Ревенков Павел Владимирович
д-р экон. наук, профессор
Крупенко Дмитрий Сергеевич
аспирант
Чебарь Александр Геннадьевич
аспирант
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

ЦИФРОВОЙ БАНКИНГ: ПРЕИМУЩЕСТВА, СОПУТСТВУЮЩИЕ РИСКИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КИБЕРАТАК

Аннотация*: в статье рассматриваются основные преимущества дистанционного банковского обслуживания и источники возникновения новых источников типичных банковских рисков в условиях воздействия кибератак. Приведены основные виды кибератак на банковские автоматизированные системы и даны рекомендации сотрудникам риск-подразделений банков по необходимым компетенциям для успешной работы в условиях применения систем электронного банкинга.*

Ключевые слова*: кибербезопасность, риски, системы электронного банкинга, компьютерные атаки, компетенции.*

За последние 20 лет цифровые технологии стали активно применяться для осуществления различных банковских операций. Современный банковский клиент уже давно стал отказываться от офисного обслуживания и активно использует технологии дистанционного банковского обслуживания, отдавая предпочтение системам электронного банкинга (СЭБ). В состав электронного банкинга входят: системы интернет-банкинга, мобильного банкинга, POS-терминалы, банкоматы и др.

Основные преимущества кредитной организации (КО), использующей СЭБ, связаны с экономией затрат на осуществление операционной деятельно-

сти (нет необходимости содержать офисы) и с повышением конкурентоспособности на рынке банковских услуг.

Традиционным КО все сложнее удерживать преимущество в борьбе за клиентов с более инновационными компаниями. Банковская сфера всегда была консервативной отраслью с большим количеством правил и относительно высокими барьерами для входа конкурентов. Для крупных банков масштаб бизнеса и огромные филиальные сети превращаются из конкурентных преимуществ в сдерживающие факторы развития. Однако развитие цифровых технологий – в том числе облачных, мобильных и аналитических систем – способствует появлению новых игроков в виде – цифровых банков или необанков (от англ. digital banks и neobanks). Этому содействуют и банковские регуляторы многих стран, которые с помощью законодательных изменений стимулируют инновации в банковской сфере.

Согласно данным отчета Juniper Research «Futureproofing Digital Banking 2018» (https://www.juniperresearch.com/document-library/white-papers/futureproofing-digital-banking-2018), общее число пользователей мобильных банковских приложений приближается к двум миллиардам, что составляет порядка 40% всего взрослого населения. Мобильным банком пользуется каждый третий (34%) россиянин старше 18 лет.

России удалось обогнать многие страны по уровню цифровизации банкинга за счет того, что становление рынка происходило уже в цифровую эпоху. Средний возраст российского банка с момента последней смены бизнес-модели – восемь-десять лет, что позволило им быстрее адаптироваться по сравнению со старейшими мировыми банками с выстроенной системой классического офлайн-банкинга.

Однако работа КО в киберпространстве сопряжена с постоянным возникновением новых источников банковских рисков, основными из которых являются:

– *отсутствие «прямого контакта» банка со своими клиентами*. Фактически после оформления договора на оказание дистанционных банковских услуг

у КО нет полной гарантии, что все операции инициируются непосредственно клиентом, а не злоумышленником от его имени;

– *осуществление самих банковских операций, выполняемых с помощью СЭБ, осуществляется за доли секунд.* Как следствие, значительно увеличиваются требования к выполнению принципа «знай своего клиента» [1, с. 57];

– *возможности удаленного обслуживания клиентов предоставили преимущества кибермошенникам, использующим особенности функционирования СЭБ для осуществления мошеннических действий.* За счет недостаточного контроля со стороны регуляторов, в том числе на международном уровне, высокие скорости выполнения самих операций и возможности скрывать некоторые данные о реальном исполнителе способствуют тому, что данные технологии используются различными преступными группировками для мошенничества, отмывания денег и продажи запрещенных товаров;

– *возрастание активности киберпреступников и постоянное усложнение кибератак на банки и их клиентов*. Согласно данным отчета «Hi-Tech Crime Trends 2019/2020» известной российской компании Group-IB (https://www.group-ib.ru/resources/threat-research/2019-report.html), специализирующейся на расследовании киберпреступлений, за второе полугодие 2018 года и первое полугодие 2019 года потери КО от целевых атак составили 93 млн. рублей, совокупные потери в системах интернет-банкинга составили 172 млн. рублей;

– *уязвимости и угрозы мобильных приложений.* В настоящее время злоумышленнику редко требуется физический доступ к смартфону, чтобы украсть данные. По данным отчета компании Positive Technologies «Уязвимости и угрозы мобильных приложений» компании Positive Technologies за 2019 год (https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Mobile-Application-Vulnerabilities-and-Threats-2019-rus.pdf) – 89% уязвимостей могут быть проэксплуатированы с использованием вредоносного программного обеспечения (ВПО). Успех кибератаки на мобильное приложение напрямую зависит от того, насколько внимательно сам пользователь относится к сохранности своих дан-

ных. Предпосылкой ко взлому могут стать повышенные привилегии или загруженные из неофициального источника программы.

