**pISSN 2071-4688**
**eISSN 2311-8709**

*Банковская деятельность*

# РАСШИРЕНИЕ ПРОФИЛЕЙ БАНКОВСКИХ РИСКОВ В УСЛОВИЯХ РАБОТЫ В КИБЕРПРОСТРАНСТВЕ

**Павел Владимирович РЕВЕНКОВ**

доктор экономических наук, профессор кафедры информационной безопасности,
Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
pavel.revenkov@mail.ru
https://orcid.org/0000-0002-0354-0665
SPIN-код: 3491-4700

**История статьи:**
Получена 24.07.2018
Получена в доработанном виде 15.08.2018
Одобрена 29.08.2018
Доступна онлайн 29.11.2018

**УДК** 336:004.056
**JEL:** G21, G32, L86

**Ключевые слова:**
киберпространство, кибербезопасность, электронный банкинг, риски, компьютерные атаки

**Аннотация**

**Предмет.** Учет возможных последствий проявления различных факторов рисков, связанных с работой в киберпространстве, в том числе в условиях воздействия компьютерных атак на банковские автоматизированные системы, может повысить качество работы риск-подразделений и служб внутреннего контроля банков.

**Цели.** Исследовать особенности ведения банковского бизнеса в киберпространстве. Проанализировать источники возникновения дополнительных рисков в условиях применения систем электронного банкинга и компьютерных атак. Выявить причины, сдерживающие развитие технологий дистанционного банковского обслуживания, и причинно-следственные связи при воздействии компьютерных атак на банковские автоматизированные системы.

**Методология.** Применены общенаучные методы познания: анализ и синтез, индукция и дедукция, метод аналогии. Использованы приемы системного анализа научной литературы. Реализован графический метод интерпретации исследуемых явлений.

**Результаты.** Выявлены основные факторы, повышающие банковские риски при работе в киберпространстве. Установлено, что компьютерные атаки на банковские автоматизированные системы приводят к повышению операционного, правового, стратегического, репутационного рисков, а также риска ликвидности.

**Область применения.** Результаты исследования могут быть использованы для совершенствования методов регулирования и надзора за организациями кредитно-финансовой сферы в условиях применения систем электронного банкинга, а также для повышения качества работы риск-подразделений и служб внутреннего контроля.

**Выводы и значимость.** Применение полученных результатов может способствовать повышению эффективности функционирования системы управления рисками в условиях использования систем электронного банкинга, в том числе минимизировать последствия компьютерных атак на банковские автоматизированные системы.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2018

**Для цитирования:** Ревенков П.В. Расширение профилей банковских рисков в условиях работы в киберпространстве // Финансы и кредит. — 2018. — Т. 24, № 11. — С. 2471 — 2485.
https://doi.org/10.24891/fc.24.11.2471

## Киберпространство и кибербезопасность

Новейшие достижения в области информационно-телекоммуникационных технологий и средств связи существенно изменили процесс ведения банковского бизнеса и стали основой для активного внедрения систем электронного банкинга (СЭБ)[1], фактически переводя весь процесс взаимодействия банка с клиентами в виртуальную среду, или другими словами — в киберпространство.

Понятия «киберпространство»[2] и «кибербезопасность» в настоящее время

[1] Наиболее распространенными вариантами электронного банкинга являются: интернет-банкинг (управление банковскими счетами и картами через Интернет и web-браузер в режиме on-line) и мобильный банкинг (управление банковскими счетами и картами с КПК, коммуникаторов, смартфонов и других аналогичных устройств).

[2] Термин Cyberspace (киберпространство) был впервые использован в романе Neuromancer В. Гибсона (W. Gibson) о прямой сетевой организации искусственного интеллекта и относится к коллективной сфере компьютерных коммуникаций.

отсутствуют в законодательстве Российской Федерации (традиционно используются термины «информационное пространство» и «информационная безопасность»). Однако в ряде международных и национальных стандартов, а также в некоторых научных работах можно встретить понятия «киберпространство» и «кибербезопасность». Если объединить подходы к определению данных понятий, то под киберпространством чаще всего понимают среду информационного взаимодействия и обмена данными, реализуемую в компьютерных сетях и сетях связи, где элементами киберпространства являются серверы, компьютеры, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети, а под кибербезопасностью — сохранение конфиденциальности, целостности и доступности информации в киберпространстве[3].

Банковский бизнес одним из первых стал использовать преимущества работы в киберпространстве. В первую очередь из-за значительной экономии операционной деятельности (нет необходимости содержать банковские офисы, а функции операциониста выполняет сам клиент со своего компьютера, планшета или смартфона). Эксперты банковского дела полагают, что дистанционное обслуживание клиента в среднем обходится в 10 раз дешевле, чем оформление документов в офисе[4]. Международная компания «Бостонская консалтинговая группа» (The Boston Consulting Group), которая специализируется на управленческом консалтинге (наряду с McKinsey и Bain & Company входит в большую тройку управленческого консалтинга), по результатам проведенного исследования западных банков делает вывод, что за счет меньшей стоимости «удержания» клиента, большего объема продаж услуг и снижения стоимости обслуживания онлайновый банковский клиент на 26% прибыльнее для банков, чем офлайновый.

