ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ПРИМЕНЕНИЯ СИСТЕМ МОБИЛЬНОГО БАНКИНГА

Ревенков П.В.[1], Крупенко Д.С.[2]

Цель статьи: *исследование и оценка рисков информационной безопасности, возникающих при предоставлении финансовыми организациями клиентам услуг мобильного банкинга, а также разработка предложений по применению мер и средств, направленных на снижение указанных рисков.*

Метод: *применены общенаучные методы познания: анализ и синтез, индукция и дедукция, метод аналогии. Проведен системный анализ научной литературы в области теоретических и прикладных исследований. Реализован графический метод интерпретации исследуемых явлений.*

Полученный результат: *сформулированы предложения по основным направлениям регулирования операционного риска в кредитно-финансовой сфере в условиях применения мобильного банкинга. Приведены рекомендации как для кредитно-финансовых организаций, так и для регулирующих органов для повышения эффективности функционирования систем электронного банкинга и, в частности, мобильного банкинга, а также снижения операционного риска в данной области. Рассмотрены наиболее значимые угрозы безопасности мобильных приложений. Сформулированы предложения по применению необходимых мер и средств обеспечения информационной безопасности мобильных приложений с целью снижения рисков. Предложенные меры и средства можно использовать при разработке систем мобильного банкинга.*

Ключевые слова: *дистанционное банковское обслуживание, финансовая организация, операционный риск, мобильное приложение, угрозы безопасности, уязвимость приложения, информационная безопасность.*

DOI: *10.21681/2311-3456-2019-2-21-28*

1. Введение

В настоящее время финансовые организации находятся в высококонкурентной среды, поэтому руководство финансовых организаций постоянно ищет новые методы достижения конкурентных преимуществ, в том числе, путем минимизации операционных расходов, при условии сохранения своей конкурентоспособности. В последние несколько лет у финансовых организаций появился новый вид конкурентов финтех–компаний, предоставляющие сервисы по переводу валютных средств и предлагающие клиентам (которые также как и пользователи электронного банкинга[3] сами выполняют роль операционных работников, заполняя транзакционные поручения на своих мобильных устройствах) более выгодные условия по сравнению с предложениями традиционных финансовых институтов [1, 2].

Постоянное расширение конкурентного профиля вынуждает финансовые организации активно развивать современные финансовые сервисы, в том числе, технологии электронного банкинга. Кроме того, у них значительно время вывода на рынок новых сервисов (time to market), включая время на изучение сопутствующих рисков. Также сокращается время и у регулирующих органов на анализ текущей ситуации и выпуск регламентирующих документов в части обеспечению должного уровня информационной безопасности [3].

В этих условиях финансовые организации должны внедрять новые методы анализа рисков, на основе которых они могут более эффективно расходовать свои средства, в том числе при формировании бюджета служб информационной безопасности (включая расходы на внедрение аппаратно-программного обеспечения, обеспечивающего защитные меры) [4].

В статье рассмотрены общие подходы к оценке сопутствующих рисков при использовании систем мобильного банкинга (СМБ), учитывая, что данный вид электронного банкинга получает наиболее широкое распространение как в России, так и за рубежом.

2. Направления мобильного бизнеса

Перед тем как перейти непосредственно к оценке рисков при внедрении СМБ, рассмотрим, что включает в себя более широкое понятие – мобильный бизнес.

В целом мобильный бизнес можно применять в трех направлениях:

1. Мобильный банкинг;
2. Мобильные платежи;

1 Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, Москва. Россия. E-mail: pavel.revenkov@mail.ru

2 Крупенко Дмитрий Сергеевич, аспирант кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, Москва. Россия. E-mail: krupenkods@mail.ru

