ЛЕКЦИЯ «ПЛАТЕЖНЫЕ ИНСТРУМЕНТЫ»

Платежные карты

Платежные карты предназначены для оплаты товаров, услуг и в некоторых случаях — для получения наличных денег. Карты могут выпускать (эмитировать) банки, а также другие организации, например, магазины.

Банковские карты

Банковские платежные карты всегда привязаны к банковскому счету и работают в рамках определенной платежной системы. В рамках этой системы держатель карты может осуществлять финансовые транзакции: рассчитываться в безналичной форме за товары и услуги – через POS-терминалы, банкоматы, платежные терминалы, через Интернет. Платежная система обеспечивает расчеты между разными банками. Различают международные и локальные системы.

Карту международной платежной системы можно использовать для расчетов в большинстве стран мира. Крупнейшие в мире сети электронных платежей принадлежат компаниям VISA и MasterCard. Также к числу международных платежных систем относят American Express и Diners Club (последняя компания в свое время была первым в истории платежного рынка организатором эмиссии банковских карт). Наибольшее распространение на российском рынке получили карты систем VISA и MasterCard. Необходимо отметить, что такие «карточные» бренды как American Express и Diners Club были в определенной степени скомпрометированы несколькими эксклюзивно эмитирующими их российскими банками либо вследствие агрессивной политики кредитования (ситуация с American Express, эмитент – банк «Русский стандарт»), либо вследствие неудачного бизнеса (ситуация с Diners Club, эмитент – банк «Славянский»).

Локальные платежные системы действуют на территории одной или нескольких сопредельных стран. Крупнейшие из локальных систем – китайская система Union Pay и японская система JCB. В России в 2014 году началось развитие национальной системы платежных карт «Мир». Кроме того, на территории России действует несколько частных локальных платежных систем, их которых наиболее известны «Золотая Корона», СТБ и «Юнион Кард/NCC» (см. таблицу 1).

Таблица 1. Основные платежные системы:

Система	Страна
VISA	США
MasterCard	США
American Express	США
Diners Club	США
Union Pay	Китай
JCB	Япония
«Мир»	Россия

В России выпускают банковские карты, номинированные в рублях, долларах и евро. Срок действия карты составляет, как правило, от 2 до 5 лет. Для получения карты необходимо подать заявление в банк и предъявить документ, удостоверяющий личность. По своим функциям банковские карты делятся на три вида: дебетовые, дебетовые с овердрафтом и кредитные. В отдельном ряду стоят предоплаченные карты, которые могут эмитировать не только банки.

Дебетовые карты

Дебет означает зачисление на счет. Соответственно, дебетовые карты позволяют расходовать только средства со счета держателя карты. Сколько зачислите, столько и потратите.

Дебетовую карту можно использовать для расчетов за товары и услуги как альтернативу наличным деньгам, а также для расчетов через Интернет. С помощью карты можно осуществлять различные

операции через банкомат, например, оплачивать счета за коммунальные услуги, налоги, государственные пошлины, штрафы ГИБДД, переводить деньги на банковские счета, вносить платежи по кредиту.

Также через банкомат можно снимать наличные с банковского счета в пределах лимита, установленного банком. Если снимать наличные через банкомат эмитента или банка-партнера, держатель карты ничего за это не платит. За получение наличных через банкомат другого банка взимается фиксированная комиссия, которая в среднем составляет 100–200 рублей. Для привлечения клиентов банки могут предложить бонус в виде CashBack: каждый раз при расчете картой за товар или услугу держатель карты получает от банка от 0,5 до 10% потраченной суммы.

Карта с овердрафтом

Овердрафт в переводе с английского означает «перерасход». Карта с овердрафтом допускает перерасход средств, ее держатель может потратить больше, чем имеет.

«Кредит в форме овердрафта (overdraft facility) означает заключенное сторонами кредитное соглашение, в соответствии с которым кредитор предоставляет потребителю доступ к финансированию, превышающему остаток на текущем счете потребителя».[1]

При недостатке собственных средств держатель карты может использовать кредитные средства в пределах установленного лимита. Размер кредитного лимита, как правило, не превышает двукратного ежемесячного дохода держателя карты. Если держатель карты с овердрафтом истратил больше средств, чем установлено лимитом, на сумму сверхлимитного перерасхода начисляют более высокие проценты. Иногда ставка может превышать базовую в два раза и больше. За пользование овердрафтом банк начисляет проценты, как за пользование любыми кредитными средствами. Срок погашения задолженности по карте с овердрафтом фиксируется в договоре. Чаще всего это небольшой срок, один-два месяца. За этот срок необходимо полностью погасить задолженность перед банком. После этого можно снова использовать овердрафт.

В более редких случаях овердрафт предоставляется на длительный срок, когда нужно ежемесячно вносить минимальный платеж и оплачивать проценты, начисленные за использование овердрафта. За просрочку платежа взимается штраф и пени за каждый день просрочки.

Кредитные карты

Особенность кредитных карт состоит в том, что для платежей не используются собственные средства. Держателю карты предоставляется кредит на определенную сумму, который необходимо погашать по определенным правилам.

Стандартные правила позволяют погасить долг по кредиту в течение 30–60 дней после использования заемных средств без начисления процентов. Этот срок называется грейс-периодом. Например, продолжительность грейс-периода составляет 45 дней. С 1 января по 1 февраля держатель карты потратил 50 тыс. рублей. Если он внесет эту сумму на счет кредитной карты до 15 февраля, то проценты за пользование заемными средствами начислять не будут.

Несмотря на грейс-период, кредитные карты выгодны банкам, так как большинству держателей кредитных карт не удается своевременно погасить долг и сэкономить на процентах за пользование заемными средствами.

Если держатель карты не погасит задолженность за время действия грейс-периода, ему начисляют проценты за пользование заемными средствами с момента их использования. После окончания грейс-периода держатель карты обязан ежемесячно вносить минимальный платеж, который обычно составляет 5–10% от суммы долга с процентами.

За просрочку минимального платежа начисляется штраф, а за каждый день просрочки – пени.

1 О. М. Иванов. Стоимость кредита: правовое регулирование. / О. М. Иванов. – М.: Инфотропик Медиа, 2012. 110 с.

Кредитные карты предназначены главным образом для расчетов, хотя снимать наличные с такой карты тоже можно. Но за снятие наличных взимается очень высокая комиссия, в среднем 3–5 % от снятой суммы, и даже минимальная комиссия будет в несколько раз больше, чем комиссия за снятие наличных с дебетовой карты. При этом чаще всего грейс-период не действует для операции по снятию наличных, так что за использование этих средств придется заплатить проценты в обязательном порядке.

«Кредитные карты международных платежных систем одинаково принимают к оплате в России и за ее пределами. Причем, если наличные для заграничного вояжа придется менять на местную валюту, то кредитку вы сможете использовать, осуществляя платеж в любой валюте (в какой бы валюте сама кредитная карта ни была бы номинирована). За границей ваши деньги при расчетах будут автоматически конвертироваться в местную валюту. Кстати, наличные за границу можно в ограниченном количестве, а на банковской пластиковой карте можно взять с собой любую сумму».[2]

Особенности банковских карт

Все банковские карты, кроме предоплаченных, различаются уровнями. От уровня карты зависит набор возможностей и стоимость годового обслуживания.

Пример карт начального уровня – это Visa Electron и MasterCard Electronic. Их возможности авторизации ограничены, поэтому такие карты не всегда можно использовать для оплаты через Интернет. Информация на такие карты наносится только с помощью магнитной полосы. Плата за годовое обслуживание таких карт минимальна или даже полностью отсутствует. Карты начального уровня популярны у людей с низким достатком – учащихся, студентов, пенсионеров, а также их нередко используют в «зарплатных проектах».