Основатель первого в мире банка, предоставляющего только мобильные услуги (Movenbank), Бретт Кинг в своем выступлении на форуме инновационных технологий «Финополис-2017», прошедшем 5 октября 2017 г. в Сочи, отметил, что «банкам не нужны отделения. Крупнейший банковский продукт в мире принадлежит китайской компании Alibaba: пользователи платформы разместили 60 млрд депозитов всего за четыре года. Чтобы внести деньги на счет в Alibaba, достаточно телефона»[5].

Однако помимо явных преимуществ, работа в киберпространстве сопряжена с рядом факторов, повышающих уровни банковских рисков:

– виртуальный характер дистанционных банковских операций (фактически клиент после оформления счета и оформления договора на оказание услуг с применением СЭБ не имеет прямого контакта с банком). Такой порядок взаимодействия предъявляет повышенные требования к идентификации клиента (включая выполнение принципа «знай своего клиента») — в противном случае от имени клиента может инициировать операции злоумышленник [1, 2];

– доступность открытых телекоммуникационных систем (доступность глобальной сети Интернет и сотовой связи при отсутствии должного контроля за этими видами коммуникаций осложняют контроль за фактическими их пользователями);

[3] Для анализа подходов к определению понятий «киберпространство» и «кибербезопасность» использовались: Межгосударственный стандарт ГОСТ 34009-2016 «Средства и системы управления железнодорожным тяговым подвижным составом. Требования к программному обеспечению (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11.01.2017 № 3-ст.), проект Концепции стратегии кибербезопасности Российской Федерации от 10.01.2014 (URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf, Национальный стандарт Российской Федерации ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1 Терминология, концептуальные положения и модели (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 10.11.2014 № 1493-ст.).

[4] *Юденков Ю.Н., Тысячникова Н.А., Сандалов И.В., Ермаков С.Л.* Интернет-технологии в банковском бизнесе: перспективы и риски: учеб.-практич. пособ. М.: КноРус, 2014. 318 с.

[5] *Кинг Б.* Людям больше не нужны банки. URL: https://bankir.ru/publikacii/20171005/brett-king-lyudyam-bolshe-ne-nuzhny-banki-10009228/

– чрезвычайно высокая скорость выполнения транзакций (банковские операции с помощью СЭБ становятся просто мгновенными, что также предъявляет повышенные требования к контролю);

– глобальный характер межсетевого операционного взаимодействия (так как с помощью СЭБ выполняются операции не только в нашей стране, но и за ее пределами — возникают дополнительные источники рисков, связанные с особенностями законодательства в каждой отдельной стране, через которую проходят платежи клиентов. Надо учитывать особенности офшорных зон, где помимо налоговых льгот, существует определенный запрет на выдачу информации о клиентах) [3];

– участие компаний-провайдеров в реализации банковского обслуживания (в настоящее время данные компании, хотя и задействованы в информационном контуре банковской деятельности в условиях применения СЭБ, но не являются объектами контроля со стороны банковских регулирующих органов, то есть не предоставляют отчетность регулятору и не подвергаются проверкам с его стороны);

– возможность использования СЭБ для противоправной деятельности (опять же за счет недостаточного контроля со стороны регуляторов, скорости выполнения самих операций и возможности скрывать некоторые данные о реальном исполнителе и т.д.) [4].

**Что сдерживает развитие электронного банкинга**

Международная консалтинговая компания Deloitte включила Россию в пятерку наиболее развитых стран в регионе EMEA[6] в сфере цифрового банкинга (фактически речь идет о применении СЭБ). Это связано с тем, что Россия стала безоговорочным европейским лидером по количеству пользователей Интернета, поднявшись в общемировом рейтинге на шестое место. По прогнозам, к 2025 г. доля чистой цифровой экономики (интернет-рынков) в России может достигнуть 8—10% ВВП (сейчас — 4%), то есть уровня США и Китая на данный момент. На достижение этих целей в рамках программы «Цифровая экономика» будет направлено 520 млрд руб., из которых 150 млрд руб. будет выделено из бюджета[7].

Согласно данным исследования, проводимого экспертами Института экономической политики им. Е.Т. Гайдара и Российской академии народного хозяйства и государственной службы при Президенте РФ «Мониторинг экономической ситуации в России», количество активных банковских карт в России на конец 2017 г. составляло 157,6 млн единиц, что в 1,4 раза больше, чем в конце 2013 г. и в 2,8 раза — чем в конце 2008 г. При этом объемы операций выросли более существенно: в 2,1 раза с 2013 г. и в 6,8 раза с 2008 г.[8].

Начиная с 2004 г. в Банк России стала поступать отчетность от коммерческих банков по форме 0409070[9] об использовании ими интернет-технологий. По информации представителей надзорных подразделений регулятора, 98% от всех кредитных организаций используют СЭБ. Но если сравнивать по количеству клиентов банков, активно использующих СЭБ, наша страна пока уступает Европе и США[10].

