pISSN 2071-4688
eISSN 2311-8709

Банковская деятельность

ВНУТРЕННИЙ КОНТРОЛЬ В БАНКАХ: ОЦЕНКА РИСКА ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ АТАК

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 13.12.2018
Получена в доработанном виде 05.02.2019
Одобрена 19.02.2019
Доступна онлайн 29.03.2019

УДК 336:004.056
JEL: G21, G32, L86

Ключевые слова:
внутренний контроль, компьютерные атаки, кибербезопасность, риски, оценка рисков

Аннотация

Предмет. Для повышения качества управления банковскими рисками в условиях воздействия компьютерных атак необходимо совершенствование систем внутреннего контроля и их центральных звеньев — служб внутреннего контроля. Специалисты служб внутреннего контроля должны уметь оценивать риски воздействия компьютерных атак и своевременно информировать руководство кредитных организаций о возможных последствиях.

Цели. Разработать способы оценки риска воздействия компьютерных атак на банковские автоматизированные системы, которые могут использоваться специалистами служб внутреннего контроля в ходе проверок качества риск-менеджмента.

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

Результаты. Разработан общий подход к оценке риска воздействия компьютерных атак на банки, который может использоваться специалистами служб внутреннего контроля.

Область применения. Результаты исследования могут быть использованы для совершенствования методического обеспечения служб внутреннего контроля, а также для повышения качества функционирования общей системы управления рисками в банках.

Выводы и значимость. Ценность данной работы и новизна полученных результатов могут способствовать повышению эффективности функционирования системы управления рисками в банках в условиях воздействия компьютерных атак на банковские автоматизированные системы кредитных организаций.

Для цитирования: Ревенков П.В. Внутренний контроль в банках: оценка риска воздействия компьютерных атак // Финансы и кредит. — 2019. — Т. 25, № 3. — С. 500 — 513.
https://doi.org/10.24891/fc.25.3.500

Внутренний контроль

Внедрение новейших достижений в области цифровых технологий в банковский бизнес сопряжено не только с изменениями процессов осуществления банковских операций, но и с совершенствованием процессов управления. Одним из составляющих успешного управления любой организации, включая банк, является контроль[1].

Контроль, как правило, рассматривают с трех позиций:

1) самостоятельная функция управления (особый вид управленческой деятельности);

2) заключительный этап цикла управления;

3) составляющая процесса принятия и реализации управленческих решений, непрерывно участвующая в этом процессе [1].

[1] Еще основоположник кибернетики Норберт Винер считал, что организация эффективного управления возможна только при наличии обратной связи, функции которой и выполняет контроль. См.: *Винер Н.* Кибернетика, или управление и связь в животном и машине. М.: Наука, 1983. 344 с.

В банковской сфере одним из наиболее регулируемых видов контроля является внутренний контроль и его центральное звено — служба внутреннего контроля (СВК).

С учетом активного внедрения в банковский бизнес систем электронного банкинга[2] (СЭБ), очевидно, что зоны контроля со стороны СВК должны расширяться, включая контроль за организацией работы в киберпространстве и совершенствованием системы управления сопутствующими рисками [2].

В основу современного понимания внутреннего контроля положены принципы Комитета спонсорских организаций Комиссии Тредуэя (Committee of Sponsoring Organizations of the Treadway Commission — COSO), опубликованные в США еще в 1992 г. в Интегрированной концепции внутреннего контроля (Internal Control — Integrated Framework). В 2013 г. вышла обновленная версия данного документа под названием «Интегрированная концепция построения системы внутреннего контроля»[3] (так называемая Модель 2013). В соответствии с подходами COSO под внутренним контролем понимается процесс, встроенный в текущую деятельность любой организации, осуществляемый ее руководителями и всеми сотрудниками для достижения трех целей:

1) производственная и финансовая эффективность (операционные цели);
2) достоверность финансовой и управленческой информации (информационные цели);
3) соблюдение установленных требований (комплаенс-цели).

Концепция COSO построена на пяти взаимосвязанных элементах внутреннего контроля: контрольная среда, оценка рисков, контрольные процедуры, обмен информацией и мониторинг. Именно эти элементы и легли в основу построения системы внутреннего контроля в банках.

