Глазунов Н. В.**Кредитные карты будущего. Защита кредитных карт***Оренбургский государственный университет
(Россия, Оренбург)**doi:10.18411/spc-20-01-2018-02**idsp: 000001:spc-20-01-2018-02*

В настоящее время, очень сложно встретить человека, которому бы не предлагали кредитную карту. Можно затронуть любую сферу человеческой деятельности, и везде человек пользуется кредитными картами, будь это интернет или магазин, банки или телевидение. Опросы среди россиян, которые проводятся MasterIndex, подтверждают, что число держателей кредитных карт с каждым годом становится гораздо больше. "Кредитки", как их чаще называют, с недавних пор, стали неотъемлемой частью повседневной жизни общества.

Специалисты по кредитованию считают, что кредитные карты способны составить конкуренцию микрозаймам. Уже сегодня, кредитные карты занимают первые позиции. К 2016 году была тенденция того, что кредитные карты могут стать основным видом кредитования. Но в итоге, Россия всё же отстает по показателям распространенности кредитных карт среди населения, в отличие от тех же Соединенных Штатов. В России одна карта приходится на десять человек, в то время как в Америке, на одного человека приходится три кредитные карты. Однако, планируется быстрое изменение ситуации на рынке банковского кредитования [2].

У каждого банка есть свой широкий ассортимент кредитного продукта, и каждый из этих продуктов обладает определенными достоинствами и недостатками. То есть, человек, в буквальном смысле знакомится с кредитной картой. Сейчас эта процедура не вызывает каких-либо трудностей. Достаточно просто зайти на сайт нужного банка и выбрать карту с наиболее оптимальными условиями. Под условиями принято понимать размер процентной ставки, стоимость годового обслуживания, продолжительность беспроцентного периода, а также различные комиссии.

Современные технологии движутся настолько быстро, что вчерашние фантазии одержимых разработчиков сегодня вовсю применяются на практике, а завтра — станут уделом истории. Касается это и финансовых инструментов, чье развитие направлено на постоянное совершенствование механизмов оплаты, повышение удобства оплаты и рост качества обслуживания клиентов.

Первая в истории покупка товара через сеть Интернет свершилась в 1994 г. В ней использовалась технология eCash, которую разработали буквально за год до дебюта. Прошел еще год и в 1995 г. была создана первая версия электронного кошелька. В России первая система электронных платежей, получившая название PayCash, начала работать лишь в 1998 г.

Все системы электронных платежей, по большому счету, делятся на три основные группы: онлайн-банкинг, системы мгновенных платежей и электронные валюты. Онлайн-банкинг — это самый сложный механизм, позволяющий клиентам использовать защищенный сайт в сети, с помощью которого можно оплачивать коммунальные услуги, пополнять баланс на мобильном, переводить средства со счета на счет себе и другим. Проще говоря, онлайн-банк, по большей части, заменяет клиенту необходимость идти в ближайшее отделение или искать банкомат — все делается прямо из дома, быстро и просто. Для того, чтобы войти в свой личный кабинет, достаточно ввести предварительно полученные по СМС-сообщению либо в банкомате одноразовые пароли.

Второй вид электронных расчетов, где также может применяться банковская карта — это мгновенные платежи. Всевозможные интернет-сервисы позволяют не только пополнять счета с помощью карт, но и напрямую расплачиваться с помощью

них в интернет-магазинах. Систем мгновенных платежей существует достаточно много, однако, если рассматривать наиболее популярные в России сервисы, то стоит назвать системы WebMoney, «Яндекс.Деньги», PayPal, Деньги@Mail.Ru, RBK Money и другие. Помимо возможности оплачивать покупки по сети, часть сервисов позволяет оплачивать также квитанции и штрафы, собирая с клиента комиссию в размере фиксированной суммы или небольшого процента от суммы платежа. Интересно, что при ведении личного счета на остаток суммы начисляется процент.

Прямая оплата в сети через банковскую карту все равно считается наиболее оперативным и удобным способом оплаты товаров. Можно считать, что банковские карты перешагнули порог реальности и внедрились в виртуальный мир, освоившись в нем и став наиболее совершенным инструментом оплаты в Интернете. Но одновременно с ростом популярности электронной коммерции, растет и уровень информационной оснащенности самих карт. К примеру, традиционные банковские карты с одной только магнитной лентой позволяют просто хранить персональные данные об имени держателя и сроке действия карты. А вот современные карточки со встроенным микрочипом обеспечивают возможность разместить куда больше информации, а также работать с бонусными баллами при всевозможных партнерских программах.

