доступной валюте. Кроме того, эквайринг также увеличивает число потенциальных покупателей, ведь сегодня многие отказываются от шопинга, когда узнают, что к оплате принимается только наличность. А при возможности безналичного расчета, покупатели и пользователи различных услуг чаще тратят больше средств.

* По статистике средний чек по платежной карте выше наличного чека на 30–40%.
* Традиционно, расчетам с использованием банковских карт в большей степени отдают предпочтение состоятельные слои населения. Поэтому эквайринг для организации – это потенциальное увеличение процента обеспеченных клиентов, что увеличивает объемы продаж в среднем на 20–30%. Тем не менее и среди населения со средним доходом наметился существенный рост использования банковских карт для ежедневных покупок или покупок выходного дня.
* Помимо этого, эквайринг обеспечивает экономию средств за счет отсутствия необходимости инкассации наличности и полностью исключает риск приема фальшивых купюр. Банки в свою очередь предоставляют партнерам различные льготы: дисконтные программы, скидки на банковские услуги и т.д., а также проводят бесплатное обучение сотрудников компании.
* Эквайринг выгоден не только покупателям и компаниям, но и банкам, которые получают новые возможности для расширения своей деятельности за счет дополнительных денежных средств и увеличения числа постоянных клиентов.

### Рынок эквайринга в России

Несмотря на популярность во всем мире, в России эквайринг сегодня все еще находится на стадии развития. При этом в последнее время он является одним из приоритетных и наиболее интенсивно развивающихся направлений карточного бизнеса в России. Так, общее количество выпущенных банковских карт в стране уже превысило численность населения с коэффициентом покрытия больше единицы. Конечно, в развитых европейских странах и США данный показатель выше в два, а в некоторых из них – даже в четыре раза.

Одним из важных факторов развития является общий уровень финансовой и банковской культуры населения. В последние десятилетия он значительно вырос, и сегодня все большее количество людей предпочитает безналичный расчет. Карта сегодня воспринимается удобным инструментом для повседневного использования своего счета и доступа к кредитным ресурсам, предоставляемым банком. Компаниям также выгодно упростить процедуру оплаты своих товаров и услуг, а также процесс доставки денег на свой счет в банке.

К сожалению, эксперты единогласно отмечают, что в России развитие эквайринга происходит медленнее, чем хотелось бы и прогнозировалось ранее. Так, 15 лет назад соотношение оплаты наличными деньгами и оплаты картами в торговых сетях составляло 97% и 3% соответственно. Сегодня аналитики приводят цифры 85% (из которых до 70% снято с банковских карт) и 15%. Прогресс очевиден, хотя и очень растянут во времени. Поэтому сегодня задача создать больше возможностей оплаты товаров и услуг картой актуальна не менее, чем 15 лет назад. В развитых странах она решена полностью, а вот для России подобная практика еще не стала правилом.

Таким образом, совершенно очевидно, что любой организации, еще не использующей преимущества эквайринга, при этом желающей развивать бизнес и увеличивать объем продаж, стоит серьезно задуматься о возможности установки оборудования для безналичного расчета. Лидируют на рынке эквайринга Сбербанк, Газпромбанк, Росбанк, «Русский Стандарт».

### Виды эквайринга

Среди видов эквайринга можно выделить:

1. Торговый эквайринг – представлен в магазинах, ресторанах, гостиницах, фитнес-клубах и т.д.;
2. Интернет-эквайринг – относится к покупкам во всемирной сети Интернет с помощью специального интерфейса;
3. ATM-эквайринг – различные терминалы и банкоматы, где можно снять наличность.

Наибольший интерес, как правило, представляет совместная услуга торговой организации и банка, предоставляемая владельцам карт, а именно – торговый эквайринг и интернет-эквайринг, а также то, как в этой сфере осуществляется взаимодействие.

Итак, в случае торгового эквайринга, предприятие, предоставляющее клиентам товары или услуги, для использования эквайринга обязано:

* обеспечить размещение устройств для приема карт на территории своих помещений;
* принимать для оплаты пластиковые карты на основании договора об эквайринговом обслуживании с банком;
* выплатить банку, указанную в данном договоре комиссию за обслуживание.

Банк же обязуется:

* установить на территории организации оборудование для эквайринга (терминалы эквайринга и т.д.);
* обучить работников компании обслуживанию клиентов-держателей платежных карт;
* обеспечить проверку достаточного количества средств на карте в момент проведения операций на оборудовании для торгового эквайринга;
* возместить организации оплаченную с помощью карты сумму в установленные в договоре сроки;
* предоставить организации все необходимые расходные материалы;
* предоставлять профессиональную консультацию при возникновении трудностей в проведении расчетных операций с картами.

Однако в последние годы общество постепенно переходит на покупки товаров и услуг через интернет, и такой подход, рано или поздно, может затмить привычные покупки в магазине, рассмотрим подробнее интернет-эквайринг.

