ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

*Ващекин А.Н., Ващекина И.В.**

Ключевые слова: *банк, платежная система, дистанционное банковское обслуживание, цифровые технологии, информационная безопасность, компьютерное мошенничество, вредоносные программы, противодействие, специальное приложение, инновационные мероприятия.*

Аннотация.

Цель работы: *совершенствование научно-методической базы теории информационной безопасности в банковской сфере.*

Метод: *системно-правовой анализ комплекса технологических средств и организационных приемов, позволяющих снизить финансовые потери и защитить клиентов банков от преступных действий компьютерных мошенников.*

Результаты: *систематизированы приемы и средства нелегального проникновения в системы дистанционного банковского обслуживания; предложены меры противодействия мошенническим операциям; даны характеристики новым продуктам и услугам в исследуемой сфере, как с точки зрения потенциальной информационной уязвимости для преступной деятельности, так и с точки зрения экономической эффективности; для разработки оптимальной стратегии по осуществлению инновационного развития дистанционного банковского обслуживания представлен комплекс взаимосвязанных мер, образующий перечень соответствующих мероприятий.*

DOI: 10.21681/1994-1404-2019-4-86-95

На протяжении последних лет рынок *дистанционного банковского обслуживания* (ДБО) растет, при этом, на первый взгляд парадоксально, увеличиваются и убытки клиентов систем ДБО [9]. Кредитные организации увеличивают финансирование технических мероприятий по поддержанию безопасности серверов, приобретают новейшие программы защиты, однако мошенники придумывают все новые способы присвоения денег банковских клиентов. Принципиально неразрешимой эту *проблему* информационной безопасности делает тот факт, что защитные средства не могут действовать с упреждением, так как их модификация проходит по мере обнаружения новых приемов, наблюдаемых в уже совершенных мошеннических действиях. Преступники, таким образом, всегда обладают инициативой.

Эти персонажи по своему моральному облику заметно отличаются от классических, традиционных преступников, которым приходится в ходе совершения мошенничества или кражи непосредственно контактировать с жертвой или, по крайней мере, с вещами или денежными средствами, которыми они хотят завладеть (для чего от лица, совершающего преступление, требуются определенные волевые усилия). При совершении преступных действий в сфере *«компьютерной» информации* прямое (физическое) воздействие отсутствует, и это обстоятельство расширяет потенциальный круг злоумышленников (многие из которых воспринимают свое участие в преступной схеме как компьютерную игру).

При этом мошенничество в информационно-компьютерной среде наносит существенно больший урон общественным отношениям, чем традиционное мошенничество, поскольку предполагает получение *конфиденциальной информации* о жертве, которая в дальнейшем может использоваться не только в корыстных целях злоумышленника. Нередко происходит продажа соответствующих данных третьим лицам для совершения последующих преступлений, т.е. с одной стороны, жертва подвергается мультипликативной опасности, а с другой – количество потенциальных жертв множится,

* ***Ващекин Андрей Николаевич,*** *кандидат экономических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.*
Email: vaschekin@mail.ru

Ващекина Ирина Викторовна, *кандидат экономических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.*
Email: vaschekina@mail.ru

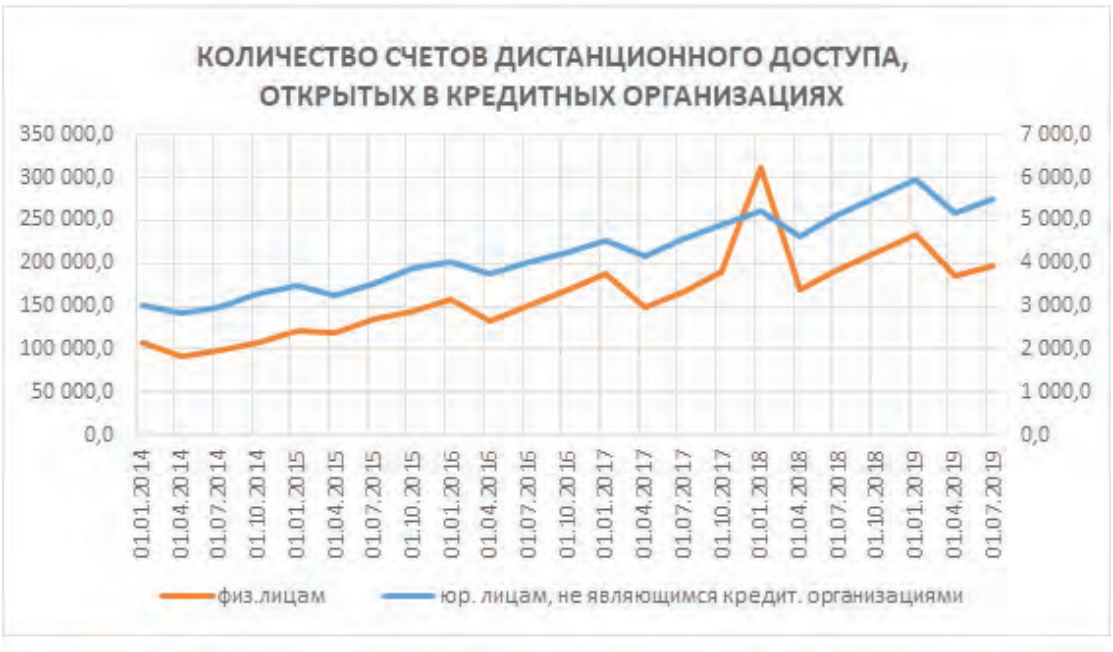

Рис. 1. Количество счетов дистанционного доступа, открытых в кредитных организациях

ими могут стать как физические лица, так и юридические (предприятия и организации), и даже целые государства [1].