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

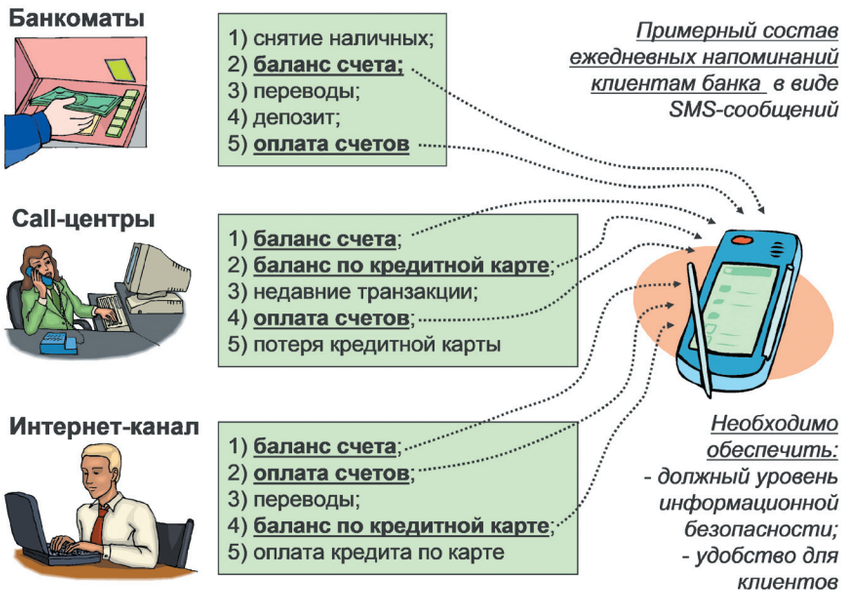

Рис. 1. Наиболее востребованная информация, которая может направляться клиентам на мобильный телефон

3. Банковские операции для людей, у которых отсутствуют банковские счета.

Мобильный банкинг позволяет осуществлять круглосуточный доступ с помощью смартфона или планшета к банковским услугам[4].

В целом мобильный банкинг становится одним из основных каналов взаимодействия банка с клиентами и вносит значительный вклад в формирование клиентского опыта. Кроме того, мобильный банкинг становится важным каналом по продвижению новых продуктов и услуг, позволяющим, в конечном счете, повысить доходность бизнеса.

Результаты аналитических опросов позволили выявить пять наиболее востребованных ежемесячных запросов или активных транзакций, которые клиенты осуществляют через различные каналы обслуживания: банкоматы, call-центры и интернет-банк [5, 6].

Представленные результаты могут служить базой для разработки приложений для мобильных устройств[5].

Мобильные платежи относятся к группе альтернативных методов оплаты. Чаще всего клиенты используют мобильные платежи для покупки продуктов или услуг, вместо оплаты банковскими картами, наличными или чеками. Продукты и услуги, которые уже можно купить, используя «банк в кармане», – это видео и аудио контент, рингтоны для мобильного телефона, on-line-игры, оплата проезда или парковки, печатная продукция, фастфуд и многое другое. Мобильные платежи включают несколько основных методов:

– мобильные интернет-платежи;

– транзакционные платежи средствами SMS сообщений;

– биллинговая система платежей;

– бесконтактные платежи (например, NFC[6]).

Банкинг для тех, у кого отсутствуют банковские счета (на основе мобильных платежей) получает распространение не только на более развитых рынках, но и в развивающихся экономиках. В развивающихся странах значительное количество домохозяйств из-за отсутствия доступа к финансовым услугам прибегают к мобильным платежам (мобильные денежные переводы между частными лицами).

Наряду с очевидными преимуществами технологии мобильного банкинга приводят к дополнительным рискам в банковском секторе. Точнее, перечень традиционных банковских рисков[7] не изменяется, но значительно увеличивается их техническая составляющая. Возрастающая техническая составляющая источников традиционных банковских рисков приводит к необходимости совершенствования некоторых аспектов регулирования в банковской отрасли, в том числе, в области мобильного банкинга. Наиболее актуальными, по мнению авторов, являются два направления, связанные с:

1) расширением профиля операционного риска в условиях распространения технологии электронного банкинга и мобильного банкинга в частности;

2) повышением требований к обеспечению информационной безопасности в связи с внушительным ростом киберпреступлений, направленных на клиентов, использующих СМБ [7].

4 В статье под термином «мобильный банкинг» понимается предоставление клиенту финансовых услуг посредством мобильного приложения, установленного на смартфоне клиента, и не рассматриваются услуги, предоставляемые посредством SMS-сообщений и web-браузера, установленного на смартфоне клиента.

5 Пожалуй, единственное, что нельзя сделать посредством мобильного телефона – это снимать наличные, но по мере того как мобильные платежи будут входить в нашу жизнь, наличные перестанут пользоваться спросом.

6 NFC (Near Field Communication – коммуникация ближнего поля) – технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров.

7 Перечень типичных банковских рисков приведен в Письме Банка России «О типичных банковских рисках» от 23 июня 2004 г. № 70-Т.

3. Операционный риск в условиях применения СМБ

Операционный риск не является единственным риском, на который влияют особенности функционирования СМБ, но в подавляющем большинстве случаев источники операционного риска влияют на расширение многих традиционных банковских рисков.