## Интернет-эквайринг

Сегодня продажи в интернете стали такой же обыденностью, как ежедневный ритуал похода в продуктовый магазин. И если к первым появившимся интернет-магазинам люди относились с некой осторожностью и опасались быть обманутыми, то сейчас аудитория стала более чем лояльной. Теперь многие предпочитают приобретать определённую категорию товаров в интернете, так как это удобно и выгодно. И всё больше покупателей готовы совершать онлайн-платежи с использованием банковской карты. Раньше продажи в интернете осуществлялись по следующей схеме: покупатель заказывал товар, его доставлял курьер и на месте принимал оплату. Или же товар отправлялся по почте наложенным платежом. С приходом интернет-эквайринга рассчитываться и принимать оплату за купленный товар стало намного проще. Причём выгоды здесь очевидны как для покупателя, так и для продавца, однако подключение и работа с интернет-эквайрингом достаточно трудоемкая задача.

Этот инструмент позволяет получить доступ к новым группам покупателей и предоставить более привлекательные условия оплаты для новых клиентов. Процесс интернет-эквайринга помогает сократить затраты на поддержание наличных денежных расчетов, инкассацию, обслуживание кассовой техники и т.п.

**Электронная коммерция** – это сфера экономики, которая включает в себя все финансовые и торговые транзакции, осуществляемые при помощи компьютерных сетей, и бизнес-процессы, связанные с проведением таких транзакций.

**Интернет эквайринг** – общий термин, которым обозначается прием платежей по пластиковым картам через Интернет с использованием специально разработанного web-интерфейса. Интернет-эквайринг, как составляющая электронной коммерции, представляет собой деятельность кредитной организации (банка-эквайера), включающую в себя осуществление расчетов с организациями электронной коммерции по операциям, совершаемым с использованием банковских карт в сети Интернет. Подключение организаций электронной коммерции банком-эквайером, как правило, осуществляется при технической поддержке Cервис-провайдеров, которые обеспечивают безопасность платежей, используя протокол аутентификации 3-D Secure и SSL, и отвечают за фрод-мониторинг операций, проводимых в Интернет-магазине. Чтобы расплатиться с помощью данной системы необходимо иметь кредитную карту, счет которой предназначен специально для оплаты товаров и услуг не только в интернете, но и в реальных магазинах.

Для того чтобы человек мог воспользоваться интернет-эквайрингом для оплаты товаров, у него должна быть карточка банка-эмитента, допускающего совершение подобных денежных операций. А также поставщик или продавец товаров и услуг должен предоставлять возможность покупателям совершать оплаты через платёжный интерфейс.

Для оплаты в интернете покупателю достаточно ввести в специальную форму номер банковской карты, её срок действия или трёхзначный код CV2, нанесённый с обратной стороны карты (над считывающей полосой справа). После введения всех этих данных с карточки списывается требуемая сумма и перечисляется продавцу. Занимает обычно такая процедура не более 1-2-х минут.

Каждый предприниматель, задумывающийся открыть интернет-магазин, обязательно должен позаботиться о подключении интернет-эквайринга. Так как это увеличит количество продаж и лояльность покупателей. Причём на налогообложение интернет-магазина это никак не повлияет.

### Преимущества и недостатки интернет-эквайринга

Количество продающих сайтов в России с каждым годом возрастает, увеличивается и эмиссия банковских карт. Соответственно растет спрос на услуги интернет-эквайринга. Рассмотрим основные преимущества использования данной услуги.

Для продавца или организации.

* Увеличение продаж и лояльности покупателей или клиентов за счёт возможности выбора удобного способа оплаты.
* Улучшение качества взаимодействия с покупателем и увеличение скорости доставки товара или оказания услуг.
* Возможность продавать товары через интернет по всему миру – глобальные масштабы бизнеса.
* Возможность торговать более широким ассортиментом продукции, чем в помещении.
* Компания, организуя продающий сайт с различными способами оплаты, снижает издержки на организацию оффлайн-магазина: аренду торгового зала, содержание персонала, инкассацию и другие затраты.
* Непрерывная работа интернет-магазина, покупатели имеют возможность оплачивать заказ в любое время суток, каждый день.
* В Интернете покупатель более склонен к спонтанным действиям, приобретает больше, чем в торговых точках, тем более при переводе денег с электронной карты.
* Отсутствие риска получить отказ в оплате от покупателя при получении товара, так как оплата была совершена заранее – до отправки товара.
* Частичная автоматизация бизнеса – оплата и зачисление денег на счёт происходит автоматически. Продавцу надо лишь отправить товар или оказать услугу.

Для покупателя или потребителя

* Удобство оплаты, так как для этого не нужно идти в банк или оплачивать товар наложенным платежом на почте. Отсутствие комиссий. Оплатить покупку можно из дома или офиса, имея под рукой компьютер, ноутбук или смартфон с доступом в интернет.
* Выбрать, оплатить товар или услугу можно в любое удобное время и день, ознакомившись лишь с условиями доставки или оказания услуг.
* Уверенность в том, что товар есть на складе продавца и гарантия того, что он будет доставлен в указанные сроки.
* Широкий ассортимент качественных или эксклюзивных товаров по цене значительно ниже, чем в офлайн-магазинах.
* Снижение риска от взимания дополнительных плат не указанных в условиях сотрудничества с продавцом или организацией оказывающей услуги.
* Получение возможности оперативного возврата денежных средств при несоответствии купленного товара (при условии его возврата продавцу).

Список можно продолжать. Продающие сайты значительно увеличивает возможности бизнеса. Однако на ряду с преимуществами существуют также и некоторые недостатки.