К числу так называемых классических карт относятся Visa Classic и MasterCard Standard. Они не имеют ограничений по использованию, обладают более высоким уровнем защиты от мошеннических действий, нежели карты начального уровня.

Информация на таких картах защищается специальным чипом, предохраняющим от мошеннических действий. Плата за годовое обслуживание относительно невысока. Эти карты предназначены для людей среднего достатка.

Премиальные карты предназначены для людей с высокими доходами. Плата за годовое обслуживание таких карт может достигать нескольких десятков тысяч рублей. Держателям таких карт нередко предоставляются индивидуальное обслуживание и дополнительные услуги, например, консьерж-сервис. Кроме того, держатели премиальных карт могут пользоваться множеством льгот, предоставленных партнерами платежных систем. Наиболее распространены скидки на номера в отелях, на аренду автомобилей, в ресторанах и кафе.

Для привлечения клиентов банки выпускают кобрендовые карты. Это значит, что карта выпущена сразу под двумя брендами: самого банка и компании-партнера.

Чаще всего это авиакомпания либо сеть автозаправочных станций. Расплачиваясь такой картой, за каждую транзакцию держатель получает бонусные баллы либо мили, которые можно обменять на авиабилет либо на литры топлива на автозаправке. Часто участниками таких кобрендинговых программ становятся также бутики различных типов, однако ввиду немассовости продукта такие кобренды многие эксперты банковского рынка оценивают, как неэффективные («сувенирные кобренды»).

Предоплаченные карты

Предоплаченные карты не привязаны к банковскому счету и представляют собой эквивалент фиксированной суммы денег. Они анонимны, поэтому их можно передавать другим лицам, без ограничений. Как правило, предоплачен-

2 Арт Я. А. Внятное руководство для обычного человека, где, как и на что взять деньги / Арт Я. А. – М.: Астрель, 2012. – с. 70.

ные карты номинированы в рублях, хотя встречаются и карты, номинированные в иностранной валюте. Предоплаченные карты могут выпускать как банки, так и другие организации. Самый распространенный пример предоплаченных карт – подарочные карты магазинов, салонов красоты, туристических агентств, автозаправок, автосервисов, прокатов автомобилей, ресторанов. Возможность использования таких карт ограничена: ими можно рассчитываться за товары или услуги только той организации, которая выпустила карту.

Банки выпускают три разных вида предоплаченных карт: без возможности пополнения (подарочные), пополняемые и виртуальные.

Банковские предоплаченные карты, как без возможности пополнения, так и пополняемые, можно использовать для расчетов за товары и услуги в точках продаж и через Интернет. Снимать наличные можно только с пополняемых карт.

Виртуальные карты используются только для расчетов через Интернет, эти карты не имеют физического носителя и представляют собой набор цифр: 16-значный номер карты, срок ее действия и коды безопасности CVV2 или CVC2.

Банковская предоплаченная карта может оформляться без идентификации клиента, поэтому ее можно приобрести без предъявления документов. Однако для оформления виртуальной и пополняемой карт необходимо подать заявление в банк. В одних случаях при этом достаточно идентификации по номеру телефона, в других требуется предъявить документ, удостоверяющий личность.

В России без предъявления документов можно получить предоплаченную карту, как правило, лимитом не больше 15 тыс. рублей. Хотя по российскому законодательству лимит предоплаченной карты может составлять до 100 тыс. рублей и пополнять ее можно на сумму до 40 тыс. рублей в месяц. Но чтобы получить карту с лимитом выше 15 тыс. рублей, придется предъявить документы. Таким образом, пополняемая предоплаченная карта фактически является анонимной дебетовой картой начального уровня.

Распространение получили кобрендовые предоплаченные карты с торговыми сетями. Их отличает возможность получать скидки и бонусы за каждую покупку.

Срок действия небанковских подарочных карт обычно неограничен, они прекращают свое действие после того, как лимит их средств исчерпан. Срок действия банковских предоплаченных карт без пополнения обычно составляет 1 год, у пополняемых карт срок действия дольше.

Банки могут брать комиссию за выпуск предоплаченной карты или плату за годовое обслуживание.

Электронные деньги

Электронные деньги используются для оплаты товаров и услуг, расчетов между людьми и организациями. Для расчетов электронными деньгами используются специальные платежные сервисы, в России наиболее распространены Яндекс.Деньги, QIWI, WebMoney, PayPal.

Для расчетов электронными деньгами используют электронные кошельки, которые выступают аналогом банковского счета. Электронный кошелек открывает платежный сервис после получения денежных средств от клиента. Платежный сервис удерживает комиссию за перевод средств, хотя некоторые виды операций могут осуществляться бесплатно.

Для зачисления средств в электронный кошелек используются разные способы. Можно пополнить баланс переводом из другого электронного кошелька; по почте; через систему денежных переводов; с банковского счета через банкомат или Интернет-банк; со счета телефона; из электронного кошелька другого платежного сервиса; наличным платежом через платежные терминалы, отделения банков и почтовые отделения.

Обналичить электронные деньги можно несколькими способами. Самый простой и распространенный способ – перечислить их на банковский счет или на банковскую карту. Также можно использовать почтовый или денежный перевод. Российские платежные сервисы Яндекс.Деньги и QIWI эмитируют собственные платежные карты, которые

можно использовать для наличных расчетов или снимать деньги в банкомате.

С точки зрения безопасности электронные кошельки намного лучше защищены от мошеннических действий, чем банковские карты.

Мобильная коммерция и мобильные платежи

Мобильные платежи производятся с помощью смс-сообщений и специальных приложений для мобильных устройств – смартфонов и планшетов. Мобильные платежи используются для расчетов по счетам абонентов операторов связи, банковских карт, электронных кошельков.

«Продолжающийся рост числа мобильных телефонов на руках у населения фактически привел к созданию еще одной всемирной сети, пользовательскими терминалами которой служат мобильные телефоны».[3]

С помощью мобильных платежей можно оплачивать различные услуги, осуществлять платежи по кредитам и денежные переводы, оплачивать штрафы ГИБДД, покупки цифрового контента – музыки, фильмов, электронных книг, компьютерных игр, а также билеты в театр, кино, на концерты.

Набирает популярность особый вид мобильных платежей, основанный на технологии бесконтактной оплаты NFC. В смартфон устанавливается приложение, к которому привязывается банковская карта, и мобильное устройство начинает выполнять функции этой карты: его подносят к платежному терминалу, и оплата за товар или услугу списывается с банковского счета. В России из приложений бесконтактной оплаты наиболее известны Apple Pay и Samsung Pay.

Особенности российского законодательства в сфере электронных платежей

В 2011 году в России был принят Федеральный закон «О национальной платежной системе». Он регулирует порядок оказания платежных услуг и электронной коммерции.

Закон устанавливает требования и правила деятельности для всех участников платежной системы: банков и небанковских кредитных организаций, платежных систем и сервисов, систем денежных переводов. Также законом установлено, что надзор за участниками национальной платежной системы осуществляет Банк России.

Введение санкций против России со стороны Запада в 2014 году обусловило создание Национальной системы платежных карт, которая призвана обеспечить бесперебойность, эффективность и доступность оказания услуг по переводу денежных средств для населения страны.

Также введен беспрецедентный законодательный запрет: платежные системы, в том числе международные, не имеют права прекращать оказывать услуги по переводу денежных средств в одностороннем порядке.

Дополнением к закону «О национальной платежной системе» были установлены серьезные санкции за нарушение этого запрета. Запрет был принят в ответ на действия международных платежных систем Visa и MasterCard, которые 21 марта 2014 года без предварительного уведомления заблокировали операции по картам ряда российских банков в рамках санкций, введенных США против России.