Причиной возрастания внимания в банковском секторе к операционному риску стала публикация Базельского комитета по банковскому надзору «Международная конвергенция изменения капитала и стандартов капитала: новые подходы» (Basel II).

Basel II определяет операционный риск как риск убытков, возникающий в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или в результате внешних событий.

Можно определить следующие типы событий в качестве проявлений операционного риска:

– внешние воздействия (наводнения, пожары, аварии и т.п.);

– внутренние (угрозы со стороны инсайдеров) и внешние (угрозы, как со стороны одиночных хакеров, так и преступных групп) мошенничества;

– ошибки персонала;

– сбои в реализации бизнес-процессов и обслуживании клиентов;

– физический ущерб активам;

– сбои информационных систем;

– нарушение процессов обработки и хранения данных (в том числе вызванные воздействием кибератак на организации кредитно-финансовой сферы).

Необходимо отметить, что операционный риск один из основных традиционных банковских рисков, на который технологии мобильных платежей оказывают наибольшее влияние. Операционный риск можно определить как вероятность образования убытков и/или неполучение прибыли вследствие сбоев в выполнении каждодневных, рутинных банковских операций. По отношению к технологиям мобильного банкинга можно выделить три основные области операционного риска:

– функционирование систем безопасности;

– привлечение внешних по отношению к кредитной организации подрядных организаций к процессу предоставлению клиентам банковских услуг (аутсорсинг);

– освоение сотрудниками банка новых технологий и процессов [8, 9].

В случае функционирования систем безопасности речь идет о рисках нарушения при обработке, передаче и хранении информации в электронном виде информации (нарушение целостности, уничтожение, перехват информации или злоупотребление ими в результате технических нарушений, действий злоумышленников, ошибок или мошеннических действий собственных сотрудников и клиентов) и отказы в работе банковских автоматизированных систем (перегрузки из-за недостаточной мощности ресурсов и таргетированных DDoS-атак[8] на web-серверы финансовых организаций) [10, 11, 12].

Значимость второй сферы с точки зрения операционного риска весьма высока в последнее время. Финансовые организации становятся зависимыми от своих подрядчиков, а уровень банковского обслуживания в целом определяется качеством работы компаний, сотрудники которых могут не обладать в необходимой степени знаниями о мобильном банкинге.

Риски, относящиеся к третьей области связаны с постоянно повышающими в последнее время требованиями а адаптационным способностям персонала финансовых организаций из-за ускорения процессов совершенствования бизнес-процессов и ускорения модернизации автоматизированных банковских систем. Данная проблема увеличивает риски возникновения трудностей при внедрении более сложных технологий и решений.

Для проверки качества управления операционным риском в кредитных организациях необходимо адаптировать соответствующие методики под условия активного внедрения в банковский бизнес технологии электронного банкинга. Данные методики необходимо дополнить конкретными вопросами, на которые должен ответить эксперт, чтобы в итоге сформировать информацию об эффективности управления операционным риском в финансовой организации, например:

– имеется ли подразделение или сотрудник, выполняющее функции оценки операционного риска?

– является ли данное подразделение (сотрудник) независимым по отношению к осуществляющим бизнес процессы подразделениям?

– введены ли в действие внутренние нормативные и распорядительные документы по управлению операционным риском?

– содержат ли внутренние нормативных и распорядительные документы порядок оценки операционного риска?

– обеспечивают ли принятые кредитной организацией меры достаточный уровень сохранность информации и возможность восстановления после сбоев автоматизированных систем?

– проводится ли на регулярной основе оценка операционного риска?

– имеется ли в аналитическая информация о роизошедших операционных убытках в контексте бизнес направлений деятельности с описанием ситуаций, приведших к реализации риска, позволяющая определить наиболее критические с точки зрения ОР области?

– имеется ли в кредитной организации система показателей уровня операционного риска, используемых в процессе его мониторинга?

– существуют ли в кредитной организации процессы прогнозирования потенциально возможной величины операционных убытков?

– формируется ли в кредитной организации управленческая отчётность, содержащая результаты мониторинга операционного риска?

8 DDoS-атака (от англ. Distributed Denial of Service, распределённый отказ в обслуживании) – это разновидности атак на вычислительную систему. Цель этих атак – довести систему до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

– существуют ли в кредитной организации процессы проведения самооценки процессов управления операционным риском?

Выходным результатом может быть агрегированный показатель, который формируется из отдельных составляющих. Ответу на каждому вопрос соответствует определённый балл по 5-балльной шкале, при этом ответу «да» соответствует 1 балл, а ответу «нет» – 5 баллов.