Для продавца или организации

* Низкая осведомлённость отечественных потребителей обо всех возможностях и преимуществах интернет-эквайринга, а также недоверие, связанное с мошенничеством в интернете и страхом кражи данных банковских карт.
* Ограниченное количество банков, дающих возможность работать с системой оплат интернет-эквайринга.
* В электронной платёжной системе может произойти сбой, который способен привести к существенной потере покупателей или клиентов – особенно если сбои систематические.
* Комиссия банков-эквайеров до 6% взымаемая с каждого платежа.
* Необходимость предоставления банку-эквайеру документов и информации об осуществляемой экономической деятельности.
* Банк может отказать в предоставлении услуги интернет-эквайринга без разъяснения причин.
* Необходимость использовать защитные протоколы и проходить обязательную сертификацию.

Для покупателя или потребителя.

* Наличие небольшого риска быть обманутым мошенниками или недобросовестными продавцами.
* Присутствует риск кражи личных данных пластиковой карты при неосторожных платежах в интернете на подозрительных сайтах.
* Сложно проверить принадлежность той или иной организации к конкретной компании, а также убедиться в законности экономической деятельности продавца.
* Доставка товара большинства интернет-магазинов хоть и оперативная, но нередко приходится ожидать купленный товар от нескольких дней до 2-х месяцев.
* При оплате товара или услуги система может дать сбой, что способно привести к списанию денежных средств, но не зачислению их продавцу.
* Не все пластиковые банковские карточки доступны для совершения онлайн-платежей через интернет.

Стоит отметить, что ряд недостатков не являются критическими и они временны. Например, плохая осведомлённость отечественных потребителей о возможностях оплат в интернете и о безопасности данной процедуры вызвана тем, что популярность интернет-торговли в СНГ ещё не так велика, как в Европе или США. Однако ежедневно всё больше людей начинают приобретать товары на отечественных и зарубежных торговых интернет-площадках. Яркий пример тому AliExpress [3].

### Участники интернет-эквайринга

Чтобы в полной мере понять суть интернет-эквайринга, нужно познакомиться со всеми участниками подобной платёжной системы.

**Мерчант – продавец**, интернет-магазин, который занимается продажей товара/услуги, представляет собой веб-приложение, в котором клиент может оплатить товар/услугу.

**Клиент** – покупатель, владелец пластиковой карты, который хочет заказать в интернет-магазине товар (услугу) и оплатить ее картой.

**Банк-эквайер** – банк, предоставляющий услуги по обработке платежей по банковским картам; с процессинговым центром, в котором у продавца открыт действующий расчётный счёт, куда поступают все денежные средства, перечисляемые покупателями. получивший лицензию от международных платежных систем (Visa, MasterCard) на осуществление интернет-эквайринга. В банке может быть собственный процессинговый центр или заключен договор со сторонней организацией.

Международная платежная система (МПС) – система расчетов между банками разных стран, которые используют единые стандарты платежных средств, обеспечивающие использование пластиковых карт как средств платежа (Visa, Master Card, American Express).

**Банк-эмитент** – банк выпустивший банковскую карту, которой клиент пытается оплатить товар/услугу. и является гарантом выполнения финансовых обязательств клиента.

**Расчетный банк платежной системы** – кредитная организация, осуществляющая взаиморасчеты между участниками платежной системы по поручению процессингового центра.

**Электронная платежная система (ПС)** – сервис, принимающий оплату электронными деньгами, банковскими картами (и не только) через Интернет (Яндекс.Деньги, WebMoney), являющаяся посредником между всеми перечисленными выше участниками.

Кроме этих участников, в цепочку интернет-эквайринга может быть включен агрегатор платежей, который сначала «собирает» средства на своем расчетном счету, а потом передает их в банк-эквайер. Подключение к агрегатору – вариант для тех, кто хочет избежать сложного взаимодействия с банком напрямую и предоставить пользователю сразу большой выбор платежных средств. Платеж по банковской карте также может сопровождать специализированная компания – провайдер платежей. Он осуществляет маршрутизацию платежа и обеспечивает высокий уровень безопасности. На вариант работы с провайдером следует обратить внимание, если вы хотите обеспечить дополнительную защиту платежей и получить дополнительные сервисы и надстройки.

**Процессинговый центр** (другие названия – компания-интегратор, провайдер электронных платежей, платежный шлюз) располагает программно-аппаратным комплексом для обработки интернет-платежей. Центр может входить в состав банка или быть отдельной компанией, самые известные из которых PayOnline, Assist, PayU, Uniteller, МультиКарта, ChronoPay.

Процессинговый центр:

– проводит техническую интеграцию интернет-магазина с платежным шлюзом;

– предоставляет продавцу доступ в личный кабинет для просмотра статистики по заказам и их оплате;

– предоставляет услуги по оформлению платежной страницы под корпоративный стиль магазина;

– обеспечивает заключение договора с банком-эквайером.