Наряду с описанной морально-психологической причиной, имеются и объективные, квантитативные и качественные, также способствующие росту мошенничества в ДБО и возникновению новых направлений нелегальных действий. Среди причин *первого* типа укажем постоянное нарастание количества лиц, использующих эти услуги (на рис. 1 представлена динамика развития ДБО юридических и физических лиц за последние пять лет), а также увеличение объемов и ассортимента предлагаемых продуктов и услуг. Пример причины *второго* типа – использование разных, несогласованных друг с другом платформ для обслуживания клиентов. Следует помнить, что любое взаимодействие в экономике носит *информационный характер*, причем несогласованность между сторонами снижает количество информации, доступной добросовестным контрагентом, и эта информационная неполнота является потенциально уязвимым местом [4].

В настоящее время основная доля мошеннических операций в банковской системе осуществляется в сфере электронных финансовых расчетов, ставших выгодными для хакеров [7]. По прогнозам, хакерские атаки на вычислительную систему с целью доведения ее до отказа или затруднения доступа к системным ресурсам (*DDoS*-атаки) постепенно уйдут на второй план, поскольку уровень безопасности компьютерных систем в коммерческих организациях плавно, но качественно повышается. Кроме того, для осуществления подобных атак необходимы куда большие усилия, чем при применении бот-сетей для организации кражи средств из систем ДБО. При проведении финансовых операций используются компьютеры, обеспеченные интернет-обслуживанием, между которыми происходит переписка по электронной почте, осуществляется обмен файлами [11]. Подобные действия повышают риск заражения компьютеров вредоносным программным обеспечением («вирусами», «троянами» и др. [11]). Используемые антивирусные программы не гарантируют полной защиты от целенаправленных злонамеренных действий, например, с применением технологии руткитов (многопрофильные и самые вредоносные программы) и их варианта – буткитов (*bootkits*), захватывающих управление компьютером ещё до загрузки операционной системы и потому незаметных для обычных антивирусов. Остается не решенной также *проблема* несанкционированного доступа по *скрытым* (нетрадиционным) каналам[1] [12, 16].

Вместе с тем основные угрозы безопасности при использовании ДБО традиционно порождаются *человеческим фактором* (доверчивость, рассеянность, низкая квалификация или злой умысел сотрудников). В связи с этим следует отметить необходимость повышения лояльности работников банков как необходимое условие защиты от подобных преступлений. Исторически важнейшей чертой банковских служащих была преданность интересам банка и лояльность по отношению к клиентам. Современные банки также должны находить действенные средства для поощрения работников, особенно высококвалифицированных, а также обладающих высокой степенью самостоятель-

[1] *См. например:* Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // РАН. Сер. 2. Информ. процессы и системы. – 2005. – № 2. – С. 1 – 7; Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. – 2006. – № 9. – С. 1 – 9.

ности в служебных обязанностях. При несоблюдении этих *условий* риски возрастают: имея информацию об использовании на постоянной основе ДБО с одного и того же компьютера, преступники могут организовать установку вредоносного приложения на него с *USB*-накопителя, принесенного клиентом, или его запуск инсайдером вручную.

Наряду с давно используемыми разнообразными вредоносными программами («вирусами») возрастающее значение среди угроз приобретают «черви» и «трояны», с помощью которых могут вымогаться деньги (типа *Trojan.Winlocker* и *Trojan.Ransom*), неявно собираться информация о пользователе (пароли и списки контактов) или постепенно списываться некоторые суммы денег без ведома владельца.

Эволюция методов взлома систем ДБО выглядит следующим образом. Самый простой и потому до сих пор распространенный способ – завладение приватным ключом электронной подписи (ЭП). Легкости применения мошенниками этого способствует описанная выше людская безответственность, вследствие которой приватные ключи ЭП могут храниться в легкодоступных местах: на *USB*-накопителе, на жестком диске персонального компьютера, на сервере и др. Для завладения данными самых наивных пользователей применяют так называемый фишинг (вылавливание сведений с помощью электронных сообщений от мошенника под видом сообщения от банка или провайдера). Если потенциальная жертва обеспечивает защиту хранения своего приватного ключа ЭП, злоумышленниками применяется более сложный способ: ключ извлекается из закрытой области памяти устройства (оперативной памяти) [14].

Куда более сложным технически оказывается несанкционированный доступ к криптографическим возможностям смарт-карты. Его применение требует от злоумышленника использования специальных средств удаленного управления компьютером клиента (класса *TeamViewer*), либо удаленного подключения к *USB*-порту (технология *USB-over-IP*). Дополнительную сложность для преступника составляет необходимость уловить момент подключения смарт-карты (токена), необходимой для проведения операции.