Также, каждому вопросу присваивается весовой коэффициент, который эксперт самостоятельно определяет экспертным путем, согласовав предварительно с руководством банка свои действия. Агрегированный показатель качества системы управления операционным риском в кредитной организации рассчитывается по формуле

$$AGR = \sum (Балл \times Вес) / \sum Весов \quad (1)$$

Значение агрегированного показателя обратно пропорционально качеству системы управления операционным рисков в кредитной организации. Другими словами, более низкое значение показателя соответствует более высокому уровню качества управления операционным риском, и наоборот, более высокое значение показателя соответствует более низкому уровню качества управления.

В Таблице 1 содержатся рекомендации как для кредитно-финансовых организаций, так и для регулирующих органов для повышения эффективности функционирования систем электронного банкинга и, в частности, мобильного банкинга, а также снижению операционного риска в данной области.

Предложенные направления охватывают далеко не весь необходимый перечень мероприятий в рамках управления операционного риска в условиях применения СМБ.

4. Информационная безопасность в условиях применения СМБ

Принимая во внимание, что кредитно-финансовая сфера в последнее время является, пожалуй, самой привлекательной сферой интересов киберпреступников (в пользу этого свидетельствует постоянный рост числа киберпреступлений в последние годы на финансовые организации), а также учитывая процессы оптимизации финансовых решений в сфере применения СМБ, необходимо принимать меры, направленные на достижение высокого уровня информационной безопасности [13].

В подавляющем большинстве случаев эксперты в области информационной безопасности используют качественные методы оценки рисков, так как для количественной оценки необходимо иметь достоверную статистику по уязвимостям атакуемых систем (или отдельно взятой ЭВМ) и способам совершения компьютерных атак. Учитывая, что аппаратно-программное обеспечение, конфигурация систем и способы совер-

Таблица 1. Основные направления регулирования операционного риска в кредитно-финансовой сфере в условиях применения мобильного банкинга.

Направления регулирования	Рекомендации РЕГУЛЯТОРУ	Рекомендации БАНКАМ
Совершенствование методов дистанционного и контактного надзора за операционным риском в банках в условиях применения мобильного банкинга	Разработать и внедрить методы дистанционного и контактного надзора для проверки качества управления операционным риском в банках в условиях применения мобильного банкинга (включая методики проведения проверок инспекционными подразделениями вопроса качества управления операционным риском)	Реализовать систему управления операционным риском в соответствии с рекомендации регулятора и пройти, при необходимости, успешно пройти проверку регулятора (без замечаний, по которым возможны меры воздействия)
Достижение приемлемого уровня обеспечения информационной безопасности (включая выявление угроз информационной безопасности и оперативное информирование регулятора)	Разработать и внедрить нормативные и регламентирующие документы по обеспечению приемлемого уровня информационной безопасности в банках (включая разработку порядка оперативного информирование регулятора об инцидентах информационной безопасности и атаках на ресурсы кредитных организаций)	Выполнить рекомендации регулятора по обеспечению приемлемого уровня информационной безопасности (включая внедрения схемы реагирования на инциденты информационной безопасности и компьютерные атаки на информационные ресурсы банка)
Усиление уровня подготовки специалистов по управлению операционным риском	Разработать нормативные документы, обязывающие кредитные организации иметь в штате специалистов по управлению операционного риска	Обеспечить наличие в штате собственных специалистов в области управления операционным риском в соответствии с рекомендациями регулятора

шения атак быстро меняются, собрать своевременно статистику для оценки рисков крайне затруднительно.

Международным открытым проектом обеспечения безопасности web-приложений Open Web Application Security Project (OWASP) в рамках проекта Mobile Security Project[9] определены десять наиболее значимых угроз безопасности мобильных приложений (Таблица 2).[10]

Анализируя приведенные в Таблице 2 угрозы, можно сделать вывод, что некоторые из них (например, M1, M7) характерны только для мобильных приложений (мобильного банкинга).

Перечень указанных в Таблице 2 угроз значительно отличается от десяти наиболее критичных рисков безопасности web-приложений, определенных в проекте OWASP «The Ten Most Critical Web Application Security Risks»[11].

Учитывая уникальный характер угроз информационной безопасности, свойственных СМБ, необходима разработка мер и средств информационной безопасности для митигации указанных угроз.