Процессинговые центры финансовые операции по картам не осуществляют. У них другая задача – техническое обеспечение расчетов и организация информационных потоков:

– сбор данных о карте покупателя в безопасном интерфейсе;

– передача данных банку-эквайеру и обратно;

– передача клиенту данных о платеже;

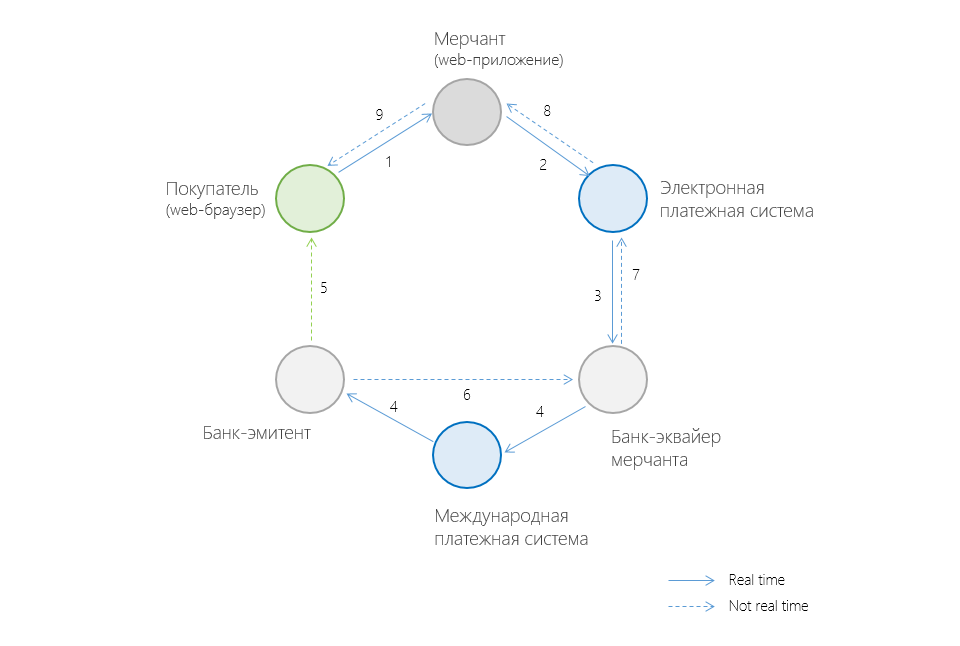
– защита от мошеннических операций;

– в отдельных случаях – информационная поддержка покупателей в виде колл-центра.

Услуги интернет-эквайринга может предложить только банк. Провайдеры и агрегаторы платежей являются в этом деле «посредниками», упрощающими взаимодействие между интернет-магазином и банком, обеспечивающими дополнительную защиту платежей или широкий выбор способов оплаты для клиента.

Банк, в первую очередь, должен получить лицензию от международных платежных систем (VISA, MasterCard, American Express и пр.) на осуществление интернет-эквайринга. Также банк должен располагать собственным или сторонним процессинговым центром – программно-аппаратным комплексом для обработки интернет-платежей. Для автоматизации приема электронных платежей должен иметься и специализированный платежный шлюз. Организация постоянной поддержки работы системы также лежит на плечах банка [4].

На рис. 1 представлена схема интернет-эквайринга.



*Рис. 1. Схема интернет эквайринга*

Покупатель находит интересующий его товар в каталоге интернет-магазина и оформляет покупку, выбрав вариант оплаты пластиковой картой.

Данные по заказу клиента регистрируются магазином и направляются в процессинговый центр. Покупатель направляется на страницу авторизации процессингового центра В появившийся интерфейс вводится вся необходимая информация банковской карты.

Далее провайдер формирует аутентификационный запрос и направляет клиента в систему аутентификации банка-эмитента (ACS). После аутентификации происходит авторизационный запрос, перенаправляемый в международную платёжную систему.

Платежная система пересылает запрос в банк-эмитент. Банк-эмитент проверяет остаток по счету покупателя, блокирует нужную сумму, если она есть, посылает в платежную систему ответ с разрешением (отказом) оплаты. Платежная система сообщает о транзакции банку-эквайеру, а тот дальше процессинговому центру.

Затем интернет-магазин получает ответ об успешном проведении транзакции (или отказе) от процессингового центра, далее доставляет товар. А специальный клиринговый файл отправляется в Расчётный банк, который переводит возмещение на счёт продавца. Расчетный банк переводит возмещение по совершенным операциям на счет Интернет-магазина.

### Способы подключения

**Подключение через банк-эквайер.**

Работа с банком-эквайером имеет ряд плюсов:

* прямое сотрудничество с банком (отсутствие посредников);
* низкая процентная ставка комиссии;
* защита денежных средств.

Из недостатков можно отметить:

* сложность подключения (ожидание решения до 1 месяца, риск получения отказа и большой пакет документов);
* нужно подстраиваться под условия банка и менять ряд настроек в сайте интернет-магазина;

**Подключение с помощью агрегатора.** Данный способ подключения интернет-эквайринга намного проще, чем в банке. Агрегаторы позволяют покупателям самостоятельно решать каким наиболее удобным способом будет произведена оплата товара – банковская карта, электронные деньги, списание средств с баланса мобильного телефона и т.д.

Положительной стороной использования агрегаторов является:

* возможность предложить покупателям практически все доступные способы оплаты приобретаемого товара;
* отсутствие оплаты за подключение интернет-магазина к агрегатору:
* минимальный пакет документов;
* интеграция ложится на руки агрегатора.

Негативная сторона агрегаторов это:

* высокая комиссия – почти 5% независимо от оборотов;
* наличие лишнего звена в цепочке клиент-банк.

## Обеспечение безопасности платежей

Вопрос безопасности интересует не только покупателей, но и продавца, банка-эквайра и банка-эмитента. Поэтому сегодня онлайн-платежи защищаются от мошенников следующими технологиями.