[6] EMEA (Europe, the Middle East and Africa). Исследование EMEA Digital Banking Maturity было проведено в начале 2018 г. в 38 странах Европы, Ближнего Востока и Африки и охватило 238 банков (в том числе 12 российских) и 10 финтех-компаний. Всего экспертами было выделено 826 различных элементов цифровой оснащенности банка, которые были разделены на шесть направлений: поиск информации, открытие счета, адаптация нового клиента, повседневный банкинг, расширение предоставляемых банком услуг (в том числе кросс-продажи) и конечный этап сделки.

[7] На реализацию программы «Цифровая экономика» из бюджета будет выделено 150 млрд рублей. URL: http://tass.ru/ekonomika/4821743

[8] Мониторинг экономической ситуации в России: тенденции и вызовы социально-экономического развития. URL: https://www.ranepa.ru/images/docs/monitoring/monitoring-13-74.pdf

[9] Банковская отчетность по форме 0409070 «Сведения об использовании кредитной организацией интернет-технологий» введена Указанием Банка России от 01.03.2004 № 1390-У «О порядке информирования кредитными организациями Центрального банка Российской Федерации об использовании в своей деятельности интернет-технологий».

[10] Информация получена на семинаре Банка России «Технология интернет-банкинга: сопутствующие риски, организация банковского регулирования и надзора, внутреннего контроля и обеспечения информационной безопасности в кредитных организациях», март 2015 г.

По мнению автора, основными причинами, сдерживающими развитие технологий дистанционного банковского обслуживания (включая СЭБ), являются:

- недостаточно высокий уровень доверия клиентов банков к СЭБ (на это влияет не только большое количество различных способов мошенничества в Интернете и компьютерных атак на аппаратно-программное обеспечение (АПО) СЭБ, но и риски утечки конфиденциальных данных со стороны различного рода провайдеров услуг);
- низкий уровень финансовой грамотности населения, незнание возможностей современных СЭБ и способов обеспечения кибербезопасности в них;
- недостаточное качество дистанционных банковских услуг.

Остановимся подробнее на каждой причине.

Доверие к СЭБ основывается на уверенности клиентов кредитных организаций в том, что деньги, находящиеся на их счетах, надежно защищены. Обеспечение должного уровня кибербезопасности является одним из основных условий повышения доверия к СЭБ.

На основании данных отчета известной российской компании Group-IB, которая занимается расследованием компьютерных преступлений, совокупный ущерб от хищений в системах интернет-банкинга у юридических лиц за 2017 г. по России оценивается в 10 млн долл. США. При этом специалисты компании отмечают, что количество самих атак на системы интернет-банкинга и совокупный ущерб от них уменьшился по сравнению с предыдущим годом, но зато увеличился средний размер ущерба. Это свидетельствует о том, что атакующие стали более тщательно подбирать жертв. Ущерб от одной подобной атаки на организацию в среднем составляет от 3 до 10 млн руб.[11].

Рекламируя достоинства СЭБ, кредитные организации стремятся повысить свою конкурентоспособность и занять лидирующие позиции на рынке банковских услуг. При этом те из них, которые предоставляют банковские услуги, несут ответственность за их качество [5, 6].

При использовании СЭБ риски возникают чаще всего на стороне клиента. Для того чтобы минимизировать риски в условиях применения СЭБ, нужны усилия со стороны как кредитных организаций, так и клиентов. Специалисты кредитных организаций должны подробно разъяснять клиентам, пожелавшим выполнять свои банковские операции с использованием СЭБ, не только особенности применения данного вида банковского обслуживания, но и возможные способы обеспечения кибербезопасности при их использовании.

В связи с принятием Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее — Закон № 161-ФЗ) создаются реальные предпосылки для повышения доверия клиентов к СЭБ. На основании п. 15 ст. 9 Закона № 161-ФЗ у банка возникает обязанность возместить суммы, перечисленные со счета клиента в результате не санкционированной им операции, если только не будет доказано нарушение клиентом — физическим лицом порядка использования электронного средства платежа.

Заметим, что подобные меры защиты клиентов, использующих для выполнения своих операций СЭБ, соответствуют мировой практике. При этом у банка появляется возможность правомерной блокировки электронного средства платежа, которым пользуется клиент, при подозрении на мошенничество.

В соответствии с Федеральным законом от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» банкам разрешается без согласия клиента на срок до двух рабочих дней блокировать кредитные карты, если у финансовой организации появились подозрения в хищении с них средств.

[11] Итоги 2017. URL: www.group-ib.ru/blog/report2017

Согласно тексту закона «оператор по переводу денежных средств при выявлении им операции, соответствующей признаку осуществления списания денежных средств без согласия клиента, обязан до осуществления списания денежных средств с банковского счета клиента на срок не более двух рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента». Такие признаки устанавливаются Банком России и публикуются на сайте регулятора.

Блокировка будет касаться не только банковских карт, но и электронных кошельков, мобильных приложений и других средств дистанционного банковского обслуживания. Связаться с физическим лицом при возникновении подозрения банк может посредством электронной почты или телефона, с юридическим — в порядке, установленном договором об использовании электронного средства платежа.

Этим же законопроектом на банки возлагается обязанность направлять в Банк России информацию обо всех случаях или попытках осуществления таких переводов.