В дополнение к принципам внутреннего контроля в 2004 г. COSO была издана «Концепция управления рисками предприятия» (Enterprise Risk Management Framework — ERM)[4]. Согласно ERM управление рисками представляет собой процесс, осуществляемый советом директоров, руководством и другими сотрудниками в контексте стратегии организации, направленный на выявление и оценку потенциальных угроз, которые могут иметь негативные последствия. В 2017 г. вышла обновленная версия ERM, в которой приведены 20 принципов, распространяющихся на процессы стратегического планирования и управления эффективностью организации. Один из принципов (оценка риска) включает в себя рекомендацию оценивать риски по воздействию и вероятности. Воздействие риска измеряется в отношении цели, на которую риск оказывает влияние. Вероятность риска может быть выражена экспертной оценкой, количественной оценкой и частотой реализации риска. Описание профиля риска должно включать описание источников (факторов) риска и возможные последствия их проявления, в том числе и при организации бизнеса в киберпространстве с использованием СЭБ.

Добавим, что в 2015 г. специалистами Deloutte специально для COSO был подготовлен документ COSO In the Cyber age, в котором отмечается, что в то время как компании проявляют большую осторожность при обмене информацией о своих технологиях, как внутри организации, так и с внешними партнерами, для защиты своих бизнес-операций, кибермошенники могут открыто обмениваться информацией без границ, практически не опасаясь юридических последствий, и часто действуют в условиях жесткой анонимности. Кибермошенники используют технологии для атаки практически из любого места, и их целью становится практически любой вид данных [3]. Исходя из

[2] В состав электронного банкинга входят: системы интернет-банкинга, мобильного банкинга, POS-терминалы, банкоматы и др.

[3] Доступна по ссылке. URL: https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf

[4] «Концепция управления рисками организации» (Enterprise Risk Management — Integrated Framework). Комитет спонсорских организаций Комиссии Трэдуэйя (COSO), 2004. URL: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

этого можно сделать вывод о том, что киберриск или риск воздействия компьютерных атак (РВКА) — не то, чего можно избежать, а то, чем необходимо управлять. В рамках данной статьи под РВКА мы будем понимать возможные прямые и косвенные потери для организации, вызванные воздействием компьютерных атак.

Отдельно следует остановиться на роли совета директоров. Советы директоров должны понимать, что киберугрозы могут негативно влиять на возможности организации достичь поставленные перед ней цели. Ведь не важно, по какой причине банк теряет деньги (невозврат выданных кредитов или воздействие компьютерных атак), главное — это то, что потери могут иметь самые серьезные последствия для кредитной организации (КО) (вплоть до отзыва лицензии на осуществление банковской деятельности).

Эффективные коммуникации между советом директоров и руководством КО, включая высших исполнительных лиц и оперативное руководство, являются важным элементом для совета в целях выполнения им своих обязательств по надзору за внутренним контролем. При определении требований к информации для совета директоров КО можно использовать подходы и стандарты в сфере информационной безопасности и применения информационных технологий (COBIT[5], ISO[6], модель Cybersecurity Framework от NIST[7] и др.).

По мнению ведущих экспертов в области кибербезопасности, с 2000 по 2020 г. рынок кибербезопасности вырастет с 3,5 млрд долл. США до 175 млрд долл. США [4]. Этот бизнес стал в последнее время настолько важным, что почти каждый председатель правления компании из списка Fortune 500 делает все возможное для того, чтобы в состав правления входил хотя бы один человек с опытом в области кибернетики. Немногим более 10 лет назад обязательным условием считалось наличие в правлении специалиста в области аудита. Можно ожидать, что через ближайшие 5 лет отсутствие в правлении компании специалиста по вопросам кибербезопасности будет восприниматься как недостаток корпоративного руководства.

Ключевой частью использования Модели 2013 для управления РВКА является определение информационных систем ценностей и проведение оценки рисков для таких активов.

В соответствии с Принципом 6 COSO Модели 2013 необходимо провести инвентаризацию информационных активов и определить критически важные информационные системы. Далее следует выявить, каким образом информация собирается, используется, передается, хранится и архивируется, а также кто является владельцем бизнеса, отдельных систем и приложений для информационных активов.

На основании собранных данных СВК должна создать систему мониторинга перемещения различных потоков данных. В первую очередь для понимания того, как информация перемещается в бизнес-процессах, системах и приложениях.

Затем необходимо построить приоритетные элементы управления (исходя из анализа инвентаризации активов и потоков данных), выявить наиболее вероятные цели компьютерных атак и какие способы (методы) их осуществления могут быть использованы (по возможности — с какой долей вероятности). Результатом таких исследований должно стать определение средств контроля для устранения выявленных рисков (методики проверок СВК критически важных систем КО на основе риск-ориентированного подхода, включая процессы, системы или приложения)[8] [5, 6].