Подавляющее большинство хищений денег (свыше 90 процентов) с использованием удаленных каналов обслуживания происходит с помощью методов "социальной инженерии". Это не требует каких-то специальных средств: потерпевший либо сам переводит деньги, либо выдает преступникам все реквизиты карт, контрольную информацию и так далее. Многие клиенты так глубоко попадают под обаяние мошенников, что подтверждают правомерность операций даже после того, как к ним обращается служба безопасности банка

Сегодня защита электронных платежей имеет высокий показатель надёжности и постоянно совершенствуется. Все приведённые средства используют как банки-эквайеры, так и агрегаторы, а также банки-эмитенты.

Чтобы данные карты прошли этот путь без потерь, используются различные технологии защиты данных. Существуют как обязательные, так и рекомендованные технологии защиты.

Первое, что логично сделать, – защитить страницу передачи данных в Интернете. Для этого используется Secure Sockets Layer (SSL) – протокол шифрования, обеспечивающий безопасное соединение между покупателем и сервером [5].

Для получения права на интернет-эквайринг организация должна обладать сертификатом соответствия PCI DSS. Стандарт PCI DSS (Payment Card Industry Data Security Standard) – установленные для процессинговых центров (банковских и самостоятельных) требования к безопасности обслуживания платежных карт. Стандарт утвержден платежными системами Visa, MasterCard, American Express, JCB, Discover. Влючает в себя 288 процедур проверки от программно-аппаратных сбоев до ошибок в программе.

Для дополнительной защиты платежа существует технология 3-D Secure, разработанная компанией VISA. 3-D Secure представляет собой XML-протокол, реализующий двухфакторную аутентификацию пользователя. Проще говоря, к процессу финансовой авторизации (ввод карточных данных на сайте) добавляется еще и онлайн-проверка. Чаще всего она реализована в виде sms-сообщения с одноразовым кодом на номер мобильного телефона, привязанный в банковской карте. После ввода карточных данных покупатель переходит на специальную страницу банка-эмитента и на ней вводит полученный код

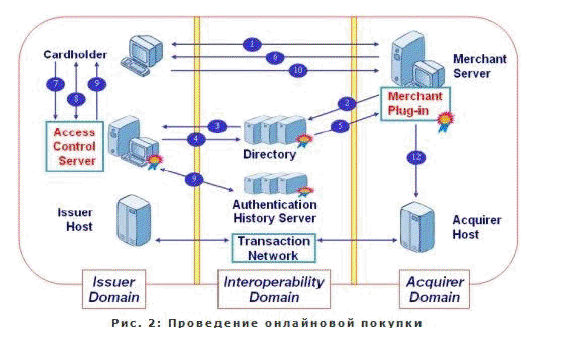
В не защищенных 3-D Secure транзакциях ответственность ложится на интернет-предприятие, на сайте которого была совершена покупка. В случае, когда работа идет с применением 3-D Secure, происходит т.н. «перенос ответственности», и отвечать за фрод будет уже банк, эмитировавший карту.

Модель 3-D Secure реализована на основе 3х доменов (рис. 2), в которых происходит порождение и проверка транзакций:

Домен Эмитента, который включает в себя Держателя карты и Банк, выпускающий карты.

Домен Эквайера, который включает в себя банк-Эквайер и его клиентов (онлайновых торговцев).

Домен взаимодействия содержит элементы, которые делают возможным проведение транзакций между двумя другими домена. Он, главным образом, содержит сети и сервисы карточных ассоциаций.



*Рис. 2. Проведение платежа с использование 3-D Secure*

Домены независимы в своих правах и являются важной частью процесса передачи информации в общей 3-D Secure-инфраструктуре. Для каждого домена определена собственная сфера ответственности в проведении транзакций.

В домене Эмитента банк-эмитент ответственен за аутентификацию покупателя и предоставление верной информации для проведения транзакции.

В домене Эквайера онлайновый торговец ответственен за коммерческие отношения с покупателем, а также гарантию того, что покупатель был направлен в верный банк-эмитент для верификации. В этом же домене Эквайер несёт ответственность за согласование проведения транзакции через традиционные сети Visa или MasterCard.

В домене взаимодействия платежная система Visa или MasterCard ответственна за сохранность информации по каждому эмитенту (банк держателя карты, интернет-адрес эмитента) и предоставление данной информации для вынесения решения в случае конфликтных ситуаций.

Модель 3-D Secure предоставляет стандартный протокол взаимодействия между доменами для обмена и проверки транзакций. Она не вызывает необходимости изменений в отношениях между участниками одного домена. Торговец и Эквайер свободны в выборе любого способа проведения своих транзакций и в управлении отношениями в своих доменах. Эмитенты свободны в выборе любых предпочитаемых ими механизмов для аутентификации держателя карты.

### Антифрод

Для всех участников за исключением держателей карт мошеннические транзакции подразумевают как значительные финансовые издержки, так и репутационные риски.

Термин «фрод» произошел от английского слова «fraud», что в переводе на русский язык переводится как «мошенничество». В широком значении фрод – это несанкционированные действия и неправомочное пользование ресурсами в сфере IT. Существует множество типов фрода, при этом обманутыми могут оказаться и пользователи, и продавцы, и банки. В большинстве случаев объектом фрода становятся данные платежных инструментов – банковских карт, электронных кошельков, мобильных средств, хотя фродом можно назвать любую утечку персональных данных, ведущую к обогащению злоумышленника.