Существующая законодательная база оставляет нерешенными ряд проблем и вопросов, связанных с электронными платежами. В частности, потребители испытывают сложности с получением компенсаций в случае программных сбоев, с получением средств, размещенных в платежных сервисах, несут практически все риски, связанные с мошенническими действиями. Правовая незащищенность пользователей электронных платежей также связана с недостаточным контролем за соблюдением конфиденциальности предоставления персональных данных операторами платежных систем и сервисов.

---

3 Электронные деньги и мобильные платежи / коллектив авторов. – М.: КНОРУС; Центр исследования платежных систем и расчетов, 2009. – с. 8.

Специфические виды мошенничества и обеспечение безопасности при использовании платежных карт и электронных платежей

Использование платежных карт, электронных денег и мобильных платежей связано с рисками потерь от специфических видов мошенничества.

С платежными картами связаны риск физической утраты в результате кражи или потери. Этот риск усугубляется распространением дурной привычки записывать ПИН-код карты прямо на ней либо хранить записанный на бумаге ПИН-код в кошельке рядом с картой. Если кошелек попадет в руки непорядочному человеку, снять все деньги с карты не составит труда. Но и без ПИН-кода несложно израсходовать деньги с карты в торговых точках, где транзакции осуществляются без идентификации.

Случается, что банковскую карту без разрешения используют люди, которые могут незаметно ее достать, либо подсмотреть ее данные, либо прямо воспользоваться ею в своих целях. По данным МВД Российской Федерации в роли мошенников довольно часто выступают члены семьи, коллеги по работе, хорошие знакомые держателя карты. По той же причине рискованно отдавать карту для оплаты официантам.

Помимо риска утраты самой карты существует риск кражи персональных данных банковской карты.

Множество мошеннических действий совершается с целью похитить персональные данные карты.

Один из самых известных способов такого мошенничества – скимминг – применяется для кражи данных карт во время использования банкомата. Специальное устройство (скиммер) монтируется на банкомате и считывает данные с магнитной полосы карты, а накладная клавиатура или миниатюрная видеокамера фиксирует ПИН-код. Далее мошенники создают дубликат чужой карты и, зная ПИН-код, похищают с нее деньги.

Скопировать данные можно только с магнитной полосы, карты с чипом от этого риска защищены.

По данным МВД Российской Федерации, чаще всего скимминговые устройства устанавливают на банкоматах, установленных в офисах банков. Поэтому даже охраняемый офис не защищает от риска стать жертвой мошенников.

Однако наибольшее число мошеннических действий связано с онлайн-расчетами. Типичным примером такого рода служит фишинг. Чтобы похитить информацию о карте, мошенники создают фальшивый сайт банка или отправляют поддельный запрос якобы от банка с просьбой сообщить свои персональные данные. Держатель карты вводит на фальшивом сайте свои логин и пароль или отправляет данные в письме. Мошенники их фиксируют и получают доступ к личному кабинету в интернет-банке.

Схожая схема фишинга используется и для кражи электронных денег, а также для мобильных платежей.

Широкое распространение получило так называемое мошенничество «на доверии». Под разными предлогами мошенники (как правило, по телефону или электронной почте) получают индивидуальные данные карты и паспортные данные ее держателя, а затем используют их для получения доступа к личному кабинету в интернет-банке.

Элементарные меры безопасности позволяют в значительной мере снизить риски, связанные с использованием банковских карт и электронных платежей.

Ни в коем случае нельзя хранить ПИН-код в легкодоступном месте, тем более записывать его на самой карте. Нельзя оставлять карту без присмотра.

Никому нельзя сообщать персональные данные карты или электронного кошелька и ПИН-код – даже работники банка или платежного сервиса не имеют права требовать эту информацию ни при каких обстоятельствах.

При использовании интернет-банка или электронного кошелька нельзя заходить по ссылкам с посторонних веб-ресурсов или из писем сомнительного происхождения, поскольку они могут вести на фишинговый сайт.

Контролировать движение средств на своем счете и сразу отследить несан-

кционированное списание средств помогает система смс-оповещения об операциях по карте по мобильному телефону.

Дополнительной мерой безопасности для держателей банковских карт служит страхование от риска утраты в результате кражи или потери, от мошеннических действий в Интернете. При этом, как правило, действие страховки не распространяется на скимминг.

Основные тенденции изменений потребительского поведения и потребления информации, связанные с развитием цифровых и мобильных технологий

Развитие цифровых и мобильных технологий сокращает повседневное использование наличных денег. По данным опроса Национального агентства финансовых исследований (НАФИ), в 2013 году 69% респондентов каждый день расплачивались наличными, а к началу 2016 года эта доля снизилась до 56%.

Результаты опросов НАФИ наглядно свидетельствуют о том, как меняется потребительское поведение. Все больше клиентов использует безналичные способы оплаты, об этом говорит ежегодное увеличение числа держателей банковских карт и аудитории онлайн-магазинов, получают распространение новые технологии мобильных платежей (см. таблицу 2).

Около трети россиян (30%) в 2016 году регулярно оплачивали повседневные покупки безналичным способом, чаще одного раза в неделю безналичные расчеты использовали 37% опрошенных.

Бесконтактные банковские карты использовали 24% опрошенных. О возможности совершать бесконтактные платежи с помощью мобильного телефона осведомлены 65% опрошенных, пользовались этой возможностью 5%. При этом каждый десятый респондент считает определяющей характеристикой покупки следующего смартфона наличие в телефоне технической возможности проводить бесконтактные платежи, а для 30% это будет весомым бонусом (данные НАФИ).

Три четверти россиян (73%) пользовались банковскими картами, в 2009 году эта доля составляла 31%, таким образом, за семь лет она выросла более чем в два раза. Число держателей «зарплатных»

Таблица 2. Эмиссия банковских карт в Российской Федерации, 2007–2016 гг., в млн. ед.

Период	Всего	Расчетных карт	Карт с овердрафтом	Кредитных карт
На 10.2016	250,96	221,35	35,50	29,61
На 01.2016	243,90	214,44	37,62	29,46
На 01.2015	227,67	195,90	39,73	31,76
На 01.2014	217,46	188,28	39,46	29,19
На 01.2013	191,50	169,01	31,79	22,48
На 01.2012	162,90	147,87	25,83	15,03
На 01.2011	137,83	127,79	22,45	10,05
На 01.2010	123,99	115,39	21,27	8,60
На 01.2009	118,53	109,34	26,83	9,30
На 01.2008	103,04	94,10	-	8,94
На 01.2007	74,76	68,92	-	5,66

Источник: Банк России.

и социальных карт за этот же период увеличилось с 24% до 63%.

Драйвером роста безналичных платежей выступает онлайн-торговля. Значительно выросла доля безналичных платежей в онлайн-магазинах (с 14% в 2013 году до 55% в 2016 году).

«Рост финансовой грамотности населения позволит более активно развиваться сектору безналичных финансовых транзакций, поддержит тенденцию к снижению наличного денежного оборота, что также будет вести к увеличению собираемости налогов, прозрачности и подконтрольности финансового сектора».[4]

Разнообразие технологий и способов безналичной оплаты и электронных платежей, постоянное появление новых технологий и устройств формирует в обществе запрос на получение информации по их использованию. При этом население, в основном, ищет ответы на возникающие вопросы не в специализированных изданиях и не на тематических веб-ресурсах, а в популярных массовых СМИ.

Возрастная и региональная специфика пользования новыми технологиями

О возрастной и региональной специфике пользования новыми технологиями для денежных расчетов и переводов можно судить по результатам опросов НАФИ за 2016 год.

Дебетовые карты чаще оформляют респонденты 25–34 лет (44%). Кредитные карты наиболее востребованы среди 25–44-летних (27–28%).

Регулярно оплачивать повседневные покупки безналичным способом в большей степени свойственно молодежи в возрасте 24–35 лет (40%).