Решать задачу повышения уровня финансовой грамотности населения следует комплексно, начиная с начальной школы. В колледжах и высших учебных заведениях предмет «информационная безопасность» должен быть обязательным. Надо признать, что уровень финансовой грамотности населения уступает уровню и скорости развития мошеннических технологий [7, 8].

Нельзя не учитывать, что наряду с развитием банковских технологий, применяемых в сфере розничных платежных услуг (в том числе направленных на повышение уровня безопасного использования платежных карт), совершенствуются и методы проведения мошеннических операций (в том числе используемое мошенниками оборудование и программное обеспечение) [9, 10].

Качество дистанционных банковских услуг во многом зависит от удобства используемого программного продукта для СЭБ.

Очевидно, что восприятие каналов дистанционного банковского обслуживания розничными клиентами базируется на ключевом пользовательском опыте:

– удобство и понятность интерфейсов;

– наличие необходимого функционала;

– уникальные инструменты и сервисы, отличающие данный банк от конкурентов.

Банкам и разработчикам программных продуктов для СЭБ необходимо уделять повышенное внимание удобству и клиентоориентированности своих разработок. Например, разрабатывать меню с изменяющимся содержанием, которое регулируется как самим банком, так и пользователем — розничным клиентом.

В основе такого меню сразу несколько идей:

– объединить наиболее востребованные для конкретного пользователя функции, как избранные, так и последние совершенные;

– мотивировать клиента к совершению дополнительных операций;

– повысить персонализированность решения для каждого клиента [11].

Немаловажным для клиентов является наличие встроенного обучения и дополнительного пояснения в пользовательских интерфейсах[12].

Внедрение новых технологий в банковское обслуживание (включая СЭБ) приводит к тому, что основными проблемами в части расширения профилей банковских рисков становятся безопасность и доступность банковских автоматизированных систем. Одним из самых негативных факторов, связанным с применением СЭБ и в целом с работой в киберпространстве, является рост числа успешных атак на банковские

[12] Следующее поколение СЭБ будет способно анализировать собственную популярность и помогать менеджерам банка создавать эффективные каналы дистанционного обслуживания. Такие возможности позволят каждому банку оценить востребованность собственных функций и пути повышения их популярности — в области комиссий, маркетинга или повышения финансовой грамотности клиентов банка.

автоматизированные системы (БАС) кредитных организаций.

**Компьютерные атаки на БАС**

В данной статье мы не ставим своей целью рассмотреть все возможные компьютерные атаки на БАС кредитных организаций, а остановимся лишь на наиболее актуальных в последнее время.

Согласно отчетам ФинЦЕРТ Банка России[13], в 2016 и 2017 гг. кредитные организации подвергались следующим компьютерным атакам:

- атаки на АРМ КБР[14];
- атаки на АРМ SWIFT;
- атаки на АРМ СЭБ;
- атаки на устройства самообслуживания (банкоматы).

Для реализации всех перечисленных атак сначала необходимо осуществить загрузку вредоносного программного обеспечения (ВПО) в локальную вычислительную сеть кредитной организации.

С этой целью в адрес сотрудника банка направляется электронное письмо, которое включает в себя не детектируемое антивирусами ВПО. После проникновения на компьютеры, входящие в локальную вычислительную сеть (ЛВС) кредитной организации, ВПО с помощью SMB-запросов выполняло сканирование доступного зараженной машине сегмента локальной вычислительной сети для заражения новых автоматизированных рабочих мест сотрудников банка[15] [12, 13].

Далее на зараженные компьютеры загружалось дополнительное ВПО, выполняющее функции ботнет-клиента и обладающее возможностями удаленного управления, а также ВПО для хищения паролей.

Далее рассмотрим, что происходит в каждом отдельном случае из перечисленных атак.

Атака на АРМ КБР[16] осуществляется в целях подмены входных данных для АРМ КБР (изменение содержимого XML-документа, используемого для формирования электронного сообщения, направляемого в Банк России). После проникновения ВПО в ЛВС кредитной организации злоумышленники, получив полный контроль над захваченным сегментом ЛВС банка, проводят его мониторинг для определения АРМ КБР и компьютера, используемого для подготовки XML-документа. В дальнейшем происходит создание подложного XML-документа, который подписывается уполномоченными лицами кредитной организации и направляется в платежную систему Банка России.

Атака на АРМ SWIFT. Основное отличие атак на АРМ SWIFT от атак на АРМ КБР — это использование не платежной системы Банка России для несанкционированных денежных переводов, а международной системы передачи финансовой информации SWIFT для вывода денег сразу за границу. Из громких преступлений с использованием SWIFT можно назвать атаку 2016 г. на Центральный банк Республики Бангладеш, когда мошенники вывели средства на сумму 81 млн долл. США (при этом покушались они на сумму около 1 млрд долл. США).

В начале октября 2017 г. хакеры атаковали крупнейший банк Тайваня Far Eastern International Bank и украли оттуда 60 млн

[13] ФинЦЕРТ — специализированное подразделение департамента информационной безопасности Банка России, в функции которого входит противодействие компьютерным атакам на организации кредитно-финансовой сферы. В данной статье использованы данные ежегодных отчетов ФинЦЕРТ Банка России (за 2016 и 2017 гг.), размещенные на официальном сайте Банка России (URL: http://www.cbr.ru).