Наиболее сложный вид атаки – осуществление подмены документа при передаче его на подпись в смарт-карту. При этом жертва видит на своем экране картинку, не совпадающую с той информацией, которая отправляется на подпись в смарт-карту. Одновременно может быть произведена модификация других отчетно-финансовых данных.

Задача технического разрешения *проблемы* взломов непроста, но осуществима [6]. В качестве одного из вариантов предлагается перенос функций контроля основных параметров значимого документа из операционной системы в замкнутую среду, создаваемую на внешнем устройстве. Отчужденный защищенный носитель при этом должен соответствовать следующим требованиям:

– запрещать внесение изменений в алгоритмы своей работы;

– обеспечивать возможность текущего визуального контроля целостности значимых полей документа (номер счета, сумма транзакции, банк-получатель и др.) во внешней (доверенной) среде с последующей передачей его напрямую в смарт-карту на подпись;

– работать со смарт-картами, которые аппаратно реализуют отечественные криптоалгоритмы[2], в соответствии с требованиями Федерального закона от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи»;

– не допускать осуществления подписи до того, как будет нажата кнопка подтверждения транзакции.

Общая проблема существующих систем ДБО состоит в слабой парольной политике и недостаточной защите от подбора учетных данных (*Brute Force*). В этих системах неизбежно заложен недостаток механизма идентификации пользователей – предсказуемый формат идентификаторов или раскрытие информации о существующих в системе идентификаторах. Многие системы ДБО до сих пор не применяют принцип двухфакторной авторизации при проведении транзакции, что облегчает получение нелегального доступа в личные кабинеты пользователей путем подбора идентификаторов и паролей для последующего проведения транзакций.

Кроме технических, имеются также финансовые и социальные факторы, ограничивающие развитие новых вариантов защиты систем ДБО и подготовку соответствующих программ, поскольку необходимо учитывать:

– необходимость укладываться в приемлемые затраты для пользователя (клиента банка) с учетом снижения репутационных рисков;

– обеспечивать возможность работы со смарт-картами и поддержку соответствующих технологий (отечественные криптоалгоритмы на базе чипов платежных банковских карт дают возможность физическому лицу иметь с собой ключ квалифицированной ЭП);

– сохранять для пользователя привычную ему последовательность действий. При внедрении нового решения необходимо учитывать, что усложнение в использовании (например, необходимость постоянного подключения внешних носителей для запуска виртуальных сред, а также многоразовый ввод платежных реквизитов вручную) отталкивает клиентов.

[2] ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.– М.: Стандартинформ, 2018; ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2018; ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2018; ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2018; ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Гос. комитет СССР по стандартам, 1989.