По данным портала [www.banki.ru](http://www.banki.ru/news/lenta/?id=5646217), самый популярный тип мошенничества с банковскими картами – это так называемый «friendly fraud» («дружеский фрод»). Владелец карты совершает покупку в Интернете, а затем требует от банка проведения чарджбэка (charge-back) – возврата средств на карту вследствие неоказания услуги. И, если магазин не может доказать необоснованность претензий плательщика, банк должен возместить владельцу карты требуемую сумму. А «косты» ложатся на интернет-магазин [6].

Интернет-магазины могут пострадать от хакеров, незаконно проникающих в систему сайта, собственных сотрудников, неправомочно использующих базы данных компании, недобросовестных клиентов, указывающих неверные платежные данные с целью неоплаты, либо инициирующих возврат средств уже после отгрузки товара или оказании услуги.

От карточного фрода может пострадать и интернет-магазин, и банк, и непосредственно сам держатель карты. В случае утечки данных карт, злоумышленники стараются снять максимальную сумму денег и не оставить следов, чтобы интернет-магазины разбирались с банками, кто же всё-таки должен возместить утраченную сумму. За владельцами карт уследить невозможно – интернет-магазин не может знать, кто находится по ту сторону экрана: злоумышленник или добропорядочный клиент. Риск есть всегда, но чтобы приблизить его значение к нулю существует множество инструментов проверки платежей и верификации плательщиков.

Наличие системы распознания мошеннических платежей (antifraud-система) для любого серьезного участника проведения online-платежа (опять же, кроме покупателя) – рыночная необходимость. В то же время хорошая антифрод-система – это чаще всего долго и дорого.

И если для банка затраты на антифрод-системы – это, в масштабах бизнеса, вполне приемлемая сумма; для платежной системы – составная часть бизнес-процесса; то мерчанты часто не имеют финансовой возможности и/или понимания, как создавать и поддерживать подобные системы.

Но и игнорировать фрод мерчант не может: деньги за мошеннические платежи в лучшем случае просто не достанутся мерчанту (даже если услуга уже оказана), в худшем – мерчант еще и будет оштрафован. Размер штрафа, в общем случае, начинает с 10$ и растет пропорционально объему мошеннических транзакций. Кроме того, при большом количестве фрода МПС (Visa, MasterCard) могут наложить (не побоюсь этого слова) санкции на мерчанта.

Но стоит учитывать, что добавление таких шагов, требующих от пользователя дополнительных действий, нередко ведут драматическому снижению количества успешно завершенных транзакций.

Плюсы системы мониторинга мошеннических операций очевидны – автоматическое отклонение сомнительных транзакций, защита интернет-магазина от последующих разбирательств с банками, платежными системами и реальными владельцами карт. И, конечно же, минимизация репутационных и финансовых рисков. Репутация магазина не пострадает, и пользователи будут доверять такому ресурсу, а значит, их лояльность будет расти.

Но, как и у любого сервиса, у системы фрод-мониторинга есть свои «издержки производства». Отклонение платежей может привести к потере клиентов, а значит, прибыли. Без должной настройки фильтры могут не пропускать значимые для интернет-магазина транзакции, что точно не понравится покупателям.

При выборе платежного сервис-провайдера стоит обратить внимание на заявленную конверсию в успешные платежи: сервисы, гарантирующие «100% успешных оплат», скорее всего, либо намеренно переоценивают свой функционал, либо подвергают клиентов риску стать жертвой злоумышленников. Например, уровень конверсии в успешные платежи после «ручной» настройки (или у стандартных интернет-магазинов со стандартной клиентской аудиторией) системы электронных платежей PayOnline варьируется в рамках 93-96% – и это очень хороший показатель для рынка.

Еще одним неприятным, но важным моментом, с которым придется столкнуться при разработке системы фрод-мониторинга на стороне интернет-магазина, станет защита данных пользователей, как персональных, так и платежных. Необходимо будет пройти сертификацию соответствия требованием стандарта PCI DSS, а также учесть ограничения на хранение и обработку данных, регулируемые законом. Это относится скорее к тем, кто всё-таки берется за самостоятельную разработку антифрода, поэтому подробно вдаваться в детали в данной статье мы не будем.

## Существующие системы антифрода

На текущий момент на Российском рынке существуют небольшое количество модульных систем антифрода (системы антифрода, использующиеся в банках не рассматриваются). В основном их предоставляют платежные шлюзы России:

* <http://www.fraudwall.ru/>;
* <http://payler.com/antifraud/>;
* <https://payonline.ru/instruments/>;
* <http://www.jetinfo.ru/stati/jet-detective>;
* <http://www.bssys.com/solutions/financial-institutions/fraud/>.

К сожалению, проанализировать используемый принцип работы и используемые алгоритмы не представляется возможным, так как эта информация является конфиденциальной и внутреннее устройство систем не подлежит разглашению. Однако, все эти системы работают по одному общему сценарию.

