Ревенков Павел Владимирович
д-р экон. наук, профессор
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва
Дудка Александр Борисович
канд. экон. наук, доцент
ФГБОУ ВО «Омский государственный
университет им. Ф.М. Достоевского»
г. Омск, Омская область
Чебарь Александр Геннадьевич
ассистент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

НОВЫЕ ИСТОЧНИКИ БАНКОВСКИХ РИСКОВ В УСЛОВИЯХ РАБОТЫ В КИБЕРПРОСТРАНСТВЕ

Аннотация*: в статье рассмотрены основные преимущества работы банков в киберпространстве и новые источники банковских рисков при отсутствии «прямого контакта» банка с клиентом. Приведены основные виды компьютерных атак на банковские автоматизированные системы кредитных организаций и последствия их влияния на типичные банковские риски.*

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

Новые возможности информационно-телекоммуникационных технологий и средств связи значительно изменили процесс ведения банковского бизнеса и стали основой для активного внедрения систем электронного банкинга (СЭБ), фактически переводя весь процесс взаимодействия банка с клиентами в киберпространство.

Примечание. Наиболее распространёнными 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 планшетных компьютеров, смартфонов и других аналогичных устройств).

Понятия «киберпространство» и «кибербезопасность» в настоящее время не определены в законодательстве Российской Федерации (традиционно используются термины «информационное пространство» и «информационная безопасность»). Однако в ряде международных и национальных стандартах, а также в некоторых научных работах можно встретить понятия «киберпространство» и «кибербезопасность». Чаще всего под киберпространством понимают среду информационного взаимодействия и обмена данными, реализуемой 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.

Примечание. Термин cyberspace (киберпространство) был впервые использован в романе «Neuromancer» Вильяма Гибсона (William Gibson) о прямой сетевой организации искусственного интеллекта и относится к коллективной сфере компьютерных коммуникаций.

Примечание. 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 января 2017 г. № 3-ст.), проект Концепции стратегии кибербезопасности Российской Федерации от 10.01.2014 (URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 14 июля 2018 года), 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 ноября 2014 г. № 1493-ст.).

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 оформлять документы в офисе [1].

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 оформление 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;

– доступность «открытых» телекоммуникационных систем (доступность глобальной сети Интернет и сотовой связи при отсутствие должного контроля за этими видами коммуникаций, осложняют контроль за фактическими пользователями данных видов связи);

– чрезвычайно высокая скорость выполнения транзакций (скорость выполнения банковских операций, выполняемых с помощью СЭБ, становится просто мгновенная, что также предъявляет повышенные требования к контролю);

– глобальный характер межсетевого операционного взаимодействия (т. к. с помощью СЭБ выполняются операции не только в нашей стране, но и за ее пределами – возникают дополнительные источники рисков, связанные особен-

ностями законодательства в каждой отдельной стране через которые проходят платежи клиентов. Надо учитывать особенности офшорных зон, где помимо налоговых льгот, существует определенный запрет на выдачу информации о клиентах) [2];

– 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, т.е. 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.).

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 автоматизированные системы (БАС) кредитных организаций.

Согласно отчетам ФинЦЕРТ Банка России в 2017 и 2018 годах кредитные организации подвергались следующим компьютерным атакам:

– атаки на АРМ КБР;

– атаки на АРМ SWIFT;

– атаки на АРМ СЭБ;

– атаки на устройства самообслуживания (банкоматы).

Примечание. 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 2017 и 2018 годы), размещенные на официальном сайте Банка России (www.cbr.ru).

Примечание. АРМ КБР – автоматизированное рабочее место клиента Банка России.

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 с целью заражения новых автоматизированных рабочих мест сотрудников банка [3; 4].

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

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

Также к причинам можно отнести:

– отсутствие сегментирования локальных вычислительных сетей;

– низкая 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).

Примечание. 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.

Примечание. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России За период с 01 июня 2015 г. по 31 мая 2016 г. (http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf, дата обращения 10.07.2018).

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).

Примечание. Полный перечень типичных банковских рисков приведен в Письме Банка России от 23 июня 2004 года «О типичных банковских рисках» № 70-Т.

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.