[14] АРМ КБР — автоматизированное рабочее место клиента Банка России.

[15] *Ревенков П.В., Бердюгин А.А.* Компьютерные атаки как источник операционного риска в условиях электронного банкинга // Финансы и кредит. 2018. Т. 24. № 3. С. 629—640. URL: https://doi.org/10.24891/fc.24.3.629

[16] За период с октября 2015 г. по март 2016 г. ФинЦЕРТ Банка России зафиксировал 21 атаку на инфраструктуру кредитных организаций. Злоумышленниками были совершены попытки хищения денежных средств на общую сумму порядка 2,87 млрд руб. При этом предотвращено хищение порядка 1,6 млрд руб. и по фактам хищений правоохранительными органами возбуждено 12 уголовных дел. URL: http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf

долл. США (в дальнейшем почти все похищенные средства удалось вернуть). В декабре 2017 г., используя SWIFT, хакеры пытались украсть у дочернего банка ВЭБа — «Глобэкс» 1 млн долл. США[17].

Атака на СЭБ. Данные атаки осуществлялись преимущественно на юридических лиц. Атака связана с подменой входных данных (платежных реквизитов) для СЭБ в момент отправки платежного поручения в банк. Обычно заражение происходит путем рассылки спам-писем с вложениями, содержащими макрос или Watering Hole attack, происходящих через зараженные веб-сайты. После заражения злоумышленник получает удаленный доступ к зараженному компьютеру и может установить необходимые компоненты ВПО для работы с конкретными СЭБ.

Атаки на устройства самообслуживания (банкоматы) можно разделить на два основных типа:

1) логические атаки (устройство не повреждается или не вскрывается, не устанавливаются дополнительные аппаратные компоненты с подключением к шинам устройства, все операции выполняются через удаленный доступ с использованием программных средств);

2) физические атаки (повреждение или вскрытие устройства, установка дополнительных аппаратных компонентов, подключение внешних устройств, в том числе для возможности удаленного управления).

Вне зависимости от типа атаки все из них за исключением подмены процессинга направлены на опустошение диспенсера банкомата путем генерации соответствующих команд, якобы полученных от процессинга с нарушением логики работы устройства [14, 15].

Основной тренд логических атак во второй половине 2016 г. и первой половине 2017 г. — использование ВПО Cobalt Strike, изначально предназначенного для проведения тестирования на проникновение.

Согласно отчету компании Group-IB существует преступная группа Cobalt (эксперты компании предполагают, что преступления с использованием ВПО Cobalt Strike совершает организованная группа). одним из первых крупных хищений Cobalt был First Bank на Тайване. В ходе атаки на банкоматы хакерам удалось похитить 2,18 млн долл. США. В сентябре 2016 г. они сумели получить доступ в один из банков Казахстана (процесс подготовки атаки и изучения инфраструктуры банка занял два месяца). В 2017 г., используя этот метод хищения, хакеры Cobalt установили абсолютный рекорд и предприняли попытку похитить 25 млн евро в одном из европейских банков[18].

«Физические» атаки включают в себя: скимминг, шимминг, Black Box, атаки на бесконтактные карты (NFC), подмена процессинга и Transaction Reversal Fraud и др.

Основная причина, по которой перечисленные атаки носили успешный характер — человеческий фактор, проявляющийся в виде ненадлежащего контроля ответственными работниками кредитной организации установленной технологии подготовки, обработки и передачи электронных сообщений, содержащих распоряжения клиентов.

Такой точки зрения придерживаются многие эксперты в области кибербезопасности. Так, например, генеральный директор группы компаний InfoWatch Н.И. Касперская отмечает, что слабым звеном, постоянной скрытой угрозой для банков является человеческий фактор, только не таинственные киберпреступники и не клиенты — дилетанты в информационной безопасности, а его же собственные сотрудники. Они могут поддаться соблазну вначале получить несанкционированный доступ к данным, а потом использовать их к своей выгоде и в ущерб банку[19].

[17] Хакеры украли из дочернего банка ВЭБа $1 млн // Ведомости. 2017, 20 дек. № 4475

[18] Group-IB: новые атаки Cobalt подтверждают связь с Anunak. URL: https://www.group-ib.ru/media/group-ib-cobalts-latest-attacks-on-banks-confirms-connection-to-anunak/

[19] *Касперская Н.* Интернет — чудо, но в нем есть и // BIS Journal. 2013. № 3.

В п. 5.4 Стандарта Банка России СТО БР ИББС-1.0-2014[20] указывается, что наибольшими возможностями для нанесения ущерба организации банковской системы Российской Федерации обладает ее собственный персонал.

Также к причинам можно отнести:

- отсутствие сегментирования локальных вычислительных сетей[21];
- низкую осведомленность работников кредитных организаций в области кибербезопасности;
- отсутствие блокировки автоматического запуска макросов в документах Microsoft Office;
- присвоение пользователям избыточных прав локального администратора;
- отсутствие средств антивирусной защиты (или их базы были устаревшими)[22].