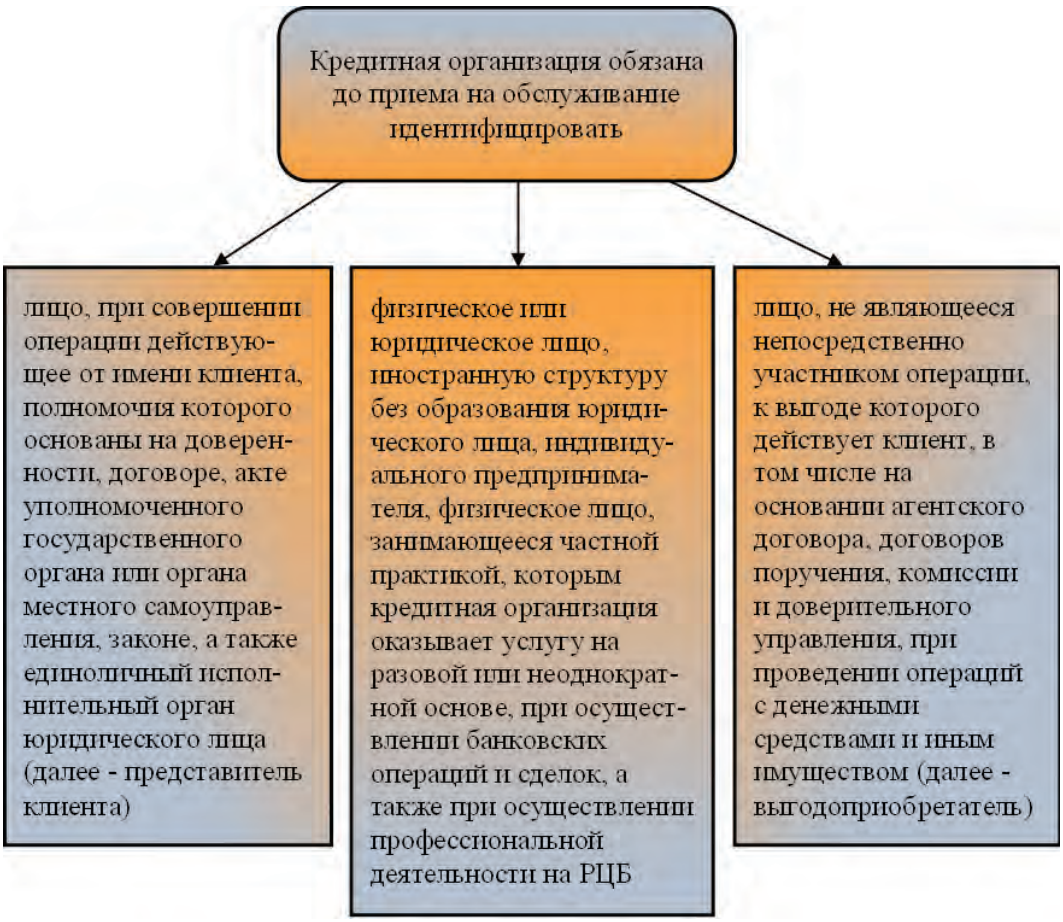

Рис. 2. Идентификация лиц кредитной организацией

Кроме того, в соответствии с Положением Центрального банка (ЦБ) РФ от 15 октября 2015 г. № 499 «Об индентификации кредитными организациями клиентов, представителей клиентов, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» кредитные организации обязаны идентифицировать клиентов в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ), и надо заметить, что эта работа в Российской Федерации ведется системно и целенаправленно [8]. Классификация лиц, к которым применяются требования Положения № 499 ЦБ РФ, представлена на рис. 2.

При проведении идентификации обязательно оценивается степень риска клиента в соответствии с Положением ЦБ РФ от 2 марта 2012 г. № 375 «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Оценка уровня риска клиента проводится независимо от вида и характера операции, проводимой клиентом, а также не влияет продолжительность отношений между банком и клиентом.

Кредитная организация, за исключением случаев, установленных законодательством, обязана принимать меры по идентификации клиентов –физических лиц, которые прямо или косвенно владеют более 25% в капитале, а также юридических лиц, прямо или косвенно контролирующих действия клиента (бенефициарных владельцев).

Идентификация не проводится в отношении клиента – выгодоприобретателя, являющегося органом государственной власти или субъекта Российской Федерации, местного самоуправления, Банка России, иностранного государства.

Банк, как правило, обновляет сведения, полученные в результате идентификации клиентов не реже одного раза в год, а также обновляет оценку степени риска клиента. Повторная идентификация клиента, представителя клиента, выгодоприобретателя, бенефициарного владельца; повторная упрощенная идентификация клиента – физического лица не проводится, если одновременно соблюдаются следующие условия:

– она проведена ранее и клиент находится на обслуживании;

– сомнения в достоверности и точности ранее полученной информации отсутствуют;

– к сведениям перечисленных лиц обеспечен оперативный доступ в постоянном режиме в порядке, установленном кредитной организацией в правилах внутреннего контроля.

Сведения о клиенте, его представителе, выгодоприобретателе, бенефициарном владельце заносятся коммерческим банком в анкету (досье) клиента, форма которого определяется кредитной организацией по собственным правилам, удовлетворяющим целям ПОД/ФТ. Досье клиента сохраняется в банке в течении не менее чем пятилетнего срока со дня прекращения отношений с клиентом.

Добавим, что ответственная деятельность банков по обеспечению надежности и безопасности расчетов по ДБО не может обеспечить успех без соответствующих усилий со стороны клиентов, в особенности, от юридических лиц, которые не в меньшей степени страдают от утечки данных, в случаях, если они держат привилегированную информацию в публичных облачных хранилищах, чрезвычайно уязвимых для злоумышленников. Однако все большее количество российских компаний уделяют внимание защите от хакерских атак и компьютерного мошенничества. Это соответственно увеличивает затраты на поддержание безопасности поскольку IT-инфраструктура усложняется [13]. Предприятия вынуждены обращаться к экспертам по компьютерной безопасности. Чтобы сохранить мобильность действий, они вынуждены использовать гибридные сервисы, отделять критически важную информацию, хранимую на собственных защищенных серверах, оставляя в облачных дата-центрах большие объемы менее важных сведений. Готовность больше инвестировать в информационную безопасность показывает, что профессионалы рынка в полной мере осознают важность создания комплексной системы защиты. С другой стороны, они стоят перед необходимостью следовать требованиям регуляторов в России и странах СНГ.

Дистанционный банкинг невозможен без мобильной связи и предполагает ее использование параллельно с другими средствами коммуникации. Определенный вклад в защиту ДБО делается и производителями мобильных устройств, которые устанавливают специальное программное обеспечение для предотвращения атак. Чаще всего пользователи сталкиваются с банковскими и *SMS*-«троянцами», отправляющими короткие платные сообщения без ведома владельца.

И все же наиболее ответственные задачи по обеспечению безопасности ДБО, ложатся на компании, создающие в настоящее время эти системы и внедряющие их в сложившиеся коммуникации банков.

Тенденции развития рынка ДБО определяются запросами клиентов (конечных пользователей), потребностями кредитных организаций (непосредственно банков), а также достижениями в сфере информационных технологий – новых устройств, каналов связи, математических методов и алгоритмов [15]. Кроме того, на развитие рынка ДБО оказывают влияние развитие законодательства, складывающаяся в стране экономическая ситуация, инфраструктурные особенности региона, формирующие локальные особенности цифрового пространства [2].

Основные потребительские ожидания клиентов от системы включают интуитивный интерфейс, эргономику, многоканальность и мультибраузерность, высокую производительность и общую функциональность. Со своей стороны российские банки предоставляют привлекательные услуги в рамках интернет-банкинга: планирование и контроль расходов и ведение «домашней бухгалтерии» в режиме онлайн. Клиенты банка имеют возможность получать детальные отчеты о расходах, перечислениях и поступлениях в структурированном виде.