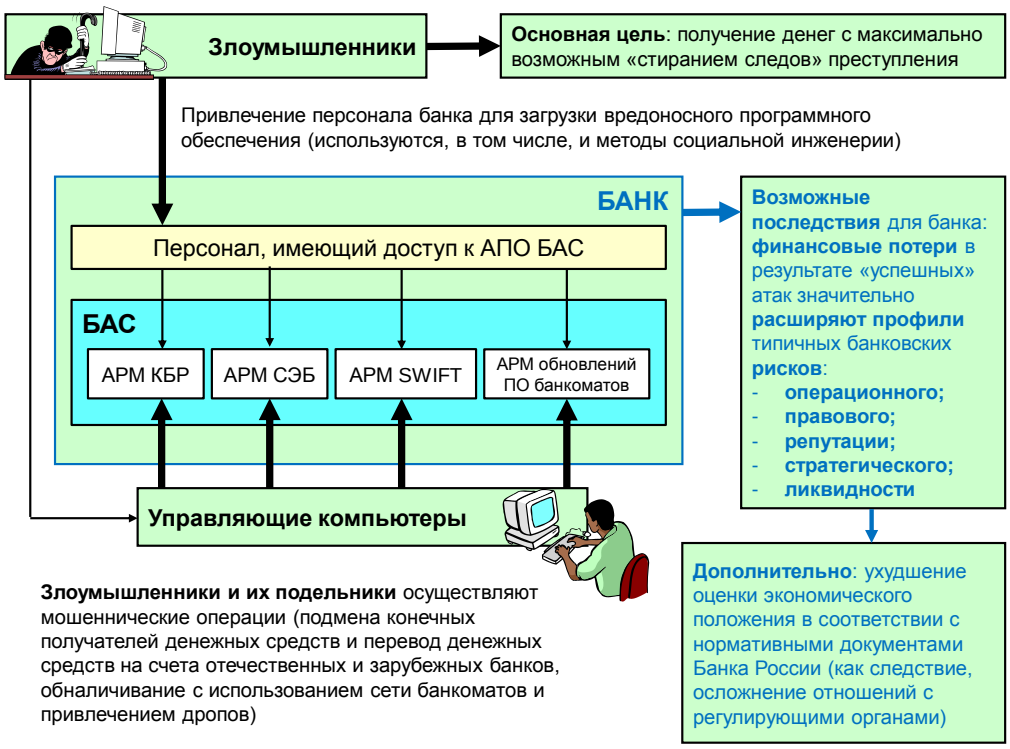

Рис. Взаимосвязь некоторых видов атак на АПО БАС и возможных последствий для банка (составлено автором)

Минимизировать возможности киберпреступности 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. Большую работу в этом направлении проводит Банк России. Регулятор постоянно работает над выпуском новых и совершенствованием уже действующих стандартов по информационной безопасности. Стандарты носят рекомендательный характер, но многие кредитные организации делают его их обязательными (на основании своих внутренних приказов), тем самым стремятся поднять уровень обеспечения кибербезопасности [5].

Примечание. С содержанием стандартов по информационной безопасности можно ознакомиться на сайте Банка России (www.cbr.ru) и на сайте организации ABISS (www.abiss.ru). Сообщество организаций ABISS было создано для развития и продвижения стандартов Банка России по обеспечению информационной безопасности.

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;

– 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 из этого – ухудшение оценки экономического положения в соответствие 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.

Список литературы

1. Юденков Ю.Н. Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практическое пособие / Ю.Н. Юденков [и др.]. – М.: КНОРУС, 2014. – 318 с.

2. Ревенков П.В. Операционный риск в условиях возрастания кибератак на банки // Банковское дело. – 2018. – №3. – С. 56–60.

3. Конявский В.А. Компьютерная преступность: в 2 т. Т. 1 / В.А. Конявский, С.В. Лопаткин. – М.: РФК-Имидж Лаб, 2006. – 560 с.

4. Ревенков П.В. Компьютерные атаки как источник операционного риска в условиях электронного банкинга / П.В. Ревенков, А.А. Бердюгин // Финансы и кредит. – 2018. – Т. 24, №3. – С. 629–640 [Электронный ресурс]. – Режим доступа: https://doi.org/10.24891/fc.24.3.629

5. Милославская Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 130 с.