Общая схема работы практически любого механизма фрод-мониторинга выглядит следующим образом: в момент совершения оплаты с помощью банковской карты собирается несколько показателей (у каждой антифрод системы они разные) – начиная от IP адреса компьютера и заканчивая статистикой оплат по этой карте. Количество фильтров может превышать сотню (например, у системы электронных платежей PayOnline их более 120). Система имеет набор правил, то есть лимитов фильтров безопасности. Каждый из фильтров проверяет пользователя – его персональные и карточные данные. Цель системы – убедиться в том, что пользователь является реальным владельцем карты, совершающим покупку на сайте. В случае выявления подозрительной активности, то есть превышения какого-либо значения параметра, фильтр автоматически блокирует возможность совершения платежа по этой карте. Рассмотрим процесс работы антифрод системы пошагово.

Пользователь совершат оплату на сайте. Информация о платеже попадает в систему fraud-мониторинга. В этот момент антифрод обладает двумя информационными пакетами: информацией о данном единичном платеже и профилем среднестатистического плательщика данного интернет-магазина. Алгоритмы работы системы fraud-мониторинга позволяют оценить ряд факторов, среди которых основными являются:

* страна, из которой совершается платеж;
* страна банка, выпустившего карту;
* размер платежа;
* количество платежей с карты;
* платежная история банковской карты;
* профиль среднестатистического плательщика магазина.

Транзакция проходит первичный анализ на основании этих и других факторов. На основании анализа ей присваивается «метка», которая характеризует способ обработки транзакции. Существуют три типа меток. «Зеленая» отмечает транзакции с низкой вероятностью возникновения мошеннической операции. «Желтой» меткой отмечаются транзакции, в которых шанс возникновения мошеннической операции выше среднего, и для проведения платежа потребуются дополнительного внимания. «Красной» отмечаются транзакции, которые с наибольшей вероятностью могут оказаться мошенническими, и при их проведении потребуется документальное подтверждение аутентичности владельца карты [7].

# ПОСТАНОВКА ЗАДАЧИ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ И ВЫБОР МЕТОДОВ ЕЁ РЕШЕНИЯ

В процессе разработки антифрод-системы неизбежно придется столкнуться с такой ответственной сферой как защита клиентских и платежных данных, а также с формальной частью этого вопроса – сертификации по одному из уровней PCI DSS, рассмотренной ранее. При разработке антифрод-системы необходимо также учитывать некоторые законодательные ограничения на хранение/обмен платежных и персональных данных клиента. В России это «О персональных данных» (152-ФЗ).

Антифрод-система является business-critical системой, т.к. ее простой будет вести либо к остановке бизнес-процесса, либо, при некорректной работе системы, к увеличению рисков финансовых потерь для компании. Отсюда повышенные требования к надежности работы, безопасности хранения данных, отказоустойчивости, масштабируемости системы.

Во всей цепочке проведения online-платежа мерчант находится в одном из наиболее сложных положений: мерчант в отличие от покупателя отвечает за фрод собственными средствами, и в то же время, в отличие от банка зачастую не обладает достаточными ресурсами для эффективного противодействия мошенничеству.

Но у мерчанта есть и преимущество – уникальная информация о покупателе товара/услуги, которая чаще всего недоступна другим участникам online-платежа (например, банку эмитенту или МПС). Так ECN-площадки с большой вероятностью обладают реальным именем плательщика; интернет-магазины, предлагающие услугу доставки, с большой вероятностью знают реальную страну, город проживания плательщика и т.д.

Имя, фамилия владельца учетной записи, время существования учетной записи, количество ранее совершенных успешных платежей через сайт мерчанта, информация о хосте, с которого пришел http-запрос, информация о браузере – это лишь короткий перечень той информации, которая нередко доступна мерчанту и которая способна значительно улучшить эффективность поиска мошеннических транзакций.

## Постановка задачи

Целью диссертационной работы является разработка собственной системы распознавания мошеннических платежей, т. е. antifraud-системы. Результат будет встроен в существующий платежный шлюз Payler. Компания предоставит базу данных мошеннических транзакций для выявления зависимостей.

Для начала рассмотрим некоторые параметры, которые, скорее всего, составят основные проверки в системе мониторинга мошеннических операций.

• Оплата по одной карте происходит с различных устройств, идентифицированных различными IP адресами.

• Обратная ситуация – с одного и того же устройства (IP адреса) производятся операции с помощью большого количества карт.

• С одной карты совершается несколько неудачных попыток оплаты (вероятно, пользователь не имеет возможности пройти процедуру подтверждения).

• Один клиент регистрируется под несколькими аккаунтами, используя разные адреса электронной почты, и платит с одной карты

• Имя плательщика, указанное на платежной форме, отличается от имени владельца карты.

• Разные страны регистрации интернет-магазина, банка-эмитента карты и покупателя.

• Лимитирование количества операций –покупок – одним физическим или юридическим лицом за конкретный отрезок времени.

• Лимитирование количества банковских карт для одного пользователя.

• Лимит максимальной суммы одноразовой финансовой операции за строго ограниченный период времени.

• Ограничение количества покупок по данной банковской карте за обозначенный период.

Этот перечень «спорных ситуаций» может дать нам общее представление о логике работы системы. Специалисты по рискам и бизнес-аналитики стараются учесть все нюансы, добавляя новые фильтры, защищающие бизнес интернет-компаний от злоумышленников. Стоит отметить, что в зависимости от платежного сервис-провайдера логика работы системы фрод-мониторинга и ее параметры изменяются.