Исходя из данных опросов, можно отметить, что к новым технологиям и сервисам наиболее активно закономерно приобщается молодежь, проживающая в крупных городах.

Роль т. н. «гражданской журналистики» в обучении потребителей безопасному пользованию современными технологиями при осуществлении платежей

Средства массовой информации играют ключевую роль в обучении потребителей безопасному пользованию современными технологиями при осуществлении платежей. Население получает через СМИ основную массу информации о различных способах осуществления электронных платежей и расчетов, их возможностях и правилах использования, особенностях и рисках.

«Опыт реализации различных программ повышения финансовой грамотности, как в России, так и за рубежом, показывает, что целесообразно использовать возможности всех каналов передачи знаний для более широкого охвата аудитории. Печатные издания и публикации, телевидение, радио, тематические конференции и выступления информационно-просветительского характера в совокупности обладают синергетическим эффектом при формировании цивилизованных форм эффективного экономического поведения».[5] В случае с практикой использования банковских карт влияние СМИ можно оценить как одно из наиболее эффективных: большинство россиян освоили основные способы обеспечения безопасности своих карт.

Одной из важных задач СМИ является информирование населения о способах мошенничества в сфере электронных платежей и расчетов и популяризация мер безопасности, которые необходимо предпринимать, чтобы максимально снизить риск оказаться жертвой мошенников.

«При должной расстановке приоритетов информирование населения о правилах совершения безопасных транзакций позволяет значительно сократить риски понести финансовые убытки клиента-

4 Зеленцова А.В. Повышение финансовой грамотности населения: международный опыт и российская практика. / Зеленцова А. В., Блискавка Е. А., Демидов Д. Н. – М.: ЦИПСиР, КНОРУС, 2012. – с. 7.

5 Зеленцова А.В. Повышение финансовой грамотности населения: международный опыт и российская практика. / Зеленцова А. В., Блискавка Е. А., Демидов Д. Н. – М.: ЦИПСиР, КНОРУС, 2012. – с. 100

ми банков и позволит повысить доверие к финансовой системе в целом».[6]

Задача СМИ состоит в том, чтобы донести до населения актуальную информацию в наиболее доступной форме. Для этого журналист должен ответственно относиться к подготовке материалов, использовать только проверенные источники информации и привлекать авторитетных профессиональных экспертов. В данной ситуации некорректная информация, транслированная СМИ, может стать причиной финансовых потерь введенного в заблуждение человека.

Разбор материалов СМИ по теме лекции

Примером распространения СМИ некорректной информации стала **серия публикаций об уязвимости для хакерских атак платежных карт «Мир»**, которые с 2016 года выпускают в рамках Национальной системы платежных карт. С появлением этих карт их начали использовать для «зарплатных» проектов бюджетных организаций и государственных органов. В связи с этим консультант Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России Александр Чебарь публично предупредил, что возможен всплеск хищений с карт «Мир» при использовании дистанционных каналов обслуживания, так как многие впервые получат в руки подобное платежное средство. Многие СМИ неверно интерпретировали это высказывание как сообщение об уязвимости карт «Мир» для хакерских атак, а некоторые ради броских заголовков подали информацию таким образом, будто Центральный банк РФ обеспокоен уязвимостью карт «Мир» (**статья «Центробанк обеспокоен уязвимостью карт «Мир»**, портал News.ru.com, 15.06.2016). Хотя в тексте публикаций уточнялось, что имеется в виду уязвимость при использовании дистанционных каналов, эта фраза практически ничего не объяснила потребителям, которые запомнили только то, что карта «Мир» небезопасна.

Многие СМИ не посчитали нужным или не смогли объяснить, что консультант Центрального банка РФ имел в виду совсем другое – мошеннические схемы «на доверии», когда держатели карт из-за низкого уровня финансовой грамотности сами сообщают посторонним людям свои конфиденциальные данные, тем самым открывая доступ к деньгам на своем карточном счете. В связи с большим общественным резонансом вызванных волной публикаций об уязвимости карт «Мир», Центральному банку РФ пришлось сделать официальное заявление о том, что использование карты «Мир» не менее безопасно, чем карт международных платежных систем. Однако репутация проекта развития Национальной системы платежных карт очевидным образом пострадала.

Источник: http://www.newsru.com/finance/15jun2016/mircards.html

В статье «Как защитить себя от кибермошенников» (газета МК, 05.04.2015) описываются наиболее распространенные схемы мошенничества, которые используются для похищения денежных средств при использовании платежных инструментов – банковских карт, электронных кошельков и платежных сервисов. Это распространенный тип статьи для массовых изданий, который содержит советы читателям, описывает признаки, по которым можно распознать мошеннические действия.

Чтобы усилить авторитетность рекомендаций, используются данные и комментарии экспертов – «Лаборатории Касперского» и платежного сервиса «Яндекс-Деньги»: «Обращайте внимание на названия сайтов, – советует специалист «Яндекс. Денег» по вопросам безопасности Анна Ложкина. – Были случаи, когда мошенники делали сайты-двойники, но вместо, к примеру, www.moybank.ru использовали название www.mybank.ru – невнимательность приводила к тому, что люди собственноручно передавали все свои платежные данные ворам».

6 Сборник практических кейсов по теме «Финансовая грамотность и массовая информация». / [Янин Д. Д.и др.]; под. ред. Тайца М. Ю./ – Министерство финансов Российской Федерации. – 2016. – с. 125.

В целом материал изложен доступным языком, однако встречаются специфические термины, непонятные массовому читателю. Их следует избегать в подобных материалах: «Самая многочисленная и популярная среди злоумышленников группа – банкеры. Этот тип программ включает банковские трояны и бэкдоры для кражи денег со счетов либо для получения информации, необходимой для кражи». В данном случае использование профессиональной лексики ничем не оправдано и легко могло быть заменено на понятные массовому читателю определения.

Источник: http://www.mk.ru/economics/2015/04/05/kak-zashhitit-sebya-ot-kibermoshennikov.html

Событийная заметка на портале РБК «AliExpress позволит россиянам оплачивать покупки с мобильного телефона» (портал РБК, 24.03.2015) сообщает о новой услуге – оплате покупок на интернет-площадке с помощью мобильного телефона. Это типичный для делового издания вид публикации, информирующий о новых услугах с использованием платежных сервисов.

В заметке указываются ключевые сведения о внедрении нового способа оплаты: когда его можно будет начать использовать, и сколько это будет стоить для покупателя.

Отличительной чертой публикаций в деловых СМИ является наличие информации не только потребительской направленности, но и связанной с бизнес-процессами. Причем по законам жанра нужно обязательно указывать источник таких сведений, как это сделано в заметке РБК: «Для вывода услуги на рынок AliExpress заключила партнерство с процессинговой компанией «Союзтелеком» и платежной системой НКО «Рапида», которые отвечают за техническое обеспечение расчетов. Все операторы подтвердили РБК сотрудничество с китайской площадкой».

Также в заметке цитируется комментарий ньюсмейкера заметки – представителя Alibaba Group, владельца торговой площадки AliExpress. Такой комментарий также входит в число обязательных требований к событийным заметкам в деловых изданиях.