Компании-разработчики стремятся соответствовать этим тенденциям, и оснащают свои варианты систем ДБО новыми функциями, такими, как «личные финансы», система «*iPhone*-Клиент», киоск самообслуживания, приложения в *AppStore, Google.Play*, «Сервер Нотификации», «Телефон-Клиент» и др. с высокой функциональностью, не уступающей по объему полноценному интернет-банкингу. Предлагаемые программы *мобильного* банкинга работают со всеми самыми распространенными мобильными операционными системами (*iPhone, Android, WindowsPhone, Java* и др.), а также поддерживает различные мобильные браузеры (*OperaMini, Safari, Chrome* и др.).

Спектр предложений по видам ДБО среди лидеров российского банковского рынка (в порядке уменьшения предложений) выглядит так:

– интернет-банк: собственный интернет-банк (сайт), интернет-банк через сервис партера, собственный интернет-банк (программа);

– *SMS*-банк;

– мобильный банк (мобильный сайт, приложение *Java*, приложение *iPhone*, приложение *Android*, приложение *Win Mobile*).

Как уже указывалось, на развитие рынка систем ДБО заметно влияет эволюция *информационных технологий*. Общая тенденция к увеличению количества пользователей смартфонов и планшетных компьютеров сохраняется, поэтому мобильные банковские продукты в настоящее время для развития систем ДБО составляют основной потенциал.

Для оптимизации процесса внедрения и развития современных технологий банковского обслуживания необходимо искать возможности объединения всех преимуществ инновационной деятельности. На российской почве технологии ДБО поначалу внедрялись с относительно низкими темпами по отношению к ведущим мировым банкам. Это было вызвано отсутствием на российском рынке финансовых услуг конкурентного воздействия со стороны иностранных банков – одного из мощных стимуляторов инновационной деятельности.

Технологии ДБО в российских банках развиваются в основном под влиянием клиентов, которые стремятся улучшить свои возможности в управлении счетами. Долгое время системы интернет-банкинга ограничивались так называемыми пассивными операциями (клиент мог получить удаленный информативный доступ