Все перечисленные источники рисков должны подлежать учету при формировании общей системы управления рисками в соответствии с актуальными бизнес-целями и бизнес-процессами КО, оказывать влияние на процессы совершенствования системы риск-менеджмента и повышение качества работы риск-подразделений.

Одним из основных направлений работы риск-подразделений является проведение проверок структурных подразделений банка и результатов их деятельности на предмет соответствия допустимому уровню рисков, принимаемых каждой КО самостоятельно.

Работа в киберпространстве, в первую очередь, увеличивает составляющую технологическую составляющую всех типичных банковских рисков, среди которых в большей степени выделяются следующие виды:

– операционный;

– правовой;

– стратегический;

– репутационный;

– риск ликвидности [2, с. 62].

Приведем развернутые определения упомянутых рисков, чтобы нагляднее показать, какие последствия могут быть у банка в случае работы в киберпространстве:

Операционный риск включает в себя возможные текущие и перспективные финансовые потери, обусловленные ошибками при выполнении банковских операций, мошенническими действиями в отношении банка, нарушением непрерывности и/или нештатным функционированием автоматизированных систем кредитной организации.

Риск ликвидности связан с возможными финансовыми потерями, обусловленные неспособностью банка своевременно и полностью выполнить свои обязательства перед клиентами из-за изменения характеристик управления лик-

видностью в условиях открытого сетевого взаимодействия (непредвиденный отток средств, хищения в крупных размерах, несанкционированные переводы средств).

Правовой риск включает в себя возможные финансовые потери, связанные с нарушением банком требований федеральных законов в области регулирования банковской деятельности, а также нормативных документов, Банка России.

Риск репутации связан с возможными в перспективе финансовыми потерями по причине возникновения негативного общественного мнения в отношении банка из-за нарушения им каких-либо обязательств перед клиентами (включая функциональную недоступность ее автоматизированных систем, невыполнение обязательств перед клиентами и/или потерю банковских и/или клиентских данных из-за отказов оборудования – как в самой КО, так и у ее провайдеров, потерю денежных средств банка и его клиентов, в том числе по причине воздействия компьютерных атак.

Стратегический риск включает в себя возможные в перспективе финансовые потери, связанные с ошибочными деловыми решениями и/или несоответствующей реализацией основных бизнес-решений в банке, что приводит к невозможности достижения ею своих стратегических целей и/или непредвиденно высоким затратам на внедрение и сопровождение используемых СЭБ.

Процесс анализа источников рисков необходимо проводить непрерывно, а методики выявления, анализа и мониторинга рисков (находящиеся в арсенале риск-подразделений) должны регулярно пересматриваться для обеспечения их полноты и актуальности ввиду высоких темпов технологических инноваций в банковском деле.

Приведем основные виды кибератак на банковские автоматизированные системы (БАС), отмеченные в ежегодных отчетах ФинЦЕРТ (специализированное подразделение Департамента информационной безопасности Банка России), в функции которого входит противодействие компьютерным атакам на организации кредитно-финансовой сферы:

– атаки на автоматизированное рабочее место клиента Банка России (АРМ КБР);

– атаки на автоматизированное рабочее место клиента SWIFT (АРМ SWIFT);

– атаки на автоматизированное рабочее место клиента СЭБ (АРМ СЭБ);

– атаки на устройства самообслуживания (банкоматы).

Для реализации всех перечисленных атак сначала необходимо осуществить загрузку ВПО в локальную вычислительную сеть (ЛВС) КО. Для этого, в большинстве случаев, в КО злоумышленниками направляется электронное письмо, содержащее ВПО, не детектируемое антивирусными средствами. Письмо содержит хорошо оформленный сопроводительный текст, якобы от имени, известных в финансовых кругах людей, банков или финансовых регуляторов, с вредоносным вложением сопровождающееся качественной приманкой, используются подменные адреса на бесплатных почтовых сервисах.