Одним из основных институтов по разработке рекомендаций в области банковского регулирования и надзора, включая вопросы

[5] Ассоциация аудита и контроля информационных систем (ISACA), COBIT. URL: http://isaca.org/cobit/pages/default.aspx

[6] Международная организация по стандартизации (ISO), ISO/IEC 27001 — Управление информационной безопасностью.

[7] Национальный институт стандартов и технологий (NIST). Модель повышения уровня информационной безопасности критически важных объектов.

[8] *Лямин Л.В.* Применение технологий электронного банкинга: риск-ориентированный подход. М.: ЦИПСиР, 2011. 336 с.

совершенствования внутреннего контроля в банках, является Базельский комитет по банковскому надзору (БКБН). Еще 20 лет назад БКБН выпустил документ «Система внутреннего контроля в банках: основы организации»[9], из которого следует, что система внутреннего контроля является необходимым условием надежного функционирования банков и обеспечения стабильности финансовой системы[10].

Основополагающим нормативным актом, устанавливающим порядок осуществления внутреннего контроля в кредитных организациях и банковских группах на территории Российской Федерации, а также порядок осуществления Банком России надзора за соблюдением указанных правил, является Положение Банка России № 242-П[11].

В соответствии с Положением Банка России № 242-П в части управления банковскими рисками система внутреннего контроля[12] КО должна обеспечивать контроль:

- над функционированием системы управления банковскими рисками;
- над оценкой банковских рисков;
- над управлением информационными потоками (получением и передачей информации);
- над обеспечением информационной безопасности.

Учитывая распространение СЭБ, а также рост технической составляющей большинства типичных банковских рисков, регулятор ужесточил требования к уровню обеспечения информационной безопасности при осуществлении переводов денежных средств. Результатом стал выпуск ряда нормативных документов, основными из которых являются положения Банка России № 382-П[13] и № 552-П[14].

Новая реальность и вопросы безопасности, с которыми вынуждены сталкиваться кредитные организации и их клиенты при использовании СЭБ, требуют модернизации, а в ряде случаев — и значительного пересмотра процедур управления рисками (включая новые процедуры внутреннего контроля и наличие соответствующей квалификации у специалистов СВК КО)[15].

Одной из наиболее актуальных угроз для банков выступают компьютерные атаки, главной целью которых является хищение денежных средств как у самих банков, так у их клиентов.

Общие подходы к оценке РВКА

Чаще всего возможные последствия проявления РВКА рассматривают как одну из составляющих операционного риска банка. Такой подход, в частности, рекомендует использовать БКБН. В соответствии с рекомендациями соглашения БКБН «Международная конвергенция измерения капитала и стандартов капитала: новые подходы» (Basel II) коммерческим банкам

[9] Система внутреннего контроля в банках: основы организации (Framework for Internal Control Systems in Banking Organizations). Рекомендации Базельского комитета по банковскому надзору № 40, сентябрь 1998: Письмо Банка России от 10.07.2001 № 87-Т.

[10] При этом цели создания системы внутреннего контроля в кредитных организациях аналогичны целям, изложенным в концепции COSO от 1992 г.

[11] Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (далее — Положение № 242-П).

[12] В Положении Банка России № 242-П под системой органов внутреннего контроля понимается определенная учредительными и внутренними документами кредитной организации совокупность органов управления, а также подразделений и служащих (ответственных сотрудников), выполняющих функции в рамках системы внутреннего контроля.

[13] 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».

[14] Положение Банка России от 24.08.2016 № 552-П «О требованиях к защите информации в платежной системе 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; О методах комплексной защиты от мошенничества в системах ДБО. URL: https://banktech.ru/articles/o-metodah-kompleksnoy-zaschity-ot-moshennichestva-v-sistemah-dbo; *Набигаев Э.* Безнаказанность как бензин для кибератак на банки // Банковское обозрение. 2017. № 2. С. 78—79. URL: https://bosfera.ru/bo/beznakazannost-kak-benzin-dlya-kiberatak-na-banki

следует создавать резерв под операционный риск, в том числе с учетом активного использования современных информационных технологий. Поэтому для оценки капитала, резервируемого под РВКА, можно воспользоваться базовым индикативным методом, который предлагается:

$$K_{РВКА} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^{3} ВД_i,$$

где $K_{РВКА}$ — размер капитала, выделяемого для покрытия РВКА;

$\frac{1}{3} \cdot \sum_{i=1}^{3} ВД_i$ — средняя величина валового дохода за последние 3 года при условии, что $ВД_i > 1$, $\alpha = 15\%$ — коэффициент, установленный БКБН на основе результатов эмпирических исследований и давлением банковского сообщества (которое составляют преимущественно кредитные организации Европы)[16].