Источник: http://www.rbc.ru/technology_and_media/24/03/2015/55113d059a79477ccffd8d71

Литература:

1. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе». // Собрание законодательства Российской Федерации. – 2016. – № 27. – ст. 4223.
2. Федеральный закон от 02.12.1990 № 395–1-ФЗ «О банках и банковской деятельности». / Собрание законодательства Российской Федерации. – 2016. – № 27. – ст. 4295.
3. Сборник практических кейсов по теме «Финансовая грамотность и массовая информация». / [Янин Д. Д. и др.]; под. ред. Тайца М. Ю./ – Министерство финансов Российской Федерации, 2016. – 137 с.
4. Гид по финансовой грамотности / коллектив авторов. – М.: КноРус. Центр исследования платежных систем и расчетов, 2010. – 456 с.
5. О. М. Иванов. Стоимость кредита: правовое регулирование. / О. М. Иванов. – М.: Инфотропик Медиа, 2012. – 672 с.
6. Электронные деньги и мобильные платежи / коллектив авторов. – М.: КНОРУС; Центр исследования платежных систем и расчетов, 2009. – 368 с.
7. Янов В. В. Деньги, кредит, банки / учеб. пособие для вузов по направлению подгот. «Экономика» (квалификация (степень) «бакалавр») / В. В. Янов, И. Ю. Бубнова. – М.: КноРус, 2014. – 424 с.
8. Зеленцова А. В. Повышение финансовой грамотности населения: международный опыт и российская практика. / Зеленцова А. В., Блискавка Е. А., Демидов Д. Н. – М.: ЦИПСиР, КНОРУС, 2012. – 112 с.
9. Шамраев В. Предоплаченные инструменты розничных платежей – от дорожного чека до электронных денег / ред. Кузнецов и др. – М.: Маркет ДС, 2016. – 304 с.
10. Воронцова, С. В. Преступления в сфере электронных расчетов и платежей. Правовые и организационно-тактические основы противодействия / С. В. Воронцова. – М.: Юркомпани, 2015. – 336 с.
11. Арт Я. А. Внятное руководство для обычного человека, где, как и на что взять деньги / Арт Я. А. – М.: Астрель, 2012. – 320 с.

Контрольные вопросы лекции:

1. Виды платежных карт.
2. Виды банковских карт. Чем отличаются банковские карты разного уровня?
3. Основные особенности дебетовых карт.
4. Основные особенности карт с овердрафтом.
5. Основные особенности кредитных карт.
6. Виды предоплаченных карт, их основное отличие от других банковских карт.
7. Принцип использования электронных денег.
8. Принцип действия мобильных платежей.
9. В чем заключаются особенности российского законодательства в сфере электронных платежей?
10. Какие виды мошенничества в сфере электронных платежей наиболее распространены?

Методические рекомендации к лекции «Платежные инструменты»

Данная **тема** является обязательной, так как изучает самый динамично развивающийся в России сегмент финансового рынка – безналичные платежи, а именно, розничные платежные инструменты, такие как карты, электронные деньги и мобильные электронные технологии.

Актуальность включения данной темы в курс дисциплины усиливается тем, что регулирование обращения электронных средств платежа только формируется. Риски при использовании современных платежных инструментов высоки, поэтому на журналистах лежит ответственность знакомить потребителей с грамотным поведением и безопасным использованием электронных технологий.

Количество занятий по теме: 1.

Цель занятия – изучить особенности и функционирование разных видов платежных карт, электронных денег, ознакомиться с использованием мобильных приложений и других видов электронных платежей.

Особое внимание на занятии уделяется вопросам осмотрительного, грамотного поведения и потребления информации, связанной с развитием электронных технологий, а также роли журналистов в обучении эффективному пользованию современными платежными инструментами.

Ключевые понятия: платежная карта, банковская карта, дебетовая карта, кредитная карта, грейс-период, карта с овердрафтом, предоплаченная карта, кобрендинговая карта, платежная система, международная платежная система, локальная платежная система, электронные деньги, электронный кошелек, мобильный платеж, бесконтактная оплата, мобильная коммерция, скимминг, фишинг.

Умения

В результате изучения данной темы студенты должны уметь:

- различать виды платежных карт;
- выбирать оптимальный вариант платежной карты;
- грамотно пользоваться платежными банковскими и виртуальными картами;
- пользоваться электронными деньгами;
- осуществлять мобильные платежи;
- определять сложности и проблемы, связанные с регулированием электронных платежей в российском законодательстве;
- определять риски, связанные с использованием современных платежных инструментов.

Базовые знания

В результате изучения данной темы студенты должны знать:

- каковы особенности банковской платежной карты;
- каков механизм эмиссии международных и локальных банковских платежных карт;
- каковы основные характеристики дебетовых карт;
- каковы особенности использования карт с овердрафтом;
- в чем отличия кредитных карт от остальных видов банковских платежных карт;
- каковы уровни банковских карт, в чем их отличия;
- что представляют собой предоплаченные карты;
- в чем особенности использования электронных денег;
- каковы особенности российского законодательства в сфере электронных платежей;
- каковы основные виды мошенничества с платежными инструментами;
- каковы тенденции изменения потребительского поведения и потребления

информации, связанные с развитием электронных технологий;
- какие задачи решают СМИ в сфере использования населением электронных платежей и расчетов.

Личностные характеристики и установки:

- закрепление навыков ответственного отношения к профессиональной деятельности;
- отношение к профессиональной деятельности как к возможности предупреждения неграмотного потребительского поведения при использовании платежных инструментов;
- понимание роли СМИ в ознакомлении населения с рисками использования платежных инструментов;
- осознание ответственности СМИ за распространение некорректной информации, усложняющей реализацию национальных проектов по развитию российских платежных инструментов.

Формы организации занятия

- аудиторное занятия (лекция);
- групповая форма работы – обсуждение публикаций;
- подготовка ответов на вопросы, выполняемая самостоятельно после занятия;

Аудиторные занятия (лекции), включающие в том числе рассмотрение примеров влияния информации СМИ и т. н. «гражданской журналистики» на запуск платежной карты «Мир», изменение потребительского поведения населения в результате раскрытия разных видов кибермошенничества, а также ознакомления потребителей с новой платежной услугой.

Описание хода занятия

1. В начале лекции можно выяснить, кто из присутствующих является активным пользователем платежных карт. Выяснить, какими видами карт пользуются слушатели и почему. После краткого обсуждения можно приступить к изложению основного материала.
2. При изложении материала о кобрендинговых картах можно попросить аудиторию привести знакомые им примеры кобрендинговых карт. Далее можно разделить аудиторию на 2 группы и предложить каждой группе свой кобрендинговый проект. Во время обсуждения обосновать его целесообразность, в том числе с коммерческой точки зрения.
3. При переходе к рассмотрению особенностей электронных денег можно также поинтересоваться у аудитории, кто является активным пользователем данного вида платежей, и выяснить особенности. Затем перейти к изложению материала, добавив или поправив при необходимости ответы студентов.
4. После изложения материала о рисках и видах мошенничества можно обсудить со студентами, сталкивались ли они с фактами обмана при использовании современных платежных инструментов.
5. В конце занятия можно перейти к обсуждению 3 статей СМИ. Разделите аудиторию на 3 группы. Каждой группе раздайте по статье. После прочтения статей студенты каждой группы должны оценить профессионализм раскрытия финансовой проблематики, ее влияние на решение освещаемой проблемы и озвучить выводы для остальной аудитории. Лектор в случае необходимости дает свои комментарии после выступления каждой группы. Время – 20 мин.

Формы текущей оценки

Преподаватель осуществляет текущий контроль, оценивая аудиторную работу студентов:

- активность в дискуссиях на лекции;
- активность при обсуждении статьи в командах.

Самостоятельная работа студентов оценивается после сдачи решенных задач на следующем занятии.

ЦЕНТРОБАНК ОБЕСПОКОЕН УЯЗВИМОСТЬЮ КАРТ «МИР»

NEWSru.com, 15.06.2016

Национальная система платежных карт (НСПК) «Мир» на начальном этапе использования может быть крайне уязвимой для злоумышленников через дистанционные каналы обслуживания.

Такое мнение во время заседания комитета Торгово-промышленной палаты по финансовым рынкам и кредитным организациям высказал консультант центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовый сфере (FinCERT) Банка России Александр Чебарь, пишет РБК.