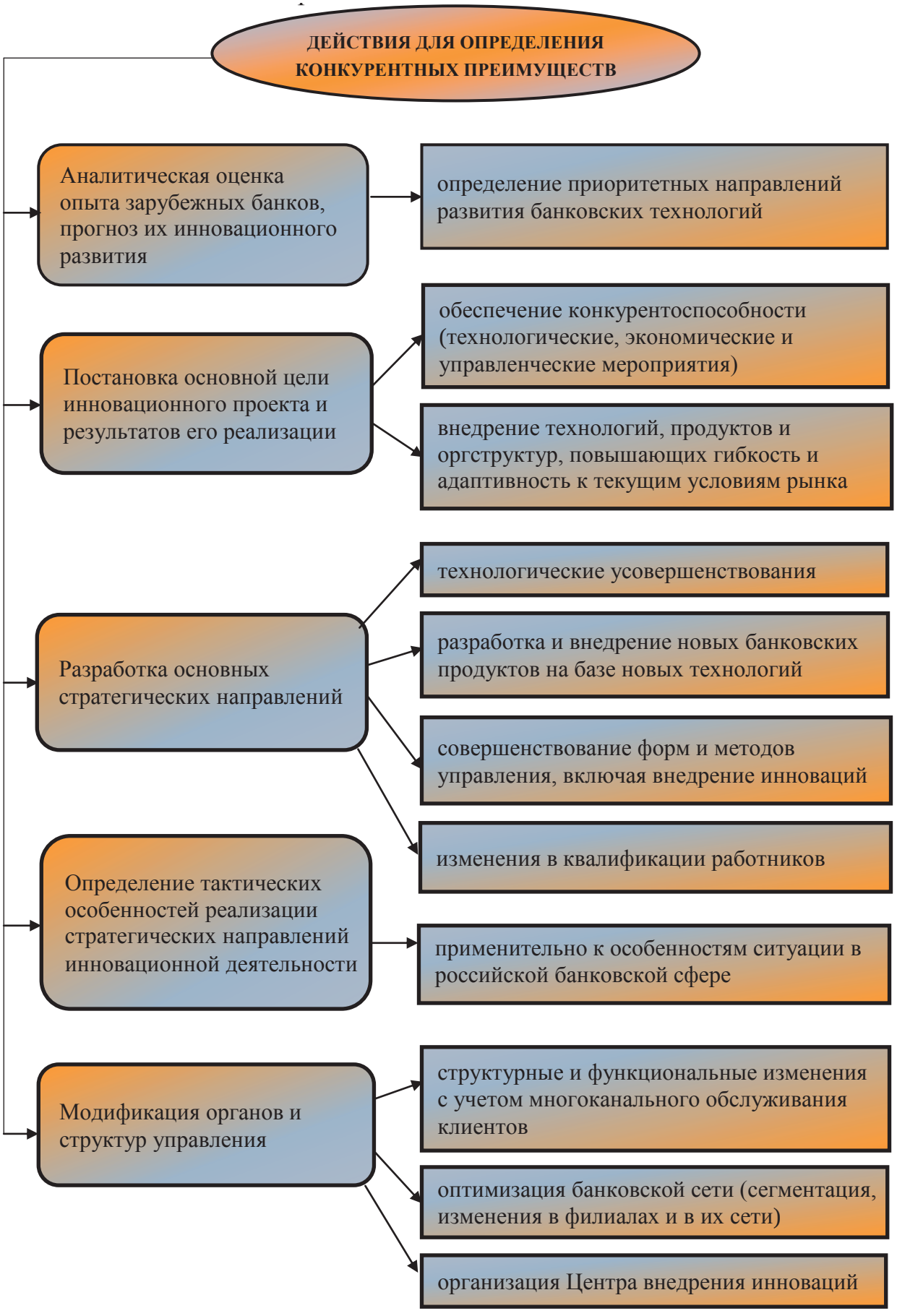

Рис. 3. Инновационные мероприятия коммерческих банков по внедрению новых технологий ДБО

к своим счетам, однако он не мог совершать активные операции, например, переводить средства с одного счета на другой). В последние два-три года ситуация изменилась коренным образом, в том числе благодаря активной позиции Правительства РФ и руководства крупнейших банков, стремящихся сократить оборот наличных денег в стране.

При этом, в небольших российских банках полноценно интернет-банкинг не применяется – фактически между моментом подачи заявки на списание средств со счета при дистанционном обслуживании и временем их реального списания промежуток довольно велик.

Развитие отечественной безналичной коммерции сдерживает неспособность банков обеспечить дешевые оперативные платежи. Существует два *направления* решения этой проблемы: переход абсолютного большинства национальных банков к массовому использованию систем ДБО и совершенствование тарифной политики банков, которая была бы направлена на учет размера платежей, чтобы предоставить клиентам удобства по осуществлению микроплатежей – расчетов в нижнем ценовом диапазоне. Лучших результатов в этой области добиваются торговые корпорации, построенные по принципу открытых систем [3].

В России наличествует несколько до некоторой степени ошибочных представлений о сущности ДБО, которые влияют на принятии решений по его развитию. Например, мнение о том, что системы ДБО обслуживают клиентов только в виртуальном пространстве, т.е. существуют в сети и функционируют благодаря минимизации своих расходов. На самом деле ДБО представляет собой одну из моделей работы реальных банков, которая в идеале должна быть многоканальной и сочетать в себе всевозможные каналы доступа клиентов, в том числе Интернет, телефон, сотовую связь. Другое ложное предположение: ДБО вскоре полностью устранит операционистов банка из процесса обслуживания клиентов, и все информационное взаимодействие между ними и банком будет происходить автоматически. Очевидно, однако, что участие квалифицированного сотрудника необходимо для отслеживания возможных ошибок, а также (и, в первую очередь, в рамках нашей темы) в целях повышения степени информационной безопасности. Приведем еще одно заблуждение: ДБО – это последняя стадия развития банковского обслуживания. Это, очевидно, не так, поскольку происходит постоянное развитие, как информационных технологий, так и организационных форм банковского обслуживания [5].

Стратегия по осуществлению инновационной деятельности в рамках развития ДБО, представляет собой комплекс взаимосвязанных мер. Примерный перечень соответствующих мероприятий коммерческого банка представлен на рис. 3.

Для того, чтобы все сервисы ДБО нашли своего пользователя, соответствующие инновационные технологии должны внедряться в соответствии с реальной структурой спроса и характеристик целевой клиентской группы. Прямое использование зарубежного опыта вероятнее всего приведет к отрицательному результату. Необходимо тщательное изучение потенциального спроса на банковские операции и услуги российских пользователей. На современном этапе наибольший интерес клиентов отечественных банков представляют услуги по дистанционной оплате текущих счетов за мобильную связь, Интернет, спутниковое телевидение, коммунальные услуги, счетов страховых компаний, штрафов, а также бронирование отелей, выкуп туристических туров, приобретение театральных билетов и др.

Очевидно, что российский рынок дистанционных банковских услуг будет в дальнейшем увеличивать темпы своего развития, используя, в частности, возможности корпоративной интеграции и предоставления новых дополнительных услуг. В качестве примера можно привести сервис комплексное обслуживание корпоративных клиентов в целях поддержки сложных схем обслуживания крупных организаций с территориально разнесенными подразделениями, филиалами и дочерними структурами.

Одним из новых направлений развития дистанционного обслуживания является внедрение инструментов для приема платежей на смартфоны или планшеты клиентов банка. Происходит смещение возможностей оплаты с использованием *POS*-терминалов для осуществления платежа на смартфоны, планшеты. В частности, услуги таксистов, курьеров, официантов, которые могут принимать платежи от клиентов на свои смартфоны и планшеты. Коммерческие организации массово внедряют технологии, позволяющие подобные бесконтактные транзакции.

Для использования смартфона или планшета в качестве *POS*-терминала, необходимо установить специальное приложение банка. Для этого с банком заключается договор эквайринга[3] (от англ. *acquire* – получать). При оплате товара или услуги продавец должен открыть приложение и ввести нужную сумму, а покупатель – приложить к смартфону бесконтактную карту либо *NFC*-устройство, поддерживающее *Apple Pay, Samsung Pay* или *Google Pay* (это могут быть смартфон, «умные» часы или браслет). Такие продукты уже работают у Сбербанка, ВТБ и Промсвязьбанка. Сбербанк запустил такую услугу совместно с *Mastercard* в декабре 2018 г. и расширяет сотрудничество в этой сфере с системами *Visa* или ПС «Мир».