Тем не менее отечественные условия не всегда соответствуют европейским стандартам. Это требует разработки метода, адаптированного к особенностям банков Российской Федерации. Согласно отчетам ФинЦЕРТ[17] в период с 2016 по 2018 г. кредитным организациям наибольший урон нанесли компьютерные атаки на АРМ КБР[18], на АРМ SWIFT и на АРМ СЭБ, а также атаки на устройства самообслуживания (банкоматы). Аналогичные выводы представлены в годовом отчете известной российской компании Group-IB[19] (вышел в октябре 2018 г.), специализирующейся на расследовании компьютерных преступлений. Согласно отчету на сегодняшний день активно действуют четыре преступные группы (Cobalt, MoneyTaker, Silence, состоящие из русскоговорящих хакеров, а также северокорейская Lazarus). В среднем в России каждый месяц киберограблениям подвергались 1—2 банка (средний ущерб от одного «успешного» ограбления составляет 132 млн руб.).

Из всех перечисленных видов компьютерных атак мы остановимся только на атаках на банкоматы (так как все перечисленные преступные группы, кроме Lazarus, участвуют в организации данного вида атак[20]). Есть еще одна причина, по которой следует внимательнее относиться к атакам на банкоматы, — это распространение различных предложений от хакеров по полному сопровождению атаки, так называемая услуга атака как сервис[21].

По данным Европола, хакеры преступной группы Cobalt похитили свыше 1 млрд евро. Согласно исследованию компании Group-IB только в одном из инцидентов в европейском банке данная группа попыталась вывести 25 млн евро[22].

Отметим, что все перечисленные атаки начинались с внедрения в локальную вычислительную сеть (ЛВС) КО вредоносного программного обеспечения (ВПО). Обычно это происходило с помощью рассылки электронных писем, содержащих ВПО (чаще всего такое ВПО не обнаруживалось антивирусными программами)[23] [7, 8].

---

[16] *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

[17] ФинЦЕРТ — специализированное подразделение Департамента информационной безопасности Банка России, в функции которого входит противодействие компьютерным атакам на организации кредитно-финансовой сферы. В настоящей статье использованы данные ежегодных отчетов ФинЦЕРТ Банка России (за 2016, 2017 и 2018 гг., размещенные на официальном сайте Банка России в разделе ФинЦЕРТ).

[18] АРМ КБР — автоматизированное рабочее место клиента Банка России. Далее соответственно: АРМ SWIFT — автоматизированное рабочее место клиента системы SWIFT, автоматизированное рабочее место клиента СЭБ.

[19] Отчет представлен на официальном сайте компании Group-IB. URL: http://www.group-ib.ru

[20] Невзирая на арест лидера группы Cobalt (весной 2018 г. в Испании), данная преступная группа по-прежнему остается одной из самых активных и агрессивных, 2—3 раза в месяц атакуя финансовые организации в России и за рубежом.

[21] Новейшие методы хакерских атак на банки и банкоматы. URL: http://www.reglament.net/bank/control/2016_4/get_article.htm?id=4921

[22] Новые атаки хакерской группы Cobalt. URL: http://www.icpress.ru/catalog/bsm/detail.php?ID=20440

[23] Подробнее о характере распространения перечисленных компьютерных атак автор говорил в своей статье «Расширение профилей банковских рисков в условиях работы в киберпространстве» (Финансы и кредит. 2018. Т. 24. № 11. С. 2471—2485). Также см.: *Торчиков В.* Мыслить, как преступник // Банковское обозрение. 2018. № 5. С. 84—86. URL: https://bosfera.ru/bo/myslit-kak-prestupnik

РВКА могут серьезно повлиять на устойчивость банка. Поэтому такие риски должны оцениваться специалистами риск-подразделений и СВК, чтобы руководство КО могло своевременно принимать превентивные меры.