**Риски в условиях применения СЭБ**

Рассмотренные ранее факторы, повышающие уровни банковских рисков из-за работы в киберпространстве и воздействия компьютерных атак, повлекли за собой значительное расширение профилей операционного, правового, стратегического, репутационного рисков, а также риска ликвидности (все перечисленные риски входят в состав типичных банковских рисков[23]) [16].

Приведем развернутые определения упомянутых рисков, чтобы нагляднее показать, какие последствия могут быть у кредитных организаций в случае работы в киберпространстве.

Операционный риск связан с возможными текущими и перспективными финансовыми потерями, которые могут возникнуть из-за ошибок при выполнении банковских операций, мошеннических действий в отношении банка, нарушением непрерывности и/или нештатным функционированием БАС кредитной организации (по причине возможных аварий, отказов и сбоев оборудования как самого банка, так и различного рода провайдеров услуг) [17].

Риск ликвидности связан с возможными финансовыми потерями, обусловленными неспособностью кредитной организации своевременно и полностью выполнить свои обязательства перед клиентами из-за изменения характеристик управления ликвидностью в условиях открытого сетевого взаимодействия (непредвиденный отток средств, хищения в крупных размерах, несанкционированные переводы средств, другие потери высоколиквидных активов, сбои в работе программного обеспечения, отказы и нарушения непрерывности функционирования оборудования, применяемого для осуществления банковской деятельности, ведущие к невыполнению соответствующих обязательств перед клиентами).

Правовой риск включает в себя возможные финансовые потери, связанные с нарушением кредитной организацией 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 кредитной организации из-за нарушения ею каких-либо обязательств перед клиентами (включая функциональную недоступность ее автоматизированных систем, невыполнение обязательств перед клиентами и/или потерю

[20] Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014). URL: http://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf

[21] Например, АРМ КБР и компьютер, используемый для подготовки XML-документа, находились в пользовательской локальной вычислительной сети. Аналогично использовались АРМ SWIFT, АРМ СЭБ и АРМ обновления программного обеспечения банкоматов.

[22] Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01.06.2015 по 31.05.2016. URL: http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf

[23] Полный перечень типичных банковских рисков приведен в Письме Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

банковских и/или клиентских данных из-за отказов оборудования как в самой кредитной организации, так и у ее провайдеров), потерю денежных средств банка и его клиентов, в том числе по причине воздействия компьютерных атак (сюда же можно отнести потери от судебных исков, связанных с успешными компьютерными атаками).

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

Процесс анализа источников рисков рекомендуется проводить непрерывно, а методики выявления, анализа и мониторинга рисков должны регулярно пересматриваться для обеспечения их полноты и актуальности ввиду высоких темпов технологических инноваций в банковском деле. В первую очередь это касается риск-подразделений и служб внутреннего контроля кредитных организаций (*рис. 1*).

Минимизировать киберпреступность можно за счет комплексного подхода по усилению мер, направленных на обеспечение кибербезопасности в кредитно-финансовой сфере. И начинать надо с правовых мер, которые должны устанавливать правила ведения бизнеса в киберпространстве. Большое внимание этому направлению уделяет Банк России. Регулятор постоянно работает над выпуском новых и совершенствованием уже действующих стандартов по информационной безопасности[24]. Стандарты носят рекомендательный характер, но многие кредитные организации делают его обязательным (на основании своих внутренних приказов), тем самым стремятся поднять уровень обеспечения кибербезопасности[25].

В заключение хотелось бы сказать о выходе Указания Банка России от 07.05.2018 № 4793-У, в котором есть ряд существенных дополнений в Положение Банка России № 382-П[26], направленых на усиление мер по обеспечению информационной безопасности. Так, в частности, оператору по переводу денежных средств, оператору услуг платежной инфраструктуры на стадиях создания и эксплуатации объектов информационной инфраструктуры необходимо обеспечить: использование для осуществления переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4[27], а также ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Этим же указанием определена обязанность оператора по переводу денежных средств, оператора услуг платежной инфраструктуры

[24] С содержанием стандартов по информационной безопасности можно ознакомиться на сайте Банка России (URL: http://www.cbr.ru) и на сайте организации ABISS (URL: http://www.abiss.ru). Сообщество организаций ABISS было создано для развития и продвижения стандартов Банка России по обеспечению информационной безопасности.

[25] *Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Управление рисками информационной безопасности. М.: Горячая линия — Телеком, 2014. 130 с.

[26] Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

[27] ОУД — оценочный уровень доверия. В соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.11.2013 № 1340-ст «Об утверждении национального стандарта».

информировать Банк России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе включенных в перечень типов инцидентов, а также о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая размещение информации на официальных сайтах в сети Интернет, выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до проведения мероприятия[28].

## Выводы

Внедрение СЭБ расширяет возможности кредитных организаций по оказанию банковских услуг и значительно сокращает расходы на операционную деятельность. При этом работа в киберпространстве сопряжена с дополнительными источниками типичных банковских рисков, которые необходимо учитывать при формировании общей системы управления рисками в кредитных организациях.

Выявлено, что основными сдерживающими факторами распространения СЭБ являются отсутствие доверия клиентов кредитных организаций к СЭБ (в связи с возрастанием активности киберпреступников и недостаточной надежностью АПО СЭБ), недостаточный уровень финансовой грамотности населения, а также недостаточное качество дистанционных банковских услуг.