Первым в атакуемую КО попадает модульное ВПО, оно предварительно анализирует среду запуска и загружает стартовые модули, отвечающие за сбор информации о системе, а также загрузку и запуск основного инструмента для развития атаки.

После процесса заражения, ВПО выполняет сканирование доступного зараженной машине сегмента ЛВС с целью заражения новых рабочих станций.

В дальнейшем на зараженные станции загружается дополнительное ВПО, выполняющее функции ботнет-клиента и обладающее возможностями удаленного управления (скрытый рабочий стол, в результате чего удаленное управление осуществлялось незаметно для пользователя), а также ВПО для хищения различных аутентификационных данных.

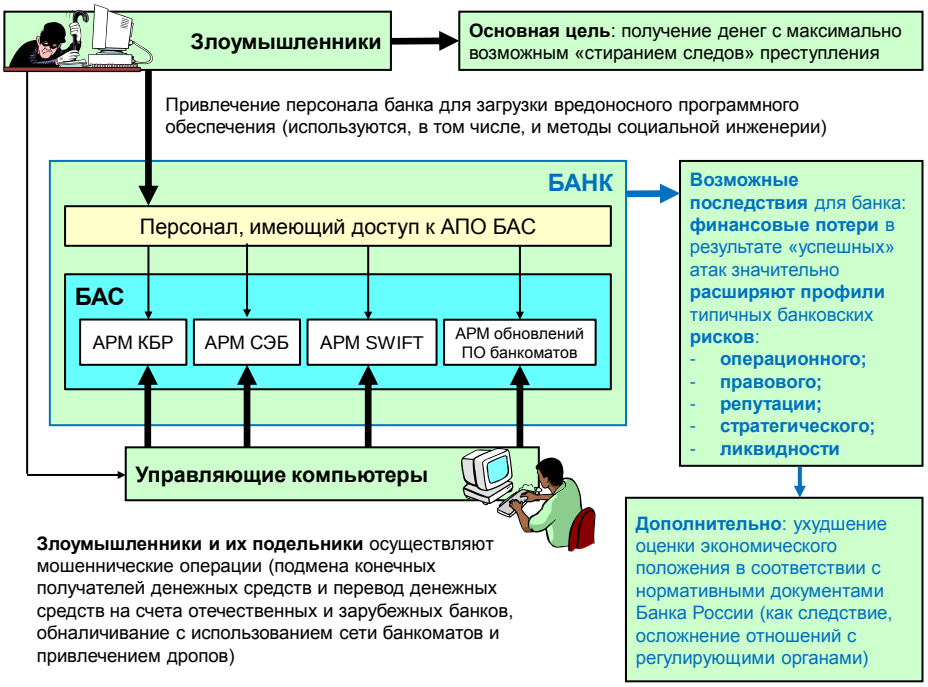

Рис. Взаимосвязь некоторых видов атак на АПО БАС и возможных последствий для банка

Основная причина, по которой вышеперечисленные атаки носили «успешный» характер – человеческий фактор, который проявляется в виде ненадлежащего контроля ответственными работниками банка установленной технологии подготовки, обработки и передачи электронных сообщений, содержащих распоряжение клиентов.

Очевидно, что для эффективного управления данными рисками, необходимо чтобы сотрудники риск-подразделений банка обладали соответствующим образованием (как правило помимо экономического или юридического необходимо иметь и техническое образование) и навыками проведения аудита информационных систем и технологий.

Так, сотруднику риск-подразделения, в частности, необходимо:

– анализировать информационный контур банковской деятельности, который формируется в условиях применения СЭБ;

– находить на этом контуре все точки наибольшей концентрации рисков и знать какими компенсационными мерами можно минимизировать возможные негативные последствия;

– понимать актуальные принципы атак на информационные системы;

– иметь актуальный перечень информационных потоков и бизнес-процессов;

– определять соответствие документации и текущей архитектуры и логики работы аудируемых информационных систем;

– реализовывать принцип «знай свой периметр», т. е. уметь находить точки с неопределённым владельцем (внутренним подразделением и\или внешней организацией).

Список литературы

1. Ревенков П.В. Противодействие компьютерным атакам в условиях применения систем электронного банкинга: учебное пособие / П.В. Ревенков, П.А. Пименов, И.В. Ожеред. – М.: Прометей, 2019. – 158 с.

2. Лямин Л.В. Применение технологий электронного банкинга: риск-ориентированный подход. – М.: КноРус, 2011. – 336 с.