Учитывать и оценивать РВКА следует таким образом, чтобы каждой угрозе от компьютерных атак соответствовала оценка с позиции возможных последствий для банка (включая нарушение непрерывности осуществления банковской деятельности, снижение качества предоставляемых банковских услуг, финансовые потери и др.), то есть на основе так называемого риск-ориентированного подхода. В подавляющем большинстве случаев банку не важно за счет чего он может потерять деньги (невозврат выданных кредитов, компьютерная атака и т.д.), главное, что последствия от этих потерь могут носить разрушительный характер для бизнеса.

В арсенале риск-менеджеров и специалистов СВК должны быть методики оценки РВКА, которые учитывают взаимосвязи конкретных уязвимостей в банковских автоматизированных системах (БАС), недостатков в действующих бизнес-процессах КО с размерами возможного ущерба конкретного банка.

Для оценки возможных потерь можно использовать формулу, в которой риск (R) рассчитывается на основании коэффициентов качества обеспечения кибербезопасности и «суммы под риском» (S_R).

Для удобства разделим все мероприятия по обеспечению кибербезопасности только на две группы: организационные и технические ($K_{ОРГ}$ и $K_{ТЕХ}$)[24].

Исходя из этого, формула будет иметь следующий вид:

$$R = S_R \cdot (K_{ОРГ} + K_{ТЕХ}),$$

где R — денежное выражение риска;

S_R — «сумма под риском»;

$K_{ОРГ}$ — коэффициент полноты выполнения организационных мероприятий;

$K_{ТЕХ}$ — коэффициент полноты выполнения технических мероприятий.

Специалисты СВК должны уметь оценивать влияние каждого из недостатков в обеспечении кибербезопасности, выявленного в ходе проверок БАС КО, на совокупную оценку каждого коэффициента и присвоить ему числовое значение, исходя из тяжести возможных последствий («вес» угрозы). Для оценки качества управления РВКА составляется перечень конкретных вопросов, на которые должен ответить аналитик-эксперт [9]. Ряд вопросов приведен далее.

Примерные вопросы об организационных и технических мероприятиях и их вес.

1. Имеются ли биометрические системы контроля управления доступом? (4).
2. Имеется ли в банке экранирование кабельных коммуникаций? (2).
3. Компьютеры сотрудников подключены к источникам бесперебойного питания? (4).
4. Снабжены ли аудитории банка камерами видеонаблюдения? (4).
5. Оснащены ли помещения банка датчиками разбития окон? (3).
6. Какова степень осведомленности работников кредитных организаций в области кибербезопасности[25]? (4).
7. Существуют ли внутренние распорядительные документы на организацию отдельных работ в БАС КО[26]? (4).
8. Проведено ли сегментирование локальных вычислительных сетей [10]? (3).
9. Блокируется ли автоматический запуск макросов в документах Microsoft Office на компьютерах специалистов [10]? (2).

[24] При необходимости деление может быть шире и включать, например, правовые, аппаратно-программные, криптографические, экономические и другие меры по обеспечению кибербезопасности.

[25] *Олифер В.Г., Олифер Н.А.* Безопасность компьютерных сетей: учеб. М.: Горячая линия — Телеком, 2017. 644 с.

[26] Там же.

10. Запрещено ли присвоение пользователям избыточных прав локального администратора не уполномоченными сотрудниками? (4).

11. Снабжены ли рабочие компьютеры средствами антивирусной защиты[27]? (4).

12. Включена ли опция регулярного обновления антивирусных баз[28]? (3).

13. Рассылка приказов высшего руководства банка организована безошибочно? (2).

Ответы на эти и другие вопросы[29] аналитик-эксперт дает самостоятельно (в зависимости от ситуации в банке) по пятибалльной шкале. Значение веса тоже может определяться независимо от цифр, приведенных в статье.

Индекс соответствия параметров банка положениям перечня вопросов определяется следующим образом:

$$K_{ОРГ+ТЕХ}=\frac{\sum(Балл\cdot Вес)}{\sum Весов}.$$

Значение индекса $K_{ОРГ+ТЕХ}$ обратно пропорционально уровню качества менеджмента РВКА в организации и отображает вероятность реализации риска. Формула (1) приобретает более простой вид:

$$R=S_R\cdot K_{ОРГ+ТЕХ}.$$

С учетом того, что в последнее время одним из наиболее распространенных видов компьютерных атак на КО являются атаки на банкоматы, рассмотрим, как может работать такой подход при оценке возможных последствий данного вида риска (дополнительно можно отметить, что само место размещения банкомата(ов) может обладать факторами риска. Например, отсутствует освещение в темное время суток, нет поблизости проезжей части и т.п).