Для обеспечения безопасности мобильного приложения необходимо разработать модель рисков, учитывающую уязвимости, потенциальных нарушителей, угрозы и вероятности реализации успешных атак.[12]

Можно выделить качественные и количественные методы оценки рисков информационной безопасности, а также комбинированные методы.

Таблица 2. Наиболее значимые угрозы безопасности мобильных приложений.

Шифр	Название угрозы	Краткое описание
M1	Обход архитектурных ограничений (Improper Platform Usage)	Эта категория охватывает злоупотребление особенностями платформы, обхода ограничений или неиспользования систем контроля управления безопасности платформы. Затрагивает системы контроля безопасности, которые являются частью мобильной операционной системы.
M2	Небезопасное хранение данных (Insecure Data Storage)	К ней относятся небезопасное хранение и непреднамеренные утечки данных.
M3	Небезопасная передача данных (Insecure Communication)	Недостаточное подтверждение достоверности источников связи, некорректные версии TLS, SSL, недостаточная проверка согласования, передача чувствительных данных в открытом виде и т.д.
M4	Небезопасная аутентификация (Insecure Authentication)	Эта категория относится к аутентификации пользователя и некорректное управление сеансами.
M5	Слабая криптостойкость (Insufficient Cryptography)	Применение криптографически стойких алгоритмов для передачи критичной информации. Эта категория для случаев, когда криптография была использована, но это было сделано некорректно.
M6	Небезопасная авторизация (Insecure Authorization)	Недостатки процедуры авторизации (проверка (валидация) на стороне клиента и т.д.).
M7	Контроль содержимого клиентских приложений (Client Code Quality)	Ненадлежащий контроль входных данных. Проблемы реализации исходного кода клиентских приложений.
M8	Модификация данных (Code Tampering)	Данная категория относится к изменению исполняемых файлов, линформационных ресурсов, перехват вызовов сторонних процессов, подмена runtime методов и динамическую модификацию памяти.
M9	Анализ исходного кода (Reverse Engineering)	К этой категории относятся анализ бинарных файлов для восстановления алгоритмов, исходного кода, библиотек и т. д. Использование инструментов реверс-инжиниринга позволяют получитить информацию о внутренней работе приложения. Данная информация, на следующем шаге, используется для определения уязвимостей в приложении, извлечения из приложения (например, ключи шифрования и т. д.)..
M10	Скрытый функционал (Extraneous Functionality)	Зачастую разработчики с целью упрощения процедуры отладки включают в код скрытые функциональные возможности, которых официально не должны быть в приложении.

9 OWASP Mobile Security Project. URL: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project (дата обращения 5.03.2019).
10 OWASP Mobile Top 10. URL: https://defcon.ru/mobile-security/3033/ (дата обращения 5.03.2019).
11 OWASP Top 10 - 2017. The Ten Most Critical Web Application Security Risks. URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (дата обращения 6.03.2019).
12 В. А. Артамонов. Безопасность мобильных устройств, систем и приложений. URL: http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_Artamonov.pdf (дата обращения 6.03.2019).

Количественные методы оценки риска используют математические и статистические инструменты для представления риска. В качественных методах анализа риск анализируется с помощью субъективных описательных оценок вместо использования математики.

Количественные методы оценки рисков информационной безопасности содержатся в ГОСТ Р 52448-2005, а также в ряде зарубежных стандартов, наиболее известными из которых являются NISP SP 800-30[13], CRAMM (CCTA Risk Analysis and Management Method) и OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evalua-tion)[14].

К качественным методам оценки рисков можно отнести, например, ISRAM (information security risk analysis method)[15].

В наиболее общем виде оценку риска можно выразить в виде формулы:

Риск = Вероятность х Воздействие (2)

Рассмотрим общий подход к качественной оценке рисков информационной безопасности.

Далее рассматриваются факторы, которые составляют основу таких понятий, как «вероятность» и «воздействие» (ущерб) и показывается, как объединить эти факторы для того, чтобы в итоге определить уровень риска [14, 15, 16].

Прежде всего, необходимо идентифицировать риск, т.е. определить угрозу безопасности, которая ведет к появлению потенциального риска.

Далее необходимо провести оценку вероятности реализации риска (первый множитель в формуле для оценки риска).

Зачастую практически невозможно использовать точные количественные значения для оценки, поэтому используются качественные оценки, например, отнесение вероятности реализации риска к одной из нескольких категорий. Здесь можно выделить факторы, относящиеся к нарушителю, и факторы, относящиеся к уязвимости, возможная эксплуатация которой приводит к возникновению потенциального риска [17, 18, 19].