Установлено, что компьютерные атаки на БАС значительно расширяют профили операционного, правового, стратегического, репутационного рисков, а также риска ликвидности. Последствиями успешных атак на банки могут стать существенные финансовые потери как для самих кредитных организаций, так и для их клиентов, а как следствие этого — ухудшение оценки экономического положения в соответствии с требованиями Банка России. В связи с этим рекомендуется постоянно совершенствовать методики выявления, анализа и мониторинга рисков, которые используют риск-подразделения и службы внутреннего контроля кредитных организаций.

[28] Сведения будут поступать в ФинЦЕРТ Банка России с использованием автоматизированной системы обработки инцидентов.

***Рисунок 1***
**Взаимосвязь некоторых видов атак на АПО БАС и возможных последствий для банка**

***Figure 1***
**The relationship between a certain type of attacks on hardware and software of automated banking systems and implications for the bank**


*Источник:* составлено автором

*Source:* Authoring

**Список литературы**


1. *Лямин Л.В.* Применение технологий электронного банкинга: риск-ориентированный подход. М.: ЦИПСиР; КноРус, 2011. 336 с.
2. *Шеремет И.А.* Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества России. 2018. Т. 210. № 2. С. 23—34. URL: http://www.veorus.ru/upload/iblock/473/veo_210.pdf
3. *Ревенков П.В.* Операционный риск в условиях возрастания кибератак на банки // Банковское дело. 2018. № 3. С. 56—60.
4. *Конявский В.А., Лопаткин С.В.* Компьютерная преступность. В 2-х т. Т. 1. М.: РФК-Имидж Лаб, 2006. 840 с.
5. *Антипов А.А., Липатов А.О., Мищенко В.В.* Финансовая доступность инфраструктуры платежных услуг на территории Алтайского края // Деньги и кредит. 2017. № 8. С. 55—61. URL: http://cbr.demo.pointid.ru/Collection/Collection/File/8491/SODER8-2017.pdf
6. *Georgescu M., Jeflea V.* The Particularity of the Banking Information System. *Procedia Economics and Finance*, 2015, vol. 20, pp. 268–276. URL: https://doi.org/10.1016/S2212-5671(15)00074-X
7. *Малюк А.А.* Глобальная культура кибербезопасности. М.: Горячая линия — Телеком, 2017. 308 с.
8. *Демидов О.В.* Глобальное управление Интернетом и безопасность в сфере использования ИКТ: ключевые вызовы для мирового сообщества. М.: Альпина Паблишер, 2016. 198 с.
9. *Салтевский М.В., Литвинов А.Н., Чернец Н.Г.* Проблемы противодействия преступности в сфере компьютерных технологий. М.: Юркнига, 2006. 95 с.
10. *Грень И.В.* Компьютерная преступность. Минск: Новое знание, 2007. 412 с.
11. *Кинг Б.* Банк 3.0. Почему сегодня банк — это не то, куда вы ходите, а то, что вы делаете. М.: Олимп-Бизнес, 2017. 520 с.
12. *Бирюков А.А.* Информационная безопасность: защита и нападение. М.: ДМК-Пресс, 2017. 434 с.
13. *Масалков А.С.* Особенности киберпреступлений в России. Инструменты нападения и защита информации. М.: ДМК-Пресс, 2018. 226 с.
14. *Смирнов А.А.* Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского союза. М.: Юнити-Дана, 2011. 196 с.
15. *Keyun Ruan*. Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk. *Computers & Security*, 2017, vol. 65, pp. 77–89. URL: https://doi.org/10.1016/j.cose.2016.10.009
16. *Лямин Л.В.* Анализ факторов риска, связанных с интернет-банкингом. Ч. 1 // Расчеты и операционная работа в коммерческом банке. 2006. № 5. С. 52—63.
17. *Бердюгин А.А.* Способ управления операционными рисками финансовой организации // Защита информации. Инсайд. 2018. № 2. С. 78—81.

**Информация о конфликте интересов**

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

**pISSN 2071-4688**
**eISSN 2311-8709**

*Banking*

# EXTENDING THE PROFILE OF BANK RISK UNDER CONDITIONS OF WORK IN CYBERSPACE

**Pavel V. REVENKOV**

Financial University under Government of Russian Federation, Moscow, Russian Federation
pavel.revenkov@mail.ru
https://orcid.org/0000-0002-0354-0665

**Article history:**
Received 24 July 2018
Received in revised form
15 August 2018
Accepted 29 August 2018
Available online
29 November 2018

**JEL classification:** G21, G32, L86

**Keywords:** cyberspace, cybersecurity, electronic banking, risk, cyber attack

**Abstract**

**Subject** Consideration of the potential impact of various risks associated with work in cyberspace, including computer attacks on automated banking systems, can improve the quality of risk departments and internal control services of banks, and ensure customer confidence in electronic banking systems.

**Objectives** The study aims to investigate the specifics of doing banking business in cyberspace, analyze sources of additional risks for banks using electronic banking systems and under computer attacks, identify obstacles to remote banking services and cause-and-effect relations in the event of computer attacks on automated banking systems of credit institutions.