Следующий шаг в будущее не так давно осуществили крупнейшие в мире операторы платежных систем Visa и MasterCard, представив карты со встроенным дисплеем. Благодаря установленному на карте экрану держатель карты может получать коды для активации карты, разовые пароли, остаток средств, информацию о последних платежах, ну и наконец, список компаний-партнеров, предоставляющих бонусы и специальные предложения [1].

Дело в том, что ещё совсем недавно кредитные карты были очень уязвимы. Причина тому - архаичная система защиты банковских карт. Информация на магнитной дорожке записана "открытым текстом", а единственным ключом доступа служит короткий PIN-код, который было несложно украсть так называемыми "кардерами".

Однако, финансовая индустрия, теряющая от рук мошенников большие суммы, не дремлет, пытаясь внедрить более совершенные методы защиты транзакции. Одним из их успешных проектов является карта с чипом, по стандарту EMV (EMV или Europay & MasterCard & VISA - международный стандарт для операций по банковским картам с чипом. Этот стандарт разработан совместными усилиями компаний Europay, MasterCard и Visa, чтобы повысить уровень безопасности финансовых операций). После того, как эти карты были распространены по Европе и в Канаде, количество преступлений с использованием клонированных карт в этих регионах резко снизилось. Кардеры начали свою охоту на территории США и азиатских стран, поскольку там таких нововведений не было.

С одной стороны, система EMV является большим шагом вперед, с другой, она тоже далека от идеала и не сможет защитить от всех угроз, с учетом того, как быстро совершенствуются криминальные технологии. Вполне возможно, что скоро мы будем пользоваться немного другими кредитными картами.

Самое простое решение проблемы слабой защиты — добавить еще один уровень безопасности. Так, например, работает ставшая уже привычной в Интернете схема двухфакторной аутентификации.

И это уже используется при покупках в Интернете. В ходе онлайн-платежа пользователь вводит не только код CVV2, напечатанный на оборотной стороне карты, но и дополнительный одноразовый пароль. Пароль приходит на телефон в виде SMS-сообщения либо создается выданным банком специальным устройством — токеном. Двухфакторная аутентификация используется кое-где и для офлайн-транзакций, особенно если речь идет о крупных суммах денег.

Похожим образом работают банковские карты со встроенными дисплеями. Здесь в обычной кредитке помещается целый компьютер с маленьким жидкокристаллическим экраном и цифровой клавиатурой. Помимо генерации одноразовых паролей он также может хранить в памяти историю совершенных операций, показывать баланс счета и так далее.

Хотя первым экспериментам с интерактивными картами уже больше пяти лет, их сегодня предлагают своим клиентам лишь отдельные банки в Европе, США и развитых странах Азии.

Еще более экзотично выглядит разработка американской компании Dynamics. На этой карте магнитная дорожка не записана постоянно, а динамически генерируется электронной начинкой. Генерируется по команде пользователя, который сначала должен ввести пароль на встроенной клавиатуре.

Нет пароля — нет информации на магнитной полосе, нет и транзакции. Более того, нет даже номера карты: часть цифр 16-значной последовательности не напечатаны, как обычно, на пластике, а отображаются на дисплее только после ввода пароля. По заявлению создателей, заряда встроенной в карту батареи хватит на три года.

Парольная защита может быть сколько угодно мощной, но теряет всякий смысл, если забывчивый пользователь не может правильно сохранить секрет. Все, наверное, слышали истории незадачливых персонажей, записывающих PIN-коды прямо на кредитках и благополучно их теряющих.

Радикальное решение парольного вопроса предлагают системы биометрической аутентификации. Норвежская компания Zwiipe вместе с MasterCard, например, сейчас проводит в Европе пилотное внедрение карты со встроенным сканером отпечатков пальцев. Все, что нужно для совершения платежа, — это приложить палец к контактной площадке на карте, никакой PIN уже не нужен.

Несмотря на десятилетия трудоемких исследований, практически применимые квантовые компьютеры по-прежнему остаются для нас недостижимой мечтой. Зато есть надежда, что необычные свойства квантового мира пригодятся для изготовления идентификаторов, которые практически невозможно подделать.