Очевидно, что самый плохой результат для банка связан с полной потерей всех денежных средств, находящихся в банкоматах, размещенных вне офисов банка или в крупных торговых центрах, где постоянно дежурит охрана). Для этого можно взять средний остаток денежных средств в банкоматах (это будет «суммой под риском»). Далее необходимо проанализировать, насколько защищены банкоматы банка от данного вида атак. Для этого необходимо совместно со специалистами подразделений безопасности провести проверки БАС на предмет выявления уязвимостей в процессах управления сетью банкоматов. Причем уязвимости могут быть связаны с недостатками в применении как организационных, так и технических мер по противодействию компьютерным атакам (такая информация будет использоваться для расчета коэффициентов полноты выполнения мероприятий по обеспечению кибербезопасности).

Например, у банка есть 20 банкоматов, расположенных вне офисных помещений и торговых центров. В каждом из них средний остаток после относительно недавней загрузки наличности может составлять около 15 млн руб.[30]. Умножая средний остаток в каждом банкомате на количество банкоматов, расположенных вне офисных помещений, получаем сумму под риском — 300 млн руб.

Предположим, проверки, проводимые специалистами СВК, выявили ряд недостатков в обеспечении безопасности сети банкоматов. Исходя из «весомости» недостатков коэффициент полноты выполнения организационных мероприятий составил 0,04, а коэффициент полноты выполнения технических мероприятий — 0,02.

Применив нашу формулу, получим, что РВКА на банкоматы составляет 18 млн руб. $(300\ 000\ 000\cdot 0{,}06=18\ 000\ 000)$.

Такой подход удобен тем, что перечень мер (включая входящие в их расчет отдельные уязвимости или недостатки) может постоянно расширятся с учетом особенностей научно-

[27] *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. 320 с.

[28] Там же.

[29] Список вопросов и их вес не являются последним вариантом и будут неизбежно пополняться вместе с развитием технологий.

[30] Из расчета, что в банкомате загружено 5 кассет по 2 000 листов (с купюрами номиналом: 5 000, 2 000, 1 000, 500 и 200 руб.). Итого: 17 400 тыс. руб.

технического прогресса и новых видов компьютерных атак на аппаратно-программное обеспечение (АПО) БАС КО (*рис. 1*).

Добавим, что согласно ГОСТ Р ИСО/МЭК 31010:2011 «Менеджмент риска. Методы оценки риска», оценка риска может быть выполнена с различной степенью глубины и детализации с использованием одного или нескольких методов разного уровня сложности. Стандарт предлагает 31 метод оценки рисков, из которых для оценки риска нарушения информационной безопасности могут быть применены:

- Метод «Дельфи» — получение мнения группы экспертов, которые выражают свое мнение индивидуально и анонимно, при этом имея возможность узнать мнения других экспертов. Результаты анализа обрабатываются статистическими методами;
- Байесовский анализ и Сети Байеса отличается от классической статистики предположением, что параметры распределений являются не постоянными, а случайными переменными. В упрощенной форме теорема Байеса выглядит так:

$$P(A|B)=\frac{\{p(A)\cdot P(B|A)\}}{P(B)},$$

где $P(X)$ — вероятность события X;

$P(X|Y)$ — вероятность события X при условии, что произошло событие Y;

- Структурированный анализ сценариев методом «Что, если?» (SWIFT[31] — Structured what-if technique) является систематизированным методом исследования сценариев, основанным на командной работе. Используются фразы-подсказки «Что, если» для идентификации опасных ситуаций и создания сценариев их развития.

В развитие теории информационных рисков большой вклад внесли научные группы и компании в сфере информационных технологий, разработавшие различные методики оценки рисков. Наиболее значимые из них:

– ГРИФ компании «Digital security»;

– CCTA Risk Analysis and Management Method (CRAMM);

– методика анализа и контроля рисков RiskWatch;

– методология Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE);

– руководство по управлению рисками от компании Microsoft.

Перечисленные методы позволяют оценить необходимый уровень инвестиций в информационную безопасность для обеспечения их максимальной эффективности.

Добавим, что последствия рассмотренных компьютерных атак могут стать причиной расширения профилей операционного, правового, стратегического, репутационного рисков, а также риска ликвидности (все перечисленные риски входят в состав типичных банковских рисков[32]). В связи с этим специалисты СВК должны учитывать возможные последствия воздействия компьютерных атак в общей системе управления рисками КО и предлагать обоснованные предложения руководству банка о принятии превентивных мер, направленных на минимизацию возможных рисков [11].