При этом, по его мнению, в целом уровень защиты карты «Мир» соответствует стандартам безопасности международных платежных систем. «Однако с точки зрения работы самих пользователей карт, да, возможен небольшой провал в течение первого времени использования этих карт. То есть явный провал с точки зрения хищения денежных средств. Атака будет не на саму карту, а на какие-то системы, которые дополняют эту карту, например на системы дистанционного банковского обслуживания, чтение информации о платежной карте», – пояснил Чебарь.

Начальник отдела по управлению инцидентами департамента защиты информации «Газпромбанка» Николай Пятиизбанцев, в свою очередь, отметил, что для снятия средств с карты «Мир» необходимо знать всего лишь номер самой карты и ПИН-код. «Ни о каких защищенных технологиях речи нет», – добавил специалист.

Напомним, еще осенью прошлого года газета «Ведомости» выяснила, что НСПК не может рассчитывать на использование системы защиты онлайн-трансакций 3D-Secure. Правами на эту технологию владеет Visa. MasterCard и другие платежные системы используют ее по лицензии. НСПК такую лицензию не получала и не может обеспечить повышенную защиту операциям по картам в интернете.

Технология 3D-Secure обеспечивает безопасность платежей в интернете, при ее использовании для аутентификации клиенту на мобильный телефон отправляется динамический код. Когда клиент проводит операцию по своей карте через банк, у которого нет дополнительной защиты, вся ответственность ложится на банк, который выдал карту клиенту. Банки, обслуживающие торговые предприятия в интернете, также могут не использовать 3D-Secure, но в этом случае ответственность за несанкционированные транзакции будет лежать на них. На долю онлайн-платежей приходится порядка 5–10% всех операций.

В конце мая СМИ писали о том, что банкам повысят плату за подключение к карте «Мир» с 450 тысяч до 600 тысяч рублей. Официально повышение тарифов названо отменой скидки в 150 тысяч рублей за «настройку начальной конфигурации» НСПК.

Не исключено и то, что к концу третьего квартала тариф зафиксируется на уровне 900 тысяч рублей, этот вопрос сейчас обсуждается в НСПК. При этом, правда, в отличие от международных платежных систем Visa и MasterCard «Мир» не будет взимать с банков так называемые взносы участников (составляют несколько десятков тысяч долларов в год).

По требованиям Центробанка подключиться к НСПК банки должны к 1 июля. На данный момент, по сведениям НСПК, только 29 банков из 93 участников платежной системы «Мир» полностью или частично открыли свои эквайринговые сети к приему национальных карт и только 13 из них приступили к выпуску.

Банки пытались пролоббировать продление крайнего срока до октября 2016 года, но регулятор не пошел им на ус-

тупки. Впрочем, первая партия банков, подключившихся к национальной платежной системе, оказалась в более выгодном положении.

В марте, напомним, ЦБ потребовал от банков представить планы выпуска карт «Мир» на 2016 год, чтобы ЦБ мог изучить степень их готовности к работе с НСПК.

Ранее банкиры провели оценку себестоимости карты и поняли, что она обойдется им в 1,5 раза дороже, чем массовые Visa и MasterCard. Отмечалось, что тарифы не удовлетворяют банкиров и снижают их интерес к выпуску подобных карт.

Российские власти, напомним, решили создать НСПК весной 2014 года, после того, как некоторые российские банки попали под американские санкции, а Visa и MasterCard, подчиняясь требованиям США, на какое-то время перестали обслуживать выпущенные этими банками карты.

В мае 2014 года президент России Владимир Путин подписал закон, согласно которому операторы, не являющиеся национально значимыми платежными системами, должны будут внести обеспечительный взнос на специальный счет в Центробанке. Позднее российские власти согласились освободить платежные системы от уплаты взноса, если те переведут процессинг в НСПК.

Сначала российское руководство думало о привлечении в качестве оператора НПС действующих платежных систем – УЭК или «Золотой короны», но потом решило, что систему надо делать с нуля.

На первом этапе (2014 год – первый квартал 2015 года) разрабатывалась технология по обработке операций по картам платежных систем, включая международные Visa и MasterCard.

На втором этапе (к концу 2015 года) было запланировано начало выпуска карт. На третьем этапе (2016–2018 годы) НСПК намерена разработать продуктовую линейку на базе своей карты (дебетовые, кредитные и предоплаченные карты) и предложить ее на российском и международном рынках.

Объявлено, что национальная карта будет приниматься на всей территории России и позволит совершать все типовые операции: снимать наличные, оплачивать покупки в торговых сетях, осуществлять бесконтактные и мобильные платежи. В течение 2016 года планируется выпустить 30 миллионов национальных платежных карт «Мир».

Первыми эмитентами карты «Мир» стали «Газпромбанк», «МДМ банк», «Московский индустриальный банк», «Связь-банк», работающий в Крыму РНКБ, а также попавшие под санкции банк «Россия» и «СМП банк».

Как заявил 15 декабря 2015 года глава НСПК Владимир Комлев, к приему карт «Мир» уже подключены более 1,5 тысячи банкоматов и сотни POS-терминалов.

КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРМОШЕННИКОВ

MK.RU, 5.04.2015

Оплачивая покупки через Интернет, можно сэкономить массу времени и сил. Но деньги в Сети могут привлечь внимание мошенника так же, как кошелек, торчащий из сумки в метро, или портмоне в заднем кармане джинсов. В Интернете мошенники действуют инкогнито, поэтому смелее и наглее, но играют они на тех же человеческих качествах, что и в реальной жизни, – чаще всего жертвой обмана пользователь становится из-за невнимательности или доверчивости. Кроме того, мошенники могут использовать специальные методы – вирусы, поддельные сайты, перехват и подбор паролей к учетным записям в социальных сетях и других сервисах, мошеннические письма. Как же обезопасить себя от воров?

90% онлайн-покупателей предпочитают отечественные магазины

Российский рынок онлайн-торговли становится более развитым: люди активно осваивают современные способы доставки и оплаты товаров. Сегодня в стране 31 млн онлайн-покупателей, из них 43% живет в городах-миллионниках. Главным образом это молодые люди в возрасте до 35 лет. Ядром потребительской аудитории являются 8 млн россиян, которые покупают в интернет-магазинах не реже одного раза в месяц.

Очевидно, интернет-коммерция, которая сейчас занимает около 3%, и дальше будет отбирать долю у офлайного ритейла. Особенно это актуально в период кризиса и падения потребительского спроса, когда многие магазины закрываются, испытывая дефицит оборотных средств, на оплату труда сотрудников, арендных платежей.

В денежном выражении объем рынка интернет-торговли в 2014 году, по данным консалтинговой компании Data Insight, оценивается в 440 млрд рублей. Речь идет только о материальных товарах. А если взять вместе с билетами и так называемым цифровым контентом (музыка, игры, видео, пин-коды, скрипты, и т. д. – «МК»), то получится 660 млрд рублей.

При этом все больше покупателей выбирают безналичные способы расчета. «Яндекс. Маркет» совместно с компанией GfK провел масштабный опрос среди интернет-покупателей. Выяснилось, что 48% респондентов, заказывавших в прошлом году товары на торговых порталах, сразу оплачивали их банковской картой. В 2013 году таких было 36%. Основными инструментами для покупок в Глобальной сети по-прежнему остаются компьютеры и ноутбуки, а не смартфоны или планшеты.