Среди факторов, относящихся к нарушителю, можно выделить:

– тип нарушителя (разработчик, внутренний пользователь, администратор, внешний пользователь (клиент));

– уровень знаний нарушителя и его мотив;

– ресурсы, необходимые нарушителю для эксплуатации уязвимости.

Каждый из этих факторов подвергается классификации (например, по шкале от 1 до 5) и затем полученные результаты усредняются.

Среди факторов, относящихся к уязвимости, можно выделить:

– простота обнаружения уязвимости;

– простота эксплуатации уязвимости;

– известность (публичность) данной уязвимости;

– простота обнаружения вторжения.

После того, как рассмотрены и оценены факторы, влияющие на вероятность реализации риска, необходимо перейти к рассмотрению и оценке факторов, влияющих на воздействие. Прежде всего, необходимо отметить, что существует два вида воздействия: техническое воздействие и влияние на бизнес.

Влияние на бизнес является наиболее важным из этих двух видов, так как именно влияние на бизнес является конечным результатом эксплуатации нарушителем той или иной уязвимости.

Среди факторов технического воздействия можно выделить такие факторы, как потеря конфиденциальности, потеря целостности и потеря доступности.

Среди факторов, влияющих на бизнес можно выделить:

– финансовые убытки;

– потери, связанные с репутационными рисками;

– несоответствие требованиям регулирующих органов;

– раскрытие персональных данных.

Затем указанные выше факторы также подвергается классификации, а полученные результаты – усредняются. Предлагается усреднять отдельно факторы, относящиеся к факторам технического воздействия, и факторы влияния на бизнес.

Можно предложить два пути: или выбрать из двух оценок факторов технического влияния и факторов влияния на бизнес большее (наиболее критичное) значение или оставить для дальнейшего рассмотрения только оценку влияния на бизнес (при условии, что при проведении такой оценки было достаточно исходной информации).

В итоге мы получаем две оценки: вероятность и влияние. Для оценки риска можно воспользоваться таблицей, в которой для каждого уровня вероятности и влияния определен тот или иной уровень риска (например, незначительный, низкий, средний, высокий и критический).

После того, как все основные риски идентифицированы и оценены, необходимо определить приоритетный список рисков, которые необходимо устранить. Прежде всего, должны быть устранены самые серьезные риски.

Основными средствам и мерами, применение которых позволяет снизить риски информационной безопасности, являются:

– проведение обфускации исходного кода;

– исключение из исходного кода библиотек, содержащие криптографические функции и содержащие уязвимости (например, библиотеки java.util.Random);

– проведение статического (SAST) и динамического (DAST) анализа исходного кода;

– защита сохраняемых на мобильном устроствe конфиденциальных данных;

– применение криптографически стойких алгоритмов шифрования для обеспечения конфиденциальности передаваемой по каналам связи информации между мобильным устройством и серверной частью системы ДБО;

13 Archived NIST Technical Series Publication. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf (дата обращения 7.03.2019).

14 Introduction to the OCTAVE® Approach. URL: https://www.itgovernance.co.uk/files/Octave.pdf (дата обращения 7.03.2019).

15 ISRAM: information security risk analysis method. URL: https://www.academia.edu/8210092/ISRAM_information_security_risk_analysis_method (дата обращения 7.03.2019).

– аутентификацию и авторизацию пользователя мобильного приложения;

и ряд других.

5. Выводы

В результате рассмотрения направлений мобильного банкинга, влияния мобильного банкинга на операционный риск кредитно-финансовых организаций, а также вопросов обеспечения информационной безопасности систем мобильного банкинга можно сформулировать следующие выводы:

– внедрение технологий электронного банкинга (включая СМБ) приводит к значительному снижению затрат на операционную деятельность (за счет отсутствия расходов на содержание офисов и операционных работников), но при этом сопряжено с ростом технической составляющей типичных банковских рисков, среди которых заметно выделяется операционный риск;

– учитывая, что операционный риск становится одним из самых значимых рисков для банков в условиях применения СМБ, необходимо своевременно принимать меры по совершенствованию подходов к управлению данным риском. Очевидно, что порядок и механизмы управления операционным риском должны совершенствоваться на основании рекомендаций регулятора, обеспечивая эффективное распределение зон ответственности за каждым компонентом данного риска;