Эти продукты дополняют традиционный эквайринговый бизнес и помогают расширить сеть приема электронных платежей в сегментах, где оплата товаров или услуг пока еще происходит за наличные. Организациями малого и среднего бизнеса и индивидуальными предприятиями, страховыми агентствами, различными службами доставки, которые работают в крупных и средних городах, этот продукт очень востребован. В

[3] Прием к оплате платежных карт в качестве средства оплаты товаров и услуг.

сельских районах, где и сотовая связь не везде доступна, эта услуга пока малоактуальна.

По некоторым оценкам через несколько лет доля приема оплаты смартфоном на рынке эквайринга может составить 10 – 15%. Использовать эту технологию будет бизнес, для которого не принципиальна высокая скорость операций, которая, впрочем, фактически ограничивается скоростью Интернета на устройстве. Согласно современным исследованиям, удобства, предоставляемые эквайринговыми схемами, существенно компенсируют риски, связанные с преступной деятельностью в этом сегменте, поскольку суммы на счетах и размеры транзакций относительно невелики [10].

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Россия.*

Литература

1. Белин А. В., Ващекин А. Н. О проблеме дифференциации коммерческой, служебной и иной охраняемой законом тайны // Российское правосудие. 2019. № 6. С. 32–41.
2. Бондаренко Т. Г., Анненков А. Ю. Fintech и Legaltech: проблемы и вызовы построения цифрового пространства // Вестник Академии права и управления. 2019. № 1 (54). С. 127–143.
3. Ващекин А. Н. Новые формы организации оптово-розничного звена в России – торговые корпорации как открытые системы // Труды Междунар. науч.-прак. конф. «Ценности и интересы современного общества» / Минобрнауки РФ. – М.: Изд-во МГУЭСИ, 2015. С. 36 – 42.
4. Ващекин А. Н. Моделирование взаимодействия субъектов в условиях неполной экономической и правовой информации // Актуальные проблемы информационно-правового пространства: Сб. ст. по материалам ежегодных Всеросс. науч.-прак. конф. – Краснодар: Изд-во СКФ РГУП, 2017. С. 14-– 20.
5. Ващекина И. В. Эволюция национальных банковских систем в свете проблем самоорганизации: монография. – М.: Изд-во РГТЭУ, 2012. 132 с.
6. Ващекина И. В. О системах телекоммуникаций, обеспечивающих расчетные операции в России // Труды Междунар. науч.-прак. конф. «Теория и практика приоритетных научных исследований». М.: Изд-во РЭУ им. Г.В. Плеханова. – 2016. С. 123 – 126.
7. Ващекина И. В. Об информационной безопасности расчетов и платежей в Российской Федерации // Труды Междунар. науч.-прак. конф. «Повышение открытости отечественной статистики», посвященной профессиональному празднику – Дню работника статистики / Росстат. – М.: Изд-во РЭУ им. Г.В. Плеханова, 2016. С. 40 – 43.
8. Ващекина И. В., Ващекин А. Н. Применение риск-ориентированного подхода при организации противодействия отмыванию нелегальных доходов в российской практике // Наука и практика. 2018. № 3. С. 61–69.
9. Ващекина И. В., Ващекин А. Н. Структурные особенности банковской системы Российской Федерации и динамика основных показателей ее функционирования // Научное обозрение. Экономические науки. – 2019. – № 1. – С. 5 – 10.
10. Велингурский В. А., Белозерова Г. И., Федосеев С. В. Построение и реализация оценки уровня мошеннических операций в банке-эквайре на основе самоорганизующейся карты Кохонена // Информационные технологии в процессе подготовки современного специалиста: Межвуз. сб. науч. тр. – Липецк: Изд-во ЛГУ, 2016. С. 24 – 32.
11. Карпов Д. С., Роганов А. А., Федорищев О. Н., Борисов Р. С. Системы передачи информации. – М: «Бестселлер», 2013. 104 с.
12. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66 – 74. DOI: 10.21681/1994-1404-2017-3-66-74
13. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3–7.
14. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. – М.: РГУП, 2016. 316 с.
15. Царькова Е. В. Информационно-математическое обеспечение задач «цифровой» экономики // Правовая информатика. 2019. № 1. С. 18 – 28. DOI:10.21681/1994-1404-2019-1-18-28
16. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23

OPPOSITION OF CRIMINAL ACTIVITY IN CONDITIONS OF THE DEVELOPMENT OF DIGITAL TECHNOLOGIES OF REMOTE BANK SERVICES

Andrey Vashchekin, *Ph.D., Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
E-mail: *vaschekin@mail.ru*

Irina Vashchekina, *Ph.D., Associate Professor of the Chair of Information Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
E-mail: *vaschekina@mail.ru*

Keywords: *bank, payment system, remote banking, digital technology, information security, computer fraud, malicious software, countermeasures, special application, innovation events.*