Половина онлайн-покупателей хотя бы раз за последний год делали заказы за границей (годом ранее – 36%). Особенно сильно выросла популярность китайских интернет-площадок. Замечена интересная тенденция: чем меньше город, тем больше доля жителей, которые делают заказы в Китае, и меньше доля тех, кто покупает товары в других странах. В Москве эта пропорция примерно одинаковая. Среди причин покупки на иностранных сайтах респонденты называют широкий ассортимент, дешевизну и высокое качество товаров. Отказываются от покупок за рубежом из-за долгих сроков доставки и опасения стать жертвой мошенников. Отчасти это оправданно, поскольку число покупателей, получивших из-за границы некачественный товар, выросло по сравнению с 2013 годом на 9%, достигнув показателя 21%.

Не случайно услугами российских магазинов по-прежнему пользуются больше 90% опрошенных. Средняя стоимость заказа в наших интернет-магазинах составляет 6591 рубль, в зарубежном – 3945. У москвичей средний чек выше, зато разница между средней суммой заказа в отечественном и иностранном магазинах меньше – 7947 рублей и 6084 рублей соответственно.

50% людей заявили, что последнюю покупку они сделали со скидкой. При этом

покупатели стали чаще пользоваться своими правами: за год доля тех, кто возвращал товар в магазин, выросла с 51% до 63%.

Что же покупают в Сети? В России большинство людей заказывают мелкую бытовую технику, одежду и обувь, мобильные телефоны и планшеты, за рубежом – одежду и обувь, детские товары, мобильные телефоны и планшеты, косметику и парфюмерию. В китайских магазинах чаще покупают мобильные устройства, в англоязычных магазинах прочих государств – косметику.

«Метод хамелеона»

Вместе со специалистами по интернет-безопасности «Лаборатории Касперского» и одним из крупнейших отечественных сервисов электронных платежей «МК» рассказывает о наиболее характерных примерах мошеннических схем в Сети, связанных с онлайн-оплатой.

Попытки запуска банковского вредоносного ПО в 2014 году были отражены на компьютерах около 2 млн пользователей.

Доля фишинговых атак, направленных на похищение финансовых данных пользователей в России, составила 20% – об этом говорят результаты исследования, проведенного «Лабораторией Касперского». При этом злоумышленники стали меньше использовать банковские бренды и сосредоточили свое внимание на интернет-магазинах и платежных системах. К примеру, впервые наблюдался резкий всплеск атак, эксплуатирующих названия сайтов, торгующих авиабилетами. Ранее подобные онлайн-площадки не пользовались такой популярностью у мошенников.

Самая многочисленная и популярная среди злоумышленников группа – банкеры. Этот тип программ включает банковские трояны и бэкдоры для кражи денег со счетов либо для получения информации, необходимой для кражи. Попав на устройство пользователя, банковский троянец закрепляется в системе, а затем приступает к выполнению поставленной задачи. Информация может быть похищена разными способами: делаются снимки экрана, на которых отображается нужная информация, перехватываются вводимые с помощью клавиатуры данные. Для перехвата клавиатурных данных существуют специальные программы – клавиатурные шпионы, предназначенные для воровства любого конфидента, не только финансового характера. Чтобы обезопасить себя от этой угрозы, достаточно регулярно обновлять антивирусы и проверять компьютер на «здоровье».

Вирусы можно подхватить, загружая вложенные файлы, переходя по ссылкам из электронных писем и сообщений из соцсетей, используя непроверенные флешки и жесткие диски, а также посещая зараженные сайты. Вирус проскакивает даже во время общения с хорошо знакомым человеком, от которого не ждешь подвоха – он и сам может не знать, что компьютер заражен.

Кроме того, «мошенник-хамелеон» может позвонить, представиться работником банка или какого-либо сервиса и попросить продиктовать ваши платежные данные, например, пароль или пин-код. Или, как вариант, на телефон придет SMS с паролем для совершения платежа – сразу после этого вам позвонит встревоженный человек, скажет, что ввел ваш номер телефона по ошибке, и попросит назвать код. На самом деле код из SMS – это пароль не к счету незнакомца, а к вашему счету. В обоих случаях злоумышленник пытается выманить данные, с помощью которых можно украсть деньги. Нужно помнить, что ни банки, ни платежные сервисы никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS.

Лучше всего в Интернете использовать те банковские карты и платежные сервисы, которые предлагают одноразовые пароли (те, что приходят в SMS или генерируются специальным бесплатным приложением для смартфона). Такие пароли, даже если их перехватит злоумышленник, бесполезны – каждый следующий пароль подтверждает только одну операцию, и повторно использовать его нельзя.

Есть и другой способ получить от вас данные, необходимые для подтверждения платежа. В этом случае мошенники предпочитают вообще обойтись без вашей помощи – им достаточно раздобыть дубликат вашей SIM-карты, чтобы получать все од-

норазовые пароли вместо вас. Правда, верно атаковать доверчивых пользователей так нельзя – слишком трудоемко и затратно. Однако если вы заметили, что на ваш телефон перестали поступать звонки, SMS и вы ни с кем не можете связаться – сразу звоните в банк или платежный сервис и останавливайте операции со счетами, к которым был привязан скомпрометированный номер. Если мошенники действительно работали по этому сценарию, заблокируйте SIM-карту и выпустите новую.

Еще один «популярный» метод. Пользователь может получить фальшивое электронное письмо от имени своего банка с информацией о том, что его счет заблокирован и для разблокировки необходимо перейти по ссылке и ввести свои данные. Сделав это, пользователь передаст в руки киберпреступников ключи к «тумбочке, где деньги лежат». Банки никогда не рассылают сообщения о блокировке счета по электронной почте, поэтому переходить по ссылкам из таких писем нельзя.

В случае перехода по ссылке из сомнительного письма проверяйте, чтобы адрес в браузере начинался с https://, а не с http:// (символ «s» указывает на безопасное соединение). При этом если браузер сигнализирует об ошибках, не рекомендует переходить дальше, сообщает о незащищенном соединении – платить однозначно не стоит. Также тревожным сигналом должно стать то, что система попросила повторно ввести логин или пароль, хотя вы не покидали свой аккаунт.

«Обращайте внимание на названия сайтов, – советует специалист «Яндекс. Денег» по вопросам безопасности Анна Ложкина. – Были случаи, когда мошенники делали сайты-двойники, но вместо, к примеру, www.moybank.ru использовали название www.mybank.ru – невнимательность приводила к тому, что люди собственноручно передавали все свои платежные данные ворам».

Одно время по Интернету ходили так называемые «нигерийские письма», в которых автор обещал жертве огромное вознаграждение в будущем в обмен на небольшие накладные расходы прямо сейчас. Смысл письма, как правило, примерно такой: мы – сбежавшая от преследователей королевская семья (принц, принцесса и т. д. – вариаций много) из Демократической Республики Конго; скоро мы получим 180 млн долл. США со своего счета, и если вы сейчас переведете немного денег (например, на оформление или доставку документов), то потом мы вас щедро отблагодарим.

Что будет дальше?

Есть менее изощренные способы обмана, которые вроде бы всем известны, но все равно кто-то периодически попадается. В Интернете часто встречаются предложения купить что-то очень выгодно – до неприличия. На первый взгляд объяснение низкой цены может быть правдоподобным: подарили – не понравилось, распродажа конфискованного на границе товара, ликвидация магазина и т. д. Оплатить такой товар предлагается, переведя деньги на банковскую карту, электронный кошелек или мобильный номер. Если это сделаете, ни товара, ни денег вы больше можете не увидеть.

Поэтому не ленитесь проверять контактные данные и реквизиты. У серьезных интернет-магазинов, как правило, есть телефон поддержки, офис. Позвоните по указанному номеру, поищите отзывы в Интернете. Дурная слава быстро расходится в Сети, и если магазин уже когда-то повел себя недобросовестно, цифровой след наверняка остался.

Вообще для интернет-покупок лучше завести отдельную дебетовую карту, деньги на которой лимитированы – кредитная карта может вогнать вас в большие долги, если доступ к ней получат злоумышленники. Безопасней платить с карт, привязанных к интернет-кошельку. Они позволяют оплачивать покупки картой, не предоставляя о ней каких-либо данных даже продавцу.