регулирующим органам необходимо разработать эффективную систему обеспечения информационной безопасности в кредитно-финансовой сфере, в том числе необходимо расширение специальных надзорных подразделений. Последовательным развитием политики регулятора в данной области должны быть разработанные рекомендации для организаций кредитно-финансовой сферы, реализация которых позволит значительно снизить возможности кибермошенников;

– внедрять методики для оценки операционного риска и рисков информационной безопасности (и своевременно их актуализировать), которые должны использоваться риск-подразделениями и службами внутреннего контроля кредитных организаций;

– обязательным условием внедрения эффективной системы обеспечения информационной безопасности в кредитно-финансовой сфере является повышение роли регулятора. Он должен выступать не только как центр взаимодействия с поднадзорными организациями по вопросам своевременного информирования о компьютерных атаках и инцидентах, но и как центр компетенций, способный, в том числе, проводить работу по повышению финансовой грамотности;

– необходимо встраивать меры и средства обеспечения информационной безопасности в жизненный цикл мобильного приложения, включающий, в общем случае, стадии формирования требований, разработки мобильного приложения, его тестирования, а также эксплуатации, поддержки и обновления.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент Московского государственного технического университета имени Н.Э. Баумана, Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература:

1. Лямин Л.В. Электронный банкинг и риски его клиентов // Банкноты стран мира. 2018. №7. С. 26–28.
2. Ревенков П.В. Дистанционное банковское обслуживание: актуальные направления регулирования // Банковское дело. № 9 (225). 2012. С. 57 – 62.
3. Малюк А.А. Глобальная культура кибербезопасности. М.: Горячая линия – Телеком, 2017. 308 с.
4. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28–38. DOI: 10.21681/2311-3456-2018-1-28-38.
5. Алек Росс. Индустрии будущего [пер. с англ. П. Миронова]. М.: Издательства АСТ, 2017. 287 с.
6. Скиннер К. Цифровой банк: как создать цифровой банк или стать им. М.: Манн, Иванов и Фербер, 2015. 320 с.
7. Набигаев Э. Безнаказанность как бензин для кибератак на банки // Банковское обозрение. 2017. №2. 78–79.
8. Ревенков П.В. Операционный риск в условиях возрастания кибератак на банки // Банковское дело. 2018. № 3. С. 56–60.
9. 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.
10. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК-Пресс, 2017. 434 с.
11. Масалков А.С. Особенности киберпреступлений в России. Инструменты нападения и защита информации. М.: ДМК-Пресс, 2018. 226 с.
12. Mr. Cyril Roux. Cybersecurity and cyber risk. BIS central bankers' speeches. The bank for International Settlements, 2015, pp. 1–6. URL: https://www.bis.org/review/r151002d.pdf.
13. Демидов О.В. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: ключевые вызовы для мирового сообщества. М.: Альпина Паблишер, 2016. 198 с.
14. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. М.: Горячая линия – Телеком, 2014. 130 с.
15. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества России. 2018. Т. 210. С. 23–34.
16. Camillo Mark. Cybersecurity: Risks and management of risks for global banks and financial institutions. Journal of Risk Management in Financial Institution, 2017, vol. 10, no. 2, pp. 196–200.
17. Хохлов А. О методах комплексной защиты от мошенничества в системах ДБО // Банковские технологии. 2012. №8. С. 66–68.
18. 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.2016.10.00917.
19. Macknight J. Cyber security: making banking safer. The Banker, 2016, vol. 166, no. 1080, pp. 110–115.

MOBILE BANKING: INFORMATION SECURITY RISK ASSESSMENT

P. Revenkov[16], D. Krupenko[17]

The purpose of the article is research and risk assessment of information security when providing by the financial organizations to clients services of mobile banking and also developing offers on application of means and measures allocated for decrease in the specified risks.

Method: general scientific methods of knowledge are applied: analysis and synthesis, induction and deduction, analogy method. Systems analysis of scientific literature in the field of theoretical and application studies is carried out. The graphic method of interpretation of the studied phenomena is implemented.

The result: offers on the main directions of regulation of operational risk in the credit and financial sphere in the conditions of application of mobile banking are formulated. Recommendations for the credit and financial organizations, and for regulators for increase in efficiency of functioning of systems of electronic banking and, in particular, mobile banking and also to decrease in operational risk in the field are provided. The most significant threats to security of mobile applications are considered. Offers on use of means of ensuring of information security of mobile applications for the purpose of reduction of risk of information security are formulated. The proposed measures and means can be used by development of systems of mobile banking.