**Methods** I employ general scientific methods of knowledge, like analysis and synthesis, induction and deduction, the analogy method, analysis of academic literature. The phenomena under study were interpreted with the help of graphical method.

**Results** The paper unveils main risk factors for banks when they operate in cyberspace. It ascertains that computer attacks on automated banking systems of credit institutions increase operational, legal, strategic, reputational, and liquidity risk.

**Conclusions** The findings may be helpful for improving the regulation and supervision of financial and credit organizations in the context of electronic banking systems application, the performance of risk departments and internal control service of banks, enhance risk management, minimize the impact of computer attacks on automated banking systems.

© Publishing house FINANCE and CREDIT, 2018

**Please cite this article as:** Revenkov P.V. Extending the Profile of Bank Risk under Conditions of Work in Cyberspace. *Finance and Credit*, 2018, vol. 24, iss. 11, pp. 2471–2485.
https://doi.org/10.24891/fc.24.11.2471

## References

1. Lyamin L.V. *Primenenie tekhnologii elektronnogo bankinga: risk-orientirovannyi podkhod* [Applying the electronic banking technologies: A risk-oriented approach]. Moscow, TsIPSiR, KnoRus Publ., 2011, 336 p.

2. Sheremet I.A. [Digital economy and cybersecurity of its financial sector]. *Nauchnye trudy Vol'nogo ekonomicheskogo obshchestva Rossii = Scientific Works of the Free Economic Society of Russia*, 2018, vol. 210, no. 2, pp. 23–34.
URL: http://www.veorus.ru/upload/iblock/473/veo_210.pdf (In Russ.)

3. Revenkov P.V. [Operational risk in conditions of increasing cyberattacks on banks]. *Bankovskoe delo = Banking*, 2018, no. 3, pp. 56–60. (In Russ.)

4. Konyavskii V.A., Lopatkin S.V. *Komp'yuternaya prestupnost'* [Cybercrime]. Moscow, RFK-Imidzh Lab Publ., 2006, 840 p.

5. Antipov A.A., Lipatov A.O., Mishchenko V.V. [Financial accessibility of payment services infrastructure in the Altai Territory]. *Den'gi i kredit = Russian Journal of Money and Finance*, 2017, no. 8, pp. 55–61. URL: http://cbr.demo.pointid.ru/Collection/Collection/File/8491/SODER8-2017.pdf (In Russ.)

6. Georgescu M., Jeflea V. The Particularity of the Banking Information System. *Procedia Economics and Finance*, 2015, vol. 20, pp. 268–276. URL: https://doi.org/10.1016/S2212-5671(15)00074-X

7. Malyuk A.A. *Global'naya kul'tura kiberbezopasnosti* [Global culture of cybersecurity]. Moscow, Goryachaya liniya – Telekom Publ., 2017, 308 p.

8. Demidov O.V. *Global'noe upravlenie Internetom i bezopasnost' v sfere ispol'zovaniya IKT: klyuchevye vyzovy dlya mirovogo soobshchestva* [Global Internet governance and security in the sphere of ICT use: Key challenges for the world community]. Moscow, Al'pina Pablisher Publ., 2016, 198 p.

9. Saltevskii M.V., Litvinov A.N., Chernets N.G. *Problemy protivodeistviya prestupnosti v sfere komp'yuternykh tekhnologii* [Problems related to counteracting crime in the field of computer technology]. Moscow, Yurkniga Publ., 2006, 95 p.

10. Gren' I.V. *Komp'yuternaya prestupnost'* [Computer crime]. Minsk, Novoe znanie Publ., 2007, 412 p.

11. King B. *Bank 3.0: Pochemu segodnya bank – eto ne to, kuda vy khodite, a to, chto vy delaete* [Bank 3.0: Why Banking Is No Longer Somewhere You Go But Something You Do]. Moscow, Olimp-Biznes Publ., 2017, 520 p.

12. Biryukov A.A. *Informatsionnaya bezopasnost': zashchita i napadenie* [Information security: Protection and attack]. Moscow, DMK-Press Publ., 2017, 434 p.

13. Masalkov A.S. *Osobennosti kiberprestuplenii v Rossii. Instrumenty napadeniya i zashchita informatsii* [Specifics of cybercrime in Russia. Attack tools and information protection]. Moscow, DMK-Press Publ., 2018, 226 p.

14. Smirnov A.A. *Obespechenie informatsionnoi bezopasnosti v usloviyakh virtualizatsii obshchestva: opyt Evropeiskogo soyuza* [Ensuring the information security in conditions of society virtualization: The European Union case]. Moscow, YUNITI-DANA Publ., 2011, 196 p.

15. Keyun Ruan. Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk. *Computers & Security*, 2017, vol. 65, pp. 77–89. URL: https://doi.org/10.1016/j.cose.2016.10.009

16. Lyamin L.V. [Analysis of risk factors associated with Internet banking. Part 1]. *Raschety i operatsionnaya rabota v kommercheskom banke*, 2006, no. 5, pp. 52–63. (In Russ.)

17. Berdyugin A.A. [Method of managing operational risks of a financial organization]. *Zashchita informatsii. Insaid*, 2018, no. 2, pp. 78–81. (In Russ.)

**Conflict-of-interest notification**

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.