«С каждым годом мы наблюдаем рост киберпреступности, – говорит антивирусный эксперт «Лаборатории Касперского» Сергей Ложкин. – Внедрение вредоносного ПО, атаки с целью получения доступа к аккаунтам онлайн-банкинга, подмены платежных реквизитов никуда не денутся в ближайшие годы. По моему мнению, тенденция такова, что мошенники переклю-

чатся с обычных пользователей на финансовые организации, где в случае успешной аферы их ждет гораздо большая прибыль. Хакеры научатся удаленно управлять выдачей денег в банкоматах, выполнять денежные переводы и незаметно манипулировать системой онлайн-банкинга».

Ограбление на миллиард

Не только торговля перемещается в Интернет, но теперь стали реальностью и виртуальные ограбления банков. Доходы киберпреступников от финансового мошенничества могут быть поистине колоссальными: в ходе совместного расследования Европола и Интерпола раскрыта беспрецедентная киберпреступная операция, в рамках которой злоумышленники похитили миллиард американских долларов.

Киберограбление продолжалось два года. За ним стоит международная группировка из России, Украины, ряда других европейских стран, а также Китая. Деятельность мошенников из банды Carbanak затронула около 100 банков, платежных систем и других финансовых организаций из почти 30 стран, в частности из России, США, Германии, Китая, Украины, Канады, Гонконга, Тайваня, Румынии, Франции, Испании, Норвегии, Индии, Великобритании, Польши, Пакистана, Непала, Марокко, Исландии, Ирландии, Чехии, Швейцарии, Бразилии, Болгарии и Австралии. Как выяснили эксперты, наиболее крупные суммы денег похищались в процессе вторжения в банковскую сеть: за каждый такой рейд киберпреступники крали до 10 миллионов долларов. В среднем ограбление одного банка – от заражения первого компьютера в корпоративной сети до кражи денег и сворачивания активностей – занимало у хакеров от двух до четырех месяцев.

Преступная схема начиналась с проникновения в компьютер одного из сотрудников организации посредством фишинговых приемов. После заражения машины вредоносным ПО злоумышленники получали доступ к внутренней сети банка, находили компьютеры администраторов систем денежных транзакций и разворачивали видеонаблюдение за их экранами. Таким образом, банда Carbanak знала каждую деталь в работе персонала банка и могла имитировать привычные действия сотрудников при переводе денег на мошеннические счета.

Эти ограбления банков отличаются от остальных тем, что киберпреступники применяли такие методы, которые позволяли им не зависеть от используемого в банке ПО, даже если оно было уникальным.

Хакерам даже не пришлось взламывать банковские сервисы. Они просто проникали в корпоративную сеть и учились, как можно замаскировать мошеннические действия под легитимные. Это по-настоящему профессиональное ограбление.

ALIEXPRESS ПОЗВОЛИТ РОССИЯНАМ ОПЛАЧИВАТЬ ПОКУПКИ С МОБИЛЬНОГО ТЕЛЕФОНА

РБК, 24.03.2015

Интернет-площадка розничной торговли AliExpress, принадлежащая китайскому гиганту Alibaba Group, пытается увеличить число российских покупателей за счет новой услуги – оплаты покупок с помощью мобильного телефона

Новый способ оплаты станет доступен на следующей неделе, сообщил во вторник представитель AliExpress в России Марк Завадский. По его словам, AliExpress станет первой интернет-площадкой из тех, что продают товары из-за рубежа, которая введет возможность оплаты со счета мобильного телефона для абонентов МТС, «МегаФона», «Билайна» и Tele² в России. Для вывода услуги на рынок AliExpress заключила партнерство с процессинговой компанией «Союзтелеком» и платежной системой НКО «Рапида», которые отвечают за техническое обеспечение расчетов. Все операторы подтвердили РБК сотрудничество с китайской площадкой.

Новый способ оплаты позволит привлечь к площадке дополнительных пользователей, говорит Богдан Задорожный, представитель компании Alipay (также входит в Alibaba Group и предоставляет платежные решения для AliExpress и других компаний холдинга). Сейчас, по данным AliExpress, число ее пользователей в России и СНГ составляет около 9 млн человек.

По словам Задорожного, при оплате покупок с мобильного телефона комиссия пользователя оператору составит около 1–3% от суммы покупки. Комиссию будет платить и AliExpress, но ее размер не разглашается.

«В России услуга мобильной коммерции появилась одной из первых в мире 7–8 лет назад. Первый проект запустил «Билайн», потом присоединялись другие операторы», – рассказал директор по продажам «Союзтелекома» Евгений Карпов. «Союзтелеком», по его словам, 15 лет занимается развитием мобильных платежей в различных сегментах, больше 10 лет компания обслуживает SMS-голосование на конкурсе «Евровидение».

По данным «Союзтелекома», в 2013 году рынок мобильной коммерции составил 50 млрд руб. В эту категорию входит оплата товаров и услуг со счета мобильного телефона и премиум-SMS (отправка сообщений на короткие номера).

Оплата со счета мобильного телефона популярна не только в Москве, утверждает Евгений Карпов. По его данным, только 35% пользователей этого сегмента живут в столице, а 65% – в других городах России. Средний чек при этом способе оплаты составляет около 2 тыс. руб., говорит он. Доля пользователей AliExpress за пределами Москвы, Санкт-Петербурга и их областей составляет более 80%, свидетельствуют данные самой компании.

Мобильные операторы говорят о росте оборота мобильных платежей. В МТС этот сегмент в четвертом квартале 2014 года вырос к тому же периоду 2013 года на 23%, до 5,3 млрд руб., количество пользователей мобильных платежей увеличилось на 38%, до 3,6 млн, рассказал представитель оператора Дмитрий Солодовников. По его словам, сейчас со счета мобильного телефона МТС можно оплатить услуги и товары десятков тысяч контрагентов, в том числе Ozon.ru, крупных магазинов цветов, косметики и других. Представитель «ВымпелКома» (бренд «Билайн») Анна Айбашева говорит, что в четвертом квартале база пользователей мобильной коммерции увеличилась более чем на 6%, а выручка мобильной коммерции выросла на 26% год к году (абсолютных цифр она не раскрыла). В «МегаФоне» число пользователей, которые оплачивают покупки с мобильного счета, выросло в 2014 году на 20%, говорит пресс-секретарь компании Алия Бекетова.

В Ozon.ru оплатить покупки со счета мобильного телефона можно с 2013 года,

говорит представитель компании Мария Назамутдинова. Только 0,6% покупок оплачивается этим способом, но при покупке цифровых товаров – игр, софта – этот тип платежа используют в 12,5% случаев. Но пик популярности оплаты со счета мобильного телефона миновал, считает она.

Помимо Ozon на российском рынке такую возможность предоставляют американский агрегатор интернет-скидок Groupon и российский продавец лицензионного программного обеспечения Softkey. У конкурентов AliExpress на международном рынке – площадок Amazon и eBay – нет опции оплаты с мобильного телефона, так же как и у онлайн-ретейлеров Lamoda, «М. Видео», «Связной», «Эльдорадо». Российская Avito позволяет пополнять таким способом виртуальный кошелек и заплатить, к примеру, за премиум-объявление, но не купить у продавца какой-либо товар.

AliExpress принадлежит китайскому холдингу Alibaba Group (капитализация – $209,6 млрд). Мобильные приложения AliExpress являются самыми популярными в России в категории «Шопинг» на платформах iOS и Android (по данным РБК. research). Российские покупатели могут оплачивать покупки банковской картой, электронными деньгами Qiwi Wallet и с помощью сервисов Webmoney и «Яндекс.Деньги».