Иногда бизнес имеет очень узкую специфику, и без индивидуальной настройки некоторые платежи просто не смогут пройти стандартные настройки антифрода, хотя и не будут являться мошенническими.

Например, ограничения по географии платежей критичны для сферы онлайн туризма: клиенту может понадобиться приобрести билет на самолет, находясь в командировке за границей, а система заблокирует такой платеж, так как он совершается не из той страны, где выпущена карта плательщика.

В этом случае применяется тонкая настройка фильтров: можно задать условия, согласно которым платеж будет пропускаться, даже если не выполняется условие, географии платежа. Подобные изменения вносятся в систему только после анализа возможных рисков, под контролем специалистов и после согласования изменений с представителем интернет-магазина.

## Требования к разработке

* Antifraud-система должна быть доступна как web-сервис, необходимо предусмотреть возможность подключения системы к сервису сторонних мерчантов.
* В решении необходимо разработать эффективную адаптивную модель проверки на основе Баесовой сети с использованием накопленных системой знаний о клиентах и их поведении. Формирование частных, т.е. заточенных под бизнес-процессы конкретного клиента, моделей поведения происходит на основе технологии машинного обучения с получением данных из больших массивов информации. Самообучение системы с учётом накопления данных со временем должно позволять снижать вероятность возникновения ошибок первого (ложная тревога) и второго (пропуск реальной атаки) родов, что положительно сказывается на их эффективности
* Модель должна гибко настраивается, в том числе, через встроенный конструктор критериев и правил.
* Работа системы должна быть прозрачна и решения, принимаемые системой, могут контролироваться и, при необходимости, корректироваться уполномоченными сотрудниками.
* Система должна хранить детальную информацию о проверке каждого платежа, строит профили плательщиков и получателей, формирует аналитические отчеты.
* Решение должно иметь гибкую систему оповещений о различных событиях (по SMS, email).
* В систему должны быть встроены политики безопасности, разграничение прав доступа, аудит действий пользователей, доменная и внутренняя аутентификация, журналирование всех операций.
* Защита не только от известных видов мошенничества, а также от мошенничества так называемого «нулевого дня». Даже при отсутствии квалифицированного специалиста обычный оператор банковского call-центра в пятницу вечером, заподозрив что-то неладное в только что проведенных транзакциях, может выставить в системе флажок, в результате чего Байесов функционал сможет перестроиться и заблокировать все последующие операции такого типа. А уже в понедельник со всем этим разберутся надлежащим образом соответствующие специалисты.

# ПЛАН РАБОТЫ НАД ДИССЕРТАЦИЕЙ

|  |  |
| --- | --- |
| Выбор алгоритма работы системы. Первичная реализация алгоритмов различных классов. | 24.07.2017 |
| Обучение и исследование получившихся моделей на примерах транзакций. Улучшение/комбинация этих алгоритмов. Составление модели/ансамбля моделей аналитического модуля системы. | 01.10.2017 |
| Проектирование архитектуры системы. | 01.12.2017 |
| Реализация интерфейса программы. | 07.12.2017 |
| Тестирование и доработка аналитического модуля. Добавление нового функционала настроек. | 01.02.2017 |
| Тестирование системы в целом. | 01.03.2017 |
| Исправление багов. Попытка внедрения в платежный шлюз. | 07.03.2017 |
| Точечная настройка параметров аналитического модуля. | 01.05.2017 |

# ЗАКЛЮЧЕНИЕ

В результате прохождения производственной практики рассмотрен процесс интернет-эквайриенга, проблема мошеннических платежей и способов их обнаружения с помощью антифрод-систем.

Сформулированы основные требования, которыми должна обладать разрабатываемая система, рассмотрены методы анализа данных для ее разработки.

Введение дополнительных технологий защиты увеличивает стоимость интернет-эквайринга, но добавляет ему надежности и уберегает от значительных материальных потерь как предприятие, так и банк.

# СПИСОК ЛИТЕРАТУРЫ

1. Что такое эквайринг и зачем он нужен? [Электронный ресурс] URL: https://www.kp.ru/guide/iekvairing.html (дата обращения 20.07.2017).
2. Эквайринг карт [Электронный ресурс] URL: http://www.banki.ru/wikibank/ekvayring/ (дата обращения 20.07.2017).
3. Что такое интернет-эквайринг, зачем он нужен, и как его подключить для онлайн-платежей [Электронный ресурс] https://bizbe.biz/base/term/57-chto-takoe-internet-ekvayring.htmlURL: (дата обращения 20.07.2017).
4. Процесс интернет-эквайринга – как все работает [Электронный ресурс] http://buh-v-seti.ru/raschetyi-dengami/process-internet-ekvajringa/ URL: (дата обращения 20.07.2017).
5. Интернет-эквайринг: от А до Я [Электронный ресурс] https://oborot.ru/articles/internet-ekvajring-ot-a-do-ya-i34700.html URL: (дата обращения 20.07.2017).
6. Анти-фрод системы и как они работают [Электронный ресурс] <http://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php> URL: (дата обращения 20.07.2017).
7. Автоматизированная борьба с мошенниками: fraud-мониторинг в интернет-эквайринге [Электронный ресурс] https://www.payonline.ru/news/smionas/373/URL: (дата обращения 20.07.2017).