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 (*рис. 2*).

В идеальной ситуации в СВК КО должны быть специально подготовленные специалисты, способные проверять защищенность различных участков информационного контура

[31] В банковской деятельности аббревиатура SWIFT означает также Общество всемирных межбанковских финансовых телекоммуникаций (от англ. *Society for Worldwide Interbank Financial Telecommunications*).

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

банковской деятельности, формируемого в каждой отдельно взятой КО (в том числе в условиях применения технологий дистанционного банковского обслуживания, включая СЭБ) от воздействия компьютерных атак. Такие специалисты в идеальной ситуации должны иметь не только экономическое или юридическое, но и техническое образования, которые позволяли бы им разбираться в распределенных компьютерных системах, иметь четкое представление о построении информационных контуров банковской деятельности при организации банковского обслуживания через Интернет и посредством сотовой связи, а также связанных с данными областями рисках.

Что касается непосредственно организации, содержания и методологии внутреннего контроля в части противодействия компьютерным атакам, то она во многом зависит от специфических факторов в отношении конкретных кредитных организаций. Большинству из них свойственны индивидуальные архитектуры внутрибанковских распределенных компьютерных систем и индивидуальный набор требований к обеспечению целостности и безопасности информационных ресурсов, а также оригинальный набор методов и средств внутреннего контроля.

Немаловажным является и такой факт, как наличие в руководстве КО менеджеров, которые могли бы обеспечить правильность принимаемых решений по результатам проведенных СВК[33] проверок.

Выводы

Компьютерные атаки значительно расширяют профили типичных банковских рисков, а также могут нанести серьезный урон бесперебойному функционированию отдельно взятой КО и повлиять на стабильность банковской системы в целом.

Для всех банков, осуществляющих свой бизнес с использованием технологий дистанционного банковского обслуживания (включая СЭБ), необходимо иметь достаточный уровень обеспечения кибербезопасности (определять уровень следует на основе риск-ориентированного подхода).

В СВК должны входить специалисты, способные оценивать РВКА.

Методическое обеспечение СВК должно своевременно обновляться, в том числе и по вопросам минимизации возможных последствий проявления РВКА (включая атаки на АПО БАС КО).

В руководстве КО должны быть менеджеры, достаточно хорошо разбирающиеся в современных БАС, включая особенности функционирования СЭБ.

[33] Данные менеджеры должны иметь достаточно хорошую техническую подготовку и представлять все возможные последствия проявления рисков, связанных с использованием технологий дистанционного банковского обслуживания, включая применение СЭБ.

Рисунок 1
Влияние компьютерных атак на стабильность банковской системы

Figure 1
Impact of cyber attacks on the banking system stability

Источник: авторская разработка

Source: Authoring

Рисунок 2
Процесс управления рисками воздействия компьютерных атак

Figure 2
Process of managing the risks associated with cyber attacks

Источник: авторская разработка

Source: Authoring

Список литературы

1. *Рудько-Силиванов В.В., Лапина К.В., Крючкова Е.А.* Концептуальные основы и практика организации системы внутреннего контроля // Деньги и кредит. 2011. № 2. С. 36–41. URL: https://www.cbr.ru/content/document/file/27026/rudko_02_11.pdf

2. *Ревенков П.В.* Управление рисками в условиях электронного банкинга: монография. М.: ИТКОР, 2011. 167 с.

3. *Galligan M.E., Rau K.* COSO in the Cyber Age. URL: https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

4. *Росс А.* Индустрии будущего. М.: АСТ, 2017. 352 с.

5. *Крышкин О.* Настольная книга по внутреннему аудиту: риски и бизнес-процессы. М.: Альпина Паблишер, 2015. 478 с.

6. *Костикова Л.В., Цангль Н.Е.* Риск-ориентированный внутренний аудит в банке: методическое пособие. М.: Регламент-Медиа, 2014. 203 с.