Abstract.
Purpose of the article: improving the scientific and methodological basis of the theory of information security in bank sphere.
Method: *system-legal analysis of complex of technological tools and organizational techniques to reduce financial losses and protect customers from criminal acts of computer fraudsters.*
Results: *the means of illegal penetration into remote banking systems are systematized, measures to counter fraudulent transactions are proposed; characteristics are given for new products and services in the field under study, both from the point of view of potential information vulnerability to criminal activity and from the point of view of economic efficiency; to develop an optimal strategy for implementing the innovative development of remote banking services, a set of interrelated measures is presented that forms a list of relevant measures.*

References

1. Belin A. V., Vashchekin A. N. O probleme differentciatcii kommer-cheskoi`, sluzhebnoi` i inoi` okhraniaemoi` zakonom tai`ny` // Rossii`skoe pravo-sudie. 2019. № 6. S. 32–41.
2. Bondarenko T. G., Annenkov A. Iu. Fintech i Legaltech: problemy` i vy`zovy` postroeniia tcifrovogo prostranstva // Vestneyk Akademii prava i upravleniia. 2019. № 1 (54). S. 127–143.
3. Vashchekin A. N. Novy`e formy` organizatcii optovo-roznichnogo zvena v Rossii – torgovy`e korporatcii kak otkry`ty`e sistemy` // Trudy` Mezhdunar. nauch.-prak. konf. «Cennosti i interesy` sovremennogo obshche-stva» / Minobrnauki RF. – M.: Izd-vo MGUE`SI, 2015. S. 36 – 42.
4. Vashchekin A. N. Modelirovanie vzaimodei`stviia sub``ektov v uslo-viiakh nepolnoi` e`konomicheskoi` i pravovoi` informatcii // Aktual`ny`e pro-blemy` informatcionno-pravovogo prostranstva: Sb. st. po materialam ezhegodny`kh Vseross. nauch.-prak. konf. – Krasnodar: Izd-vo SKF RGUP, 2017. S. 14 – 20.
5. Vashchekina I. V. E`voliutciia natcional`ny`kh bankovskikh sistem v sve-te problem samoorganizatcii: monografiia. – M.: Izd-vo RGTE`U, 2012. 132 s.
6. Vashchekina I. V. O sistemakh telekommunikatcii`, obespechivaiushchikh raschetny`e operatcii v Rossii // Trudy` Mezhdunar. nauch.-prak. konf. «Teo-riia i praktika prioritetny`kh nauchny`kh issledovanii`». M.: Izd-vo RE`U im. G. V. Plehanova. – 2016. S. 123 – 126.
7. Vashchekina I. V. Ob informatcionnoi` bezopasnosti raschetov i pla-tezhei` v Rossii`skoi` Federatcii // Trudy` Mezhdunar. nauch.-prak. konf. «Povy`shenie otkry`tosti otechestvennoi` statistiki», posviashchennoi` profes-sional`nomu prazdniku – Dniu rabotneyka statistiki / Rosstat. – M.: Izd-vo RE`U im. G.V. Plehanova, 2016. S. 40 – 43.
8. Vashchekina I. V., Vashchekin A. N. Primenenie risk-orientirovannogo podhoda pri organizatcii protivodei`stviia otmy`vaniiu nelegal`ny`kh dohodov v rossii`skoi` praktike // Nauka i praktika. 2018. № 3. S. 61–69.
9. Vashchekina I. V., Vashchekin A. N. Strukturny`e osobennosti bankov-skoi` sistemy` Rossii`skoi` Federatcii i dinamika osnovny`kh pokazatelei` ee funktcionirovaniia // Nauchnoe obozrenie. E`konomicheskie nauki. – 2019. – № 1. – S. 5 – 10.
10. Velingurskii` V. A., Belozerova G. I., Fedoseev S. V. Postroenie i realizatciia ocenki urovnia moshennicheskikh operatcii` v banke-e`kvai`re na osnove samoorganizuiushchei`sia karty` Kohonena // Informatcionny`e tekhno-logii v protcesse podgotovki sovremennogo spetcialista: Mezhvuz. sb. nauch. tr. – Leepetck: Izd-vo LGU, 2016. S. 24 – 32.
11. Karpov D. S., Roganov A. A., Fedorishchev O. N., Borisov R. S. Si-stemy` peredachi informatcii. – M: «Bestseller», 2013. 104 s.

12. Lovtcov D. A. Problema garantirovannogo obespecheniia infor-matcionnoi` bezopasnosti krupnomasshtabny`kh avtomatizirovanny`kh sistem // Pravovaia informatika. 2017. № 3. S. 66 – 74.
13. Lovtcov D. A. Obespechenie informatcionnoi` bezopasnosti v ros-sii`skikh telematicheskikh setiakh // Informatcionnoe pravo. 2012. № 4. S. 3 –7.
14. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informa-tcionny`kh otnoshenii` v infosfere: Monografiia. – M.: RGUP, 2016. 316 s.
15. TCar`kova E. V. Informatcionno-matematicheskoe obespechenie za-dach «tcifrovoi`» e`konomiki // Pravovaia informatika. 2019. № 1. S. 18 – 28.
16. Kartchiia A.A., Makarenko G.I., Sergin M.Iu. Sovremenny`e trendy` kibe-rugroz i transformatciia poniatiia kiberbezopasnosti v usloviiakh tcifrovi-zatcii sistemy` prava // Voprosy` kiberbezopasnosti. 2019. № 3 (31). S. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23