По крайней мере, так считают нидерландские исследователи из университета Твенте и технологического университета Эйндховена, предложившие идею квантовой защиты банковских карт и удостоверений личности. Их разработка, пока существующая лишь в виде лабораторной модели, получила название quantum-secure authentication (QSA).

На крошечный участок обычной пластиковой карты наносят тончайший слой частиц оксида цинка (никакой магии — по сути обычные цинковые белила). Затем по этому участку «стреляют» из лазера отдельными фотонами света. Фотоны попадают в слой наночастиц и затем случайным образом многократно переотражаются внутри. Эта «бомбардировка» меняет оптические свойства слоя частиц и таким образом формирует уникальный ключ.

Если теперь на карту посветить определенной последовательностью коротких лазерных импульсов (вопрос), то в ответ можно получить определенную картину отражения (ответ). Комбинация уникальных пар «вопрос-ответ» для каждой карты хранится в банковской информационной системе и используется для проверки подлинности ключа.

Квантовая защита срабатывает при попытке злоумышленника перехватить вопрос и ответ в ходе совершении транзакции. Любой дополнительный фотодетектор в системе нарушит квантовое состояние хотя бы части фотонов и таким образом «испортит» всю картину.

Альтернативный способ подделки карты путем анализа точного размера, положения и других свойств наночастиц с последующим созданием точной копии практически нереализуем из-за очень высокой сложности процесса.

Разработчики QSA утверждают, что, несмотря на кажущуюся сложность концепции, она легко и относительно недорого может быть реализована на практике с помощью доступных уже сегодня технологий.

Маловероятно, что всеобщее внедрение банками описанных выше систем — дело ближайшего будущего. Финансовая индустрия достаточно консервативна, а массовое внедрение новых технологий — штука весьма затратная.

Кроме того, очень важно, чтобы все преимущества хитроумных решений не сводились на нет несовершенством внедрения, как это сейчас кое-где обстоит с чиповыми картами. Ведь в чем нынче основная проблема: если старинный банкомат или платежный терминал не может прочесть защищенный чип, то он довольствуется магнитной дорожкой, оставленной именно для совместимости со старым оборудованием. И вся защита идет насмарку [3].

1. Новостной портал "Вести.ру" Что ждет рынок кредитных карт в будущем? [Электронный ресурс] - Режим доступа: - <https://www.vesti.ru>
2. Официальный сайт "MoneyMan" Что выбрать: кредитные карты или микрозаймы? [Электронный ресурс] - Режим доступа: - <https://moneyman.ru>
3. Официальный российский блог "Лаборатории Касперского" Квантовый пластик: какими будут кредитки будущего? [Электронный ресурс] - Режим доступа: - <https://www.kaspersky.ru/blog/>

Завершинская А.А.

Понятие тотального залога в Гражданском Кодексе Российской Федерации

*Оренбургский государственный университет
(Россия, Оренбург)*

doi:10.18411/spc-20-01-2018-03

idsp: 000001:spc-20-01-2018-03

Не так давно в Российском законодательстве появилось такое понятие как «тотальный залог». Федеральным законом от 21 декабря 2013 года N 367-ФЗ "О внесении изменений в часть первую Гражданского кодекса Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации" была изменена статья 339 Гражданского кодекса Российской Федерации. Законодатель ввел в оборот новую составляющую залогового права, получившую свое название «тотальный залог». Изменение вступило в силу 1 января 2015 года.

Институт тотального залога появился в Гражданском кодексе Российской Федерации в результате реформы залогового права законодателем. Тотальный залог иными словами можно назвать залогом всего имущества, из-за этого толкования возникает множество вопросов относительно практики его реализации.

Тотальный залог, как составляющая залогового права, малоизучена на сегодняшний день, поскольку вошла в российское законодательство не так давно. Но всё же новелла стала предметом внимания для многих ученых-юристов.

Новая редакция Гражданского кодекса Российской Федерации, а именно статья 339 пункта 2, установила, что залогодатель, если он является субъектом предпринимательской деятельности, вправе описать любым способом предмет залога, позволяющим идентифицировать имущество в качестве залога на момент обращения взыскания, в том числе и на все имущество, либо часть имущества, либо залог имущества определенного рода и вида.