Keywords: *remote banking, financial organization, operational risk, mobile application, security threats, vulnerability of the application, information security.*

References:

1. Lyamin L.V. [Electronic banking and the risks of its customers]. Banknoty stran mira = Banknotes of the World, 2018, no. 7, pp. 26–28. (In Russ.).
2. Revenkov P.V. Distantsionnoe bankovskoe obsluzhivanie: aktual'nye napravleniya regulirovaniya [Online banking: urgent areas for regulation]. Bankovskoe delo = Banking, 2012, no. 9, pp. 57–62.
3. Malyuk A.A. Global'naya kul'tura kiberbezopasnosti [Global culture of cybersecurity]. Moscow, Hotline – Telecom Publ., 2017, 308 p.
4. Berdyugin A.A. [Risk management of information security violation in conditions of electronic banking]. Cybersecurity issues = Voprosy kiberbezopasnosti, 2018, no. 1 (25), pp. 28–38. DOI: 10.21681/2311-3456-2018-1-28-38. (In Russ.).
5. Ross A. Industrii budushchego [The Industries of the Future]. Moscow, AST Publ., 2017, 287 p.
6. Skinner Ch. Tsifrovoi bank: kak sozdat' tsifrovoi bank ili stat' im [Digital Bank: Strategies for Launching or Becoming a Digital Bank]. Moscow, Mann, Ivanov i Ferber Publ., 2015, 320 p.
7. Nabigaev E. [Impunity as gasoline for cyber attacks on banks]. Bankovskoye obozreniye = Bank Review, 2017, no. 2, pp. 78–79. (In Russ.).
8. Revenkov P.V. [Operational risk in conditions of increasing cyberattacks on banks]. Bankovskoye delo = Banking, 2018, no. 3, pp. 56–60. (In Russ.).
9. Revenkov P.V., Berdyugin A.A. [Cyber Attacks as a Source of Operational Risk in Electronic Banking]. Finansy i kredit = Finance and Credit, 2018, vol. 24, iss. 3, pp. 629–640. URL: https://doi.org/10.24891/fc.24.3.629. (In Russ.).
10. Biryukov A.A. Informatsionnaya bezopasnost': zashchita i napadeniye [Information security: protection and attack]. Moscow, DMK-Press, 2017, 434 p.
11. Masalkov A.S. Osobennosti kiberprestupleniy v Rossii. Instrumenty napadeniya i zashchita informatsii [Features of cybercrime in. Attack tools and information protection]. Moscow, DMK-Press, 2018, 226 p.
12. Mr. Cyril Roux. Cybersecurity and cyber risk. BIS central bankers' speeches. The bank for International Settlements, 2015, pp. 1–6. URL: https://www.bis.org/review/r151002d.pdf.
13. Demidov O.V. Global'noye upravleniye Internetom i bezopasnost' v sfere ispol'zovaniya IKT: klyuchevyye vyzovy dlya mirovogo soobshchestva [Global Internet governance and security in the use of ICT: key challenges for the global community]. Moscow, Alpina Pablisher, 2016, 198 p.
14. Miloslavskaya N.G., Senatorov M.Yu., Tolstoy A.I. Upravleniye riskami informatsionnoy bezopasnosti [Information Security Risk Management]. Moscow, Hotline – Telecom Publ., 2014, 130 p.
15. Sheremet I.A. [Digital economy and cybersecurity of its financial segment]. Nauchnyye trudy Vol'nogo ekonomicheskogo obshchestva Rossii = Scientific works of the Free Economic Society of Russia, 2018, vol. 210, pp. 23–34. (In Russ.).
16. Camillo Mark. Cybersecurity: Risks and management of risks for global banks and financial institutions. Journal of Risk Management in Financial Institution, 2017, vol. 10, no. 2, pp. 196–200.
17. Khokhlov A. [On the methods of integrated protection against fraud in RBS]. Bankovskiye tekhnologii = Banking Technologies, 2012, no. 8, pp. 66–68. (In Russ.).
18. Keyun Ruan. Introducing cybernomics: A unifying economic frame-work for measuring cyber risk. Computers & Security, 2017, vol. 65, pp. 77–89. URL: https://doi.org/10.1016/j.cose.2016.10.00917.
19. Macknight J. Cyber security: making banking safer. The Banker, 2016, vol. 166, no. 1080, pp. 110–115.

16 Pavel Revenkov, Dr.Sc. (in Economic), Professor of Department «Information Security», Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: pavel.revenkov@mail.ru

17 Dmitry Krupenko, post-graduate student of Department «Information Security», Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: krupenkods@mail.ru