7. *Лямин Л.В.* Электронный банкинг и риски его клиентов // Банкноты стран мира. 2018. № 7. С. 26—28. URL: http://www.icpress.ru/catalog/bsm/detail.php?ID=20440

8. *Roux C.* Cybersecurity and Cyber Risk. URL: https://www.bis.org/review/r151002d.pdf

9. *Бердюгин А.А.* Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1. С. 28—38. URL: http://cyberrus.com/wp-content/uploads/2018/05/28-38-125-18_4.-Berdyugin.pdf

10. *Macknight J.* Cyber Security: Making Banking Safer. *The Banker*, 2016, vol. 166, no. 1080, pp. 110–115. URL: https://www.thebanker.com/Transactions-Technology/Technology/Cyber-security-making-banking-safer?ct=true

11. *Camillo M.* Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institutions. *Journal of Risk Management in Financial Institutions*, 2017, vol. 10, no. 2, pp. 196–200. URL: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf

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

INTERNAL CONTROL IN BANKS: ASSESSING THE RISK OF CYBER ATTACKS

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 13 December 2018
Received in revised form
5 February 2019
Accepted 19 February 2019
Available online
29 March 2019

JEL classification: G21, G32, L86

Keywords: internal control, cyber attack, cybersecurity, risk assessment

Abstract

Subject To enhance banking risk management, internal control service specialists should be able to assess risks associated with cyber attacks and promptly inform the management of credit institutions about possible consequences.

Objectives The article focuses on developing ways to assess the risk of computer attacks and their impact on automated banking systems, which can be used by specialists of internal control services for quality control of banking risk management in conditions of using electronic banking systems.

Methods I employ general scientific methods of cognition, like analysis and synthesis, induction and deduction, the analogy method. I also use the techniques of systems analysis of academic literature in the field of theoretical and applied research, and a graphic method to interpret the investigated phenomena.

Results I developed a general approach to assessing the risk of exposure to cyber attacks on banks. The said approach may be useful for internal control services specialists to improve the methodological support and enhance the performance of the entire risk management system in banks.

Conclusions and Relevance The novelty of the findings may contribute to enhancing the efficiency of the risk management system in banks under the impact of cyber attacks on automated banking systems.

Please cite this article as: Revenkov P.V. Internal Control in Banks: Assessing the Risk of Cyber Attacks. *Finance and Credit*, 2019, vol. 25, iss. 3, pp. 500–513.
https://doi.org/10.24891/fc.25.3.500

References

1. Rud'ko-Silivanov V.V., Lapina K.V., Kryuchkova E.A. [The Conceptual Basis and Organization of the System of Internal Control]. *Den'gi i kredit = Russian Journal of Money and Finance*, 2011, no. 2. 36–41. URL: https://www.cbr.ru/content/document/file/27026/rudko_02_11.pdf (In Russ.)
2. Revenkov P.V. *Upravlenie riskami v usloviyakh elektronnogo bankinga: monografiya* [Risk management in electronic banking: a monograph]. Moscow, ITKOR Publ., 2011, 167 p.
3. Galligan M.E., Rau K. COSO in the Cyber Age. URL: https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf
4. Ross A. *Industrii budushchego* [The Industries of the Future]. Moscow, AST Publ., 2017, 352 p.
5. Kryshkin O. *Nastol'naya kniga po vnutrennemu auditu: riski i biznes-protsessy* [Handbook on internal audit: Risks and business processes]. Moscow, Al'pina Pablisher Publ., 2015, 478 p.
6. Kostikova L.V., Tsangl' N.E. *Risk-orientirovannyi vnutrennii audit v banke: metodicheskoe posobie* [Risk-oriented internal audit in bank: a methodological guide]. Moscow, Reglament-Media Publ., 2014, 203 p.

7. Lyamin L.V. [Electronic banking and risks of its customers]. *Banknoty stran mira = Banknotes of the World*, 2018, no. 7, pp. 26–28.
URL: http://www.icpress.ru/catalog/bsm/detail.php?ID=20440 (In Russ.)

8. Roux C. Cybersecurity and Cyber Risk. URL: https://www.bis.org/review/r151002d.pdf

9. Berdyugin A.A. [Risk management of information security violation in conditions of electronic banking]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2018, no. 1, pp. 28–38.
URL: http://cyberrus.com/wp-content/uploads/2018/05/28-38-125-18_4.-Berdyugin.pdf (In Russ.)

10. Macknight J. Cyber Security: Making Banking Safer. *The Banker*, 2016, vol. 166, no. 1080, pp. 110–115. URL: https://www.thebanker.com/Transactions-Technology/Technology/Cyber-security-making-banking-safer?ct=true

11. Camillo M. Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institutions. *Journal of Risk Management in Financial Institutions*, 2017, vol. 10, no. 2, pp. 196–200. URL: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf

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.